

Kaspersky Endpoint Security For Windows

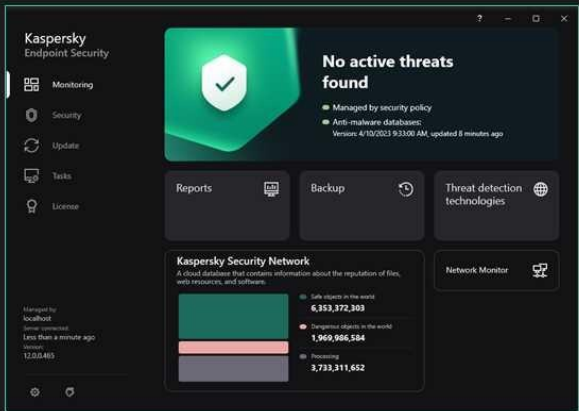
برای مدیریت حفاظت از کلاینت ها و سرورها ، دو برنامه زیر باید روی هر دستگاه نصب شوند:

— Kaspersky Endpoint Security برنامه‌ای است که نه تنها در برابر بدافزارها و فعالیت‌های دشمنان محافظت می‌کند، بلکه می‌تواند اقدامات کاربران را نیز کنترل کرده و فایل‌ها و درایوها را رمزگذاری کند.

— Kaspersky Security Center Network Agents روی همه دستگاه‌ها نصب شده‌اند و Kaspersky Endpoint Security را به سرور مدیریت متصل می‌کنند. Agent ها تنظیمات Kaspersky Endpoint Security را از سرور دریافت می‌کنند و رویدادهای Kaspersky Endpoint Security را در جهت معکوس ارسال می‌کنند.

Kaspersky Endpoint Security for Business: Kaspersky Endpoint Security

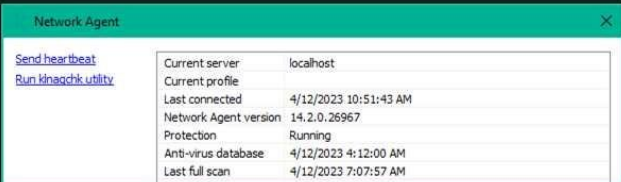
9



- Detects and blocks threats
- Controls network connections
- Allows or blocks start of various applications
- Controls access to devices and websites
- Encrypts files and disks

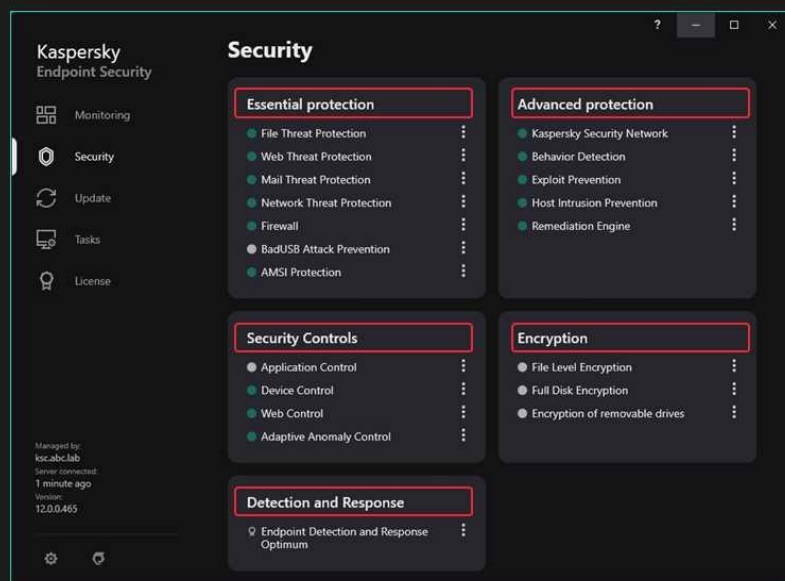
Kaspersky Security Center Agent:

- Delivers events from KES to KSC
- Delivers settings from KSC to KES
- Manages vulnerabilities



Kaspersky Endpoint Security برای ویندوز یک برنامه واحد است که شامل اجزای متعددی می‌شود.

Kaspersky Endpoint Security برای ویندوز یک رویکرد دفاعی عمیق ارائه می‌دهد که در آن می‌توان یک تهدید مشابه را توسط اجزای مختلف شناسایی و خنثی کرد. به عبارت دیگر، اگر یک جزء دچار نقص یا غیرفعال شود، بر عملکرد کلی راهکار امنیتی تأثیری نخواهد گذاشت.



In Kaspersky Endpoint Security, components are grouped as follows:

- Essential Threat Protection
- Advanced Threat Protection
- Security Controls
- Encryption
- Detection and Response

Different components can detect and neutralize the same threat, i.e., disabling or failure of one of the components will not affect the application efficiency

Thus, Kaspersky Endpoint Security provides multilayer protection

اجزای محصول را می توان به شرح زیر گروه بندی کرد:

: Essential Threat Protection

- File Threat Protection ، هر زمان که کاربر یا برنامه های فایلی را ایجاد، تغییر، کپی یا اجرا می کند، آن را اسکن می کند. این برنامه عملیات با فایل های مخرب را مسدود کرده و این فایل ها را در یک حافظه پشتیبان قرار می دهد.

- Web Threat Protection ، صفحات وب و فایل هایی را که کاربر یا برنامه ها از اینترنت دانلود می کنند، اسکن می کند. این برنامه وبسایت های خطرناک و فیشینگ را مسدود کرده و دانلود فایل های مخرب را ممنوع می کند.

- Mail Threat Protection ، پیام های ایمیل را رهگیری می کند، بدنه و پیوست های آنها را اسکن می کند و فایل های مخرب را از پیام ها حذف می کند.

- Firewall ، اتصالات ایجاد شده توسط برنامه های در حال اجرا بر روی رایانه و بسته هایی را که دریافت یا ارسال می کنند، کنترل می کند. این برنامه بسته ها را طبق قوانین پیکربندی شده مسدود می کند. این برنامه به برنامه ای که شهرت بد یا ناشناخته ای دارد، اجازه برقراری ارتباط نمی دهد.

- Network Threat Protection ، بسته‌های شبکه‌ای را که رایانه دریافت می‌کند، اسکن می‌کند. در صورت تشخیص نشانه‌های حمله شبکه، اتصال را مسدود می‌کند.

- پیشگیری از حمله BadUSB اجازه اتصال دستگاه‌های ورودی جدید (صفحه کلید و غیره) به رایانه را بدون رضایت کاربر نمی‌دهد. این برنامه در برابر دستگاه‌های USB که وانمود می‌کنند صفحه کلید هستند و دستورات مخرب را به رایانه ارسال می‌کنند، محافظت می‌کند.

- ارائه‌دهنده محافظت AMSI مسئول ادغام با رابط اسکن ضد بدافزار (AMSI) در ویندوز ۱۰ / ویندوز سرور ۲۰۱۶ و بالاتر است. AMSI یک جزء ویندوز است که به عنوان واسطه بین برنامه‌ها و یک راه‌حل آنتی‌ویروس عمل می‌کند. این برنامه امکان اسکن فایل‌ها، لینک‌ها و اسکریپت‌ها، حتی آن‌هایی که در حافظه اجرا می‌شوند را بدون ذخیره شدن در هارد دیسک، فراهم می‌کند.

- Advanced Threat Protection :

- Kaspersky Security Network اعتبار برنامه‌ها و صفحات وب را از سرورهای کسپرسکی درخواست می‌کند، آخرین اطلاعات در مورد تهدیدات را ارائه می‌دهد و در برابر حملات روز صفر و تشخیص‌های نادرست محافظت می‌کند.

- Behavior Detection ، عملکرد برنامه‌ها را رصد می‌کند و رفتار کلی یک برنامه را به جای اقدامات فردی آن تجزیه و تحلیل می‌کند. این سیستم، برنامه‌هایی را که مانند بدافزار رفتار می‌کنند، متوقف می‌کند. به طور خاص، برنامه‌هایی را که سعی در رمزگذاری فایل‌ها دارند، متوقف می‌کند.

- Exploit Prevention ، فایل‌هایی را که برنامه‌های آسیب‌پذیر را شروع می‌کنند، رصد می‌کند و تلاش‌ها برای شروع فایل‌های اجرایی را مسدود می‌کند، مگر اینکه توسط کاربر آغاز شده باشد.

- Intrusion Prevention همچنین فعالیت‌های نرم‌افزاری را در رایانه رصد می‌کند. به برنامه‌هایی که شهرت بد یا ناشناخته‌ای دارند، اجازه تغییر تنظیمات سیستم و فایل‌های کاربر را نمی‌دهد و از دستکاری آنها در سیستم عامل و سایر نرم‌افزارها جلوگیری می‌کند.

- Remediation Engine ، تغییرات سیستم عامل را ثبت می‌کند و هرگونه اقدام انجام شده توسط برنامه‌های مشکوکی را که توسط تشخیص رفتار، پیشگیری از سوءاستفاده یا محافظت از تهدید فایل شناسایی شده‌اند، به حالت اولیه برمی‌گرداند.

- Security Controls :

- Application Control ، شروع برنامه‌ها را طبق قوانین پیکربندی شده مسدود می‌کند. این برنامه با مسدود کردن هرگونه برنامه جدید، وضعیت کامپیوتر را ایمن می‌کند.

- Device Control ، دسترسی به دستگاه‌ها را طبق قوانین پیکربندی شده مسدود می‌کند. مدیر می‌تواند دسترسی به برخی یا همه درایوهای قابل جابجایی، آداپتورهای Wi-Fi یا مودم‌ها را ممنوع کند.

- Web Control ، دسترسی به صفحات وب را طبق قوانین پیکربندی شده مسدود می‌کند. مدیر می‌تواند دسترسی به شبکه‌های اجتماعی، وبسایت‌های جستجوی کار، کازینوهای آنلاین و غیره را ممنوع کند.

- Adaptive Anomaly Control شامل مجموعه‌ای از محبوب‌ترین روش‌های اکتشافی است که رفتارهای خطرناک مشخصه بدافزار را تشخیص می‌دهند. این امکان را فراهم می‌کند تا فعالیت‌های مشکوکی که برای یک کامپیوتر خاص غیرمعمول هستند، مسدود شوند. این مؤلفه در ابتدا به طور پیش‌فرض به مدت دو هفته در حالت آموزش هوشمند کار می‌کند. در این مدت، فعالیت‌ها را رصد می‌کند و مدیر را در مورد آنها مطلع می‌کند. مدیر (نه مؤلفه) تصمیم می‌گیرد که آیا یک فعالیت خاص برای یک کامپیوتر طبیعی است یا خیر.

- Data Encryption :

رمزگذاری سطح فایل (FLE) فایل‌ها و پوشه‌های تکی را طبق قوانین رمزگذاری می‌کند. این روش از فایل‌های موجود در لپ‌تاپ‌های گم‌شده یا دزدیده‌شده محافظت می‌کند.

- رمزگذاری کامل دیسک (FDE) تمام محتویات درایوها را رمزگذاری می‌کند. این روش از فایل‌های موجود در لپ‌تاپ‌های گم‌شده یا دزدیده‌شده محافظت می‌کند.

- رمزگذاری درایوهای قابل جابجایی، داده‌ها را روی درایوهای قابل جابجایی با استفاده از یکی از روش‌های شرح داده شده رمزگذاری می‌کند.

- Detection & Response :

- تشخیص و پاسخ نقطه پایانی بهینه، یک عامل داخلی برای راهکاری است که با نام تشخیص و پاسخ نقطه پایانی بهینه کسپرسکی (EDR بهینه) شناخته می‌شود. این راهکار، قابلیت تشخیص خودکار تهدید را با توانایی پاسخگویی به این تهدیدها و مقابله با حملات پیشرفته ترکیب می‌کند.

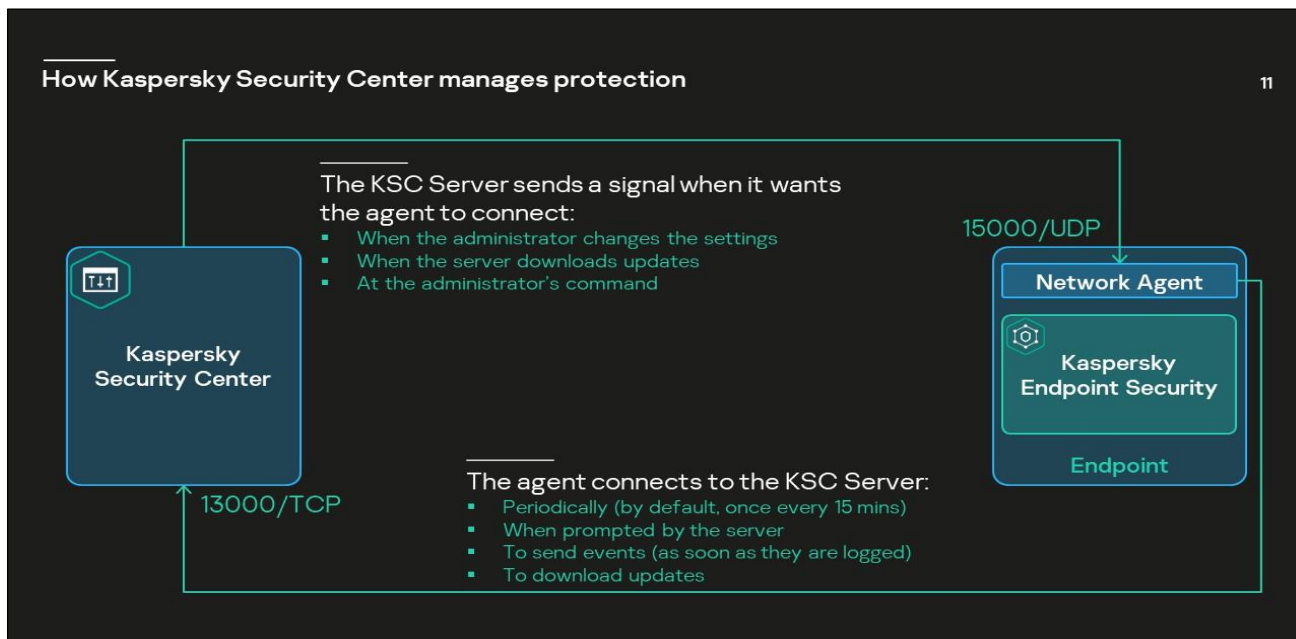
- Tasks :

- Malware Scan ، فایل‌ها را طبق برنامه پیکربندی شده اسکن می‌کند. این روش اسکن کامل‌تری نسبت به آنتی‌ویروس فایل انجام می‌دهد.

- Update ، توضیحات تهدیدها و اعتبار فایل‌ها را برای رایانه‌ها دانلود می‌کند و در صورت عدم دسترسی به شبکه امنیتی کسپرسکی، محافظت را فراهم می‌کند

- Last Update Rollback ، آخرین به‌روزرسانی مازول‌های برنامه و پایگاه‌های داده را در صورت ایجاد false positive توسط به‌روزرسانی جدید، حذف می‌کند.

- Integrity Check تضمین می‌کند که هیچ‌کس نمی‌تواند فایل‌های Kaspersky Endpoint Security را تغییر دهد.



بیاپید بررسی کنیم که چگونه برنامه‌های مختلف کسپرسکی با یکدیگر تعامل دارند.

فرض می‌کنیم که شبکه محافظت‌شده ما دارای یک سرور مدیریت مرکز امنیت کسپرسکی مستقر است و دو برنامه زیر روی هر رایانه نصب شده‌اند:

- امنیت نقطه پایانی کسپرسکی، برای حفاظت

- عامل شبکه مرکز امنیت کسپرسکی، برای مدیریت

عامل شبکه طبق برنامه مشخص شده و در صورت نیاز به سرور مدیریت متصل می‌شود. این فرآیند همگام‌سازی نامیده می‌شود و به طور پیش‌فرض هر ۱۵ دقیقه یک بار انجام می‌شود.

برای اینکه مدیر بتواند ببیند در شبکه چه اتفاقی می‌افتد، Network Agent داده‌های زیر را به سرور ارسال می‌کند:

- رویدادها به محض ثبت شدن، زمانی که Kaspersky Endpoint Security بدافزار پیدا می‌کند، نمی‌تواند به‌روزرسانی‌ها را دانلود کند، نمی‌تواند اجرا را اجرا کند و غیره، ارسال می‌شوند.

- وضعیت‌ها به محض ثبت شدن ارسال می‌شوند. مثال‌ها:

- Kaspersky Endpoint Security در حال اجرا نیست

- پایگاه‌های داده قدیمی هستند

- KSN غیرقابل دسترسی است

- اشیاء پردازش نشده خطرناکی وجود دارد

- لیست‌ها در طول هر همگام‌سازی ارسال می‌شوند. این لیست‌ها عبارتند از:

- لیست برنامه‌های نصب شده
- لیست سخت‌افزار
- لیست برنامه‌های آسیب‌پذیر
- لیست تهدیدهای پردازش نشده
- لیست اشیاء مخرب در پشتیبان‌گیری
- لیست فایل‌های اجرایی شناخته شده

سرور مدیریت، اتصالات را از Agent روی پورت TCP 13000 می‌پذیرد. Agents، اتصالات TLS/SSL را برقرار می‌کنند. آنها داده‌ها را با استفاده از سرتیفیکیت سرور مدیریت رمزگذاری و فشرده‌سازی می‌کنند.

آنچه کامپیوترها از سرور دانلود می‌کنند :

برای اینکه Kaspersky Endpoint Security بتواند از یک کامپیوتر به روشی که مدیر می‌خواهد محافظت کند، Network Agent تنظیمات Kaspersky Endpoint Security را در قالب Policy ها و Task از سرور دریافت می‌کند. در طول همگام‌سازی، Task Network Agent و Policy های کامپیوتر را با Task و Policy های سرور مدیریت مقایسه می‌کند. اگر مدیر چیزی را در سرور تغییر داده باشد، Task Agent و Policy های جدید را دانلود می‌کند. کامپیوترها معمولاً Task و Policy ها را زودتر از زمان هماهنگ‌سازی برنامه‌ریزی شده دریافت می‌کنند. Network Agent بسته‌ها را روی پورت UDP 15000 می‌پذیرند. اگر سرور بخواهد یک Agent فوراً به سرور متصل شود، سیگنال ویژه‌ای به این پورت ارسال می‌کند. هنگامی که مدیر یک Task یا Policy را تغییر می‌دهد، Administration Server با Agent های تمام کامپیوترهایی که این Task یا Policy به آنها مربوط می‌شود، ارتباط می‌گیرد. در طول همگام‌سازی، Policy ها فقط توسط کامپیوترهایی دانلود می‌شوند که سیگنال را از سرور دریافت نکرده‌اند. مدیر همچنین می‌تواند از طریق منوی میانبر کامپیوتر در کنسول مدیریت، درخواست همگام‌سازی را به صورت دستی ارسال کند. علاوه بر این، Agent ها برای دانلود به‌روزرسانی‌های Kaspersky Endpoint Security به سرور متصل می‌شوند. برای انجام این کار، آنها همچنین از طریق یک کانال رمزگذاری شده به پورت TCP 13000 متصل می‌شوند.

How the administrator manages protection

To configure different settings for different computers, the administrator groups computers and creates policies for these groups

Status	Policy name	Application	Group
☐	Kaspersky Security Center Network Agent	Kaspersky Security Center Network Agent	Managed devices
☐	Kaspersky Endpoint Security for Windows (12.0.0)	Kaspersky Endpoint Security for Windows (12.0.0)	Managed devices

The administrator defines the settings in policies and tasks:

- Application settings are configured in policies
- Anti-malware scanning and updates, in tasks
- Tasks have schedules

To monitor the protection status, the administrator uses:

- Events
- Reports
- Dashboard
- Statuses

Policy ها :

یک Policy شامل پارامترهای مشابه تنظیمات محلی Kaspersky Endpoint Security است. وقتی مدیر یک Policy را پیکربندی و اعمال می‌کند، تنظیمات حفاظت محلی را تغییر می‌دهد.

در یک Policy، هر پارامتر (یا گروهی از پارامترها) یک گزینه قفل دارد.

اگر این گزینه فعال باشد و قفل بسته باشد، پارامترها به رایانه‌هایی که Policy در آنها اجرا می‌شود اعمال می‌شوند. کاربر نمی‌تواند مقادیر این پارامترها را در رابط محلی Kaspersky Endpoint Security تغییر دهد.

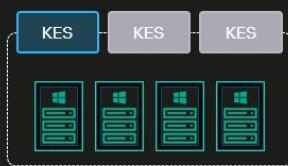
اگر این گزینه غیرفعال باشد و قفل باز باشد، رایانه طوری رفتار می‌کند که انگار این پارامتر در Policy مشخص نشده است. کاربر می‌تواند این پارامترها را در رابط محلی تغییر دهد.

How policies work in groups

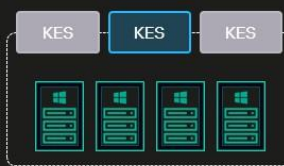
14



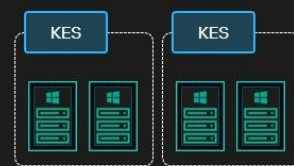
A group may contain policies for different applications



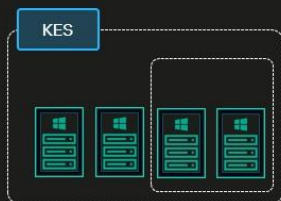
A group may contain multiple policies for the same application, but only one of them can be active



The administrator manually selects which policy to make active



To configure different settings for different computers, organize them into subgroups and create respective policies there



If a subgroup has no policy, its computers receive the policy of the parent group

Policy ها بر روی گروه های کامپیوتری اعمال می شوند.

حتی اگر کاربر هیچ گروهی ایجاد نکرده باشد، سرور مدیریت یک گروه ریشه به نام دستگاه های مدیریت شده دارد. اگر کاربر بخواهد گروه های سفارشی ایجاد کند، آنها به عنوان زیرگروه هایی در گروه دستگاه های مدیریت شده ایجاد می شوند.

Policy ها از قوانین زیر پیروی می کنند:

- ممکن است Policy هایی برای برنامه های مختلف در یک گروه وجود داشته باشد، به عنوان مثال، یک Network Policy Agent، یک Kaspersky Endpoint Security Policy برای ویندوز و یک Kaspersky Endpoint Policy Security برای لینوکس.

- یک گروه می تواند چندین Policy برای یک برنامه داشته باشد، اما فقط یکی از آنها می تواند فعال باشد.

Policy فعال، Policy ی است که سرور مدیریت به رایانه ها ارسال می کند.

یک Policy غیرفعال هیچ تاثیری ندارد، اما مدیر می تواند آن را در هر لحظه فعال کند و بنابراین به سرعت تنظیمات را در تمام رایانه ها پیکربندی مجدد کند.

اگر مدیر یک Policy را فعال کند، Policy فعال قبلی به طور خودکار غیرفعال می شود.

- اگر گروهی دارای Policy امنیتی کسپرسکی اندپوینت باشد و زیرگروهی وجود داشته باشد که در آن هیچ Policy امنیتی کسپرسکی اندپوینت وجود نداشته باشد، Policy گروه والد بر روی رایانه‌های زیرگروه نیز اعمال می‌شود، یعنی به ارث برده می‌شود.

How policies work in groups

15

Scenario 1: If a policy is configured within a subgroup, it will inherit locked settings from the policy configured in the parent group.

Scenario 2: If a lock is open in the parent group, the respective parameter can be adjusted in the child policy.

Scenario 3: The administrator can disable inheritance within a subgroup and adjust its settings as if there were no parent policy.

Policy status:

☒ Active

☐ Inactive

☐ Out-of-office

Settings inheritance

☐ Inherit settings from parent policy

☐ Force inheritance of settings in child policies

اگر Policy های فعال Kaspersky Endpoint Security در هر دو گروه والد و فرزند وجود داشته باشد، از Policy گروه فرزند با شرایط زیر استفاده می‌شود:

- پارامترهای الزامی (قفل شده) از Policy والد بر Policy زیرگروه اعمال می‌شوند و مدیر نمی‌تواند آنها را تغییر دهد.

- در یک Policy فرزند، مدیر فقط می‌تواند پارامترهایی را که در Policy والد قفل نشده‌اند، ویرایش کند.

- مدیر می‌تواند انتخاب کند که Policy والد را به یک گروه فرزند اعمال نکند: در Policy فرزند، گزینه **Inherit settings from parent policy** را غیرفعال کنید. پس از آن، مدیر قادر خواهد بود هر پارامتری را در Policy فرزند ویرایش کند.

Task ها :

How tasks work

Computers that work under a policy can run only group tasks. Local tasks are disabled

The administrator manages updates and anti-malware scanning through tasks

A local user cannot adjust the settings of a group task

Tasks don't have locks, but have a schedule

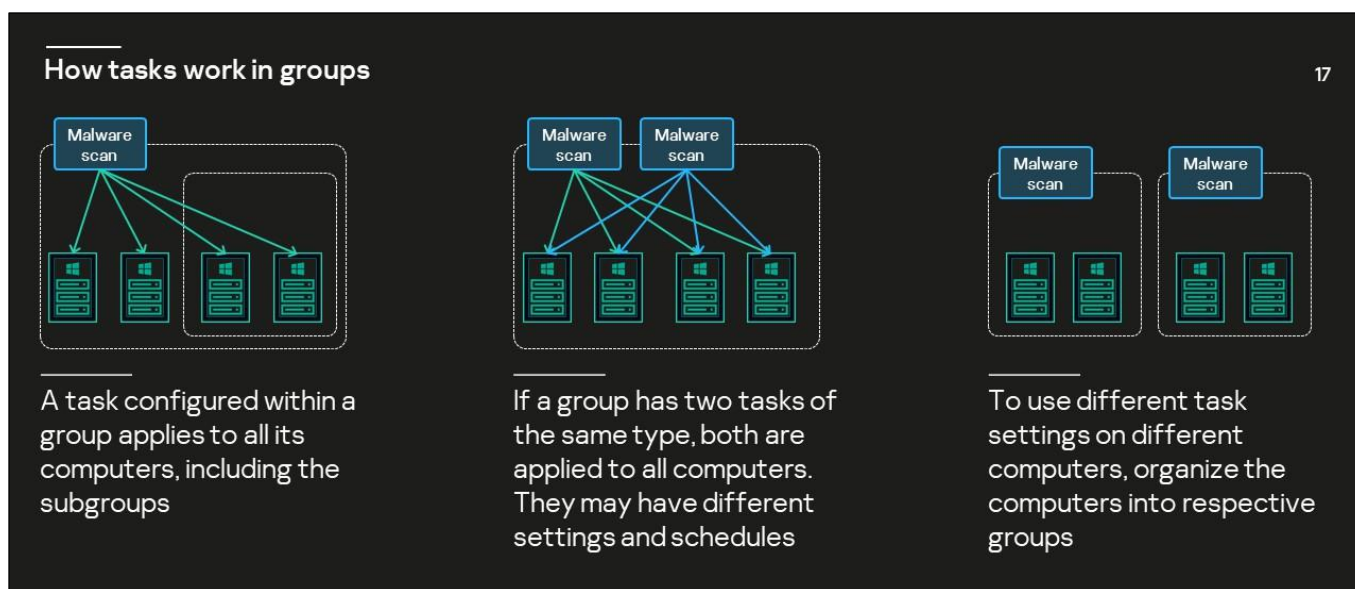
مدیر، تنظیمات به روزرسانی و اسکن بدافزار را از طریق Task مدیریت می کند، نه از طریق Policy. در حالی که فقط یک نوع Policy امنیتی Kaspersky Endpoint می تواند وجود داشته باشد، انواع Task های مختلفی در Kaspersky Endpoint Security وجود دارد:

- Malware Scan
- Update
- Update Rollback
- Inventory
- Add Key
- Integrity Check
- Change Application Component
- Manage Authentication Agent Account

هر نوع Task تنظیمات خاص خود را دارد. به عنوان مثال، یک Task اسکن بدافزار، دامنه و تنظیمات اسکن فایل خود را دارد، در حالی که یک Task به روزرسانی، منبع به روزرسانی و دستورالعمل هایی برای دانلود به روزرسانی ها دارد. هر Task دارای یک برنامه است.

برخلاف Policy ها، Task ها هیچ قفلی ندارند. همه تنظیمات Task روی رایانه‌ها اعمال می‌شوند و کاربر نمی‌تواند آنها را تغییر دهد.

Task را می‌توان نه تنها توسط مدیر در سرور مدیریت، بلکه توسط کاربر در رابط محلی نیز ایجاد کرد. با این حال، اگر یک Policy روی سرور مدیریت پیکربندی شده و روی یک رایانه اجرا شود، فقط از Task سرور مدیریت استفاده خواهد کرد. Task های محلی غیرفعال هستند و در رابط نمایش داده نمی‌شوند و کاربر نمی‌تواند Task محلی جدیدی ایجاد کند.



مدیر سیستم، Task هایی را در گروه‌ها برای فعالیت‌های منظم، مانند اسکن‌های ضد بدافزار یا دانلود به‌روزرسانی‌ها، ایجاد می‌کند.

مشابه Policy گروهی، Task گروهی نیز قوانین خود را دارند:

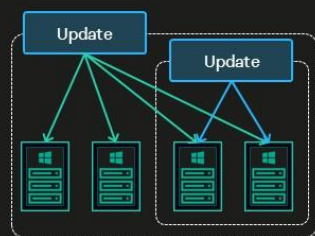
- اگر در یک گروه، زیرگروهی وجود داشته باشد، یک Task گروهی برای رایانه‌های زیرگروه اعمال می‌شود.

- در یک گروه می‌توان چندین Task از هر نوع، مثلاً چندین Task اسکن بدافزار، وجود داشته باشد. آن‌ها ممکن است در دامنه و برنامه خود متفاوت باشند. به عنوان مثال، یکی از Task ممکن است کل کامپیوتر را یک بار در هفته اسکن کند، در حالی که دیگری فقط مناطق بحرانی را اسکن می‌کند، اما این کار را روزانه انجام می‌دهد.

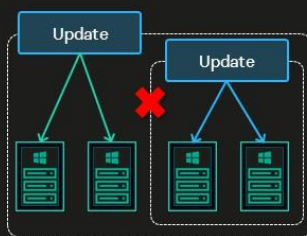
- اگر می‌خواهید دامنه یکسانی را برای تهدیدات با برنامه‌های مختلف در رایانه‌های مختلف اسکن کنید، رایانه‌ها را در گروه‌های مربوطه سازماندهی کنید و Task جداگانه‌ای را در هر گروه ایجاد کنید. به عنوان مثال، می‌توانید در آخر هفته‌ها یک اسکن کامل روی سرورها و در حالت پس‌زمینه روی ایستگاه‌های کاری در ساعات کاری انجام دهید.

How tasks work in groups

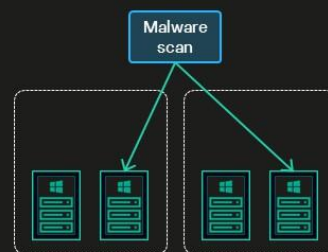
18



If tasks of the same type are configured within a group and its subgroup, all of them will run on the respective computers. This is not recommended, especially for update tasks



The administrator can exclude a subgroup from the task scope of the parent group



The administrator can create a task for specific computers that will run on computers belonging to different groups

— اگر در یک گروه یک Task وجود داشته باشد و یک زیرگروه با Task‌ای از همان نوع وجود داشته باشد، کامپیوترهای زیرگروه هر دو Task را اجرا می‌کنند. این معمولاً به این معنی است که مدیر به اندازه کافی به Task مورد نیاز فکر نکرده است.

شما باید در مورد Task به‌روزرسانی بسیار مراقب باشید. برای به‌روزرسانی Kaspersky Endpoint Security در یک رایانه، باید یک Task به‌روزرسانی واحد وجود داشته باشد. اگر یک Task به‌روزرسانی در یک گروه و یک Task به‌روزرسانی دیگر در زیرگروه آن پیکربندی شده باشد، هر دو به رایانه‌هایی که زیرگروه را تشکیل می‌دهند اعمال می‌شوند. اگر یک Task به‌روزرسانی از قبل در حال اجرا باشد، Task به‌روزرسانی دیگر در صورت شروع همزمان، خطایی را برمی‌گرداند. در نتیجه، مدیر به دلیل خطای پیکربندی، خطاهای به‌روزرسانی را دریافت خواهد کرد، حتی اگر به‌روزرسانی‌ها به درستی کار کنند.

— زیرگروه‌ها را می‌توان از محدوده یک Task مستثنی کرد. در این حالت، کامپیوترهای زیرگروه فقط Task زیرگروه را دریافت می‌کنند و Task والد استفاده نخواهد شد.

۱. چگونه Kaspersky Endpoint Security از کامپیوترها محافظت می‌کند

۱.۱ چگونه مجرمان به یک کامپیوتر حمله می‌کنند

چگونه بدافزار وارد کامپیوتر می‌شود ؟

How malware gets on a computer

3



Via a browser:

- A vulnerable browser allows malware to download and run
- The user downloads and launches malware manually (for example, mistakenly follows a malicious link)



Via email:

- In an attachment that the user opens
- Links to malicious websites in the message body



Via removable drives:

- Which the user has brought from home or found in the parking lot



From other infected computers over the network:

- The user copies a file from a shared folder
- Malware attacks vulnerable services and programs on the user's computer

بدافزار می‌تواند از طریق هر چیزی که کامپیوتر را به دنیای خارج متصل می‌کند، به ویژه از طریق اتصالات شبکه و درایوهای قابل جابجایی، وارد کامپیوتر شود. بیاید سناریوهای معمول نفوذ بدافزار به کامپیوتر و نحوه جلوگیری از آن را بررسی کنیم.

از طریق یک مرورگر

یک مرورگر وب آسیب‌پذیر

کاربر یک مرورگر آسیب‌پذیر نصب می‌کند. یک صفحه وب ممکن است از یک آسیب‌پذیری سوءاستفاده کند تا مرورگر را مجبور به دانلود و اجرای هر نرم‌افزاری روی کامپیوتر کند. کاربر از یک وب‌سایت مشکوک بازدید می‌کند که بدافزار را روی کامپیوتر اجرا می‌کند. کد مخرب می‌تواند در محتوای تبلیغاتی که وب‌سایت از سایت‌های دیگر دریافت می‌کند، به جای صفحات خود، قرار داشته باشد.

برای محافظت در برابر چنین حمله‌ای:

— به‌روزرسانی‌های مرورگرهای وب را نصب کنید

— به کاربران اجازه ندهید که بدون هیچ تمایزی هر مرورگری را باز کنند

— به کاربران اجازه ندهید که بدون هیچ تمایزی هر صفحه وب را باز کنند

— به کاربران اجازه ندهید وب‌سایت‌هایی را که آلوده شناخته شده‌اند باز کنند

— به مرورگرهای وب اجازه ندهید که فرآیندهای فرزند را شروع کنند

یک فایل آلوده

کاربر در اینترنت به دنبال نرم افزار رایگان می گردد. برای مثال، یک ابزار رایگان مفید یا یک نسخه کپی شده از یک برنامه گران قیمت، یا یک تولیدکننده کلید برای یک برنامه گران قیمت. کاربر آن را پیدا، دانلود و در رایانه اجرا می کند. برنامه مخرب از آب در می آید. شاید کاربر یک فایل به ظاهر ایمن را از یک «سطل زباله اینترنتی» دانلود کند. مهاجمان می توانند کد نرم افزار رایگان را تغییر دهند یا یک صفحه دانلود رسمی را هک کرده و نرم افزار را جایگزین کنند.

برای محافظت در برابر چنین حمله ای:

- به کاربران اجازه ندهید که بدون هدف، هر صفحه وب را باز کنند.
- به کاربران اجازه ندهید وبسایت هایی را که به توزیع بدافزار معروف هستند، باز کنند.
- از نرم افزارهای محافظتی برای اسکن فایل هایی که کاربران از اینترنت دانلود می کنند، استفاده کنید.

از طریق ایمیل

کاربر ایمیلی دریافت می کند که به نظر می رسد پیامی از یک بانک، فروشگاه، سرویس تحویل، شریک عاشقانه، آشنا و غیره است. این پیام کاربر را به کلیک روی یک لینک یا باز کردن یک پیوست ترغیب می کند. این لینک به یک وبسایت مخرب یا فیشینگ منتهی می شود. پیوست حاوی بدافزار یا سندی با بدافزار جاسازی شده است.

برای محافظت در برابر چنین حمله ای:

- فیلتر کردن ایمیل با استفاده از ابزارهای ضد هرزنامه (نرم افزاری که در برابر ایمیل های انبوه ناشناس و ناخواسته محافظت می کند)
- استفاده از نرم افزارهای محافظتی برای اسکن فایل های پیوست شده به ایمیل ها
- به کاربران اجازه ندهید فایل های اجرایی را از ایمیل ها در درایو ذخیره کنند
- در برابر لینک های موجود در پیام ها به همان روشی که در برابر حملات مبتنی بر مرورگر محافظت می کنید، محافظت کنید.

از رایانه های دیگر در شبکه

از یک پوشه مشترک

کاربر برنامه ای را از یک پوشه مشترک در رایانه دیگری کپی کرده و آن را اجرا می کند. برنامه مخرب از آب در می آید. کاربر سندی را از یک پوشه مشترک در رایانه دیگری باز می کند. سند حاوی کد مخرب است.

برای محافظت در برابر چنین حمله ای:

- نصب برنامه های محافظتی روی همه رایانه ها
- اسکن فایل هایی که کاربران کپی، باز یا اجرا می کنند

حمله شبکه

یک آسیب‌پذیری در سیستم عامل رایانه کاربر وجود دارد. با ارسال یک توالی خاص از بسته‌ها به یک پورت خاص، مهاجم می‌تواند یک سرویس آسیب‌پذیر را وادار به اجرای کد موجود در این بسته‌ها کند. یک رایانه آلوده همچنین به سرویس آسیب‌پذیر در تمام رایانه‌های شبکه دیگر حمله کرده و آنها را آلوده می‌کند.

برای محافظت در برابر چنین حمله‌ای:

- به‌روزرسانی‌های امنیتی برای سیستم‌عامل‌ها نصب کنید
- اتصال به پورت‌هایی که کاربران برای کار خود به آنها نیاز ندارند را ممنوع کنید
- از نرم‌افزارهای محافظتی برای بررسی بسته‌های ورودی برای حملات شبکه استفاده کنید

از رسانه‌های خارجی

درایو حافظه USB کاربر

کاربر یک فلش درایو USB را برای کپی کردن اسناد به رایانه متصل می‌کند. فلش درایو USB حاوی بدافزاری است که از آسیب‌پذیری سیستم عامل سوءاستفاده می‌کند تا به طور خودکار کدی را روی رایانه اجرا کند.

یا کاربر به سادگی یک فلش درایو USB را متصل می‌کند تا بفهمد چه چیزی در آن وجود دارد، یک سند یا یک فایل اجرایی با نامی جذاب پیدا می‌کند و تصمیم می‌گیرد آن را باز کند. فایل آلوده می‌شود.

برای محافظت در برابر چنین حمله‌ای:

- به کاربران اجازه ندهید فلش درایوهای USB ناشناخته (یا هر نوع) را به رایانه متصل کنند
- از نرم‌افزارهای محافظتی برای اسکن فایل‌ها روی درایوهای USB استفاده کنید
- به‌روزرسانی‌های امنیتی برای سیستم‌عامل‌ها نصب کنید

BadUSB

کاربر یک دستگاه USB شبیه فلش درایو USB را به رایانه متصل می‌کند. دستگاه به عنوان یک فلش درایو USB و یک صفحه کلید در سیستم عامل ثبت می‌شود. پس از مدتی، دستگاه با ارسال کلیدهای فشرده‌شده شروع به اجرای دستورات روی رایانه می‌کند. برای محافظت در برابر چنین حمله‌ای، از محافظت در برابر حملات BadUSB استفاده کنید.

نحوه محافظت در برابر تهدیدات

تمام روش‌های پیشگیری از تهدیدات را می‌توان به صورت زیر گروه‌بندی کرد:

ریشه‌کن کردن اهداف بالقوه حمله

- نصب به‌روزرسانی‌های امنیتی برای سیستم‌عامل‌ها
- نصب به‌روزرسانی‌ها برای مرورگرهای وب و سایر برنامه‌ها
- اجازه ندهید کاربران بدون هیچ تمایزی هر مرورگری را باز کنند
- اجازه ندهید کاربران بدون هیچ تمایزی هر صفحه وب را باز کنند
- اجازه ندهید مرورگرهای وب فرآیندهای فرزند را شروع کنند
- اجازه ندهید کاربران فایل‌های اجرایی را از ایمیل‌ها در درایو ذخیره کنند
- اتصال به پورت‌هایی که کاربران برای کار خود به آنها نیاز ندارند را ممنوع کنید
- اجازه ندهید کاربران فلش درایوهای USB ناشناخته (یا هر) را به رایانه‌ها متصل کنند

از راه‌حل‌های حفاظتی برای شناسایی حملات استفاده کنید

- برنامه‌های حفاظتی را روی همه رایانه‌ها نصب کنید
- فایل‌هایی را که کاربران کپی، باز یا اجرا می‌کنند اسکن کنید
- از نرم‌افزار حفاظتی برای اسکن فایل‌های روی درایوهای USB استفاده کنید
- از نرم‌افزار حفاظتی برای اسکن فایل‌های پیوست شده به ایمیل‌ها استفاده کنید
- از نرم‌افزار حفاظتی برای اسکن فایل‌هایی که کاربران از اینترنت دانلود می‌کنند استفاده کنید
- اجازه ندهید کاربران وبسایت‌هایی را که آلوده شناخته شده‌اند باز کنند
- اجازه ندهید کاربران وبسایت‌هایی را که به توزیع بدافزار شناخته شده‌اند باز کنند
- از نرم‌افزار حفاظتی برای بررسی بسته‌های ورودی برای حملات شبکه استفاده کنید
- از محافظت در برابر حملات BadUSB استفاده کنید

چگونه بدافزار باعث آسیب می‌شود ؟

هیچ راهکار حفاظتی نمی‌تواند در برابر ۱۰۰٪ تهدیدات محافظت کند. مجرمان ممکن است همیشه نیم قدم جلوتر باشند زیرا آنها:

- ثبت دامنه‌ها و وبسایت‌های جدید
- نوشتن بدافزار جدید
- بهره‌برداری از آسیب‌پذیری‌های روز صفر که هنوز اصلاحاتی برای آنها منتشر نشده است

حتی اگر محافظت به درستی کار کند، همیشه این خطر وجود دارد که یک کامپیوتر به بدافزار جدید آلوده شود. اگر محافظت روی برخی از رایانه‌ها نصب نشده باشد، اگر پایگاه‌های داده روی رایانه‌ها قدیمی باشند، اگر اجزای مهم محافظت غیرفعال باشند، خطر افزایش می‌یابد.

بیا یاد آسیمی را که بدافزار می‌تواند ایجاد کند و نحوه کاهش آن را بررسی کنیم.

What malware does on a computer

4



Encrypts files and demands a ransom
Gets the password from its control center (or sends it there)



Steals credit card data and passwords
Sends them to its control center



Attacks other computers
Receives commands from its control center



Downloads new malware



Uses computer resources
Cryptomining



Causes trouble: the computer runs really slow, hangs, restarts

باج‌افزار (Ransomware)

باج‌افزار اسناد و سایر فایل‌های موجود در رایانه و پوشه‌های مشترک را رمزگذاری می‌کند و سپس برای کلید رمزگذاری درخواست پول می‌کند. کلید در سرور مجرمان ذخیره می‌شود. بدافزار یا کلید را از سرور دانلود می‌کند، فایل‌ها را رمزگذاری می‌کند و کلید را حذف می‌کند؛ یا یک کلید تصادفی تولید می‌کند، آن را به سرور ارسال می‌کند، فایل‌ها را رمزگذاری می‌کند و کلید را حذف می‌کند. در هر دو حالت، باج‌افزار از طریق شبکه به سرور خود متصل می‌شود.

برای محافظت در برابر چنین حمله‌ای:

- به طور منظم از تمام فایل‌های مهم پشتیبان تهیه کنید
- به برنامه‌های ناشناخته اجازه برقراری و پذیرش اتصالات شبکه را ندهید
- از راه‌حل‌های حفاظتی استفاده کنید که رمزگذاری را به صورت اکتشافی تشخیص می‌دهند

جاسوس افزار (Spyware)

بدافزار در تنظیمات نرم افزار و فایل های روی درایو به دنبال رمزهای عبور رمزگذاری نشده یا ضعیف رمزگذاری شده می گردد. بدافزار هر چیزی را که کاربر وارد می کند، از طریق دوربین وب اسکرین شات می گیرد و تصاویر را ضبط می کند، رهگیری می کند. برنامه همه این ها را به سرور مجرمان ارسال می کند.

برای محافظت در برابر چنین حمله ای:

- به برنامه های ناشناس اجازه برقراری و پذیرش اتصالات شبکه را ندهید.
- از راه حل های حفاظتی که جاسوسی را به صورت اکتشافی تشخیص می دهند استفاده کنید.

بدافزار شبکه (Network malware)

بدافزار خود را روی فلش مموری های USB متصل به رایانه و پوشه های مشترک از طریق شبکه می نویسد. بدافزار از طریق سرویس های آسیب پذیر رایانه های مجاور را آلوده می کند. بدافزار هر زمانه ارسال می کند و در حملات DDOS به دستور مرکز کنترل شرکت می کند.

برای محافظت در برابر چنین حمله ای:

- به برنامه های ناشناس اجازه برقراری و پذیرش اتصالات شبکه را ندهید.
- از راه حل های حفاظتی که به صورت اکتشافی فعالیت های خطرناک را تشخیص می دهند استفاده کنید.

بار گذارها (Loaders)

مجرمان اغلب از فایل های بسیار ساده ای که هیچ تهدید مستقیمی ایجاد نمی کنند، برای دور زدن راه حل های حفاظتی و آلوده کردن رایانه استفاده می کنند. اما این فایل ها ممکن است فایل های مخرب دیگری را دانلود کنند که قادر به رمزگذاری اسناد، سرقت رمزهای عبور و غیره هستند.

برای محافظت در برابر چنین حمله ای، به برنامه های ناشناس اجازه ندهید که اتصالات شبکه را برقرار کرده و بپذیرند.

ماینها (Miners)

این نوع بدافزار از منابع رایانه برای استخراج مخفیانه ارز دیجیتال استفاده می کند. ماینرها منابع پردازنده و/یا کارت گرافیک را مصرف می کنند و عملکرد رایانه کاربر را کاهش می دهند.

برای محافظت در برابر چنین حمله ای، به برنامه های ناشناس اجازه ندهید که اتصالات شبکه را برقرار کرده و بپذیرند.

بدافزار درجه پایین (Low-grade malware)

بدافزار می‌تواند باعث هنگ کردن یا نقص سایر برنامه‌ها شود. می‌تواند سرعت رایانه را به میزان قابل توجهی کاهش دهد یا باعث راه‌اندازی مجدد خود به خودی یا صفحه آبی شود.

برای محافظت در برابر چنین حمله‌ای، از نرم‌افزارهای محافظتی برای اسکن منظم فایل‌های رایانه استفاده کنید.

چگونه ضررها را کاهش دهیم؟

روش‌های کاهش تلفات را می‌توان مشابه روش‌های پیشگیری از حمله دسته‌بندی کرد:

- از بین بردن اهداف بالقوه حمله

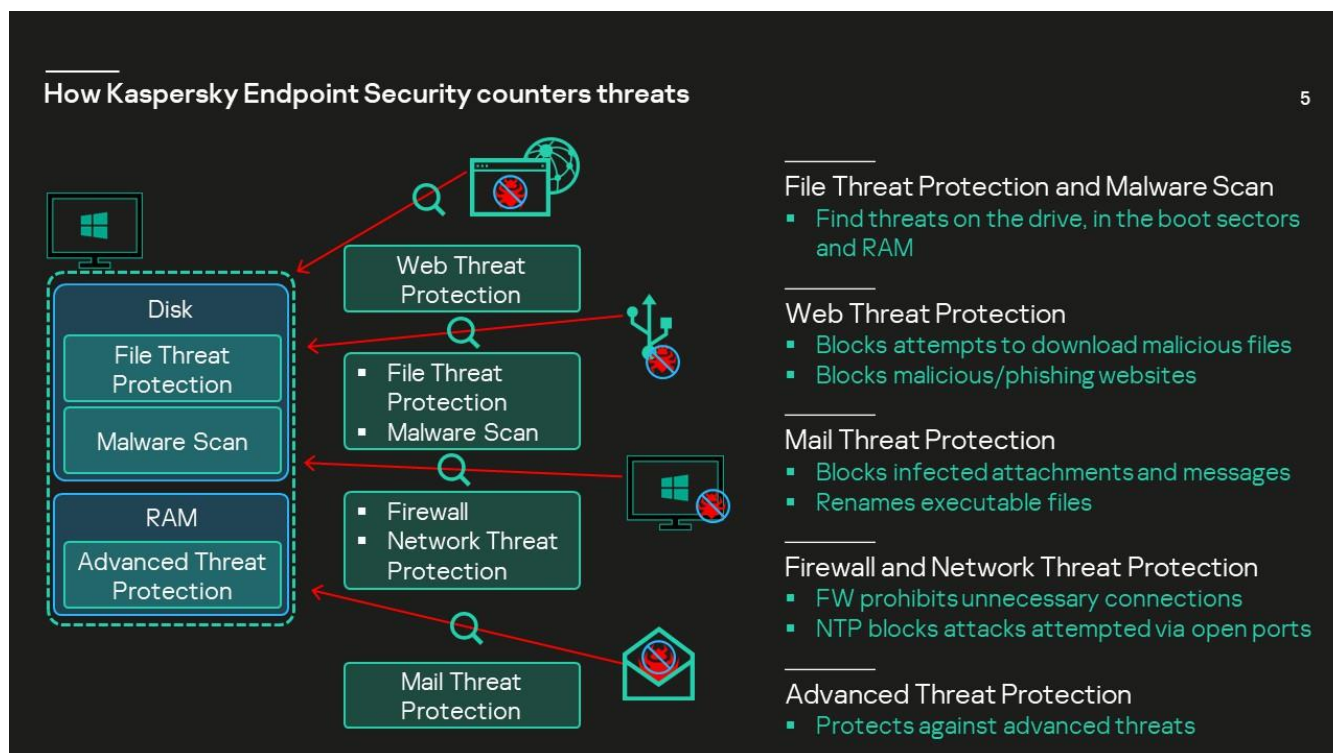
- اجازه ندادن به برنامه‌های ناشناخته برای ایجاد و پذیرش اتصالات شبکه

- استفاده از ابزارهای حفاظتی برای شناسایی حملات

- استفاده از راه‌حل‌های حفاظتی که به صورت اکتشافی فعالیت‌های خطرناک را شناسایی می‌کنند

- استفاده از نرم‌افزار حفاظتی برای اسکن منظم فایل‌های روی رایانه

۱.۲ چگونه Kaspersky Endpoint Security با حملات مقابله می‌کند ؟



اجزای Kaspersky Endpoint Security و Kaspersky Security Center تمام تلاش خود را برای محافظت در برابر حملات و جلوگیری از ضرر و زیان انجام می‌دهند.

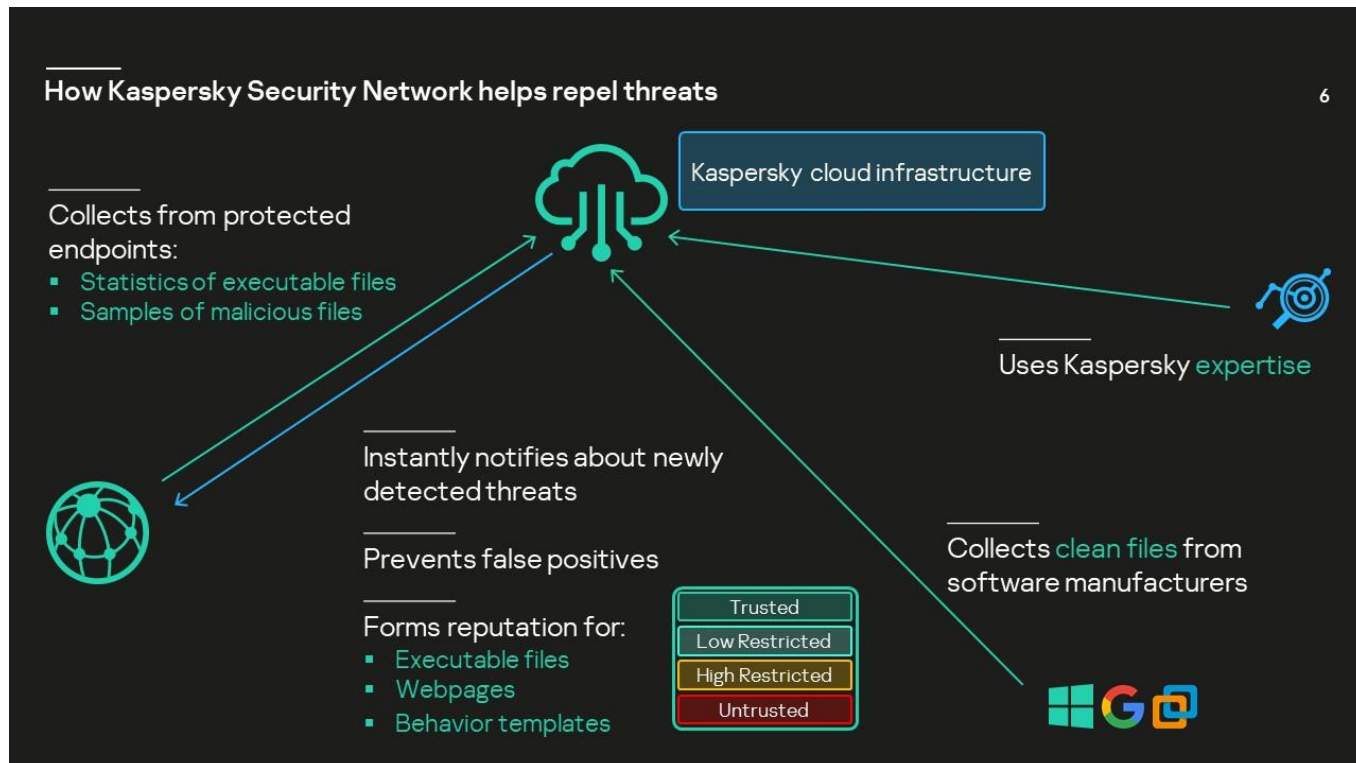
از بین بردن اهداف حمله بالقوه	
Kaspersky Security Center	نصب به‌روزرسانی‌های امنیتی برای سیستم‌عامل‌ها
Kaspersky Security Center	نصب به‌روزرسانی‌ها برای مرورگرهای وب و سایر برنامه‌ها
Application Control	به کاربران اجازه ندهید که بدون هیچ تمایزی هر مرورگری را باز کنند
Web Control	به کاربران اجازه ندهید که بی‌هدف هر صفحه وب را باز کنند
Behavior Detection Exploit Prevention	به مرورگرهای وب اجازه ندهید که فرآیندهای فرزند را شروع کنند
Mail Threat Protection	به کاربران اجازه ندهید فایل‌های اجرایی را از ایمیل‌ها در درایو ذخیره کنند
Firewall	اتصال به پورت‌هایی که کاربران برای کار خود به آنها نیاز ندارند را ممنوع کنید
Device Control	به کاربران اجازه ندهید که فلش مموری‌های USB ناشناس را به کامپیوترها متصل کنند.
Firewall	به برنامه‌های ناشناس اجازه برقراری و پذیرش اتصالات شبکه را ندهید
استفاده از راهکارهای حفاظتی برای شناسایی حملات	
Kaspersky Security Center	نصب برنامه‌های حفاظتی روی تمام رایانه‌ها
File Threat Protection	اسکن فایل‌هایی که کاربران کپی، باز یا اجرا می‌کنند
Anti-malware scanning	از نرم‌افزارهای امنیتی برای اسکن فایل‌های روی درایوهای USB استفاده کنید
Mail Threat Protection	از نرم‌افزارهای امنیتی برای اسکن فایل‌های پیوست‌شده به ایمیل‌ها استفاده کنید
Web Threat Protection	از نرم‌افزارهای حفاظتی برای اسکن فایل‌هایی که کاربران از اینترنت دانلود می‌کنند استفاده کنید.
Web Threat Protection	به کاربران اجازه ندهید وبسایت‌های آلوده و فیشینگ شناخته‌شده را باز کنند
Web Threat Protection	به کاربران اجازه ندهید وبسایت‌هایی را که به توزیع بدافزار معروف هستند، باز کنند.
Network Threat Protection	از نرم‌افزارهای حفاظتی برای بررسی بسته‌های ورودی جهت شناسایی حملات شبکه استفاده کنید.
BadUSB Attack Prevention	به کاربران اجازه ندهید که به طور خودکار هیچ دستگاه USB را به عنوان صفحه کلید متصل کنند
Behavior Detection Host Intrusion Prevention	از راهکارهای حفاظتی استفاده کنید که به صورت اکتشافی فعالیت‌های خطرناک را تشخیص می‌دهند
Malware Scan	از نرم‌افزارهای حفاظتی برای اسکن منظم فایل‌های رایانه استفاده کنید

این لیست شامل تمام اجزای Kaspersky Endpoint Security است. همه آنها یا سطح حمله را کاهش می‌دهند، یا به طور فعال تهدیدات را اسکن، شناسایی و مسدود می‌کنند.

Kaspersky Endpoint Security نه از فایل‌های روی رایانه نسخه پشتیبان تهیه می‌کند و نه در برابر هرزنامه‌ها محافظت می‌کند. برای محافظت در برابر هرزنامه‌ها، از محصولات Kaspersky برای سیستم‌های پستی باید استفاده کنید:

- Kaspersky Security for Microsoft Exchange Servers
- Kaspersky Secure Mail Gateway

چگونه شبکه امنیتی کسپرسکی به دفع تهدیدات کمک می کند ؟



برای اطمینان از اینکه اجزای Kaspersky Endpoint Security به طور قابل اعتمادی در برابر تهدیدات محافظت می کنند، به روزرسانی منظم پایگاه های داده امضا بسیار مهم است.

همچنین مهم است که به Kaspersky Endpoint Security اجازه داده شود از Kaspersky Security Network استفاده کند.

Kaspersky Security Network (KSN) یک فناوری مبتنی بر ابر است که به افزایش دقت تصمیمات اتخاذ شده توسط اجزای حفاظتی کمک می کند.

محصولات حفاظتی Kaspersky اطلاعات ناشناس در مورد فایل های اجرایی در حال اجرا بر روی رایانه های محافظت شده را به سرورهای Kaspersky Security Network ارسال می کنند. Kaspersky Security Network از فناوری های یادگیری ماشینی برای تجزیه و تحلیل این داده ها استفاده می کند.

KSN م وارد زیر را در نظر می گیرد:

- زمان کشف فایل برای اولین بار
- میزان گستردگی فایل
- در کدام مناطق
- اینکه آیا فایل مورد اعتماد کاربران نسخه های شخصی Kaspersky Security است یا خیر

- اینکه آیا فایل با certificate امضا شده است، کدام certificate و غیره. فایل‌های مشکوک علاوه بر این توسط کارشناسان Kaspersky تجزیه و تحلیل می‌شوند. پس از آن، شبکه امنیتی کسپرسکی فایل را به یک گروه اعتماد اختصاص می‌دهد:

- مورد اعتماد (Trusted)
- محدودیت کم (Low Restricted)
- محدودیت زیاد (High Restricted)
- غیر قابل اعتماد (Untrusted)

برای هر گروه اعتماد، تحلیلگران کسپرسکی سناریوهایی را توسعه داده‌اند که بسته به گروه اعتماد اختصاص داده شده (اعتبار)، توصیف می‌کنند که فایل‌ها مجاز به انجام چه کارهایی هستند و چه کارهایی نیستند.

شبکه امنیتی کسپرسکی شامل یک پایگاه داده عظیم از چک‌سام‌های فایل‌های خوب شناخته شده است. کسپرسکی چک‌سام‌های فایل‌های مرجع را از بسیاری از تولیدکنندگان نرم‌افزار شناخته شده مانند مایکروسافت، ادوبی، گوگل و غیره دریافت می‌کند. به همین دلیل است که اجزای Kaspersky Endpoint Security می‌دانند کدام فایل‌ها آلوده نیستند و برنامه‌های مربوطه را مختل نمی‌کنند.

شبکه امنیتی کسپرسکی همچنین اعتبار صفحات وب را محاسبه می‌کند.

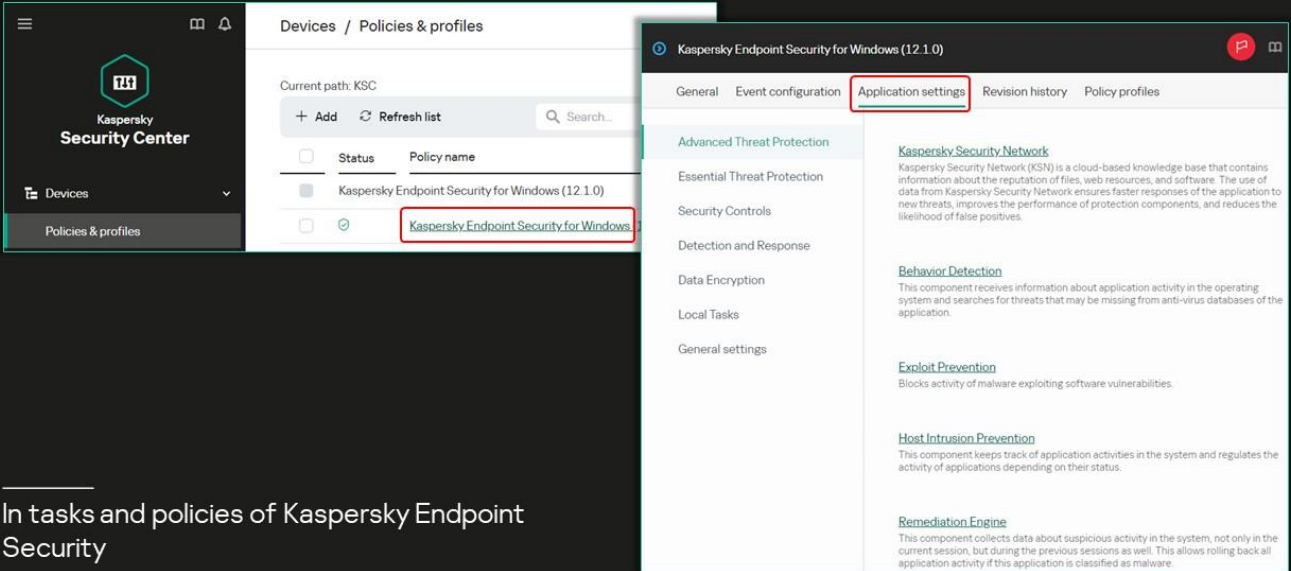
اگر کسپرسکی یک تهدید جدید را شناسایی کند، چک‌سام‌های تمام فایل‌ها و صفحات وب مخرب در کسری از ثانیه به شبکه امنیتی کسپرسکی می‌رسند و برای همه محصولات که از شبکه امنیتی کسپرسکی استفاده می‌کنند در دسترس هستند. محصولات چند ساعت قبل از دانلود امضاهای تهدید در به‌روزرسانی‌ها، از طریق شبکه امنیتی کسپرسکی از تهدیدات جدید مطلع می‌شوند. داده‌هایی که Kaspersky Endpoint Security به شبکه امنیتی کسپرسکی ارسال می‌کند، غیرشخصی و ناشناس هستند. لیست کامل را می‌توانید در توافقنامه شبکه امنیتی کسپرسکی بیابید که مدیر باید قبل از فعال کردن شبکه امنیتی کسپرسکی در سیاست امنیتی کسپرسکی اندپوینت بپذیرد.

برای اینکه بتوانید بدون ارسال چیزی به کسپرسکی از شبکه امنیتی کسپرسکی استفاده کنید، سرویس شبکه امنیتی خصوصی کسپرسکی وجود دارد.

تنظیمات Kaspersky Endpoint Security کجا قرار دارند؟

Where can I find and edit protection settings?

7



In tasks and policies of Kaspersky Endpoint Security

در این واحد، موارد زیر را بررسی خواهیم کرد:

- کدام تنظیمات در اجزای Kaspersky Endpoint Security موجود است
- مقادیر پیش فرض آنها
- چگونه تنظیمات بر رفتار اجزا تأثیر می گذارند
- چه زمانی و چگونه می توان تنظیمات را برای بهبود حفاظت از رایانه یا تجربه کاربری تغییر داد

بیشتر تنظیمات Kaspersky Endpoint Security در خط مشی قرار دارند. برخی از تنظیمات، مانند اسکن برنامه ریزی شده ضد بدافزار، به روزرسانی ها یا پاک کردن داده ها، در وظایف پیکربندی شده اند.

پیکربندی شبکه امنیتی کسپرسکی (Configure Kaspersky Security Network) :

اگر ویزارد شروع سریع را تکمیل کرده و بیانیه KSN را پذیرفته باشید، Kaspersky Security Network از قبل در سیاست Kaspersky Endpoint Security فعال خواهد بود. در غیر این صورت، می توانید به تنظیمات برنامه | حفاظت پیشرفته در برابر تهدید | Kaspersky Security Network بروید، KSN را فعال کنید و توافق نامه را بپذیرید.

Kaspersky Endpoint Security موارد زیر را به Kaspersky Security Network ارسال می‌کند:

- اطلاعات مربوط به فایل‌های اسکن شده و آدرس‌های URL بررسی شده
- داده‌های مربوط به وظیفه یا مؤلفه اسکن Kaspersky Endpoint Security که تهدیدات را شناسایی کرده است
- اطلاعات مربوط به فعال‌سازی نرم‌افزار در نقطه پایانی
- چک‌سام‌ها و کلید عمومی certificate های دیجیتال استفاده شده و غیره.

به طور پیش‌فرض، KES اطلاعات مربوط به موارد زیر را نیز به سرورهای KSN ارسال می‌کند:

- نرم‌افزارهای نصب شده روی رایانه، برنامه‌های در حال اجرا و ماژول‌های آنها
- وضعیت حفاظت ضد بدافزار
- فایل‌های دانلود شده توسط کاربر
- اشیاء بالقوه مخرب، اشیاء اسکن شده و سایر اشیاء برای غیرفعال کردن ارسال داده‌های اضافی، حالت Extended KSN را غیرفعال کنید.

به طور پیش‌فرض، Kaspersky Endpoint Security در حالت ابری (Cloud) عمل می‌کند. در این حالت، KES از نسخه سبک‌تری از پایگاه‌های داده آنتی‌ویروس استفاده می‌کند. این امر تقریباً دو برابر کاهش بار روی حافظه کامپیوتر را فراهم می‌کند، اما تعداد درخواست‌ها از طریق اینترنت را افزایش می‌دهد.

استفاده از پروکسی KSN به طور پیش‌فرض در پالیسی فعال است. Kaspersky Endpoint Security از طریق یک پروکسی با Kaspersky Security Network ارتباط برقرار می‌کند.

سرویس پروکسی KSN به طور پیش‌فرض روی سرور مدیریت اجرا می‌شود. در این حالت، سرور عملکرد یک سرور پروکسی KSN را انجام می‌دهد و اتصالات را از طریق پورت TCP 13111 می‌پذیرد.

پروکسی KSN داده‌های پردازش شده را ذخیره می‌کند و در نتیجه بار کانال ارتباطی را کاهش می‌دهد و به رایانه‌های کاربر کمک می‌کند تا اطلاعات درخواستی را سریع‌تر دریافت کنند.

تمام رایانه‌های مدیریت شده توسط یک پالیسی از طریق سرور مدیریت به KSN درخواست می‌دهند.

۲. نحوه پیکربندی محافظت از فایل :

۲.۱ چگونه Kaspersky Endpoint Security از فایل‌ها محافظت می‌کند؟

File Threat Protection (File Threat Protection) با استفاده از درایور klif.sys تمام عملیات فایل (مانند خواندن، کپی کردن، اجرا) را رهگیری می‌کند و فایل‌هایی را که مورد دسترسی قرار می‌گیرند، اسکن می‌کند. اگر فایلی آلوده باشد، این مؤلفه عملیات را مسدود کرده و فایل را ضدعفونی یا حذف می‌کند.

به جز آسیب‌پذیری‌هایی که به بدافزار اجازه می‌دهند کد را در حافظه بارگذاری کند، همه حملات فایل‌های مخرب را در درایو کامپیوتر ذخیره می‌کنند. حتی حملاتی که با اجرای کد در حافظه شروع می‌شوند، می‌توانند مقدار کمی کد را دانلود کنند. این کد می‌تواند به عنوان اولین مرحله حمله استفاده شود و ماژول‌های اضافی را به شکل فایل دانلود کرده و آنها را در درایو محلی ذخیره کند.

حتی اگر محافظت در برابر تهدید ایمیل (Mail Threat Protection) و محافظت در برابر تهدید وب (Web Threat Protection) غیرفعال باشند، کاربر قادر به اجرای یک فایل آلوده دریافت شده از طریق ایمیل یا دانلود شده از اینترنت نخواهد بود، زیرا یک فایل بدون ذخیره شدن در هارد دیسک قابل اجرا نیست. اما وقتی فایل روی دیسک ذخیره می‌شود، توسط File Threat Protection (File Threat Protection) شناسایی و مسدود می‌شود.

این امر File Threat Protection را به یکی از اجزای مهم Kaspersky Endpoint Security تبدیل می‌کند. محافظت در برابر تهدیدات فایل، فایل‌ها را برای یافتن بدافزار با استفاده از موارد زیر اسکن می‌کند:

— امضاهای بدافزار — پایگاه‌های داده‌ی Kaspersky Endpoint Security حاوی یک «لیست رد» از فایل‌های مخرب شناخته شده هستند.

اگر فایلی با هیچ یک از رکوردهای پایگاه داده مطابقت نداشته باشد، تجزیه و تحلیل امضا آن را بی‌ضرر می‌داند. یک لیست رد کامل با یک ورودی برای هر فایل مخرب یا آلوده‌ی شناخته شده، به فضای زیادی نیاز دارد. به همین دلیل است که پایگاه داده‌ی امضا بهینه شده و به اندازه‌ای محدود شده است که به راحتی در یک دستگاه قابل دانلود باشد. هر ورودی، خانواده‌ای از تهدیدات مشابه را شناسایی می‌کند.

تجزیه و تحلیل اکتشافی (شبیه‌سازی) به شناسایی فایل‌های مخرب چندریختی که کد خود را در حین اجرا تغییر می‌دهند و بنابراین تشخیص آنها با استفاده از امضاها دشوار است، کمک می‌کند.

حفاظت در برابر تهدیدات فایل، فایل‌های اجرایی را در یک محیط ایزوله‌ی ویژه شروع می‌کند و بررسی می‌کند که آیا کد در حافظه برای مطابقت با امضا تغییر می‌کند یا خیر.

- بررسی‌های KSN—File Threat Protection چک‌سام فایل را به KSN ارسال می‌کند و پاسخی دریافت می‌کند:
- اینکه آیا فایل در پایگاه داده KSN یافت می‌شود یا خیر؟
- اعتبار آن چقدر است؟

پایگاه داده شبکه امنیتی کسپرسکی فهرست بزرگی از تمام فایل‌هایی (به طور دقیق‌تر، چک‌سام‌های آنها) است که کسپرسکی آنها را می‌شناسد.

اگر فایلی اعتبار غیرقابل اعتمادی داشته باشد، در لیست ممنوعه قرار می‌گیرد و File Threat Protection آن را مسدود می‌کند. فایل‌هایی با اعتبار قابل اعتماد در لیست مجاز قرار دارند که شامل فایل‌های بی‌ضرر شناخته شده سیستم عامل‌ها و نرم‌افزارهای محبوب است. File Threat Protection این فایل‌ها را حتی اگر با امضاهای بدافزار مطابقت داشته باشند، مسدود نمی‌کند. پاسخ‌های KSN اولویت بالاتری دارند، زیرا KSN حاوی اطلاعات بیشتری نسبت به یک پایگاه داده امضای محلی است.

یک کامپیوتر می‌تواند اتصال اینترنتی غیرقابل اعتمادی داشته باشد که مانع از دریافت پاسخ از KSN توسط Kaspersky Endpoint Security می‌شود. به همین دلیل، Kaspersky Endpoint Security صرفاً به KSN متکی نیست و پایگاه داده امضا و شبیه‌سازی را نیز در بر می‌گیرد.

اعتبار یک فایل ممکن است با گذشت زمان در KSN تغییر کند. فایلی که تازه در اینترنت ظاهر شده است، در ابتدا هیچ اعتباری ندارد. با گذشت زمان، KSN اطلاعاتی در مورد اینکه چه کسی، کجا و چگونه از فایل استفاده می‌کند، جمع‌آوری می‌کند. اعتبار آن بر این اساس تغییر می‌کند و ممکن است قابل اعتماد یا غیرقابل اعتماد شود.

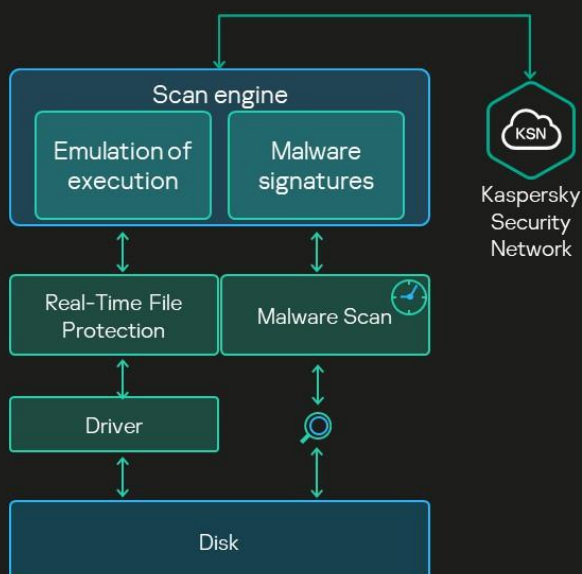
برای محافظت بهتر، Kaspersky Embedded Systems Security می‌تواند در هر عملیات فایل، درخواست‌هایی را به KSN ارسال کند. اما انجام این کار ترافیک شبکه رایانه را چند برابر می‌کند. علاوه بر این، ارسال درخواست و دریافت پاسخ، زمانی را می‌طلبد که به کیفیت کانال ارتباطی بستگی دارد.

برای جلوگیری از ایجاد ترافیک اضافی و تأخیر در عملیات فایل، Kaspersky Endpoint Security پاسخ‌های KSN را در یک حافظه پنهان محلی ذخیره می‌کند. هر پاسخ طول عمر خاص خود را دارد. برای فایل‌های جدید، این طول عمر کوتاه است و Kaspersky Endpoint Security اغلب اعتبار فایل را دوباره بررسی می‌کند. برای فایل‌هایی که مدت زیادی است شناخته شده‌اند، این زمان طولانی‌تر است.

برای جلوگیری از کند شدن کامپیوتر، File Threat Protection به طور پیش‌فرض همه فایل‌ها را اسکن نمی‌کند؛ فقط فایل‌هایی را اسکن می‌کند که ممکن است سیستم را آلوده کنند.

How Kaspersky Endpoint Security scans files

10



File Threat Protection scans files on the drive when the user or a program accesses them

An anti-malware scan task scans files according to the specified schedule

Components detect dangerous programs using:

- A local malware signature database
- Emulated file launch in a sandbox
- Kaspersky Security Network reputation database

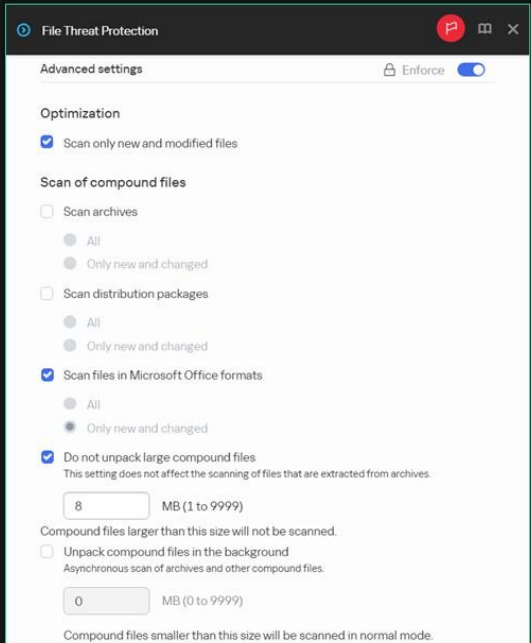
The emulator helps to detect polymorphic threats

Kaspersky Security Network helps to:

- Detect new threats
- Exclude known non-malicious files

برای مثال، File Threat Protection به طور پیش فرض فایل های آرشیو را اسکن نمی کند، زیرا یک فایل قبل از شروع باید استخراج شود. یا کاربر فایل را از آرشیو استخراج می کند، یا سیستم عامل این کار را برای کاربر انجام می دهد. در هر صورت، File Threat Protection فایل های استخراج شده را اسکن می کند (و در صورت لزوم آنها را مسدود می کند). شما باید از وظایف اسکن بدافزار برای اسکن فایل هایی که File Threat Protection از آنها صرف نظر می کند، استفاده کنید. اسکن ضد بدافزار، فایل ها را در محدوده مشخص شده بررسی می کند و از همان روش های File Threat Protection استفاده می کند.

۲.۲ پیکربندی File Threat Protection (Configure File Threat Protection) :



11

By default, real-time protection does not scan the same files repeatedly.
It scans only new files, and those that have changed

It also does not scan archives or installation packages (self-extracting archives, etc.)

It does not scan a file at each read or write operation
Depending on the file type and operation, it scans a file before it is opened or after it is closed

Do not change these settings without strong reasons

File Threat Protection باید دو هدف را دنبال کند:

- جلوگیری از آسیب رساندن بدافزار
- ایجاد مانع برای کاربر یا نرم افزارهای قانونی

هرچه File Threat Protection فایل های بیشتری را اسکن کند، بهتر به هدف اول دست می یابد، اما هدف دوم را بدتر برآورده می کند و برعکس.

تنظیمات پیش فرض، محافظت و عملکرد را متعادل می کند. با تنظیم تنظیمات، مدیر می تواند تعادل را به یک سمت یا سمت دیگر تغییر دهد.

شما می توانید تنظیمات Kaspersky Endpoint Security را در پالیسی تنظیم کنید. تنظیمات همه اجزا در بخش های مربوطه قرار دارند: می توانید File Threat Protection را در تب تنظیمات برنامه، در بخش محافظت ضروری در برابر تهدید | File Threat Protection پیدا کنید.

ابتدا اجازه دهید در مورد تنظیماتی که نباید تغییر کنند صحبت کنیم و دلیل آن را توضیح دهیم.

File Threat Protection ، فایل ها را بر اساس فرمت اسکن می کند :

فایل هایی که به کامپیوترها آسیب می رسانند، عمدتاً فایل های اجرایی هستند، اما نه همیشه. اسناد مایکروسافت آفیس ممکن است حاوی کدهای اجرایی (ماکروها) باشند که می توانند مخرب باشند. حتی اسناد بدون کد، به عنوان مثال، برخی از فایل های گرافیکی، ممکن است از آسیب پذیری های برنامه هایی که آنها را باز می کنند، سوءاستفاده کنند و باعث شوند این برنامه ها بخشی از فایل را به عنوان کد اجرا کنند.

به طور پیش فرض، File Threat Protection فایل ها را بر اساس فرمت اسکن می کند. به این ترتیب، Kaspersky Endpoint Security به طور قابل اعتمادی از کامپیوتر محافظت می کند، زیرا همه فایل های خطرناک را اسکن می کند، اما سرعت کامپیوتر را کاهش نمی دهد، زیرا همه فایل ها را اسکن نمی کند.

اسکن کردن فایل ها فقط بر اساس پسوند خطرناک است. به عنوان مثال، یک سند Word مخرب ممکن است پسوند ۱۲۳ داشته باشد که در محدوده اسکن گنجانده نشده است، اما کاربر همچنان می تواند آن را از طریق منوی میانبر آن (Open with) باز کند. همچنین، اسکن بر اساس پسوند به طور قابل توجهی سریع تر از اسکن بر اساس فرمت نیست. کاربر هیچ تفاوتی در عملکرد احساس نخواهد کرد.

این کامپوننت فایل های اجرایی، فایل های BAT، اسکریپت ها، فایل های DLL، اسناد مایکروسافت آفیس و سایر فایل ها را اسکن می کند.

اگر مدیر سیستم می خواهد عملکرد کامپیوترهای کند را بهبود بخشد، بهتر است با استثنائاتی برای برنامه هایی که کاربران با آنها کار می کنند شروع کند. نحوه ایجاد استثنائات را در انتهای این بخش توضیح می دهیم.

File Threat Protection، فایل هایی را که قبلاً اسکن شده اند، اسکن نمی کند.

بیشتر فایل های روی کامپیوتر به ندرت تغییر می کنند. برای جلوگیری از بارگذاری بیش از حد کامپیوتر، File Threat Protection فقط فایل های جدید و تغییر یافته را اسکن می کند.

در چند روز اول، زمانی که هر فایل برای Kaspersky Endpoint Security جدید است، کاربر ممکن است احساس کند که کامپیوتر کندتر کار می‌کند. اما File Threat Protection به زودی تأثیر منفی خود را بر عملکرد متوقف خواهد کرد. برای جلوگیری از کند شدن کامپیوتر، گزینه «فقط فایل‌های جدید و اصلاح‌شده را اسکن کنید» را در بخش File Threat Protection غیرفعال نکنید.

Kaspersky Endpoint Security چگونه می‌فهمد کدام فایل‌ها تغییر کرده‌اند و کدام‌ها تغییر نکرده‌اند؟

سیستم فایل NTFS (و جانشین آن ReFS) هنگام تغییر فایل‌ها، گزارش می‌گیرد و یکپارچگی این سوابق را تضمین می‌کند. بنابراین، در درایوهای NTFS، Kaspersky Endpoint Security به سادگی تاریخ تغییر فایل را بررسی می‌کند.

سیستم فایل FAT32 نمی‌تواند تاریخ تغییر را ثبت کند و نمی‌تواند از تاریخ تغییر در برابر تغییرات ناخواسته محافظت کند. بدافزار ممکن است یک فایل را تغییر دهد و سپس هر تاریخ تغییری را به آن اختصاص دهد.

Kaspersky Endpoint Security چک‌سام‌های فایل‌های اسکن شده را در یک پایگاه داده ویژه برای درایوهای FAT32 ذخیره می‌کند. دفعه بعد که به یک فایل دسترسی پیدا می‌شود، Kaspersky Endpoint Security چک‌سام را دوباره محاسبه می‌کند و آن را با چک‌سام ذخیره شده مقایسه می‌کند. اگر این مبالغ متفاوت باشند، فایل تغییر کرده است، بنابراین File Threat Protection آن را اسکن می‌کند.

اسکن فایل‌های جدید فقط یک بار خطرناک است. اگر بدافزار قبل از دریافت امضاهای Kaspersky Endpoint Security روی رایانه قرار گیرد، File Threat Protection آن را اسکن می‌کند، آن را پاک در نظر می‌گیرد و در شروع بعدی اسکن نمی‌کند.

برای جلوگیری از این امر، حتی اگر گزینه «فقط فایل‌های جدید و اصلاح‌شده را اسکن کنید» فعال باشد، File Threat Protection، تمام فایل‌های جدید را به طور مکرر، حداقل دو بار، و احتمالاً چندین بار، اسکن می‌کند.

برای این منظور، Kaspersky Endpoint Security زمان انتشار اولین و آخرین امضاهای استفاده شده برای اسکن یک فایل را ذخیره می‌کند. File Threat Protection، در صورت وجود شرایط زیر، فایل را دوباره اسکن می‌کند:

- فایل فقط یک بار اسکن شده باشد.
- نسخه فعلی امضاها با نسخه‌ای که برای اولین اسکن فایل استفاده شده است، کمتر از ۲۴ ساعت متفاوت باشد.

برای کاهش بیشتر خطر، از یک برنامه اسکن بدافزار برای بررسی تمام فایل‌های موجود در رایانه، از جمله فایل‌هایی که تغییر نکرده‌اند و قبلاً توسط File Threat Protection اسکن شده‌اند، استفاده کنید.

اگر امضاهای یک تهدید جدید ظرف ۲۴ ساعت صادر نشوند، چه می‌شود؟ این تقریباً هرگز اتفاق نمی‌افتد. علاوه بر این، علاوه بر امضاها، Kaspersky Endpoint Security از داده‌های Kaspersky Security Network استفاده می‌کند که حاوی جدیدترین اطلاعات در مورد تهدیدها است.

File Threat Protection بدافزار را شناسایی و حذف کرده است
بدافزارهای شناسایی شده توسط File Threat Protection نباید بدون پردازش رها شوند و تنظیماتی که بر عملکرد File Threat Protection حاکم هستند باید قفل شوند.

بهترین انتخاب، ضدعفونی کردن و در صورت غیرممکن بودن ضدعفونی، حذف فایل‌های آلوده است. اکثر فایل‌های مخرب را نمی‌توان ضدعفونی کرد، زیرا حاوی چیزی جز کد آلوده نیستند.

قبل از اینکه یک فایل ضدعفونی یا حذف شود، یک کپی در نسخه پشتیبان قرار می‌گیرد. اگر فایلی حاوی اطلاعات مهم باشد یا به دلیل یک خطای false positive حذف شده باشد، می‌توانید آن را بازیابی کنید.

اگر مؤلفه Remediation Engine در Advanced Threat Protection فعال باشد، Kaspersky Endpoint Security نه تنها فایل‌های مخرب را حذف می‌کند، بلکه اقدامات آنها را نیز به حالت قبل برمی‌گرداند.

پوشه یک برنامه را مستثنی کنید

Do not scan the program folder

13

Exclusions and types of detected objects

Scan exclusions
Total number of exclusions: 0, 0 of them active

Exclusions and types of detected objects
Types of detected objects and scan exclusions

+ Add

Exclusion

File or folder
c:\build\

Including subfolders

Object name

Object hash
Add hash from file
Select

Add hash from events
Select

Add hash manually

Comment

Protection components
Any
From list

File Threat Protection
Mail Threat Protection
Web Threat Protection
Host Intrusion Prevention
Scan
Behavior Detection
AMSI Protection

Add the folder to the list of exclusions in the general protection settings

Use environment variables, for example, %ProgramFiles(x86)%

Use masks

Apply the exclusion to the File Threat Protection component

استثنائات در سیاست امنیتی کسپرسکی اندپوینت پیکربندی شده‌اند: تنظیمات برنامه | تنظیمات عمومی را باز کنید و روی پیوند استثنائات و انواع اشیاء شناسایی شده کلیک کنید.

برای تنظیم استثنائات برای پوشه‌ها، روی پیوند استثنائات اسکن کلیک کنید. آنها برای همه اجزای محافظت اعمال می‌شوند.

یک استثنای اسکن شامل ویژگی‌های زیر است:

- File or folder - نام فایل یا پوشه‌ای که استثنا به آن اعمال می‌شود. نام شیء ممکن است شامل متغیرهای محیطی (%userprofile, %systemroot) و غیره) و همچنین کاراکترهای wildcard "*" و "?" باشد.
- Object name - نام تهدیدی که باید نادیده گرفته شود (معمولاً مربوط به نام بدافزار است) که می‌تواند با استفاده از کاراکترهای wildcard نیز مشخص شود.
- Object hash - مجموع کنترلی (SHA-256) فایلی که استثنا به آن اعمال می‌شود.
- Protection components - لیست اجزای محافظتی که این قانون به آنها اعمال می‌شود.

سه ویژگی اول استثنا اختیاری هستند (اما باید حداقل یکی از آنها را مشخص کنید). ویژگی آخر الزامی است.

شما می‌توانید بدون مشخص کردن نوع تهدید، برای یک فایل یا پوشه، یک استثنای اسکن ایجاد کنید. اجزای انتخاب شده، هرگونه تهدیدی را در فایل یا پوشه مشخص شده نادیده می‌گیرند.

برعکس، می‌توانید برای یک نوع تهدید خاص، مثلاً برای برنامه مدیریت از راه دور UltraVNC، یک استثنای اسکن ایجاد کنید تا اجزای حفاظتی انتخاب شده صرف نظر از محل شناسایی آن، به این تهدید پاسخ ندهند.

همچنین می‌توان همه ویژگی‌ها را به طور همزمان مشخص کرد. به عنوان مثال، می‌توانید برای ابزارهای محبوب مدیریت از راه دور مانند RAdmin، UltraVNC و غیره، استثناهایی ایجاد کنید. علاوه بر این، می‌توانید مسیر فایل اجرایی برنامه را در صورتی که در تمام رایانه‌های شبکه شما در یک پوشه نصب شده باشد، مشخص کنید. با توجه به چنین استثنائی، Kaspersky Endpoint Security به یک برنامه مدیریت از راه دور اجازه می‌دهد تا از پوشه Program Files اجرا شود، اما اگر کاربر آن را از پوشه دیگری اجرا کند، آن را یک تهدید در نظر می‌گیرد.

فایل‌هایی که توسط یک فرآیند قابل دسترسی هستند را مستثنی کنید :

14

Do not scan files that a process accesses

Exclusions and types of detected objects

Scan exclusions and trusted applications

Scan exclusions
Total number of exclusions: 0, 0 of them active

Trusted applications
Total number of trusted applications: 1, 1 of them active

Exclusions and types of detected objects
Types of detected objects and scan exclusions

+ Add

Application

Path or path mask to the application
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe

Comment

☒ Do not scan files before opening
☐ Do not monitor application activity
☐ Do not inherit restrictions of the parent process (application)
☐ Do not monitor child application activity
☐ Apply exclusion recursively
☐ Allow interaction with the application interface
☐ Do not block interaction with AMSI Protection component
☒ Do not scan network traffic
☐ Do not collect telemetry for console interactive input

Encrypted traffic only
☒ All traffic

Specified remote IP addresses

+ Add X Delete

IP address

No data

Add the program executable file to the list of trusted applications

Use **wildcards** and **environment variables**, for example,
%ProgramFiles(x86)%

Select the checkbox **Do not scan files before opening**

محافظت در برابر تهدید فایل ممکن است عملکرد برنامه‌هایی که منابع زیادی مصرف می‌کنند را کند کند. این امر به ویژه در مورد برنامه‌هایی که عملیات فایل متعددی انجام می‌دهند، مانند کپی پشتیبان یا یکپارچه‌سازی، صادق است. برای جلوگیری از کاهش سرعت، این برنامه‌ها را قابل اعتماد کنید.

برای انجام این کار، در پنجره تنظیمات استثنا، فایل اجرایی را به لیست برنامه‌های قابل اعتماد اضافه کنید. در قسمت مسیر یا ماسک مسیر برنامه، مسیر فایل اجرایی را مشخص کنید و گزینه «قبل از باز کردن، فایل‌ها را اسکن نکنید» را انتخاب کنید. مسیر ممکن است شامل متغیرهای محیطی و علامت‌های «*» و «؟» باشد.

اعمال تنظیمات روی کامپیوترها

تنظیمات پالیسی باید اعمال شوند، یعنی قفل شوند. تنظیمات قفل نشده روی کامپیوترها اعمال نمی‌شوند.

از آنجایی که همه قفل‌ها به طور پیش فرض در یک پالیسی بسته هستند، ممکن است مدیر سیستم حتی متوجه آنها نشود. می‌توانید تنظیمات را بدون لمس قفل‌ها ویرایش کنید، اما همه تنظیمات همچنان الزامی هستند و روی کامپیوترها اعمال می‌شوند.

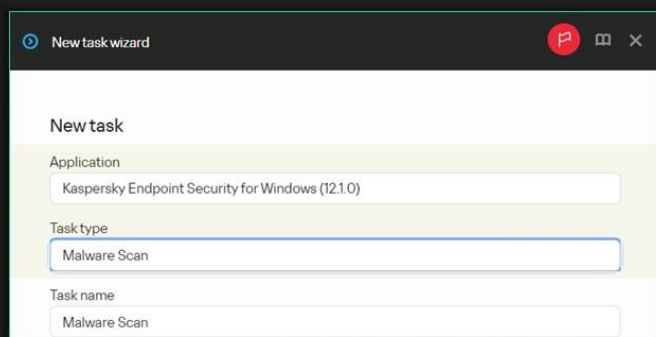
با این حال، باید به خاطر داشته باشید که اگر قفل‌ها باز باشند، تنظیمات پیکربندی شده اعمال نمی‌شوند. اگر تنظیمات را در یک پالیسی تغییر دهید، اما آنها روی کامپیوترها تغییر نکنند، قفل‌های موجود در پالیسی را بررسی کنید.

۲.۴ اسکن فایل زمان‌بندی‌شده

چرا علاوه بر محافظت در برابر تهدیدات فایل، اسکن بدافزار نیز انجام می‌شود؟

Why scan for malware in addition to File Threat Protection

18



File Threat Protection:

- Does not scan archives through which malware can spread
- Does not scan files that have not been modified, which can be dangerous

اگر File Threat Protection به هر حال همه فایل‌های خطرناک را اسکن می‌کند، اسکن ضد بدافزار چگونه می‌تواند کمک کند؟ اسکن بدافزار:

- از انتشار بدافزار بایگانی شده توسط کاربران جلوگیری می‌کند
- حافظه‌های پنهان KSN را به‌روزرسانی می‌کند
- اطلاعات مربوط به چک‌سام‌های فایل را به‌روزرسانی می‌کند و به File Threat Protection اجازه می‌دهد فایل‌های کمتری را اسکن کند.
- فایل‌هایی را که تغییر نکرده‌اند اسکن می‌کند. File Threat Protection چنین فایل‌هایی را اسکن نمی‌کند، که ممکن است خطرناک باشند.

وظایف اسکن بدافزار، اشیاء را با استفاده از همان روش‌های File Threat Protection بررسی می‌کنند: تحلیل امضا و اکتشافی و KSN. تفاوت این است که File Threat Protection فایل‌ها را در حین دسترسی بررسی می‌کند، در حالی که وظایف اسکن بدافزار فایل‌ها را بر اساس برنامه یا بر اساس تقاضا بررسی می‌کند.

File Threat Protection با کاربر کار می‌کند. هرچه برنامه‌های کاربر فعال‌تر باشند، File Threat Protection فایل‌های بیشتری را اسکن می‌کند و منابع بیشتری را مصرف می‌کند. بنابراین، تنظیمات File Threat Protection برای اطمینان از

محافظت در برابر تهدیدات فوری بهینه شده‌اند. اگر کاربر یک آرشیو را کپی کند، هیچ خطر آلودگی فوری وجود ندارد، بنابراین نیازی به اسکن آرشیو نیست.

وظایف اسکن بدافزار را می‌توان در ساعات غیرکاری، زمانی که منابع بیشتری در دسترس است و می‌توان اسکن کامل‌تری انجام داد، آغاز کرد. به همین دلیل است که وظیفه اسکن، صرف نظر از نتایج تحلیل امضا و اکتشافی، قبل از تصمیم‌گیری نهایی، منتظر پاسخی از KSN خواهد ماند.

همچنین، وظایف می‌توانند اشیایی را که از محدوده حفاظت در برابر تهدید فایل مستثنی هستند، اسکن کنند: آرشیوها، بسته‌های نصب، فایل‌هایی با فرمت‌های غیرقابل آلوده‌سازی و غیره.

یک وظیفه اسکن بدافزار را می‌توان طوری پیکربندی کرد که فرآیندهای موجود در حافظه را بررسی کند و می‌توان آن را طوری برنامه‌ریزی کرد که پس از هر به‌روزرسانی موفقیت‌آمیز پایگاه داده اجرا شود.

ایجاد و پیکربندی یک تسک Malware scan :

19

Create and configure a malware scan task

Malware Scan

General Results Settings Application settings Schedule Revision history

Scan scope

+ Add - Delete

Scan scope	Status
☐ My email	Excluded from protection scope
☐ Kernel Memory	Included in protection scope
☐ Running processes and Startup Objects	Included in protection scope
☐ Disk boot sectors	Included in protection scope
☐ System Backup	Excluded from protection scope
☐ All removable drives	Included in protection scope
☐ All network drives	Excluded from protection scope
☐ All hard drives	Included in protection scope
☐ Documents	Included in protection scope

Action on threat detection

☒ Disinfect, delete if disinfection fails

☐ Disinfect, inform if disinfection fails

☐ Inform

☐ Run Advanced Disinfection immediately

Warning! When active threats are detected, the Advanced Disinfection procedure is started without prompting the user for confirmation. The computer may be restarted when the process is completed.

☐ Scan only new and modified files

Reduces scanning time

5

Scan optimization

☒ Scan archives

*.zip, *.rar, *.cab, *.lha, *.arj, ...

☐ All

☐ Only new and changed

☒ Scan distribution packages

*.msi, *.exe, ...

☐ All

☐ Only new and changed

☒ Scan files in Microsoft Office formats

*.doc, *.docx, *.xls, *.xlsx, ...

☐ All

☐ Only new and changed

☐ Scan email formats

Saved messages and email databases

☐ Scan password-protected archives

Before files in a password-protected archive are scanned, you must enter the password. If the correct password is not entered, the files are not scanned.

☐ Do not unpack large files

100 MB

☐ Do not run multiple scans

Create a task that scans for threats:

1. Memory and boot sectors
2. Not network drives, to avoid extra load on the network
3. All local drives
4. All files, including those that have not been changed
5. Archives

شما می‌توانید اسکن ضد بدافزار را در ویژگی‌های وظایف اسکن بدافزار پیکربندی کنید.

مدیر سیستم باید به صورت دستی یک وظیفه اسکن بدافزار را در گروه دستگاه‌های مدیریت‌شده ایجاد کند. Kaspersky Endpoint Security به طور پیش‌فرض از وظیفه اسکن پس‌زمینه استفاده می‌کند.

وظیفه اسکن پس‌زمینه:

- نسبت به یک وظیفه اسکن بدافزار معمولی، منابع کمتری مصرف می‌کند.
- در حالی که رایانه قفل است اجرا می‌شود.
- هیچ اعلانی را به کاربر نمایش نمی‌دهد.
- وضعیت اسکن بدافزار را که مدت زیادی است انجام نشده است، بازنشانی نمی‌کند.

شما نمی‌توانید تنظیمات اسکن یا محدوده این وظیفه را تغییر دهید. به طور پیش‌فرض، این وظیفه اشیاء را در موارد زیر اسکن می‌کند:

- راه‌اندازی
- بخش‌های بوت دیسک
- حافظه هسته
- بخش‌های بوت دیسک

اگر می‌خواهید از یک وظیفه اسکن بدافزار سفارشی استفاده کنید، توصیه می‌کنیم اسکن پس‌زمینه را غیرفعال کنید. برای غیرفعال کردن این وظیفه، در تنظیمات خط‌مشی کسپرسکی اندپوینت سکیوریتی، تنظیمات برنامه | وظایف محلی | اسکن پس‌زمینه را باز کنید و کادر فعال کردن اسکن پس‌زمینه را بردارید.

برای ایجاد وظیفه خود، به دستگاه‌ها | وظایف بروید و یک وظیفه اسکن بدافزار اضافه کنید.

دامنه اسکن

دامنه اسکن، فهرستی از مسیرهای پوشه‌ها و فایل‌هایی است که وظیفه اسکن می‌کند. می‌توانید از موارد زیر استفاده کنید:

- متغیرهای محیطی (برای مثال، %systemroot%)
- علامت‌های * و ? برای پوشه‌ها، می‌توانید موارد زیر را انتخاب کنید:
- اسکن تمام محتویات، از جمله زیرپوشه‌ها
- اسکن فقط فایل‌های واقع در پوشه مشخص شده

علاوه بر فایل‌ها و دایرکتوری‌ها، می‌توان اشیاء اسکن زیر را مشخص کرد:

- ایمیل من - فایل‌های داده Outlook (.pst و .ost)
- حافظه هسته - حافظه هسته سیستم عامل

- فرآیندهای در حال اجرا و اشیاء Startup- فضای حافظه اختصاص داده شده برای فرآیندها و فایل‌های اجرایی برنامه‌هایی که با شروع سیستم عامل شروع می‌شوند
- سکتورهای بوت دیسک - سکتورهای بوت درایوهای ثابت و قابل جابجایی
- پشتیبان‌گیری سیستم - پوشه‌های اطلاعات حجم سیستم
- همه درایوهای قابل جابجایی - درایوهای قابل جابجایی که در حال حاضر به رایانه متصل هستند
- همه هارد دیسک‌ها - هارد دیسک‌های رایانه
- همه درایوهای شبکه—همه درایوهای شبکه متصل به رایانه

وظیفه ای ایجاد کنید که کل رایانه را هفتگی یا یک هفته در میان اسکن کند. اگر نمی‌توانید زمان بهینه برای چنین کاری پیدا کنید، حداقل نواحی بحرانی را اسکن کنید:

- حافظه هسته
- فرآیندهای در حال اجرا و اشیاء راه‌اندازی
- بخش‌های بوت دیسک
- \\.systemroot\.
- \\.systemroot%\system\.
- \\.systemroot%\system32\.
- \\.systemroot%\system32\drivers\.
- \\.systemroot%\syswow64\.
- \\.systemroot%\syswow64\drivers\.

حساب کاربری

به طور پیش‌فرض، وظایف اسکن در رایانه‌های کلاینت تحت حساب کاربری Local System آغاز می‌شوند. اگر محدوده اسکن شامل درایوهای شبکه یا سایر اشیاء با دسترسی محدود باشد، وظیفه قادر به اسکن آنها نخواهد بود. برای حل این مشکل، حسابی را مشخص کنید که دارای حقوق لازم در ویژگی‌های وظیفه باشد.

۲.۵ با نتایج false positive چه باید کرد؟

لیست برنامه مجاز :

اگر Kaspersky Endpoint Security تهدیدی را در فایل‌هایی که می‌دانید پاک است گزارش دهد، این یک false positive است.

false positive باعث کاهش بهره‌وری می‌شود. کسپرسکی امضاهای جدید را روی تعداد زیادی از فایل‌های سیستم عامل‌ها و نرم‌افزارهای محبوب به طور کامل آزمایش می‌کند تا از false positive جلوگیری کند. در طول اسکن، Kaspersky Endpoint Security فایل‌ها را با پایگاه داده نرم‌افزار معتبر که در شبکه امنیتی کسپرسکی ذخیره شده و بخشی از آن به صورت محلی دانلود شده است، بررسی می‌کند.

false positive نادر است. وقتی رخ می‌دهد، به احتمال زیاد علت آن برنامه‌ای است که ما از آن بی‌اطلاع هستیم، به عنوان مثال برنامه‌های داخلی.

اگر یک false positive رخ داد و شما ۱۰۰٪ مطمئن هستید که نرم‌افزار ایمن است، برای جلوگیری از خرابی، توصیه می‌کنیم ابتدا برنامه را به موارد استثنای اسکن اضافه کنید. در ادامه نحوه انجام این کار را بررسی خواهیم کرد. سپس با کسپرسکی تماس بگیرید تا در مورد false positive به ما اطلاع دهید تا بتوانیم سعی کنیم در آینده از این وضعیت جلوگیری کنیم.

کسپرسکی یک برنامه Allowlist ویژه برای این موارد دارد:

<https://www.kaspersky.com/partners/allowlist-program>

مشارکت در برنامه Allowlist به محصولات کسپرسکی کمک می‌کند تا هنگام اسکن نرم‌افزارهای داخلی، از تشخیص‌های false positive جلوگیری کنند.

هنگام توسعه نرم‌افزارهای سفارشی، اکیداً توصیه می‌کنیم که تمام نسخه‌های این نرم‌افزار را با امضای دیجیتال امضا کنید. در این صورت، اگر امضای دیجیتال تغییر نکرده باشد و کسپرسکی از قبل نرم‌افزار را ایمن و قابل اعتماد بداند، تقریباً هیچ شانس برای تشخیص false positive برای نسخه‌های امضا شده با certificate معتبر وجود ندارد، حتی اگر هنوز آخرین نسخه را به برنامه Allowlist ارسال نکرده باشید.

در صورت مشاهده هرگونه ناسازگاری بین نرم‌افزار شما و محصولات کسپرسکی، با پشتیبانی فنی تماس بگیرید و وضعیت را با جزئیات شرح دهید.

Allowlist program

<https://www.kaspersky.com/partners/allowlist-program>

ALLOWLIST PROGRAM

The Allowlist program lets you add legal software to the Kaspersky Allowlist system. Registration in the program is open to clients, vendors and software developers interested in proactively preventing false positives.

Program goals

- Reduce the number of false positives in Kaspersky products and lower the risk of incorrectly classifying participant software
- Significantly reduce the burden on participant and Kaspersky support teams
- Ensure the best possible user experience for Kaspersky products

Benefits

- Participation is free
- Unbiased third-party expert evaluation by Kaspersky
- Confirmed absence of false positives in current Kaspersky security solutions
- Participant support



22

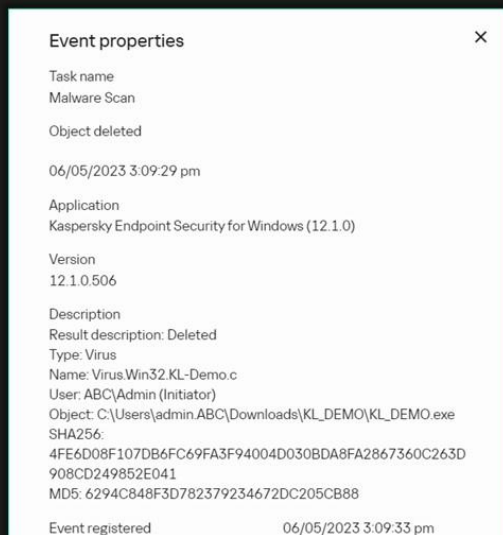
False positives in security applications installed on client computers may stop important production processes at the customer's site

To avoid this, we recommend customers inform Kaspersky about in-house software in advance

چگونه برای یک نتیجه false positive، استثنا ایجاد کنیم؟

How to create an exclusion for a false positive

23



Create an exclusion for the **specific file** and **specific threat name**

If the file name can vary, create an exclusion by **checksum**

Restore the file deleted by Kaspersky Endpoint Security from **backup**

شما می‌توانید یک استثنا را برای یک فایل خاص و برای یک تهدید خاص پیکربندی کنید. می‌توانید بر اساس نام تهدید، یک استثنا برای تهدید ایجاد کنید.

یک استثنا برای فایل می‌تواند بر اساس موارد زیر ایجاد شود:

- Name -
- Checksum -
- Certificate -

استثناها برای تهدیدها

اگر File Threat Protection یا یک وظیفه اسکن بدافزار، تهدیدی را در یک فایل سالم پیدا کرد، برای آن یک استثنا ایجاد کنید:

۱. تنظیمات منطقه مورد اعتماد را در سیاست امنیتی Kaspersky Endpoint باز کنید: تنظیمات برنامه | تنظیمات عمومی | استثناها و انواع اشیاء شناسایی شده.

۲. فایل دارای false positive را به لیست استثناهای اسکن اضافه کنید. فایل یا پوشه را انتخاب کنید. مسیر کامل فایل را مشخص کنید. از متغیرهای محیطی، به عنوان مثال، %ProgramFiles% استفاده کنید.

(ایجاد یک استثنا برای یک تهدید خاص که به اشتباه توسط Kaspersky Endpoint Security شناسایی شده است، امن تر از حذف کامل فایل است. برای انجام این کار:)

۳. در پنجره‌ی استثنا، کادر انتخاب نام شیء (Object name) را انتخاب کنید. نام تهدید را مشخص کنید. می‌توانید نام تهدید را در توضیحات رویداد تشخیص تهدید ایجاد شده توسط Kaspersky Endpoint Security پیدا کنید.

Create an exclusion for the threat

24

You can find the names of the file and threat in the respective event

Exclusion

☐ File or folder

☒ Including subfolders

☒ Object name

VirusWin32.KI-Demo.c

☐ Object hash

Add hash from file

Select

Add hash from events

Select

Add hash manually

Comment

Protection components

☒ Any

☐ From list

استثنائات بر اساس checksum :

Create an exclusion by checksum

25

Import or copy the checksum from an event

Exclusion

☐ File or folder

☒ Including subfolders

☐ Object name

☒ Object hash

Add hash from file

Select

Add hash from events

Select

Add hash manually

4FE6D08F107DB6FC69FA3F94004D030BDA8FA2867360C263

Comment

Events list

Filter

Time	Object type	Hash
6/5/2023, 3:09:15 PM	Virus.Win32.KI-Demo.c	4FE6D08F107DB6FC69FA3F94004D030BDA8FA2867360C263D908CD249852E041

اگر فایلی که نیاز به پیکربندی استثنا برای آن دارید، در دایرکتوری‌های مختلف روی رایانه‌های مختلف نصب شده باشد، چه باید کرد؟

اگر نسخه فایل یکسانی در همه رایانه‌ها استفاده می‌شود، از چک‌سام فایل استفاده کنید:

۱. تنظیمات منطقه مورد اعتماد را در خط‌مشی امنیتی کسپرسکی اندپوینت باز کنید: تنظیمات برنامه | تنظیمات عمومی | استثناها و انواع اشیاء شناسایی شده.

۲. فایلی که نتیجه‌ی false positive دارد را به لیست استثنائات اضافه کنید. کادر انتخاب Object hash را انتخاب کنید. checksum فایل را مشخص کنید. می‌توانید checksum فایل را محاسبه کرده و آن را به صورت دستی اضافه کنید، یا آن را از یک رویداد تشخیص کپی کنید.

Kaspersky Endpoint Securitychecksum فایل‌های اسکن شده را محاسبه کرده و آنها را در رویدادهای تشخیص نمایش می‌دهد.

استثناء بر اساس certificate :

Create an exclusion using a certificate

26

Enable the option
Use trusted system certificate store

Select the **store** to be trusted
by Kaspersky Endpoint Security

Exclusions and types of detected objects

Trusted system certificate store

☒ Use trusted system certificate store

Enterprise Trust

Certificate store

Name

- ☐ Trusted Root Certification Authorities
- ☒ Enterprise Trust
- ☐ Intermediate Certification Authorities
- ☐ Trusted Publishers
- ☐ NTAuth

اگر یک استثنا را پیکربندی کرده‌اید، اما نسخه جدیدی از برنامه با یک پوشه و فایل اجرایی جدید منتشر شده است و نسخه جدید نیز یک مثبت کاذب دریافت می‌کند، چه باید کرد؟

اگر نام فایل‌ها مشابه هستند، از یک ماسک مسیر استفاده کنید. در یک ماسک، علامت ستاره "*" به معنای یک توالی دلخواه از نمادها و علامت سوال "?" به معنای یک نماد دلخواه است. به عنوان مثال، ماسک file*.exe با تمام فایل‌هایی که نام آنها با "file" شروع می‌شود و پسوند exe دارند، مطابقت دارد.

اگر نام فایل‌ها کاملاً متفاوت است، اما همه فایل‌ها توسط certificate ها امضا شده‌اند، certificate ها را در فروشگاه certificate در رایانه‌هایی که برنامه در آنها استفاده می‌شود قرار دهید و Kaspersky Endpoint Security را برای اعتماد به این certificate ها پیکربندی کنید:

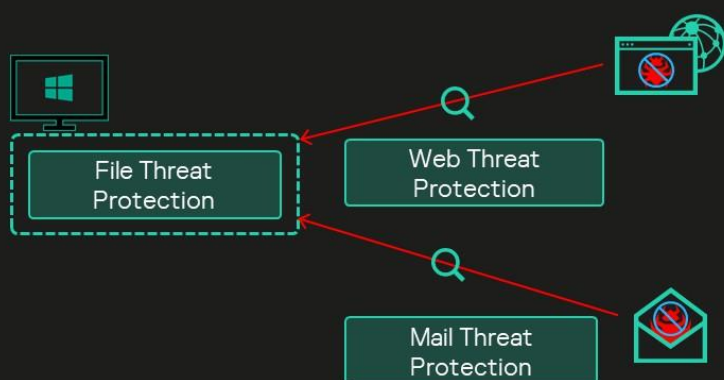
۱. تنظیمات منطقه مورد اعتماد را در سیاست Kaspersky Endpoint Security باز کنید: تنظیمات برنامه | تنظیمات عمومی | موارد استثنا و انواع اشیاء شناسایی شده.
۲. پارامتر استفاده از فروشگاه certificate سیستم مورد اعتماد را فعال کنید و یکی از انبارهای certificate موجود را انتخاب کنید. انتخاب پیش‌فرض Enterprise Trust است.
۳. certificate (های) مورد استفاده برای امضای فایل‌های برنامه را در محل انتخاب‌شده روی رایانه کلاینت قرار دهید. برای این کار، می‌توانید مثلاً از سیاست‌های گروهی Active Directory استفاده کنید.

هر رایانه دارای محل‌های نگهداری certificate کاربر و محل نگهداری certificate رایانه است. Kaspersky Endpoint Security فقط به certificate های موجود در محل نگهداری certificate رایانه اعتماد می‌کند.

برای نرم‌افزارهای داخلی، می‌توانید حتی از self-signed certificates استفاده کنید.

۳. نحوه پیکربندی محافظت در برابر تهدیدات شبکه (Network Threat) :

- ۳.۱ نحوه عملکرد حفاظت از شبکه
اجزای شبکه چه کاری انجام می‌دهند؟

**Mail Threat Protection**

- Deletes malicious code from email messages and attachments
- Renames potentially dangerous attachments

Web Threat Protection

- Blocks attempts to download malicious files
- Blocks visits to malicious and phishing websites

Together:

- Conserve computer resources because scanning a file on the drive takes longer than scanning a file in memory
- Protect against phishing

شبکه یکی از راه‌های اصلی انتشار بدافزار است. به همین دلیل است که محافظت از شبکه و اسکن ترافیک شبکه برای امنیت رایانه بسیار مهم هستند. در کسپرسکی اندپوینت سکیوریتی، اجزای محافظت در برابر تهدید ایمیل و محافظت در برابر تهدید وب مسئول اسکن ضد بدافزار ترافیک شبکه هستند:

Mail Threat Protection	- کد مخرب را از پیام‌های ایمیل و پیوست‌ها حذف می‌کند. - پیوست‌های بالقوه خطرناک را تغییر نام می‌دهد.
Web Threat Protection	- تلاش برای دانلود فایل‌های مخرب را مسدود می‌کند. - اجازه بازدید از وبسایت‌های مخرب و فیشینگ را نمی‌دهد.

چگونه Kaspersky Endpoint Security ترافیک را رهگیری می‌کند ؟

Kaspersky Endpoint Security با استفاده از یک فیلتر NDIS ترافیک شبکه را رهگیری می‌کند. درایور، اتصالات خروجی از برنامه‌های کامپیوتری را رهگیری کرده و بسته‌ها را به اجزای حفاظت شبکه منتقل می‌کند. Kaspersky Endpoint Security پروتکل اتصال را شناسایی کرده و بسته‌ها را به جزء مناسب منتقل می‌کند:

HTTP, HTTPS, FTP	Web Threat Protection, Web Control
SMTP, POP3, POP3S, IMAP, NNTP	Mail Threat Protection

بسته‌های دیگر مستقیماً به برنامه‌ها و کاربردهایی که برای آنها در نظر گرفته شده‌اند، ارسال می‌شوند.

Kaspersky Endpoint Security ترافیک برنامه‌های مورد اعتماد را رهگیری نمی‌کند، که می‌توانید این مورد را در پالیسی، در تنظیمات برنامه | حفاظت ضروری در برابر تهدید | موارد استثنا و انواع اشیاء شناسایی شده | برنامه‌های مورد اعتماد یا در تنظیمات برنامه | تنظیمات عمومی | تنظیمات شبکه | برنامه‌های مورد اعتماد پیکربندی کنید.

Kaspersky Endpoint Security می‌تواند اتصالات امن (SSL/TLS) را اسکن کند.

The image shows two screenshots from the Kaspersky Endpoint Security interface. The top screenshot is titled 'Configure the list of ports to control' and shows the 'Application settings' tab with 'Network Settings' highlighted. The bottom screenshot shows the 'Network settings' window with 'Monitored ports' set to 'Monitor selected network ports only' and '39 ports selected' indicated. A red arrow points from the 'Network Settings' in the top screenshot to the 'Network ports' window in the bottom screenshot. To the right, a table lists network ports and their status.

	Description	Port	Status
☐	FTP	20	Enabled
☐	FTP	21	Enabled
☐	SMTP	25	Enabled
☐	HTTP	80	Enabled
☐	HTTP	81	Enabled
☐	HTTP	82	Enabled
☐	HTTP	83	Enabled
☐	POP3	110	Enabled
☐	IRC	113	Enabled

Kaspersky Endpoint Security can control:

- All ports
- Selected ports only

Kaspersky Endpoint Security می‌تواند فقط اتصالات به پورت‌های مشخص شده را رهگیری کند، نه همه اتصالات خروجی را. برای پیکربندی این مورد، در سیاست کسپرسکی اندپوینت سکیوریتی، تنظیمات برنامه | تنظیمات عمومی | تنظیمات شبکه را باز کنید و در قسمت پورت‌های مانیتور شده، فقط پورت‌های شبکه انتخاب شده را مانیتور کنید. روی لینک ۳۹ پورت انتخاب شده کلیک کنید و پورت‌هایی را که قرار است مانیتور شوند، مشخص کنید.

اگر نمی‌دانید کدام پورت‌های خاص توسط یک برنامه استفاده می‌شوند، یکی از موارد زیر را انجام دهید:

- گزینه **Monitor all network ports** را فعال کنید.

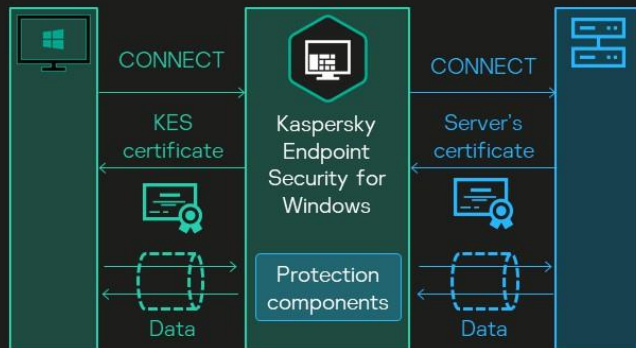
- روی لینک **applications selected** کلیک کنید و مسیر فایل اجرایی برنامه را به لیست اضافه کنید.

پورت‌ها و برنامه‌های استاندارد در فهرست پورت‌های تحت نظارت مشخص شده‌اند. در صورت استفاده از پورت‌ها یا برنامه‌های غیر استاندارد، آنها را به فهرست اضافه کنید.

چگونه Kaspersky Endpoint Security ترافیک رمزگذاری شده را اسکن می‌کند؟

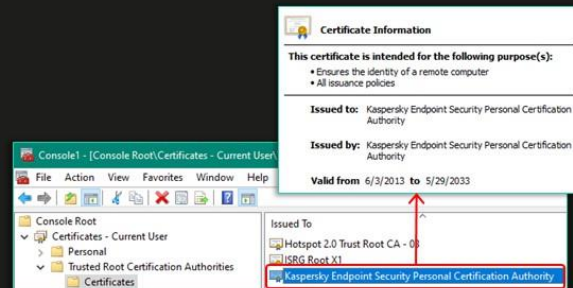
How Kaspersky Endpoint Security scans encrypted traffic

32



KES **replaces** the certificate to scan encrypted traffic

KES creates a certificate during the installation and places it in the local **Trusted Root Certification Authorities** store



At each start, KES checks whether the certificate is still there, and if it's not, **restores** it

The following components can scan encrypted traffic:

- Web Threat Protection
- Web Control
- Mail Threat Protection

در طول نصب، Kaspersky Endpoint Security یک گواهی خودامضا - گواهی ریشه شخصی Kaspersky Endpoint Security - ایجاد می‌کند و آن را در مخزن محلی مراجع صدور گواهی معتبر ریشه ذخیره می‌کند. در هر بار شروع، KES بررسی می‌کند که آیا گواهی هنوز وجود دارد یا خیر. در غیر این صورت، آن را بازیابی می‌کند. برای اسکن ترافیک رمزگذاری شده (SSL/TLS)، Kaspersky Endpoint Security گواهی را جایگزین می‌کند. کسپرسکی اندپوینت سکیوریتی:

۱. اتصال خروجی از برنامه به سرور را قطع می‌کند.
۲. گواهی سرور را دریافت می‌کند.
۳. یک گواهی جلسه معادل امضا شده توسط گواهی ریشه شخصی Kaspersky Endpoint Security تولید می‌کند.
۴. گواهی تولید شده را به برنامه کلاینت برمی‌گرداند.

این به Kaspersky Endpoint Security اجازه می‌دهد تا کلید رمزگذاری متقارن را قطع کرده و کل جلسه ارتباط را رمزگشایی کند.

مرورگر وب هیچ هشداري نشان نمی‌دهد زیرا گواهی ریشه شخصی Kaspersky Endpoint Security در مخزن گواهی معتبر قرار دارد.

اسکن ترافیک رمزگذاری شده به طور پیش فرض فعال است و مربوط به اجزای زیر است:

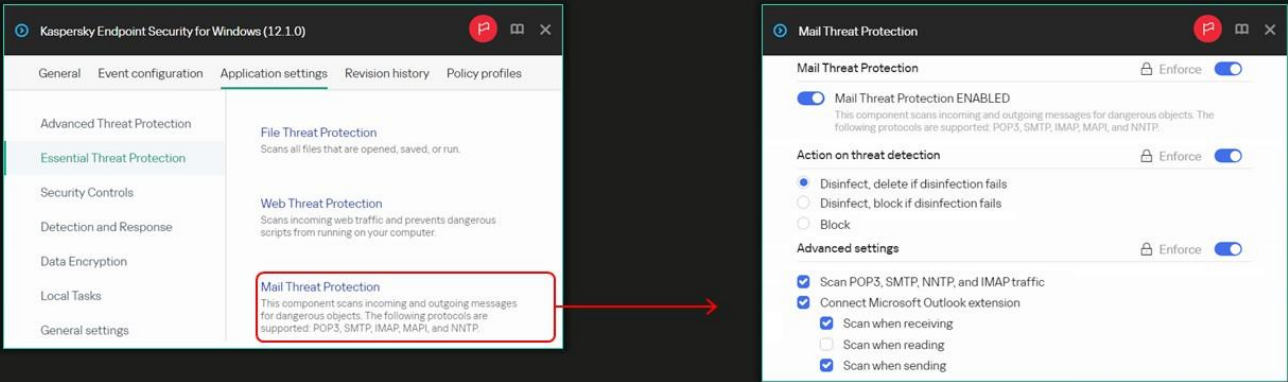
- Web Threat Protection
- Mail Threat Protection
- Web Control

۳.۲ محافظت در برابر تهدیدات ایمیل (Mail Threat Protection) :

محافظت در برابر تهدید ایمیل چه کاری انجام می دهد؟

What Mail Threat Protection does

38



Scans the user's incoming and outgoing email messages:

- Sent over SMTP, POP3, IMAP4, NNTP
- In the Microsoft Outlook mail client

Does not scan web mail messages that the user receives via a web browser

محافظت در برابر تهدیدات ایمیل، از شما در برابر تهدیدات ایمیل محافظت می کند. پیام ها در سطح پروتکل (SMTP، POP3،

IMAP و NNTP) و با جاسازی در Microsoft Office Outlook (MAPI) رهگیری می شوند.

محافظت در برابر تهدیدات ایمیل، بدافزارها را با استفاده از امضاهای بدافزار، تجزیه و تحلیل اکتشافی و شبکه امنیتی کسپرسکی شناسایی و حذف می کند.

علاوه بر این، محافظت در برابر تهدیدات ایمیل می تواند پیوست های ایمیل را مسدود یا تغییر نام دهد. می توانید لیستی از ماسک ها را برای فایل هایی که این مؤلفه باید تغییر نام دهد یا از پیوست ها حذف کند، پیکربندی کنید.

محافظت در برابر تهدیدات ایمیل، موضوع پیام های آلوده را تغییر می دهد. اقدام انجام شده در موضوع پیام توضیح داده شده است.

پیکربندی Mail Threat Protection :

محدوده محافظت :

محافظت در برابر تهدید ایمیل می تواند موارد زیر را اسکن کند:

- پیام های ورودی و خروجی
- فقط پیام های ورودی

برای اطمینان از حداقل محافظت از رایانه، می توانید فقط پیام های ورودی را اسکن کنید. اسکن پیام های خروجی می تواند از ارسال ناخواسته یک فایل آلوده بایگانی شده جلوگیری کند و از شرمساری جلوگیری کند. همچنین می توانید اگر می خواهید انواع خاصی از پیوست ها، مانند موسیقی یا ویدیو را مسدود کنید، اسکن پیام های خروجی را انتخاب کنید. به طور پیش فرض، پیام های ورودی و خروجی اسکن می شوند. شما می توانید محدوده حفاظت را فقط در کنسول مدیریت MMC تغییر دهید.

اتصال :

تنظیمات پیشرفته، محدوده حفاظت را دقیق تر تعریف می کنند:

- اسکن ترافیک POP3، SMTP، NNTP و IMAP - اسکن ایمیل ها و پیام های خبری منتقل شده از طریق پروتکل های مشخص شده را فعال می کند.

(اسکن در سطح پروتکل به کلاینت های ایمیل مورد استفاده بستگی ندارد.

با این حال، اگر به عنوان مثال از سرورهای Microsoft Exchange یا Lotus Notes استفاده کنید، پیام ها از طریق پروتکل های ارسال می شوند که Kaspersky Endpoint Security از آنها پشتیبانی نمی کند. در این حالت، Mail Threat Protection قادر به اسکن پیام ها نخواهد بود.)

- اتصال به افزونه Microsoft Office Outlook - اشیاء را هنگام دریافت، خواندن و ارسال در سطح کلاینت Microsoft Office Outlook اسکن کنید.

(در مقابل، اسکن در سطح کلاینت ایمیل صرف نظر از نحوه دریافت پیام انجام می شود.)

روش های اسکن :

این تنظیمات مربوط به فایل های ترکیبی پیوست شده است.

- اگر آرشیوها پیوست باشند، می توان آن ها را از حالت فشرده خارج و اسکن کرد. این رفتار با تنظیمات زیر کنترل می شود:
- اسکن آرشیوهای پیوست شده - این تنظیم به مدیر اجازه می دهد تا اسکن آرشیو را به طور کامل غیرفعال کند.

توصیه می‌کنیم این کادر انتخاب را علامت بزنید تا محافظت در برابر تهدید ایمیل، آرشیوها را «در حال اجرا» اسکن کند. جلوگیری از ورود یک آرشیو آلوده به پایگاه داده ایمیل بسیار آسان‌تر از حذف آن از پایگاه داده در آینده با استفاده از یک وظیفه اسکن بدافزار است.

- اسکن فایل‌های پیوست‌شده با فرمت‌های آفیس

(شما می‌توانید این تنظیمات را فقط در کنسول مدیریت MMC غیرفعال کنید. این تنظیمات را خاموش نکنید. فایل‌های مخرب اغلب در آرشیوهای پیوست‌شده و اسناد آفیس پخش می‌شوند.)

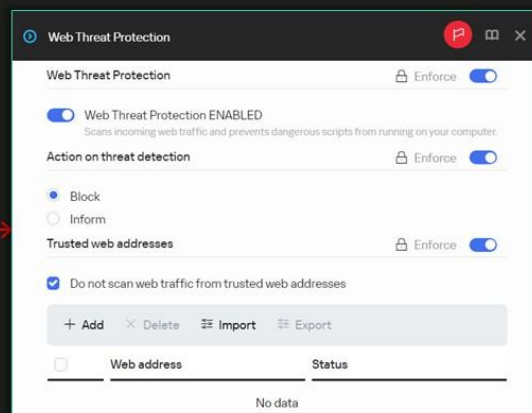
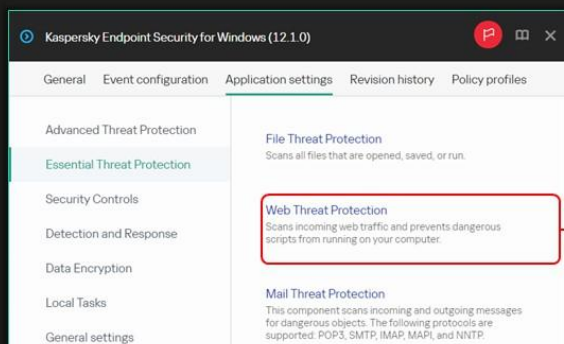
- آرشیوهای بزرگتر از NN مگابایت را اسکن نکنید - اندازه آرشیوها یا فایل‌های آفیس را برای اسکن محدود می‌کند. بدافزار به ندرت در فایل‌های بزرگ پخش می‌شود. این محدودیت را فعال کنید تا از انتظار طولانی هنگام دریافت فایل‌های ترکیبی بزرگ جلوگیری شود.

- زمان بررسی بایگانی‌ها را به NN ثانیه محدود کنید - این گزینه محافظت در برابر «بمب‌های بایگانی» را که اسکن آنها به زمان بسیار طولانی و منابع زیادی نیاز دارد و باعث کندی کامپیوتر می‌شود، پیاده‌سازی می‌کند.

۳.۳ محافظت در برابر تهدیدات وب (Web Threat Protection) :

What Web Threat Protection does

40



Scans data in HTTP, HTTPS and FTP protocols

Protects against known threats: Blocks malicious files, including archived

Blocks phishing websites

Blocks malicious websites and thus protects against unknown threats

مؤلفه حفاظت در برابر تهدیدات وب دو عملکرد مهم را انجام می‌دهد:

- آدرس صفحات وب باز شده توسط کاربر یا برنامه‌ها را تجزیه و تحلیل می‌کند و دسترسی به وبسایت‌های فیشینگ و وبسایت‌های بالقوه مضر را مسدود می‌کند.
- اشیاء دانلود شده از طریق پروتکل‌های HTTP، HTTPS و FTP را اسکن کرده و فایل‌های مخرب را مسدود می‌کند.

این مؤلفه هنگام اسکن لینک‌ها از چهار فناوری استفاده می‌کند:

- بررسی در برابر پایگاه داده آدرس‌های وب مخرب - آدرس وبسایتی که قرار است باز شود را با آدرس وبسایت‌هایی که به دلیل میزبانی بدافزار، حمله به رایانه‌ها یا سایر فعالیت‌های مضر شناخته شده‌اند، مقایسه می‌کند.
 - بررسی در برابر پایگاه داده آدرس‌های وب فیشینگ - مشابه بررسی قبلی، اما بررسی در برابر پایگاه داده سایت‌هایی که صفحات فیشینگ در آنها شناسایی شده است.
 - تجزیه و تحلیل اکتشافی برای تشخیص لینک‌های فیشینگ - محتوای سایت را برای کد HTML مشخصه فیشینگ تجزیه و تحلیل می‌کند.
 - بررسی KSN - این مؤلفه آدرس سایت‌های باز شده را به KSN ارسال می‌کند. لینک‌های خطرناک مسدود می‌شوند. پاسخ در حافظه پنهان محلی ذخیره شده و برای بررسی‌های بیشتر استفاده می‌شود.
- محافظت در برابر تهدیدات وب، فایل‌های دانلود شده را با استفاده از تمام روش‌های موجود اسکن می‌کند: تحلیل امضا و اکتشافی، و همچنین KSN.

پیکربندی محافظت در برابر تهدیدات وب (Web Threat Protection) :

اقدامات :

شما می‌توانید اقدامی را که محافظت در برابر تهدیدات وب در مورد تمام اشیاء خطرناک شناسایی شده انجام می‌دهد، پیکربندی کنید:

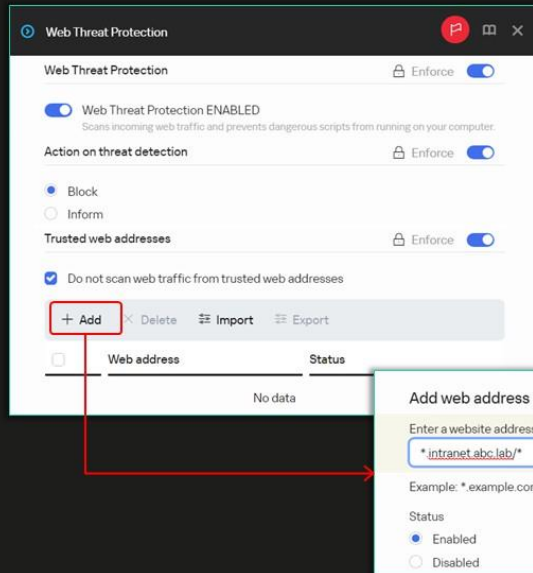
- مسدود کردن (Block)
- اطلاع‌رسانی (Inform)

توصیه می‌کنیم اقدام مسدود کردن را در پالیسی انتخاب کرده و آن را قفل کنید تا از دانلود اشیاء خطرناک یا بازدید از وبسایت‌های خطرناک توسط کاربران جلوگیری شود.

هنگامی که کاربر سعی می‌کند یک وبسایت ممنوعه را باز کند یا یک شیء آلوده را دانلود کند، مرورگر اعلانی را نمایش می‌دهد که توضیح می‌دهد Kaspersky Endpoint Security این تلاش را مسدود کرده است.

How to make a website trusted

41



Add the URL mask to the list of **trusted websites** in the Web Threat Protection settings

Use the ***** and **?** wildcards

Web Threat Protection ignores all threats in the traffic of trusted websites:

- Malicious files
- Malicious pages
- Phishing pages

اگر Web Threat Protection به اشتباه یک وبسایت را مخرب یا فیشینگ تشخیص داد، آدرس آن را به لیست Trust اضافه کنید:

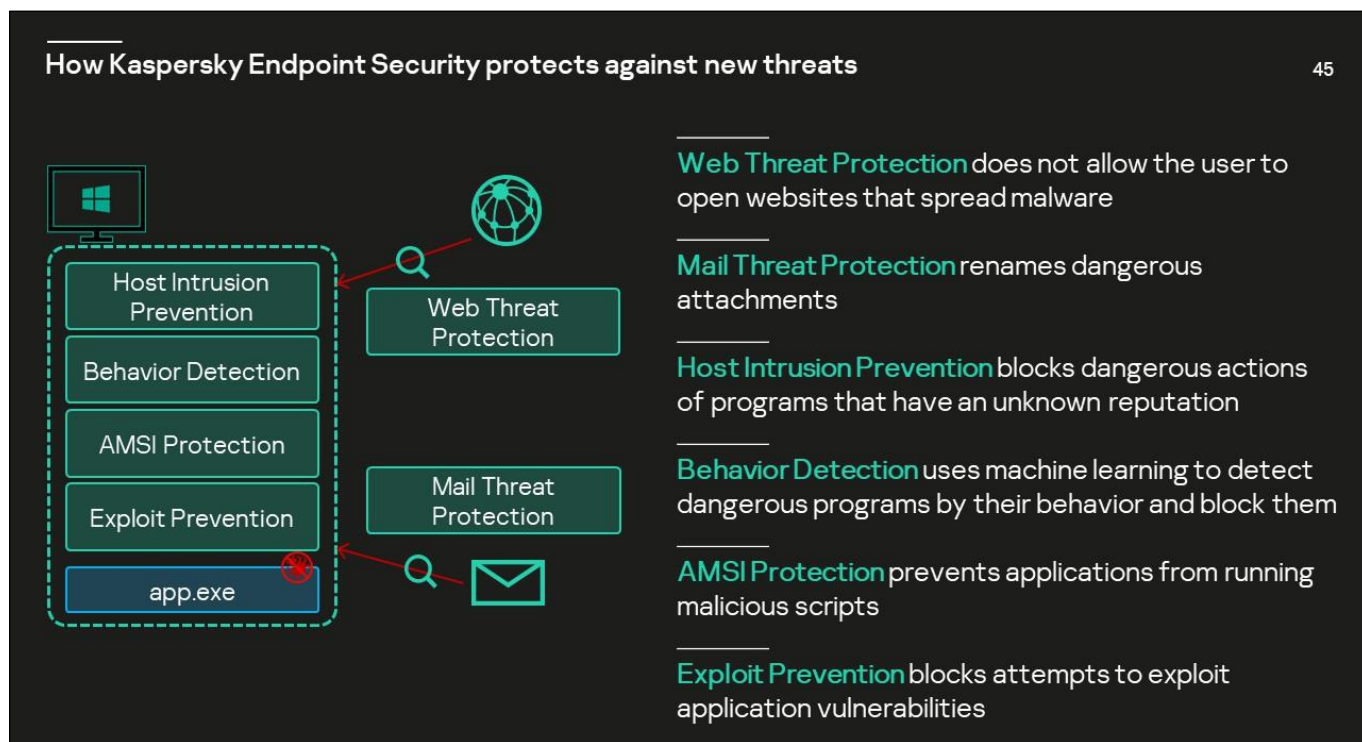
۱. در بخش Web Threat Protection، Essential threat protection را باز کنید.
 ۲. کادر انتخاب Do not scan web traffic from trusted web addresses را انتخاب کنید.
 ۳. آدرس وبسایت را به لیست اضافه کنید. برای تعیین ماسک، از کاراکترهای «*» و «?» استفاده کنید.
- Web Threat Protection نه این آدرس‌ها را بررسی می‌کند و نه فایل‌های دانلود شده از آنها را اسکن می‌کند.

اگر محافظت در برابر تهدیدات وب به اشتباه فایلی را که کاربر از یک وبسایت دانلود می‌کند، مخرب تشخیص دهد:

۱. در تنظیمات برنامه | تنظیمات عمومی | استثنائات و انواع اشیاء شناسایی شده، برای فایل استثنا ایجاد کنید.
۲. این استثنا را حداقل برای محافظت در برابر تهدیدات وب، محافظت در برابر تهدیدات فایل و اسکن بدافزار اعمال کنید.

۴. نحوه پیکربندی محافظت در برابر تهدیدات پیچیده:

۴.۱ چگونه Kaspersky Endpoint Security در برابر تهدیدات جدید محافظت می کند؟



مجرمان دائماً فایل های مخرب جدیدی ایجاد می کنند. کسپرسکی خیلی سریع تهدیدات جدید را شناسایی کرده و امضاهای آنها را به پایگاه داده اضافه می کند. چک سام های فایل های مخرب حتی سریع تر به شبکه امنیتی کسپرسکی می رسند. با این حال، مجرمان هنوز نیم قدم جلوتر هستند.

(طبق بولتن امنیتی کسپرسکی ۲۰۲۲، متخصصان کسپرسکی بیش از ۲۳۸۰۷ تغییر باج افزار و ۴۱ خانواده جدید را شناسایی کردند. طبق داده های شبکه امنیتی کسپرسکی، تروجان های باج افزار به ۲۷۱،۲۱۵ کاربر منحصر به فرد حمله کردند. تروجان های باج افزار اسناد را رمزگذاری می کنند و برای رمز عبور رمزگشایی درخواست پول می کنند. این نوع بدافزار خسارت مستقیم و بسیار پرهزینه ای به یک شرکت وارد می کند.)

۴.۲ فناوری‌های تشخیص مورد استفاده در Kaspersky Endpoint Security

اجزای Kaspersky Endpoint Security با استفاده از موتور آنتی‌ویروس، اطلاعات KSN و فناوری‌های مختلف، اشیاء را اسکن می‌کنند.

برخی از فناوری‌های تشخیص در سمت کلاینت، یعنی در موتور، و برخی دیگر در سمت کسپرسکی پیاده‌سازی شده‌اند.

فناوری‌های پیاده‌سازی شده در سمت کلاینت:

- تحلیل Signature
- تحلیل Heuristic
- تحلیل Behavior

فناوری‌های پیاده‌سازی شده در سمت کسپرسکی:

- تحلیل تخصصی
- یادگیری ماشین
- سرویس اعتبار

Threat detection technologies

46

The screenshot displays the Kaspersky Endpoint Security interface. On the left, a sidebar shows navigation options: Monitoring, Security, Update, Tasks, and License. The main area is titled 'Threat detection technologies' and lists several detection methods: Expert analysis (1,068), Cloud analysis (144), Behavior analysis (2), Automatic analysis (11), and Machine learning (242). Each method includes a brief description of how threats are detected. On the right, an 'Event properties' window is open, showing details for a 'Web Threat Protection' event. The event type is 'Dangerous link blocked', occurring on 05/15/2023 at 10:28:04 am on the desktop 'ALEX-DESKTOP'. The application is 'Kaspersky Endpoint Security for Windows (12.1.0)'. The event description states: 'Name: chrome.exe, Application path: C:\Program Files\Google\Chrome\Application, Process ID: 3660, User: ABC\alex (Initiator), Component: Web Threat Protection, Result description: Blocked, Type: Malicious link, Name: https://www.kaspersky.com/test/wmuf, Threat level: Exactly, Precision: High, Object type: Web page, Path to object: https://www.kaspersky.com/test, Object name: wmuf, Reason: Automatic analysis'.

KES uses the anti-malware engine, information from KSN and other detection technologies for scanning

KES logs which technology and which component detected a threat

فناوری‌های پیاده‌سازی‌شده در سمت کسپرسکی، فقط نتایج عملیاتی خود را به KES ارسال می‌کنند. برای مثال:

- به‌روزرسانی‌های امضا
- اعتبار برنامه
- الگوهای رفتار خطرناک
- مدل‌های یادگیری ماشین

نام مؤلفه و فناوری مورد استفاده برای یافتن تهدید در رویداد تشخیص نمایش داده می‌شوند.

در رابط محلی Kaspersky Endpoint Security، فناوری‌های تشخیص، منبعی را که از آن اطلاعات مربوط به تهدید را دریافت کرده‌اند، نمایش می‌دهند:

- تحلیل خودکار - داده‌های مربوط به تهدید از سیستم تحلیل خودکار شیء آمده است. سیستم تحلیل خودکار تمام اشیایی را که کسپرسکی دریافت می‌کند، پردازش می‌کند، به آنها اعتبار می‌دهد و امضا تولید می‌کند. اگر سیستم نتواند یک شیء را پردازش کند، آن را برای تحلیلگران ویروس ارسال می‌کند.
- تحلیل تخصصی - داده‌های مربوط به تهدید از تحلیلگران ویروس کسپرسکی آمده است. تحلیلگران ویروس، امضاهای تهدید، الگوهای فعالیت خطرناک، مدل‌های یادگیری ماشین و غیره را توسعه می‌دهند.
- تحلیل رفتار - داده‌های مربوط به تهدید از تحلیل رفتار شیء آمده است.
- تحلیل ابری - داده‌های مربوط به تهدید از فناوری Astraea آمده است. Astraea بخشی از KSN است. این سیستم، کلان‌داده‌ها را پردازش می‌کند: داده‌ها را از تمام منابع درخواست‌های KSN دریافت می‌کند، تجزیه و تحلیل می‌کند، بر اساس اهمیت آنها را مرتب می‌کند و تهدید را ارزیابی می‌کند.
- یادگیری ماشین - داده‌های مربوط به تهدید از یک مدل یادگیری ماشینی حاصل می‌شود. کسپرسکی مدل‌های یادگیری ماشینی را توسعه می‌دهد که سپس بر روی مجموعه‌ای بزرگ از داده‌های دریافتی از KSN و سیستم Astraea یادگیری انجام می‌دهند. Kaspersky Endpoint Security از مدل‌های آموزش‌دیده به موازات سایر فناوری‌های تشخیص استفاده می‌کند.

کسپرسکی به طور مداوم مدل‌های خود را بهبود می‌بخشد و آموزش می‌دهد. به‌روزرسانی‌های مدل یادگیری ماشینی به صورت دوره‌ای همراه با پایگاه‌های داده امضا به KES ارائه می‌شوند.

۴.۳ محافظت پیشرفته در برابر تهدیدات چه کاری انجام می‌دهد :

محافظت پیشرفته در برابر تهدیدات شامل اجزا و فناوری‌هایی است که از آلودگی توسط بدافزارهای جدید جلوگیری می‌کند یا حداقل تأثیر آنها را به حداقل می‌رساند. منظور ما از «بدافزار جدید»، برنامه‌هایی است که هنوز به پایگاه‌های داده امضای ما اضافه نشده‌اند.

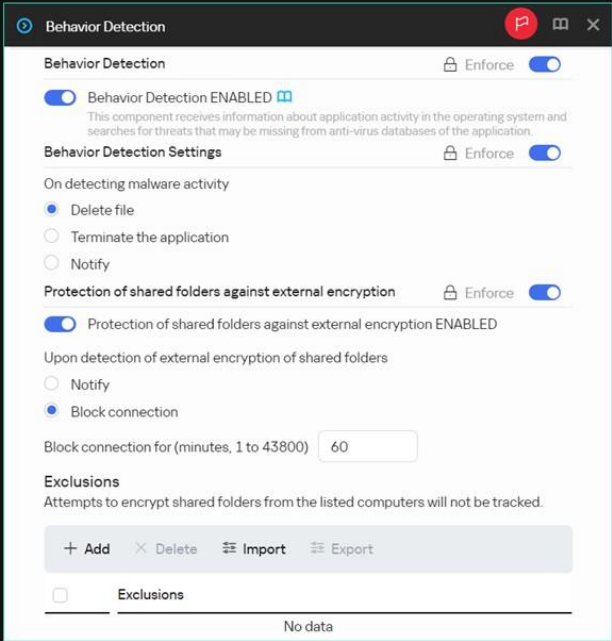
ما قبلاً تجزیه و تحلیل اکتشافی را که مربوط به محافظت پیشرفته در برابر تهدیدات است، بررسی کرده‌ایم. با این حال، نقش اصلی در این جنبه از محافظت متعلق به موارد زیر است:

- Behavior Detection
- Exploit Prevention
- Remediation Engine
- Host Intrusion Prevention
- Control components and Firewall

چگونه Behavior Detection در برابر تهدیدات جدید محافظت می‌کند ؟

How Behavior Detection protects against new threats

47



Logs what programs do:

- Which files they open
- Which connections are established
- Which system functions are used

Compares these activities with dangerous activity patterns (BSS, behavior stream signatures)

Stops dangerous programs and rolls back their actions

Protects against ransomware:

- Detects malicious encryption attempts (local and remote)
- Blocks the attacking computer to prevent it from modifying files in shared folders (for 60 minutes by default)

Behavior Detection چندین عملکرد انجام می‌دهد:

- ثبت فعالیت‌های برنامه برای مقایسه با پایگاه داده امضای رفتار
- شناسایی بدافزار و مسدود کردن اقدامات آن
- محافظت از پوشه‌های اشتراکی در برابر رمزگذاری خارجی

تشخیص بدافزار وظیفه اصلی است. برای این منظور، تشخیص رفتار، اقدامات برنامه را رصد می‌کند و آنها را با الگوهای فعالیت خطرناک مقایسه می‌کند.

پایگاه داده الگوها قابل به‌روزرسانی است، اما این به‌روزرسانی‌ها به ندرت منتشر می‌شوند. اثربخشی Behavior Detection به ندرت به تعداد دفعات به‌روزرسانی پایگاه داده بستگی دارد.

تنظیمات:

Behavior Detection تنظیمات نسبتاً کمی دارد. اساساً، می‌توانید این مؤلفه را به طور کامل فعال یا غیرفعال کنید، یا فقط محافظت از پوشه‌های مشترک در برابر رمزگذاری خارجی را فعال یا غیرفعال کنید.

اقدامات:

اگر Behavior Detection رفتار مخربی را تشخیص دهد، برنامه‌ی بدرفتار را متوقف می‌کند، فایل اجرایی آن را حذف می‌کند و آن را به پشتیبان‌گیری منتقل می‌کند.

سایر اقدامات ممکن:

- اطلاع رسانی (Notify) - هیچ کاری انجام نمی‌دهد، فقط تشخیص فعالیت مخرب را ثبت می‌کند.
- خاتمه دادن به برنامه (Terminate the program) - بدافزار را متوقف کرده و آن را از حافظه تخلیه می‌کند.
- حذف فایل (Delete file) - برنامه را متوقف می‌کند، فایل مخرب را حذف می‌کند و یک کپی از آن را در پشتیبان‌گیری قرار می‌دهد.

اگر محافظت از پوشه‌های مشترک در برابر رمزگذاری خارجی تلاشی برای رمزگذاری فایل‌ها در یک پوشه مشترک از طریق شبکه تشخیص دهد، عملیات نوشتن و حذف را برای این جلسه به مدت ۶۰ دقیقه مسدود می‌کند. سپس سعی می‌کند نسخه‌های فایل رمزگذاری نشده را از یک کپی پشتیبان با استفاده از مؤلفه موتور اصلاح بازیابی کند.

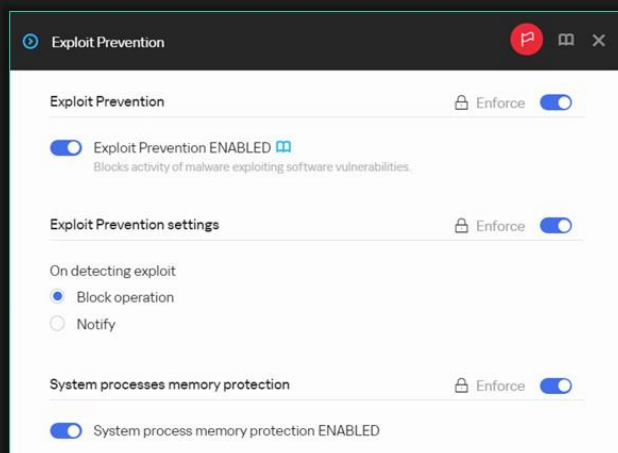
Behavior Detection را غیرفعال نکنید. این ویژگی از شما در برابر تهدیداتی محافظت می‌کند که سایر اجزا ممکن است در مقابله با آنها شکست بخورند.

برای جلوگیری از مثبت‌های کاذب یا بهبود عملکرد، exclusion ایجاد کنید.

چگونه پیشگیری از سوءاستفاده به مقابله با تهدیدات جدید کمک می‌کند؟

How Exploit Prevention protects against new threats

48



Protects against exploits:

- Applies technologies that decrease the risk of vulnerability exploitation to user and system processes
- Additionally monitors vulnerable applications (browsers, Java, Adobe Reader, etc.) to prevent them from creating suspicious child processes

Exploit Prevention، از حملات سوءاستفاده مختلفی که هدفشان کسب مجوزهای مدیریتی در سیستم یا پنهان کردن اجرای کد است، محافظت می‌کند.

به عنوان مثال، مجرمان از سوءاستفاده‌ها (exploits) در حملات سرریز بافر (buffer overflow attacks) استفاده می‌کنند. یک سوءاستفاده، پارامترهای نادرست را به یک برنامه یا سرویس آسیب‌پذیر منتقل می‌کند که آنها را پردازش کرده و برخی از پارامترها را به عنوان کد اجرا می‌کند. در نتیجه چنین حمله‌ای، سوءاستفاده می‌تواند بدافزار نصب کند.

چنین حملاتی علیه سرویس‌های سیستم که تحت حساب سیستم محلی اجرا می‌شوند، مجرمان را قادر می‌سازد تا مجوزهای مدیریتی را در رایانه دریافت کنند.

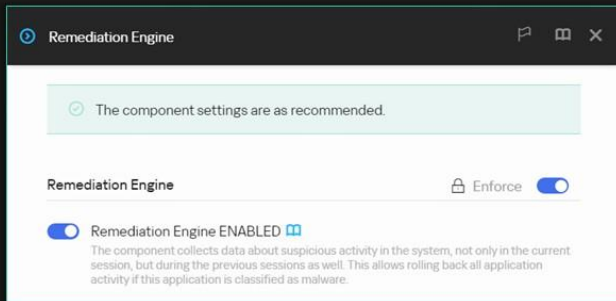
Exploit Prevention، عملیات شروع را رصد می‌کند. اگر یک برنامه آسیب‌پذیر بدون دستور صریح کاربر، یک فایل اجرایی را اجرا کند، این مؤلفه آن را مسدود می‌کند.

به طور پیش‌فرض، Exploit Prevention، فرآیندهای سیستم را نیز ردیابی می‌کند. این مؤلفه فرآیندهای خارجی را که سعی در دسترسی به فرآیندهای سیستم دارند، مسدود می‌کند.

چگونه موتور اصلاح در برابر تهدیدات جدید محافظت می‌کند ؟

How Remediation Engine protects against new threats

49



Saves file copies

Restores files damaged by malware

Rolls back other actions of dangerous programs using the Behavior Detection log

Remediation Engine - اقدامات انجام شده توسط برنامه‌های حذف شده توسط محافظت در برابر تهدید فایل، وظایف اسکن بدافزار و تشخیص رفتار را به حالت اولیه برمی‌گرداند.

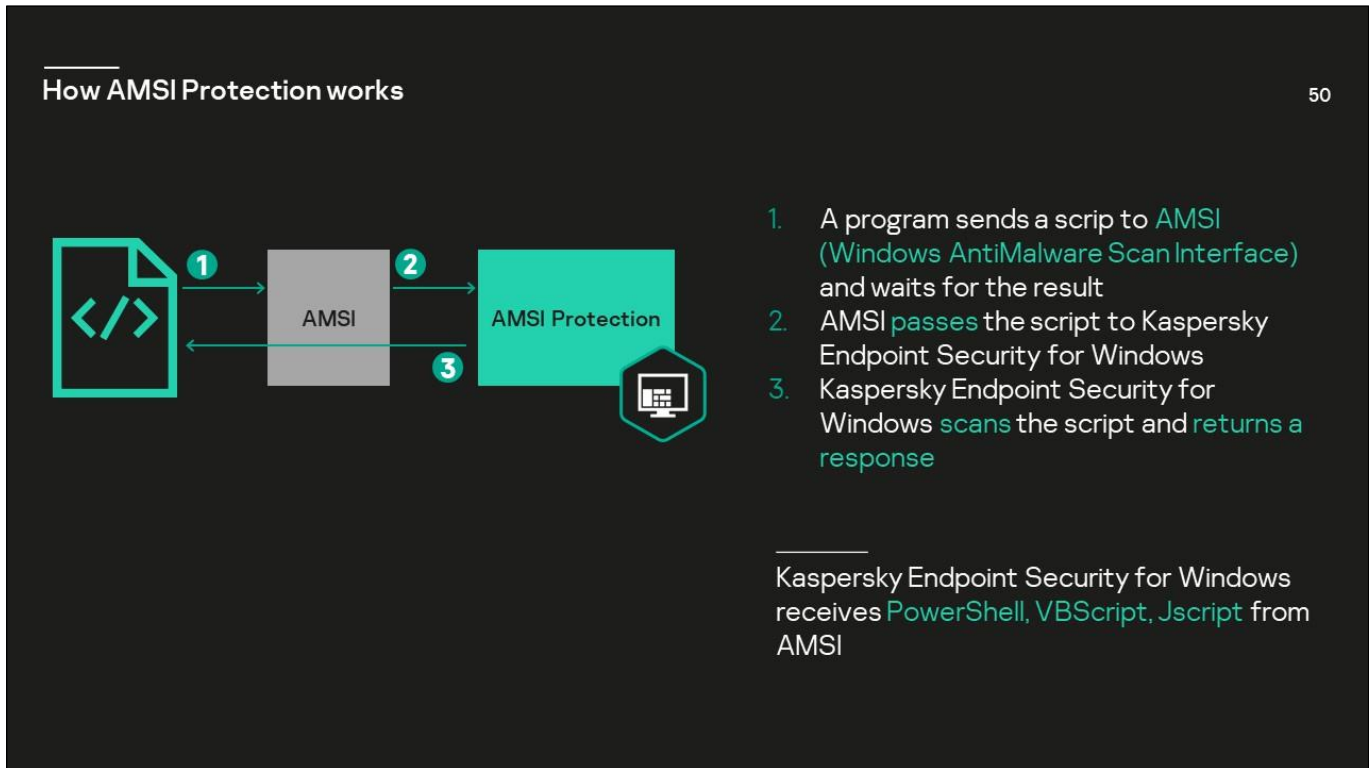
این مؤلفه تغییرات ایجاد شده در موارد زیر را به حالت اولیه برمی‌گرداند:

- File system - فایل‌های ایجاد شده را حذف کرده و فایل‌های اصلاح شده و حذف شده را بازیابی می‌کند.
- Registry - ورودی‌های ایجاد شده توسط بدافزار را حذف می‌کند.
- Processes - فرآیندهای مخرب را خاتمه می‌دهد.
- Network interactions (تعاملات شبکه) - اتصالات شبکه مخرب را مسدود می‌کند.

همچنین، هنگام شروع سیستم، یک نسخه پشتیبان از برخی فایل‌ها و کلیدها ایجاد می‌شود و در صورت تغییر این فایل‌ها و کلیدها توسط بدافزار، امکان بازگشت به این نسخه را فراهم می‌کند. این اشیاء ویژه شامل میزبان‌ها و فایل‌های boot.ini و کلیدهای رجیستری هستند که مسئول شروع برنامه‌ها و سرویس‌ها در هنگام شروع سیستم هستند. در ابتدای این فصل، به باج‌افزارهای رمزگذاری فایل اشاره کردیم که فایل‌های موجود در درایوها و پوشه‌های مشترک را رمزگذاری کرده و سپس درخواست باج می‌کنند. Remediation Engine، فایل‌های رمزگذاری شده توسط این برنامه‌ها را بازیابی می‌کند.

Remediation Engine از گزارش فعالیت برنامه که توسط مؤلفه تشخیص رفتار نوشته شده است، استفاده می‌کند.

چگونه ارائه دهنده حفاظت AMSI تهدیدات جدید را متوقف می‌کند؟



رابط اسکن ضدبدافزار (AMSI) یک API باز از میکروسافت است. نرم‌افزارهای آنتی‌ویروس و سایر راهکارهای امنیتی می‌توانند از این API برای اسکن ماکروها و سایر اسکریپت‌ها در حین اجرا استفاده کنند و از اجرای کدهای مخرب توسط برنامه‌ها جلوگیری کنند.

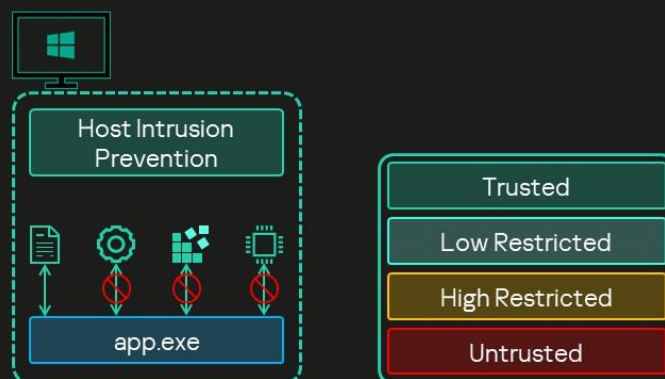
AMSI Protection component با AMSI تعامل دارد و امکان تشخیص حملات بدون فایل را فراهم می‌کند. در طول یک حمله بدون فایل، یک مجرم سایبری کنترل یک فرآیند قانونی مانند PowerShell، JavaScript یا VBScript را به دست می‌گیرد و سپس کد خود را در حافظه فرآیند اجرا می‌کند تا منابع موجود در دستگاه را دریافت کند. سپس مجرم سایبری می‌تواند سناریوهای حمله مختلفی را پیاده‌سازی کند.

تشخیص چنین حمله‌ای دشوار است، زیرا مجرمان نیازی به ذخیره برنامه‌های خود (که Kaspersky Endpoint Security for Windows می‌تواند آنها را به عنوان مخرب تشخیص دهد) در دستگاه ندارند. علاوه بر این، اغلب از تکنیک‌های مختلف پنهان‌سازی استفاده می‌شود. به عنوان مثال، مبهم‌سازی کد، که تجزیه و تحلیل کد را پیچیده می‌کند، و تکنیک‌های فرار که امکان انتقال اطلاعات لازم به رایانه را فراهم می‌کنند.

چگونه Host Intrusion Prevention ، تهدیدات جدید را متوقف می‌کند؟

How Host Intrusion Prevention stops new threats

53



Host Intrusion Prevention ، فعالیت برنامه‌های در حال اجرا را بر اساس اعتبار آنها تنظیم می‌کند. بسته به دسته برنامه، این مؤلفه موارد زیر را مجاز یا مسدود می‌کند:

- دسترسی به سیستم فایل (Access to the file system)
- دسترسی به رجیستری (Registry access)
- دسترسی به دستگاه‌های نوشتن (Access to writing devices)
- تعامل با سایر برنامه‌ها (Interaction with other programs)

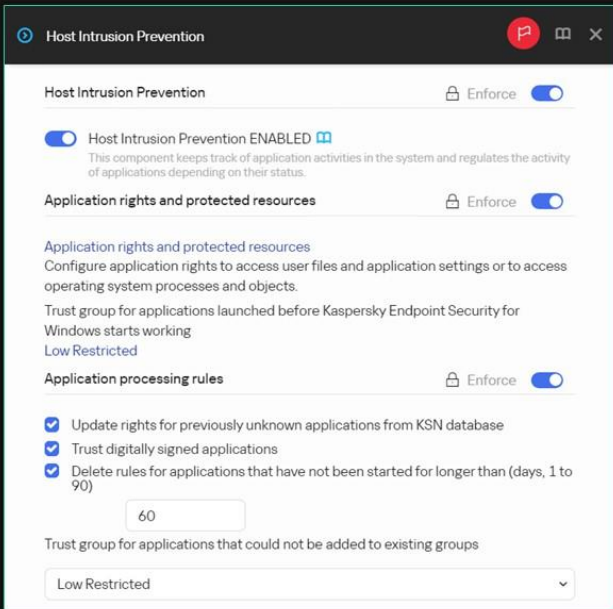
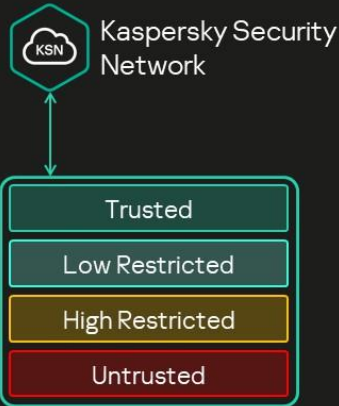
پیشگیری از نفوذ میزبان، برنامه‌ها را در گروه‌های اعتماد دسته‌بندی می‌کند:

- Trusted
- Low Restricted
- High Restricted
- Untrusted

شما می‌توانید برنامه‌ها را به صورت دستی به هر گروهی اضافه کنید.

چگونه Host Intrusion Prevention ، اعتبار یک برنامه را محاسبه می کند ؟

How Host Intrusion Prevention calculates a program's reputation 54



Kaspersky Endpoint Security برای اختصاص یک گروه اعتماد به یک برنامه هنگام شروع اولیه، با Kaspersky Security Network مشورت می کند.

اگر KSN غیرقابل دسترسی باشد یا اطلاعاتی در مورد برنامه وجود نداشته باشد، دسته اختصاص داده شده به تنظیمات policy بستگی دارد:

- گروه Trust برای برنامه هایی که نمی توانند به گروه های موجود اضافه شوند - می توانید انتخاب کنید که کدام دسته را به برنامه هایی که هنوز اعتبار ندارند اختصاص دهید: Low Restricted ، High Restricted یا Untrusted.
- به برنامه های امضا شده دیجیتالی اعتماد کنید - اگر این تنظیم فعال باشد، برنامه های امضا شده توسط گواهی های معتبر به طور خودکار در گروه قابل Trust قرار می گیرند.
- Host Intrusion Prevention ، دسترسی به فایل ها، پوشه ها و کلیدهای رجیستری روی هارد دیسک ها را محدود می کند. Host Intrusion Prevention فهرستی از منابع محافظت شده دارد. آن ها به دو دسته گروه بندی می شوند:
- سیستم عامل
- داده های شخصی

هر دسته زیرشاخه‌ها و توضیحات منابع خود را دارد: مسیرهای پوشه‌ها، ماسک‌های فایل، ماسک‌های کلید رجیستری.

در ابتدا، فهرست منابع محافظت‌شده شامل گروه‌هایی از مهم‌ترین فایل‌ها و کلیدهای رجیستری است. به عنوان مثال، دسته سیستم عامل شامل زیرشاخه تنظیمات راه‌اندازی است که شامل تمام ورودی‌های autorun در رجیستری است.

برای هر گروه از منابع، می‌توانید حقوق دسترسی را برای عملیات زیر تعریف کنید:

- Read -
- Write -
- Delete -
- Create -

به طور پیش‌فرض، Host Intrusion Prevention از منابع به شرح زیر محافظت می‌کند:

داده‌های شخصی	سیستم عامل	
دسترسی کامل	دسترسی کامل	Trusted
دسترسی کامل	دسترسی کامل به همه چیز به جز فایل‌های حیاتی سیستم عامل برای فایل‌های حیاتی سیستم عامل، فقط خواندنی	Low Restricted
دسترسی کامل	فقط خواندنی	High Restricted
بدون دسترسی	بدون دسترسی	Untrusted

محدودیت‌های برنامه به طور خودکار بر روی فرآیندهای فرزند یک برنامه اعمال می‌شوند. اگر برنامه‌ای با محدودیت، یک برنامه‌ی قابل اعتماد را اجرا کند، این برنامه‌ی قابل اعتماد نیز محدود خواهد شد. اگر یک برنامه‌ی قابل اعتماد توسط کاربر یا برنامه‌ی قابل اعتماد دیگری اجرا شود، هیچ محدودیتی وجود نخواهد داشت.

پیکربندی Host Intrusion Prevention :

مدیر می‌تواند محدودیت‌ها را برای هر گروه اعتماد و حتی برای هر برنامه‌ی جداگانه تغییر دهد. (تنظیمات Host Intrusion Prevention را تغییر ندهید، مگر اینکه دقیقاً بدانید چه کاری انجام می‌دهید).

برای یافتن گروه‌های اعتماد و محدودیت‌های آنها:

۱. در پالیسی Kaspersky Endpoint Security، Host Intrusion Prevention | Advanced Threat Protection را باز کنید.

۲. روی لینک Application rights و protected resources کلیک کنید.

۳. به تب Application rights بروید.

۴. گروه trust را در پنل سمت چپ انتخاب کنید.

۵. در بالای پنل سمت راست، در لیست کشویی، Rights را انتخاب کنید.

۶. در بالای پنل سمت راست، در لیست کشویی، گزینه **Files and system registry** را انتخاب کنید.
(در اینجا مدیر می تواند دسترسی های یک برنامه با اعتبار انتخاب شده را محدود یا گسترش دهد. برای مثال، می توانید به برنامه هایی با محدودیت کم اجازه دسترسی به وب کم را بدهید.)
در اینجا مدیر می تواند دسترسی به عملیات خواندن/نوشتن/حذف/ایجاد را برای هر گروهی از منابع محدود یا گسترش دهد.

برای اطلاع از اینکه چه زمانی پیشگیری از نفوذ میزبان (Host Intrusion Prevention) عملیاتی را مسدود می کند، گزارش گیری (logging) را فعال کنید. برای انجام این کار، روی یک عمل در جدول کلیک راست کرده و گزینه ثبت رویدادها (Log events) را انتخاب کنید. می توانید رویدادهای دسترسی-اجازه (access-allow) پیشگیری از نفوذ میزبان (Host Intrusion Prevention) را ثبت کنید تا بفهمید کدام برنامه ها با یک منبع در تعامل هستند.

پیکربندی Host Intrusion Prevention برای متوقف کردن باج افزار :

Use case: Configure Host Intrusion Prevention to stop ransomware

Configure Host Intrusion Prevention to monitor operations with documents:

1. Open the list of resources in the Host Intrusion Prevention settings
2. Add a category, for example, *Documents*
3. Add file masks to the category, for example **.doc, *.docx, *.xlsx, etc.*

با تنظیمات پیش فرض، پیشگیری از نفوذ میزبان (Host Intrusion Prevention) از سیستم عامل و سایر نرم افزارهای رایانه در برابر برنامه هایی که شهرت بدی دارند، محافظت می کند.

شما می توانید به راحتی از فایل های کاربران در برابر برنامه های ناشناخته محافظت کنید. انجام این کار آنها را در برابر تهدیدات مختلف، از جمله باج افزارهایی که اسناد را رمزگذاری می کنند، محافظت می کند.

ایده ساده است. باج افزار:

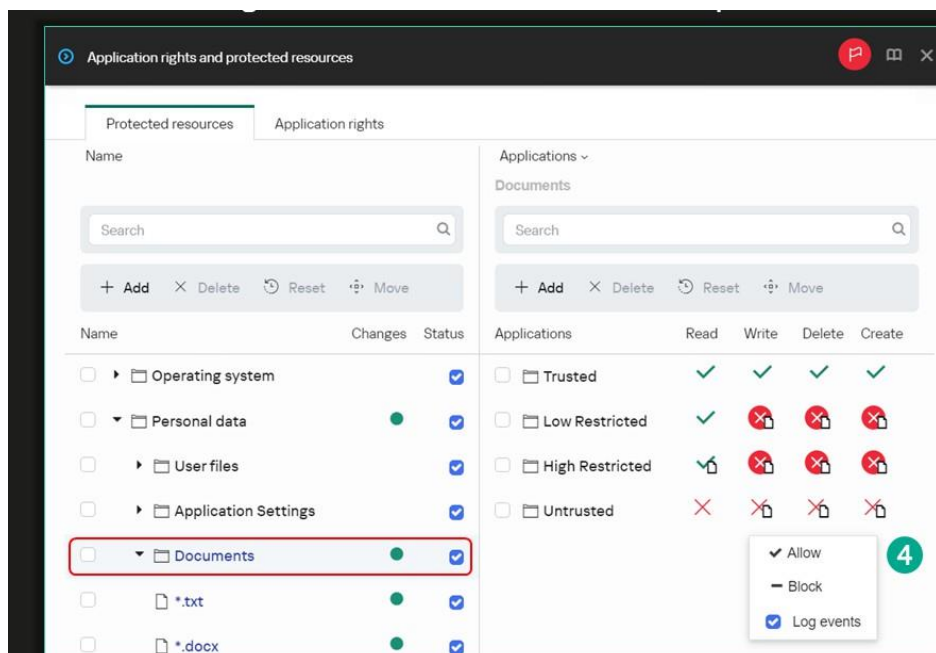
- یا از قبل در KSN شهرت بدی دارد و Kaspersky Endpoint Security اجازه شروع به کار آن را نمی‌دهد، یا
 - هیچ شهرتی در KSN ندارد و پیشگیری از نفوذ میزبان (Host Intrusion Prevention) آن را بسته به تنظیمات پیکربندی شده توسط مدیر، به صورت محدود (به طور پیش فرض) یا محدود (با محدودیت بالا) درمی‌آورد.
- برنامه‌هایی که برای کار با اسناد طراحی شده‌اند، مانند Microsoft Office، شناخته شده هستند و شهرت قابل اعتمادی دارند. بنابراین، برای محافظت از اسناد، به برنامه‌های محدود اجازه ویرایش آنها را ندهید:

۱. در سیاست امنیتی Kaspersky Endpoint Security | Host Intrusion | Advanced Threat Protection Prevention را باز کنید و Right Application و منابع محافظت شده کلیک کنید.

۲. برای افزودن اسناد به فهرست منابع محافظت شده در پیشگیری از نفوذ میزبان، در فهرست سمت چپ، دسته‌بندی داده‌های شخصی | فایل‌های کاربر را انتخاب کنید و یک زیرشاخه جدید با نام اسناد ایجاد کنید.

۳. پسوند‌های سند مانند *.docx، *.pdf، * و غیره را به دسته‌بندی اضافه کنید. برای انجام این کار، گزینه افزودن فایل یا پوشه را انتخاب کنید و یکی از پسوندها را در فیلد مسیر فایل یا پوشه مشخص کنید. این کار را برای همه پسوند‌های مربوطه تکرار کنید.

۴. برنامه‌های محدود شده را از ویرایش اسناد منع کنید. برای انجام این کار، دسته ایجاد شده را در لیست سمت چپ انتخاب کنید و حقوق را در جدول سمت راست تغییر دهید: برنامه‌های با محدودیت بالا و برنامه‌های با محدودیت پایین را از نوشتن و حذف منع کنید.



4. Prohibit all programs except trusted ones from editing documents:

Select to **Block** the **Write** and **Delete** operations for **High Restricted** and **Low Restricted** applications

۴.۴ نحوه‌ی مستثنی کردن یک برنامه از نظارت

What if Kaspersky Endpoint Security impedes a program?

60

Trust programs that have a **trustworthy digital signature**:

- In the Host Intrusion Prevention settings
- In the exclusion settings

If Host Intrusion Prevention has limited the program's rights because of its reputation, make the program **trusted**

If an Advanced Threat Protection component reports a threat, **create an exclusion** for it

If Kaspersky Endpoint Security impedes an application when monitoring its activities, make the program's executable file **trusted in the exclusions**

تقریباً هر تحلیل اکتشافی، نتایج مثبت کاذب را برمی گرداند. برای کاهش آنها، برنامه‌های پاک شناخته شده را از تحلیل حذف کنید:

- برنامه‌هایی که در Kaspersky Security Network قابل اعتماد یا Trust در نظر گرفته می‌شوند
- برنامه‌هایی که با گواهی‌های معتبر امضا شده‌اند

برای جلوگیری از مسدود کردن برنامه‌هایی که KSN آنها را قابل اعتماد می‌داند، کافیسست از KSN استفاده کنید. برای اعتماد به برنامه‌های امضا شده، از تنظیمات Host Intrusion Prevention زیر استفاده کنید: قوانین پردازش برنامه | اعتماد به برنامه‌های امضا شده دیجیتالی.

Kaspersky Endpoint Security فقط به امضاهای دیجیتال مبتنی بر گواهی‌های معتبر اعتماد می‌کند. گواهی‌های معتبر، گواهی‌هایی هستند که توسط مراجع صدور گواهی معتبر صادر می‌شوند.

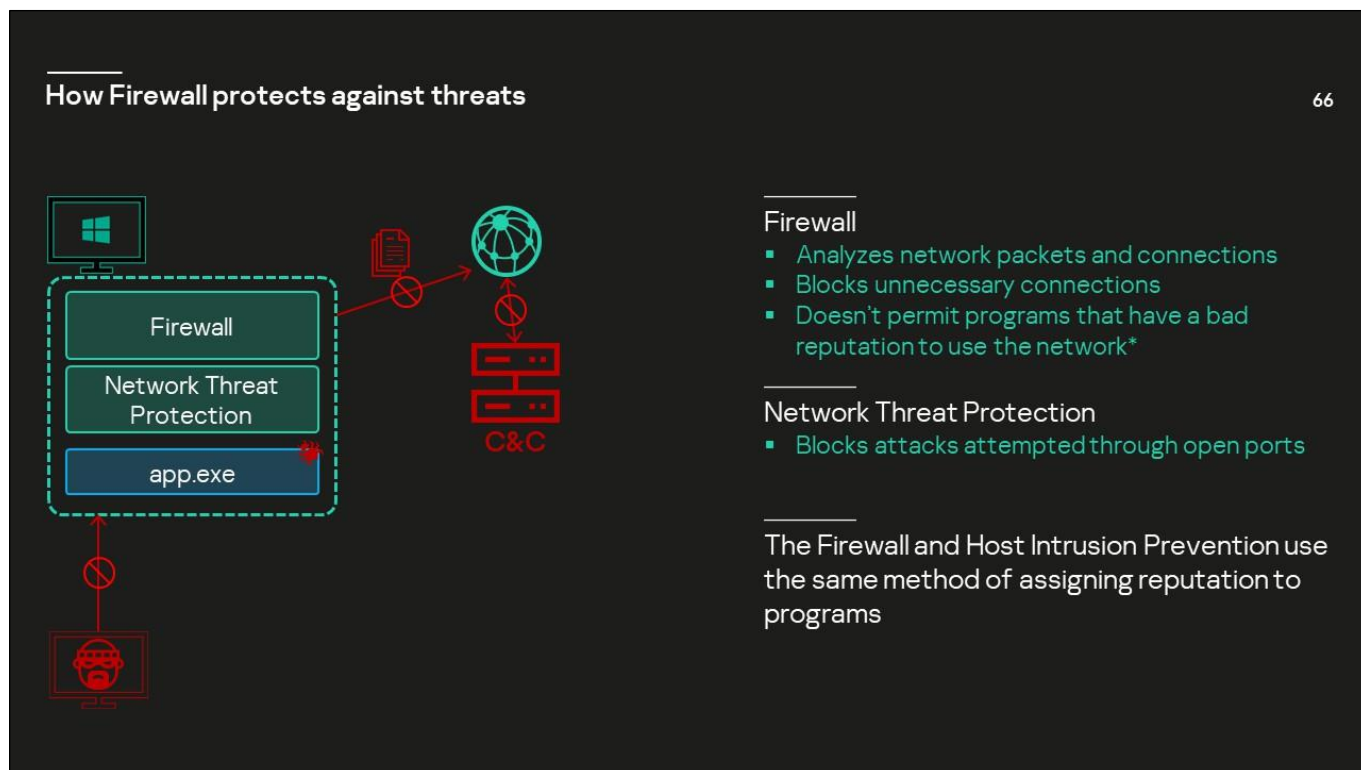
Kaspersky Endpoint Security از پایگاه داده گواهی‌های خود استفاده می‌کند و همیشه به گواهی‌های موجود در فروشگاه محلی مراجع صدور گواهی معتبر ریشه اعتماد نمی‌کند. اگر گواهی به خطر افتاده باشد، Kaspersky Endpoint Security از Kaspersky Security Network در مورد این موضوع مطلع می‌شود و سپس به فایل‌های امضا شده با آن گواهی اعتماد نمی‌کند.

Kaspersky Endpoint Security همچنین به گواهی‌های خود امضا شده اعتماد نمی‌کند. برای اعتماد به نرم‌افزار داخلی با گواهی خود امضا شده، گواهی را به منطقه مورد اعتماد Kaspersky Endpoint Security همانطور که در بخش ۲.۵ در «محرومیت بر اساس گواهی» توضیح داده شده است، اضافه کنید.

اگر برنامه‌ای امضای دیجیتال ندارد، می‌توانید آن را به صورت دستی به گروه Trusted در سیاست پیشگیری از نفوذ میزبان اضافه کنید. از طرف دیگر، می‌توانید با استفاده از تشخیص رفتار و پیشگیری از نفوذ میزبان، یک برنامه را به طور کامل از اسکن مستثنی کنید. نحوه انجام این کار را بعداً توضیح خواهیم داد.

۵. نحوه کنترل اتصالات شبکه

۵.۱ چگونه فایروال در برابر تهدیدات محافظت می‌کند؟



از دیدگاه امنیتی، فایروال دو عملکرد انجام می‌دهد:

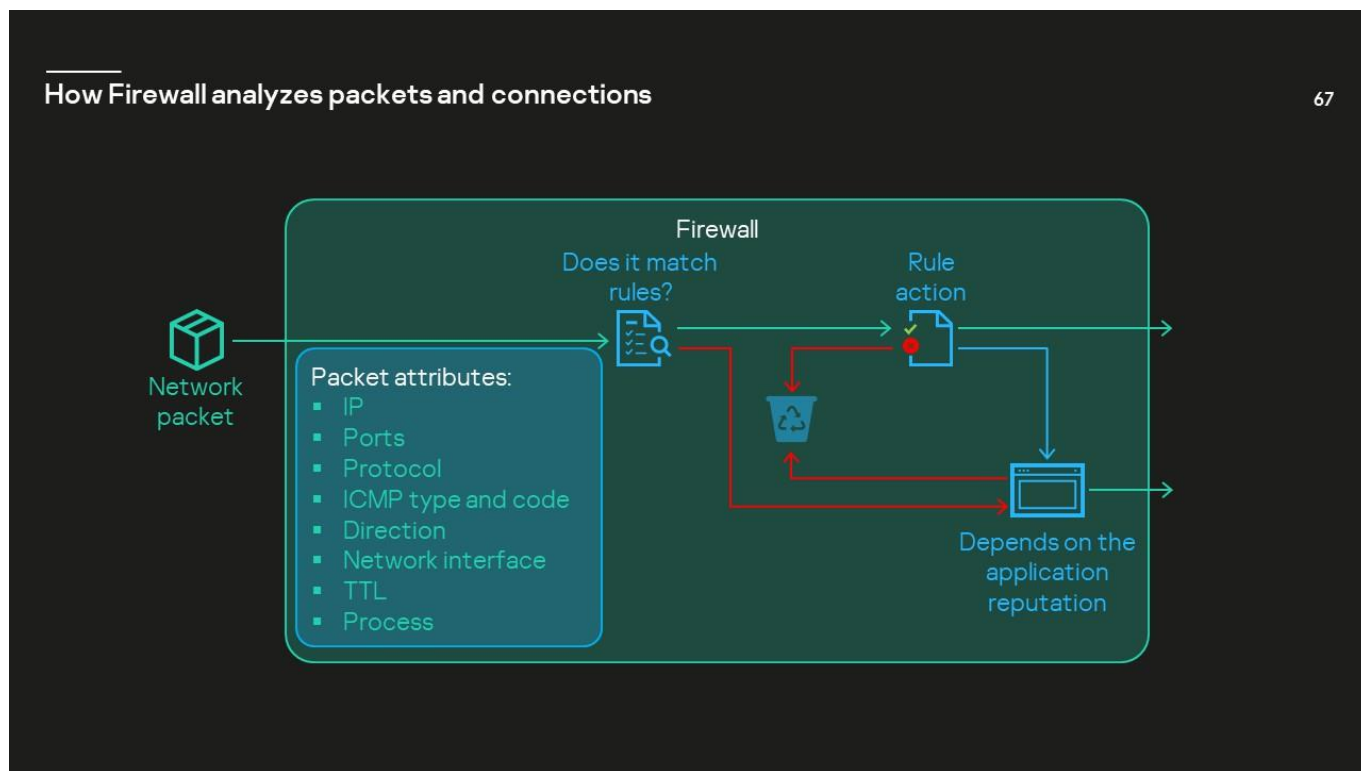
- اتصالات شبکه غیرمجاز به رایانه را بر اساس قوانین مسدود می‌کند. این امر سطح حمله را محدود کرده و خطر آلودگی را کاهش می‌دهد.

- به برنامه‌هایی که شهرت بدی دارند اجازه استفاده از شبکه را نمی‌دهد. این امر از شیوع بیماری جلوگیری می‌کند و همچنین اقدامات کاربرانی را که آگاهانه یا ناخودآگاه سیاست امنیتی را نقض می‌کنند، محدود می‌کند.

فایروال با Host Intrusion Prevention یکپارچه شده است. Host Intrusion Prevention دسترسی برنامه‌ها به تنظیمات سیستم عامل، سایر برنامه‌ها و فایل‌های کاربر را محدود می‌کند. فایروال اعتبار یک برنامه را بررسی کرده و دسترسی آن به شبکه را محدود می‌کند. به این ترتیب، فایروال از اجرای بدافزارهایی که باعث آسیب می‌شوند جلوگیری می‌کند: به عنوان مثال، با ارسال رمزهای عبور کاربر به مجرم.

مؤلفه Network Threat Protection ، فایروال را تکمیل کرده و بسته‌ها را تجزیه و تحلیل می‌کند. حفاظت از تهدید شبکه، توالی بسته‌ها را برای نشانه‌های حمله شبکه، به عنوان مثال، حمله سرریز بافر از طریق آسیب‌پذیری‌های شناخته شده، بررسی می‌کند. این محافظت، اتصالاتی را که برای انجام حمله استفاده می‌شوند، مسدود می‌کند.

۵.۲ نحوه عملکرد فایروال در Kaspersky Endpoint Security :



فایروال با استفاده از قوانین بسته، اتصالات را در سطح شبکه و انتقال کنترل می‌کند. این فایروال ویژگی‌های بسته‌های ورودی و خروجی را تجزیه و تحلیل می‌کند، آنها را با قوانین مقایسه می‌کند و یکی از دو اقدام زیر را انجام می‌دهد:

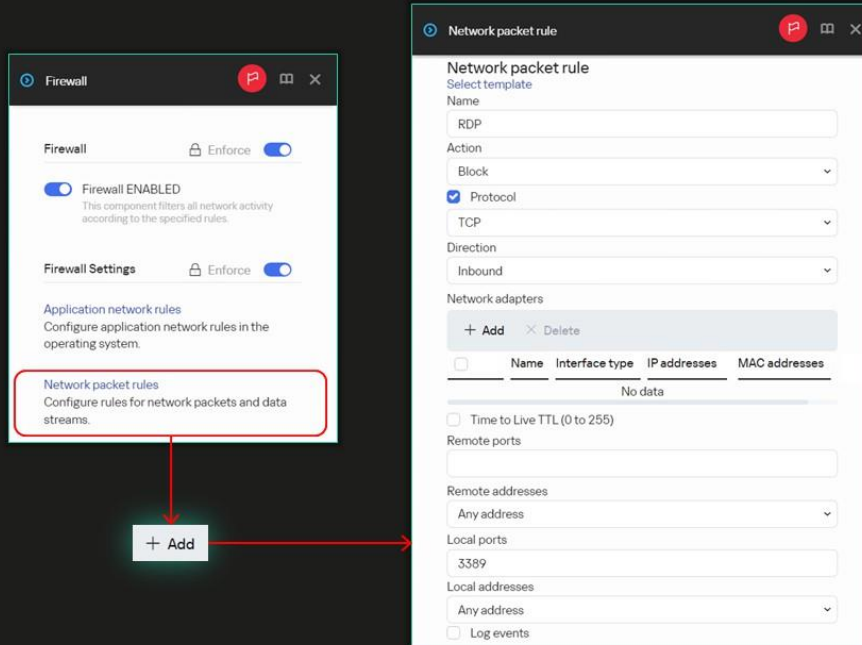
Allow -

Block -

اگر یک بسته با یک قانون خاص مطابقت نداشته باشد، فایروال بر اساس اعتبار برنامه ارسال کننده یا دریافت کننده بسته، تصمیم می‌گیرد چه کاری انجام دهد.

همچنین می‌توانید قوانین فایروال سفارشی را برای گروه‌های اعتماد برنامه پیکربندی کنید.

Configure network packet rules



The Firewall checks the packet attributes:

- Local and remote IP address
- Protocol: TCP, UDP, IGMP, GRE, ICMP, ICMPv6
- ICMP type and code
- Local and remote port (TCP, UDP)
- Direction: Inbound, Outbound
- Network interface
- TTL (time-to-live)
- Process

Looks for the first matching rule and applies it

ساده‌ترین بخش فایروال کسپر‌سکی اندپوینت سکیوریتی، فهرست قوانین شبکه بسته است. برای مشاهده آن، تنظیمات فایروال را در سیاست کسپر‌سکی اندپوینت سکیوریتی باز کنید و روی پیوند قوانین بسته شبکه کلیک کنید.

فایروال ویژگی‌های بسته را با ویژگی‌های قانون مقایسه می‌کند. اگر همه چیز (پروتکل، پورت‌ها، جهت، آداپتور شبکه، آدرس محلی، آدرس راه دور) مطابقت داشته باشد، این مؤلفه اقدام مشخص شده در قانون را اعمال می‌کند.

اعمال قوانین در صورت انتخاب کادر انتخاب رویدادهای ثبت وقایع در گزارش فایروال ثبت می‌شود.

فایروال به دنبال اولین قانون منطبق (از بالا به پایین) می‌گردد و آن را اعمال می‌کند. برای تنظیم مجدد قوانین، یک قانون را انتخاب کنید و آن را با استفاده از دکمه‌های Move up و Move down جابجا کنید.

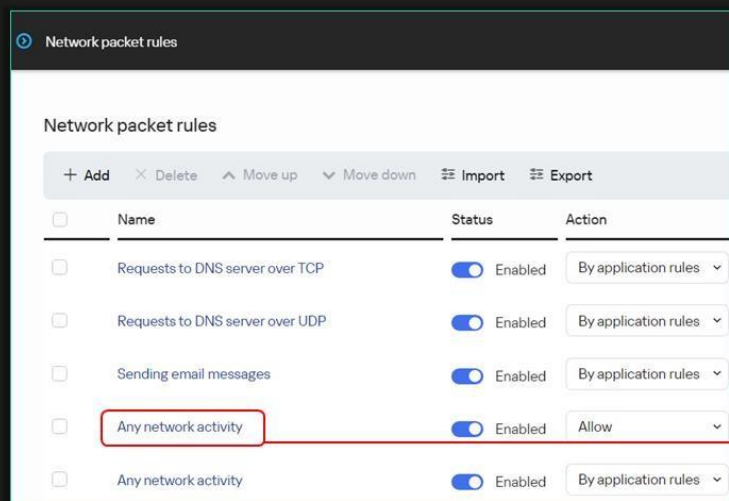
سیاست پیش‌فرض شامل فهرستی از قوانین بسته است که امنیت معقولی را برای رایانه‌ها، چه در شبکه شرکتی و چه در خارج از آن، فراهم می‌کند. تنظیمات پیش‌فرض در انتهای این فصل به تفصیل شرح داده شده است.

قوانین استاندارد بسته، کدگذاری نشده‌اند. مدیر می‌تواند آنها را ویرایش و حذف کند یا قوانین سفارشی اضافه کند. برای راحتی، پروتکل، پورت‌ها و جهت را می‌توان با قالب‌ها مشخص کرد (به عنوان مثال، هرگونه فعالیت شبکه، مرور صفحات وب، فعالیت شبکه Remote Desktop و غیره). برای انتخاب یک الگو، روی دکمه Select template در بالای فیلد Name در تنظیمات قانون کلیک کنید.

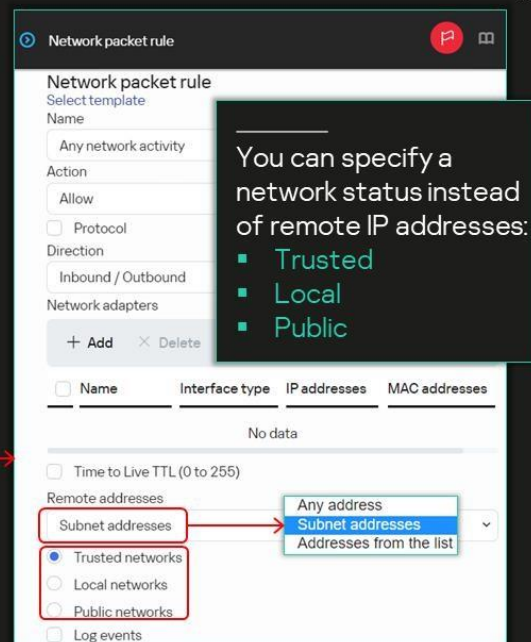
چگونه فایروال تصمیم می‌گیرد کدام شبکه‌ها محلی هستند؟

How Firewall decides which networks are local

69



Most of the pre-set Firewall rules are configured for network statuses or any address



آدرس‌های کامپیوترهای راه دور ممکن است به طور غیرمستقیم در قوانین به عنوان آدرس‌های زیرشبکه مشخص شوند: شبکه‌های قابل اعتماد، شبکه‌های محلی و شبکه‌های عمومی.

فایروال چگونه تصمیم می‌گیرد که کدام آدرس‌ها به کدام شبکه‌ها تعلق دارند؟

وضعیت‌های شبکه توسط مدیر در سیاست امنیتی کسپرسکی اندپوینت مشخص می‌شوند. اگر سیاست وضعیت شبکه را تعریف نکنند، فایروال یکی را در رایانه کلاینت تعریف می‌کند.

برای افزودن یک شبکه به سیاست و انتخاب وضعیت برای آن:

۱. روی پیوند تنظیمات شبکه در Essential Threat Protection | Firewall کلیک کنید.

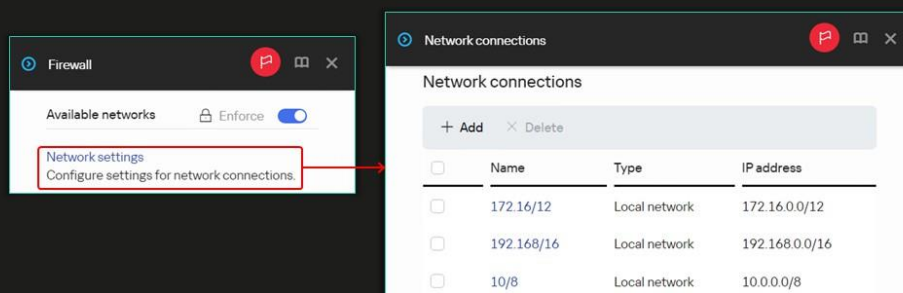
۲. روی دکمه Add در بالای لیست کلیک کنید.

۳. نامی برای زیرشبکه تایپ کنید و نوع آن را انتخاب کنید.

۴. آدرس زیرشبکه را با فرمت زیر مشخص کنید: <آدرس IP>/<طول ماسک شبکه به بیت>، به عنوان مثال ۲۴/۱۹۲.۱۶۸.۰.۰ یا cdef/96::۱۲۳۴ برای شبکه‌های IPv6.

How Firewall decides which networks are local

70



Network statuses are defined by

- The administrator via the policy
- The local KES Firewall, heuristically

Status specified in the policy has **priority** over the local status

KES takes the local connection status from the connection status in the operating system

abc.lab	Access type:	Internet
Domain network	Connections:	eth0
Unidentified network	Access type:	No network access
Public network	Connections:	eth1

در رایانه، فایروال شبکه‌های پیکربندی‌شده برای آداپتورهای شبکه رایانه را به شبکه‌های مشخص‌شده در سیاست اضافه می‌کند. اگر شبکه یک آداپتور با شبکه‌ای از سیاست منطبق باشد یا به آن تعلق داشته باشد، وضعیت مشخص‌شده در سیاست را دریافت می‌کند. اگر شبکه آداپتور متعلق به هیچ یک از شبکه‌های شرح داده‌شده در سیاست نباشد، فایروال بر اساس وضعیت آن در سیستم عامل، وضعیتی را به آن اختصاص می‌دهد. اگر شبکه یک دامنه، محل کار یا خانه باشد، فایروال وضعیت محلی را به آن اختصاص می‌دهد. اگر شبکه در سیستم عامل عمومی باشد، برای فایروال کسپرسکی اندپوینت سکيوریتی نیز عمومی خواهد بود.

تمام آدرس‌های دیگر به عنوان آدرس‌های شبکه عمومی در نظر گرفته می‌شوند.

به عنوان مثال، سیاست ممکن است شامل یک ورودی شبکه واحد برای ۱۶/۱۷۲.۱۶.۰.۰ با وضعیت شبکه محلی باشد. یک رایانه مدیریت‌شده دارای دو رابط شبکه با آدرس‌های IP 172.16.55.10/24 و ۲۴/۱۹۲.۱۶۸.۵.۱۰ است. فرض کنید Kaspersky Endpoint Security به طور خودکار وضعیت شبکه عمومی را به هر دوی این شبکه‌ها اختصاص می‌دهد. اکنون وقتی شبکه‌های محلی با این سیاست ترکیب می‌شوند، وضعیت شبکه ۲۴/۱۷۲.۱۶.۵۵.۰ به شبکه محلی تبدیل می‌شود، زیرا در سیاست، ورودی برای شبکه ۱۶/۱۷۲.۱۶.۰.۰ وجود دارد که شامل ۲۴/۱۷۲.۱۶.۵۵.۰ است. از سوی دیگر، شبکه ۲۴/۱۹۲.۱۶۸.۵.۰ وضعیت عمومی خود را حفظ می‌کند، زیرا هیچ ورودی منطقی در سیاست وجود ندارد.

در تنظیمات پیش‌فرض سیاست، سه ورودی شبکه وجود دارد که همه آنها وضعیت شبکه محلی دارند:

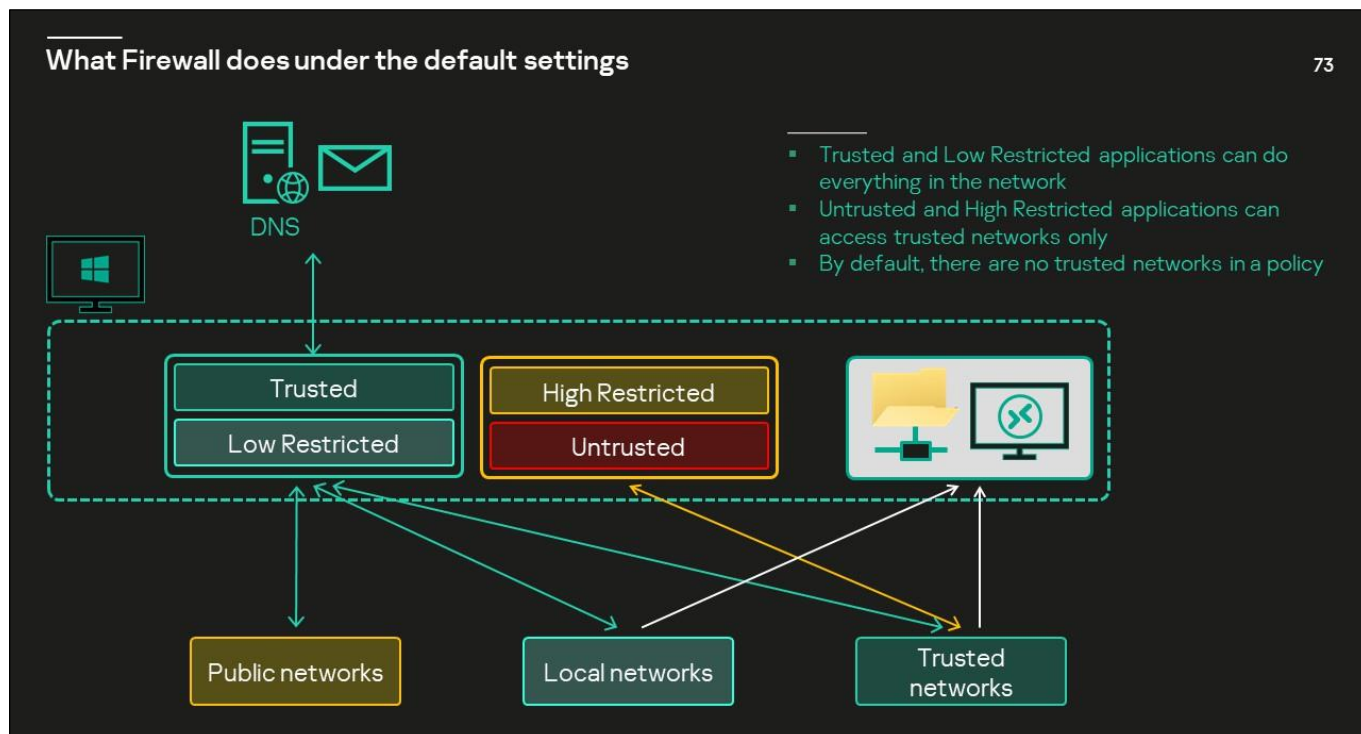
- ۸/۱۰.۰.۰.۰

- ۱۲/۱۷۲.۱۶.۰.۰

- ۱۶/۱۹۲.۱۶۸.۰.۰

اینها انتخاب‌های معقولی برای رایانه‌های داخل محیط هستند. با این حال، اگر یک کارمند در خارج از شبکه کار می‌کند، مثلاً در یک سفر کاری، باید از تنظیمات دیگری استفاده شود.

کاری که فایروال در تنظیمات پیش‌فرض انجام می‌دهد



سیاست استاندارد شامل قوانینی برای برنامه‌ها نیست (به جز قوانین استاندارد که برای اعتبارها مشخص شده‌اند). به همین دلیل است که وضعیت نهایی شبکه و اعتبارهای برنامه به صورت محلی در فایروال تعریف می‌شوند.

قوانین بسته از این سیاست به ارث می‌رسند و بر این اساس، بسته‌ها به شرح زیر فیلتر می‌شوند:

- سه قانون اول، توانایی ارسال درخواست‌های DNS (از طریق پروتکل‌های TCP و UDP، پورت خارجی ۵۳) و ایمیل (از طریق پروتکل TCP، پورت‌های خارجی ۲۵، ۴۶۵، ۱۴۳ و ۹۹۳) را تنظیم می‌کنند. در این قوانین، اقدام قانون By application انتخاب شده است. یعنی برنامه‌های موجود در گروه‌های Trusted و Low Restricted قادر به ارسال درخواست‌های DNS و ایمیل خواهند بود، اما سایر برنامه‌ها این کار را نخواهند کرد.
- قانون شماره ۴ هرگونه فعالیت شبکه‌ای را در شبکه‌های Trusted برای همه برنامه‌ها مجاز می‌داند. بنابراین، در شبکه‌های Trusted، هرگونه فعالیتی به طور پیش‌فرض مجاز است، به جز محدودیت‌های DNS و ایمیل برای برنامه‌های High Restricted و Untrusted.

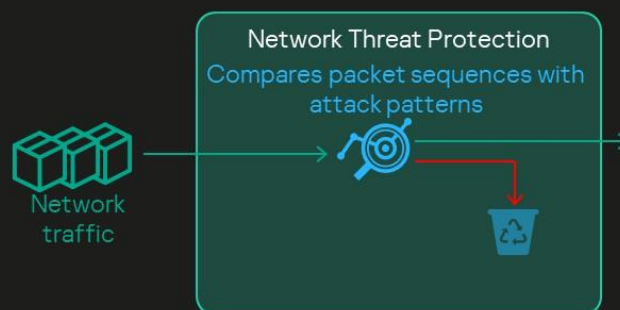
- قانون پنجم ترتیب پردازش بسته‌ها را در شبکه‌های محلی تعریف می‌کند. چنین بسته‌هایی طبق قوانین برنامه پردازش می‌شوند. قوانین پیش‌فرض برنامه‌ها می‌گویند که برنامه‌های موجود در گروه‌های Trusted و Low Restricted هیچ محدودیتی در شبکه‌های محلی ندارند، اما برنامه‌های High Restricted و Untrusted هیچ دسترسی ندارند.
- قوانین ۶ تا ۸ اتصالات ریموت دسکتاپ به کامپیوتر از شبکه‌های عمومی را مسدود می‌کنند و همچنین اتصالات به سرویس محلی DCOM، بسته‌های NetBIOS، دسترسی به پوشه‌های اشتراکی ویندوز و دسترسی به دستگاه‌های Universal Plug & Play را مسدود می‌کنند.
- قوانین ۹ و ۱۰ جریان‌های ورودی TCP و UDP را فقط به برنامه‌های موجود در گروه‌های Trusted و Low Restricted اجازه می‌دهند. با توجه به قوانین پیش‌فرض برنامه‌ها، این بدان معناست که برنامه‌های Trusted و Low Restricted می‌توانند اتصالات ورودی را از شبکه‌های عمومی دریافت کنند، در حالی که برنامه‌های High Restricted و Untrusted نمی‌توانند.
- قوانین ۱۱ تا ۱۵ درخواست‌های تشخیصی ICMP ورودی را مسدود می‌کنند، اما اجازه می‌دهند بسته‌های ICMP برای آزمایش اتصال به کامپیوترهای راه دور ارسال شوند.

۵.۴ چرا حفاظت در برابر تهدیدات شبکه ضروری است ؟

محافظت در برابر تهدیدات شبکه چه کاری انجام می‌دهد؟

What Network Threat Protection does

76

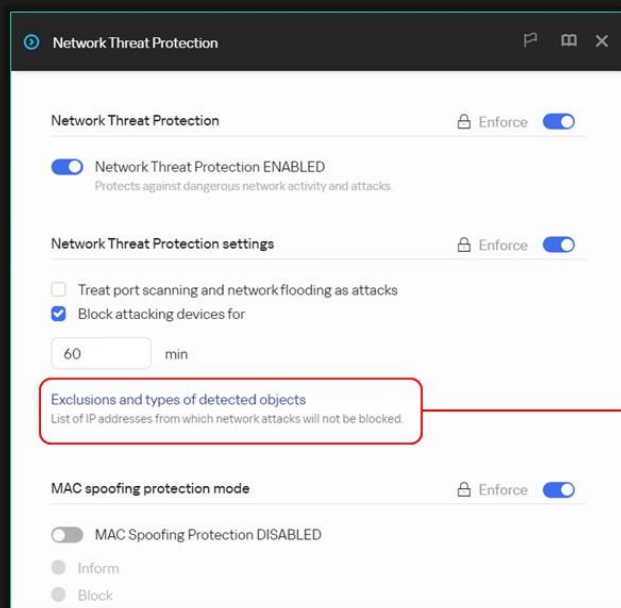


Protects against attacks via **any** (including allowed) connections

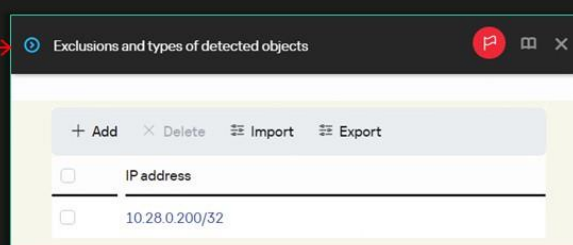
Analyzes network packets **irrespective of the Firewall** and compares **packet sequences** with network attack patterns

Configure Network Threat Protection

77



Blocks attacks and any connections from the attacking computer for **60 minutes** after the attack



هدف از مؤلفه Network Threat Protection

تهدیدات شبکه شامل موارد زیر است:

- اسکن پورت (Port scanning)
- حملات DoS (DoS attacks)
- حملات سرریز بافر (Buffer overflow attacks)
- سایر روش‌های مورد استفاده برای نفوذ مخرب از راه دور بر روی برنامه‌ها و سرویس‌های در حال اجرا بر روی یک رایانه

Network Threat Protection از امضاها استفاده می‌کند و تمام اتصالاتی را که با توصیفات حملات شبکه شناخته شده مطابقت دارند، مسدود می‌کند.

همانطور که قبلاً بحث کردیم، بدافزار همیشه کد اجرایی را در سیستم فایل ذخیره نمی‌کند تا یک رایانه را آلوده کند. به عنوان مثال، بدافزار می‌تواند از حمله سرریز بافر برای تغییر فرآیندی که از قبل در حافظه در حال اجرا است استفاده کند و در نتیجه کد مخرب را اجرا کند.

مؤلفه Network Threat Protection می‌تواند از انتشار آلودگی‌ها به این روش جلوگیری کند. به همین دلیل توصیه می‌کنیم این محافظت را فعال نگه دارید و تنظیمات آن را قفل کنید.

حفاظت از تهدید شبکه چند پارامتر قابل تنظیم دارد. اگر این مؤلفه فعال باشد، حملات به طور خودکار مسدود می‌شوند.

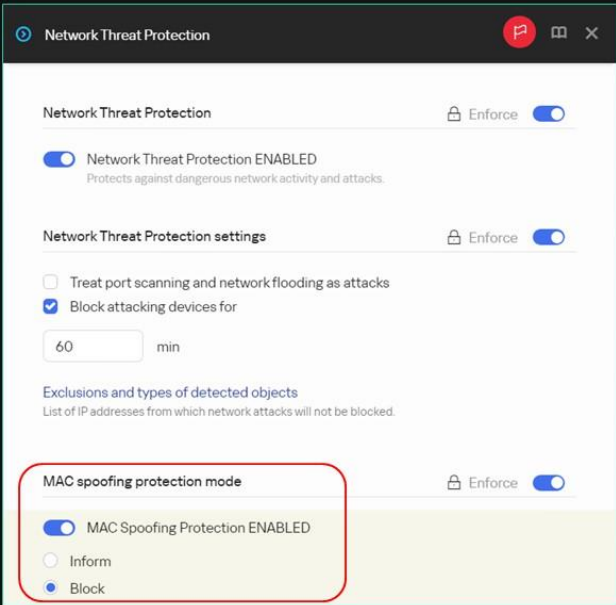
علاوه بر این، Kaspersky Endpoint Security می‌تواند بسته‌های بیشتر از رایانه مهاجم را برای مدتی مسدود کند. گزینه Block attack computer for NN min مسئول این رفتار است. به طور پیش‌فرض، فعال است و رایانه‌ها را به مدت ۶۰ دقیقه مسدود می‌کند. شما می‌توانید به صورت دستی از طریق رابط محلی Kaspersky Endpoint Security یا کنسول مدیریت Kaspersky Security Center، کامپیوتر را از حالت مسدود خارج کنید.

حفاظت از تهدید شبکه گاهی اوقات بسته‌های متعددی را که توسط دوربین‌های مداربسته و سایر دستگاه‌های مشابه ارسال می‌شوند، حمله تلقی کرده و بسته‌ها را مسدود می‌کند. برای جلوگیری از این امر، آدرس دستگاه‌ها را به موارد استثنا اضافه کنید. حفاظت از تهدید شبکه، بسته‌های ارسالی از آدرس‌های مورد اعتماد را تجزیه و تحلیل نمی‌کند.

پیکربندی محافظت در برابر جعل آدرس MAC (MAC spoofing)

Configure MAC Spoofing Protection

78



To prevent poisoning the ARP table, it accepts only those replies for which a request was sent

After an ARP request, all responses except for the first one are ignored

محافظت در برابر MAC spoofing از تغییر غیرمجاز جداول ARP در رایانه‌های محافظت‌شده جلوگیری می‌کند.

اگر گزینه محافظت در برابر MAC spoofing فعال باشد، رایانه موارد زیر را انجام می‌دهد:

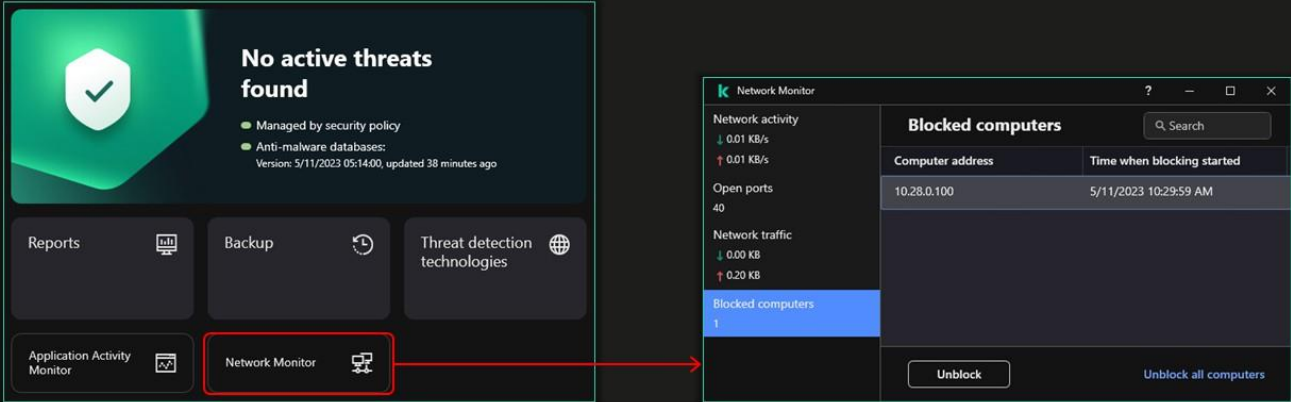
- هرگونه پاسخ ARP ورودی که به درخواست‌های ARP خودش پاسخ نمی‌دهد را نادیده می‌گیرد.
- پس از ارسال درخواست ARP، فقط اولین پاسخ را می‌پذیرد و بقیه را نادیده می‌گیرد. با این اوصاف، Kaspersky Endpoint Security اطلاعات مربوط به همه آنها را ثبت می‌کند.
- مدتی منتظر پاسخ ARP می‌ماند و پاسخ‌های دیر هنگام را نادیده می‌گیرد.
- بدون اضافه کردن رکوردی به جدول ARP سیستم، به درخواست ARP ورودی پاسخ می‌دهد.

شما می‌توانید اقدامی را که در صورت حمله انجام می‌شود پیکربندی کنید.

نحوه رفع انسداد کامپیوتر مسدود شده

How to unblock a computer blocked by Network Threat Protection

79



Computer address	Time when blocking started
10.28.0.100	5/11/2023 10:29:59 AM

Locally, in the Network Monitor window

Alternatively, in the Kaspersky Security Center console, in the computer properties, restart the task Network Threat Protection

وقتی یک کامپیوتر کلاینت به دلیل حمله شبکه، کامپیوتر کلاینت دیگری را مسدود می‌کند، مدیر سیستم فقط می‌تواند رویدادی را که در مورد حمله شبکه به او اطلاع می‌دهد، در کنسول ببیند. هیچ فهرستی از کامپیوترهای مسدود شده یا رویدادهایی که نشان دهد یک کامپیوتر مسدود شده و بعداً از حالت مسدود خارج شده است، وجود ندارد.

شما می‌توانید فهرست کامپیوترهای مسدود شده را در رابط محلی Kaspersky Endpoint Security پیدا کنید:

۱. در پنجره Kaspersky Endpoint Security Network Monitor را انتخاب کنید.

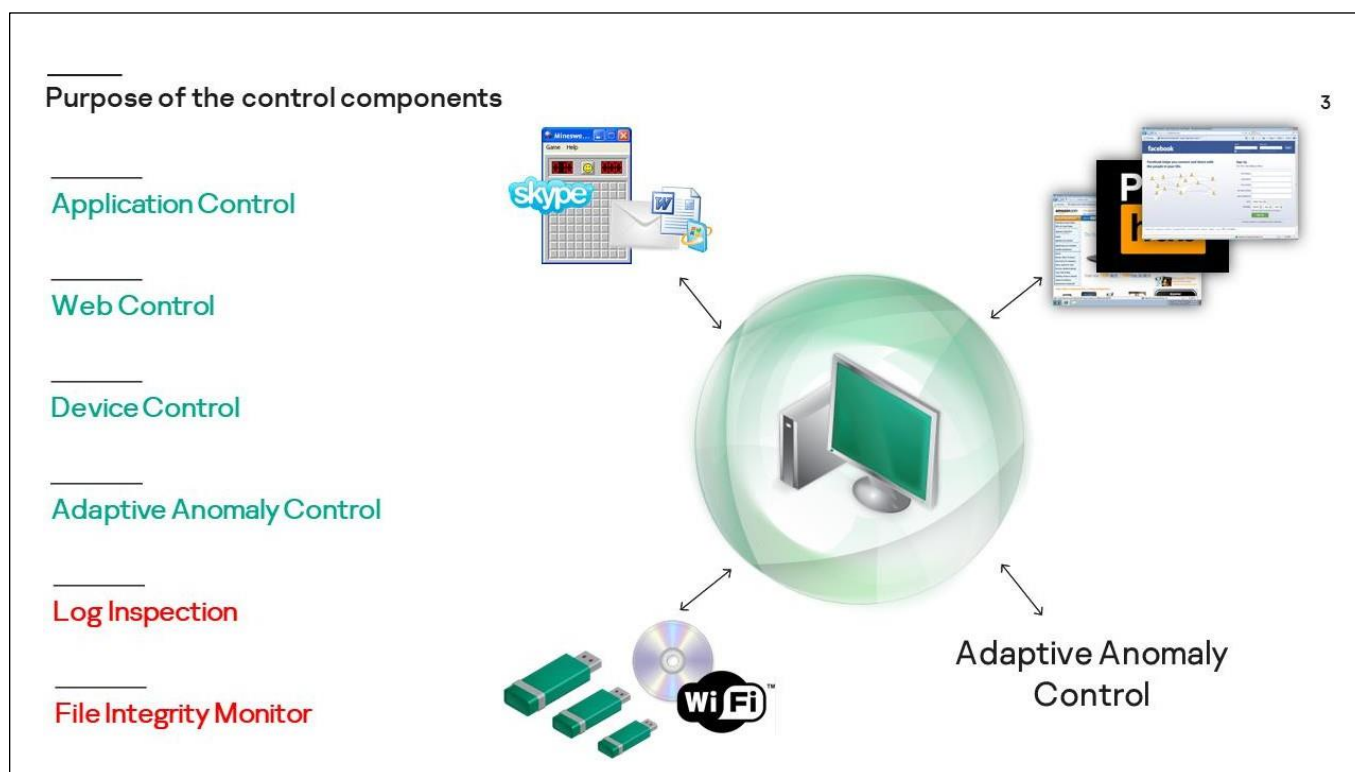
۲. در پنجره Network Monitor Blocked computers را انتخاب کنید.

۳. برای رفع انسداد یک کامپیوتر، آن را انتخاب کرده و روی Unblock کلیک کنید.

۱. عمومی

در این بخش، اجزای کنترلی Kaspersky Endpoint Security و قابلیت‌های آنها را بررسی خواهیم کرد.

۱.۱ هدف از اجزای کنترل



علاوه بر محافظت در برابر بدافزار، Kaspersky Endpoint Security شامل اجزای کنترلی است که اقدامات مضر برای رایانه‌ها یا شرکت را به طور کلی محدود می‌کند.

- Application Control ، تلاش‌های کاربران برای شروع برنامه‌ها را رصد می‌کند و راه‌اندازی برنامه‌ها را از طریق قوانینی که توسط مدیر پیکربندی شده است، تنظیم می‌کند.

- Device Control ، استفاده از دستگاه‌های مختلف را با سیاست‌های شرکت مطابقت می‌دهد. این جزء شامل ماژول Anti-Bridging است که جابجایی بین آداپتورهای شبکه را تنظیم می‌کند و در نتیجه به جلوگیری از اتصالات غیرمجاز کمک می‌کند.
- Web Control ، دسترسی به وبسایت‌ها را بسته به محتوای آنها محدود می‌کند. همچنین می‌توانید آدرس‌ها را با استفاده از ماسک مسدود کنید.
- Adaptive Anomaly Control از مجموعه‌ای از قوانین از پیش تنظیم شده برای نظارت بر رفتارهای غیرمعمول که معمولاً قبل از آلودگی رخ می‌دهد، استفاده می‌کند و به جلوگیری از آن در نطفه کمک می‌کند.
- دو مؤلفه کنترلی دیگر نیز وجود دارد، اما در این دوره بررسی نمی‌شوند زیرا برای فعال‌سازی این مؤلفه‌ها به مجوز Kaspersky Hybrid Cloud Security Enterprise نیاز است. این مؤلفه‌ها فقط روی سیستم عامل‌های سرور نصب می‌شوند و در دوره KL 020 Kaspersky Hybrid Cloud Security شرح داده شده‌اند.
- Log Inspection ، یکپارچگی سرور محافظت‌شده را رصد می‌کند، حملات و تلاش‌های نفوذ (به عنوان مثال، حملات جستجوی فراگیر) و همچنین ناهنجاری‌های ثبت‌شده در لاگ‌های ویندوز را شناسایی می‌کند. بازرسی لاگ شامل قوانین از پیش تعریف‌شده‌ای است که به تشخیص حمله کمک می‌کند.
- File Integrity Monitor ، یکپارچگی فایل‌ها یا پوشه‌ها را در محدوده مشخص‌شده رصد می‌کند. در صورت نقض یکپارچگی، این مؤلفه به مدیر در مورد تغییرات در فایل‌ها یا پوشه‌ها که ممکن است نشان دهنده به خطر افتادن داده‌ها در سرور محافظت‌شده باشد، اطلاع می‌دهد.

۱.۲ Licensing

Licensing			
	Select	Advanced	Total
Control components for Windows workstations	Yes	Yes	Yes
Control components for Windows servers	No	Yes	Yes
Adaptive Anomaly Control (workstations only)	No	Yes	Yes
Log Inspection (servers only)	No	No	No
File Integrity Monitor (servers only)	No	No	No

To activate the Log Analysis and File Integrity Monitor components, a KHCS Enterprise license is required

مجوز KESB Select به شما امکان می‌دهد از اجزای کنترل برنامه، Device Control و Web Control فقط در ایستگاه‌های کاری ویندوز استفاده کنید.

مجوز KESB Advanced قابلیت اضافی استفاده از مؤلفه Adaptive Anomaly Control را در ایستگاه‌های کاری ویندوز فراهم می‌کند و امکان استفاده از اجزای کنترل را در سرورهای ویندوز فراهم می‌کند.

۲. Application Control :

Application Control با محدود کردن اجرای نرم‌افزارها روی دستگاه‌های نهایی، به اجرای سیاست‌های امنیتی شرکت کمک می‌کند. در عین حال، کنترل برنامه با کاهش سطح حمله، خطر آلودگی رایانه را نیز کاهش می‌دهد.

۲.۱ اصول عملیاتی

How Application Control works

9

When a program starts, Kaspersky Endpoint Security checks:

1. The category the program belongs to (categories are created on the Kaspersky Security Center side and used in rules in the Kaspersky Endpoint Security policy)
2. The account that starts it
3. The mode in which Application Control works (denylist or allowlist)

Denylist



The program is allowed if there is **no deny rule** for its category and the account of the current user

Allowlist



The program is allowed only if **there is an allow rule** for its category and the account of the current user

کنترل برنامه به مدیر اجازه می‌دهد تا برنامه‌هایی را که کاربران می‌توانند روی رایانه‌ها اجرا کنند، محدود کند. مجوزهای شروع نرم‌افزار در قوانین ویژه مشخص شده‌اند.

هنگامی که یک برنامه شروع می‌شود، کنترل برنامه موارد زیر را بررسی می‌کند:

- دسته‌بندی که برنامه به آن تعلق دارد (دسته‌بندی‌ها توسط مدیر پیکربندی می‌شوند)
- حسابی که برنامه تحت آن شروع شده است

- اینکه آیا سیاست امنیتی کسپرسکی شامل قوانینی است که شروع این دسته برنامه را برای این حساب تنظیم کند یا خیر.

سپس کسپرسکی اندپوینت سکیوریتی حالت عملیاتی فعلی کنترل برنامه را مشخص می‌کند:

- **لیست ممنوعه:** همه چیز به طور پیش فرض مجاز است. فقط برنامه‌هایی که متعلق به دسته‌بندی‌هایی هستند که مدیر در سیاست امنیتی کسپرسکی اندپوینت ممنوع کرده است، مسدود می‌شوند. به این معنی که اگر هیچ قانون مسدودکننده‌ای مطابق با آن وجود نداشته باشد، برنامه مجاز به شروع خواهد بود.

- **لیست مجاز:** همه چیز به طور پیش فرض ممنوع است. فقط برنامه‌هایی که متعلق به دسته‌بندی‌هایی هستند که مدیر در سیاست امنیتی کسپرسکی اندپوینت مجاز کرده است، مجاز به شروع هستند. اگر هیچ قانون مجازکننده‌ای مطابق با آن وجود نداشته باشد، برنامه مسدود خواهد شد.

حالت لیست مجاز در رویکرد رد پیش فرض استفاده می‌شود. این در بخش مربوطه این فصل توضیح داده شده است.

۲.۲ راه‌اندازی کامپوننت

Setting up the component

10

Application Control is configured in two stages:

1. Create categories in **Kaspersky Security Center**
2. Create rules in the **Kaspersky Endpoint Security** policy for these categories

Categories created in **Kaspersky Security Center** are available in all **Kaspersky Endpoint Security** policies

You can use each category **only once** in a **Kaspersky Endpoint Security** policy

The **Application Control** component does not work without **Kaspersky Security Center**

کنترل برنامه در دو مرحله پیکربندی می‌شود:

ایجاد دسته‌ها در مرکز امنیت کسپرسکی.

به عنوان مثال، مرورگرهای وب، بازی‌ها، پیام‌رسان‌های شخص ثالث، برنامه‌های مجاز و غیره.

تمام برنامه‌هایی را که می‌خواهید کنترل کنید به این دسته‌ها اضافه کنید. نحوه انجام این کار را در بخش بعدی شرح می‌دهیم.

دسته‌ها برای کل سرور مدیریت در یک مکان واحد پیکربندی شده‌اند: عملیات | برنامه‌های شخص ثالث | دسته‌های برنامه.

برای این دسته‌ها، قوانینی را در سیاست امنیتی کسپرسکی اندپوینت ایجاد کنید.

در قوانین پیکربندی شده برای هر دسته برنامه در سیاست امنیتی کسپرسکی اندپوینت، می‌توانید عملی را که باید روی برنامه‌های متعلق به آن دسته انجام شود، مشخص کنید:

- Allow

- Block

- اطلاع دادن به مرکز امنیت کسپرسکی در مورد هر شروع

دسته‌ها در سرور مدیریت مرکز امنیت کسپرسکی ایجاد می‌شوند و به رایانه‌های کلاینت مشابه نحوه انتقال سیاست‌ها و وظایف منتقل می‌شوند. فقط تغییرات در حین همگام‌سازی ارسال می‌شوند (به جای لیست کامل و محتوای همه دسته‌ها).

توجه داشته باشید که دسته‌ها برای کل سرور مدیریت مشخص شده‌اند، اما ممکن است قوانین متفاوتی برای گروه‌های رایانه‌ای مختلف پیکربندی شده باشد. برای مثال، می‌توان اسکایپ را برای همه به جز کاربران خاص ممنوع کرد؛ علاوه بر این، می‌توان به بازاربازان اجازه استفاده از آن را داد و هر بار که شروع می‌شود، مدیر سیستم یک اعلان مربوطه دریافت می‌کند.

شما می‌توانید از هر دسته فقط یک بار در سیاست امنیتی کسپرسکی اندپوینت استفاده کنید. به عبارت دیگر، اگر یک قانون از قبل برای یک دسته خاص پیکربندی شده باشد، نمی‌توانید قانون دیگری برای این دسته ایجاد کنید.

در عوض، باید یک دسته جدید ایجاد کنید.

۲.۳ ایجاد categories

پس از اینکه مرکز امنیت کسپرسکی شروع به دریافت اطلاعات مربوط به فایل‌های اجرایی در رایانه‌های شبکه کرد، می‌توانید شروع به ایجاد دسته‌ها کنید.

Creating categories

By default, the list of categories is empty

Operations / Third-party applications / Application categories

+ Add X Delete Refresh Search...

Type	Name	Used in policies	Last updated
☐	Browsers	✓	
☐	Trusted folder		
☐	Trusted computers		
☐	Trusted applications		

New category wizard

Name: Browsers

Select category creation method

- ☒ Category with content added manually. Data of executable files is manually added to the category.
- ☐ Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category.
- ☐ Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category.

Category will include only unique conditions from the wizard.

Next

You can create and fill categories in several ways:

- Manually
- Based on folder
- Computer-based

برنامه‌ها. این لیست در عملیات | برنامه‌های شخص ثالث | دسته‌بندی‌های برنامه نمایش داده می‌شود و به طور پیش‌فرض خالی است. دسته‌بندی‌های جدید با استفاده از یک ویزارد ویژه ایجاد می‌شوند. سه نوع دسته‌بندی وجود دارد:

- پر کردن دستی - شرایط فقط به صورت دستی اضافه و تغییر می‌کنند. به عنوان مثال، تمام برنامه‌هایی که نام آنها شامل "زامبی" است، یا تمام برنامه‌هایی که با گواهی مشخص شده امضا شده‌اند.
- پر کردن خودکار از یک پوشه - مدیر یک پوشه را انتخاب می‌کند که برای فایل‌های زیر اسکن می‌شود: COM، EXE، DLL، SYS، BAT، PS1، CMD، JS، VBS، REG، MSI، MSC، CPL، HTML، HTM، DRV، OCX و SCR. سرور مدیریت همچنین محتویات این پوشه را به صورت برنامه‌ای بررسی می‌کند، چک‌سام‌های فایل‌های اجرایی (SHA256) را محاسبه می‌کند و لیست معیارهای دسته‌بندی را به‌روزرسانی می‌کند. یک پوشه شبکه که در آن همه برنامه‌های ممنوعه یا مجاز کپی می‌شوند، ممکن است مفید باشد.

- به طور خودکار از دستگاه‌های انتخاب شده پر می‌شود - مدیر یک یا چند رایانه مدیریت شده را انتخاب می‌کند و سرور مدیریت به طور خودکار فایل‌های اجرایی موجود در رایانه‌ها را در دسته‌بندی قرار می‌دهد. به این معنی که می‌توانید یک رایانه مرجع را مشخص کنید که مثلاً همه برنامه‌های مجاز در آن نصب شده‌اند.

در مرحله اول، جادوگر دسته‌بندی جدید از شما نام دسته‌بندی و روش ایجاد را می‌پرسد. اگر از محتوای دسته‌بندی حاصل راضی نیستید و می‌خواهید روش دیگری را انتخاب کنید، باید دسته‌بندی را دوباره ایجاد کنید.

۳. Device Control :

در این بخش، مؤلفه Device Control را بررسی می‌کنیم که به ما امکان می‌دهد اتصال انواع مختلف دستگاه‌ها به رایانه‌های کاربران را تنظیم کنیم.

۳.۱ چرا Device Control ضروری است و چگونه می‌تواند کمک کند؟

Why Device Control is necessary

49

This component manages access to devices and thus helps reduce the attack surface

It can block the entire connection bus or access to specific types of external devices

Manages access to Wi-Fi networks

Allows you to flexibly restrict access to data storage devices based on various criteria:

- Account
- Operation type:
 - Read
 - Modify
- Schedule

You can allow full access to trusted devices and temporary access to other devices upon request

هدف اصلی کامپوننت Device Control از نام آن مشخص است. این کامپوننت به مدیر اجازه می‌دهد تا دستگاه‌های مختلف در شبکه شرکت را رصد کند و در صورت لزوم، استفاده از برخی از آنها را ممنوع کند.

کامپوننت Device Control به مدیر اجازه می‌دهد تا با مشخص کردن اینکه کدام دستگاه‌ها می‌توانند در رایانه‌ها، توسط چه کسی و چه زمانی استفاده شوند، استانداردهای امنیتی شرکت را اجرا کند. قوانین ممکن است برای درایوهای قابل جابجایی، چاپگرها، CD/DVD، اتصالات شبکه غیر شرکتی، Wi-Fi و غیره اعمال شود.

محبوب‌ترین مورد استفاده برای این کامپوننت مسدود کردن درایوهای فلش USB است. کاربر ممکن است یک فایل آلوده را از خانه بیاورد. علاوه بر این، چه به طور تصادفی و چه عمدی، کاربر ممکن است فایل‌هایی را که برای شرکت ارزش تجاری دارند، با خود ببرد.

محدودیت‌ها به جلوگیری از چنین مشکلاتی کمک می‌کنند.

تنظیمات مختلفی برای انواع مختلف دستگاه در دسترس است. حداکثر انعطاف‌پذیری برای انواع دستگاه‌های ذخیره‌سازی زیر ارائه شده است:

- هارد دیسک‌ها
- درایوهای قابل جابجایی
- فلاپی دیسک‌ها
- درایوهای CD/DVD

می‌توانید مشخص کنید که کدام حساب‌ها اجازه دسترسی به دستگاه‌ها را دارند/ ندارند. می‌توانید فقط کپی کردن اطلاعات از دستگاه‌ها را مجاز و نوشتن را ممنوع کنید. همچنین می‌توانید برنامه‌ای را پیکربندی کنید تا دسترسی به دستگاه‌ها فقط در ساعات کاری مجاز باشد.

انواع دیگر دستگاه‌ها فقط می‌توانند مجاز یا مسدود شوند، بدون هیچ تنظیمات انعطاف‌پذیری.

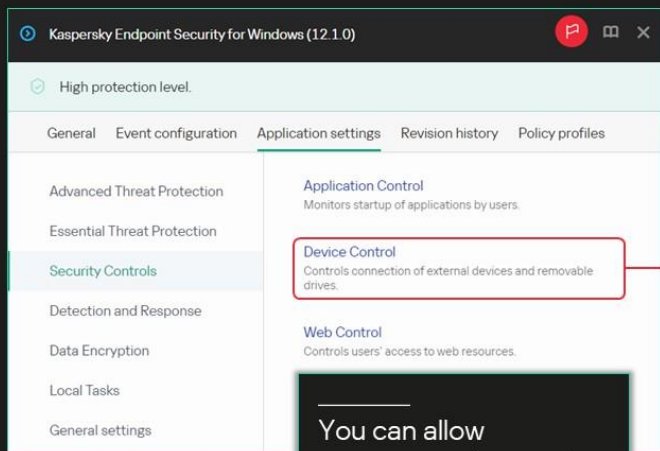
به طور کلی، Device Control می‌تواند یک گذرگاه اتصال را به طور کامل مسدود کند، به این معنی که هر دستگاهی که به یک پورت فیزیکی خاص کامپیوتر متصل است، غیرقابل دسترسی خواهد بود.

۳.۲ پیکربندی Device Control

Device Control در سیاست امنیتی کسپرسکی اندپوینت پیکربندی شده است. از طریق ویژگی‌های کامپوننت، می‌توانید قوانین مربوط به انواع دستگاه، تنظیمات گذرگاه اتصال یا لیست دستگاه‌های مورد اعتماد را باز کنید یا Anti-Bridging را پیکربندی کنید.

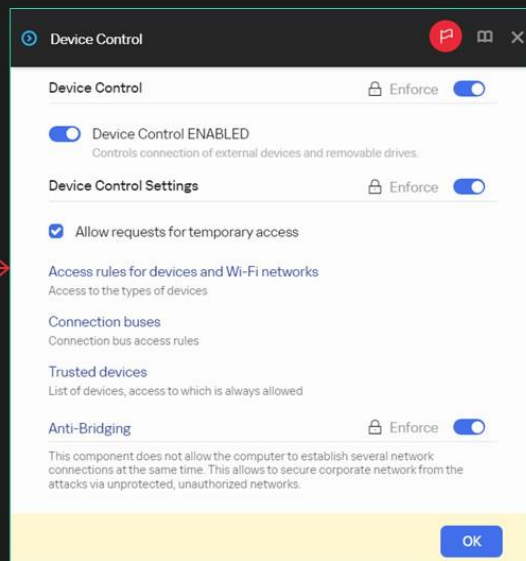
Configure Device Control

50



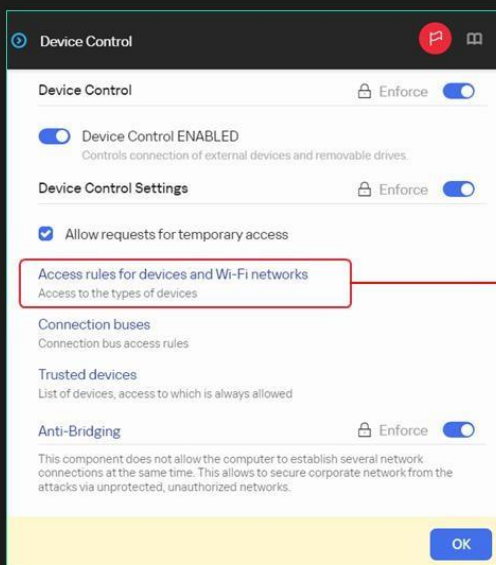
You can allow connecting devices by:

- Type
- Bus



انواع دستگاه:

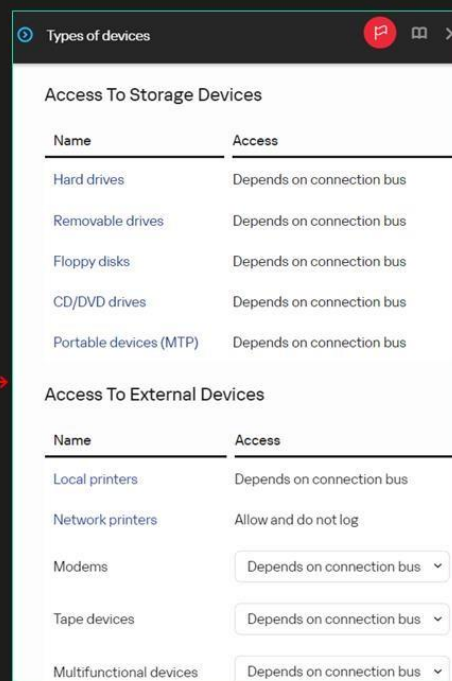
Device types



These conditions have a higher priority than conditions for buses

Rules for printers:

- Local
- Network



قوانین مربوط به دستگاه‌ها اولویت بالاتری دارند. اگر گذرگاه USB ممنوع باشد اما درایوهای قابل جابجایی مجاز باشند، درایوهای فلش USB کار خواهند کرد.

به طور پیش‌فرض، قوانین مربوط به دستگاه‌ها با عملکرد Depends on connection bus کار می‌کنند. به عبارت دیگر، اگر گذرگاه ممنوع باشد، دستگاه نیز ممنوع خواهد بود. برای اجازه اتصال دستگاهی که گذرگاه آن ممنوع است، می‌توانید به سادگی عملکرد قانون را به Allow تغییر دهید.

Kaspersky Endpoint Security فقط اجازه مسدود کردن آن نوع دستگاه‌هایی را می‌دهد که در لیست قرار دارند. شما نمی‌توانید انواع دستگاه جدیدی را به این لیست اضافه کنید.

برای دستگاه‌های ذخیره‌سازی داده، می‌توانید از قوانینی برای تعریف شرایط انعطاف‌پذیر برای دسترسی به دستگاه استفاده کنید. به عنوان مثال، می‌توانید به طور صریح لیست کاربران، نوع عملیات (خواندن/نوشتن) و زمان استفاده را تعریف کنید. می‌توانید این کار را برای موارد زیر انجام دهید:

- هارد دیسک‌ها
- Removable drives
- فلاپی دیسک‌ها
- درایوهای CD/DVD
- دستگاه‌های قابل حمل (MTP)

تمام دستگاه‌های خارجی دیگر را می‌توان مجاز یا کاملاً غیرفعال کرد.

تلفن‌های همراه، تبلت‌ها، پخش‌کننده‌های رسانه و سایر دستگاه‌های قابل حمل، هنگام اتصال به عنوان حامل‌های داده خارجی، می‌توانند به عنوان دستگاه‌های قابل حمل (MTP) یا به عنوان درایوهای قابل جابجایی در نظر گرفته شوند.

دسترسی به شبکه‌های Wi-Fi یک مورد خاص است که بعداً توضیح خواهیم داد.

قوانین مربوط به دستگاه‌های ذخیره‌سازی اطلاعات:

- برای دستگاه‌های ذخیره‌سازی داده، می‌توانید قوانین دسترسی ایجاد کنید و پارامترهای زیر را در یک قانون مشخص کنید:
- کاربران و/یا گروه‌های کاربری که مجاز به استفاده از دستگاه‌ها هستند. می‌توانید حساب‌ها را از دامنه‌ای که رایانه‌ای که کنسول مدیریت به آن تعلق دارد، یا در صورت عدم وجود دامنه، از بین کاربران محلی انتخاب کنید. این قانون روی هر رایانه‌ای که سیاست در آن اعمال می‌شود، کار خواهد کرد. حساب جهانی همه همیشه در دسترس است.

- برنامه دسترسی و نوع عملیات - چه زمانی دسترسی مجاز است و چه زمانی ممنوع است. می‌توانید مجوزهای خواندن و نوشتن را به طور مستقل مدیریت کنید. این برنامه بر اساس ساعت‌ها و روزهای هفته مشخص می‌شود. به عنوان مثال، می‌توانید عملیات خواندن را برای درایوهای قابل جابجایی هر روز کاری از ساعت ۸:۰۰ صبح تا ۹:۰۰ شب برای همه مجاز کنید، اما عملیات نوشتن را فقط برای مدیران و فقط در ساعات کاری مجاز کنید.

اگر چندین قانون با یک کاربر مطابقت داشته باشند، اولویت قانون در نظر گرفته می‌شود. اگر اولویت‌های قانون برابر باشند، محدودکننده‌ترین قانون اعمال خواهد شد.

می‌توانید قوانین را ترکیب کنید. به عنوان مثال، می‌توانید همه درایوهای قابل جابجایی را ممنوع کنید، اما برای مدیران استثنا ایجاد کنید و به آنها اجازه دهید در ساعات کاری از فلش درایوهای USB استفاده کنند.

سیاست تغییر یافته به محض اجرا شدن، عملیاتی می‌شود. برای مثال، اگر حامل‌های داده قابل جابجایی در حالی که کاربر در حال کپی کردن چیزی به یک فلش درایو USB متصل است، مسدود شوند، به محض اجرای سیاست، آن درایو از دسترس خارج شده و عملیات بعدی مسدود خواهد شد.

Rules for devices

Types of devices

Access To Storage Devices

Name	Access
Hard drives	Depends on connection bus
Removable drives	Depends on connection bus
Floppy disks	Depends on connection bus
CD/DVD drives	Depends on connection bus
Portable devices (MTP)	Depends on connection bus

Access To External Devices

Name	Access
Local printers	Depends on connection bus
Network printers	Allow and do not log
Modems	Depends on connection bus

Device Control Settings

Device Access Rules | Logging

Configuring device access rules

☐ Allow
☐ Block
☐ Depends on connection bus
☒ By rules

Users

+ Add Edit X Delete

Priority	Access schedule	Users
0	Default schedule	Everyone
1	Business hours	ABC\Alex

Device Access Rules

Rule of access to devices

Priority: 0

Users: + Add X Delete

ABC\Alex

Schedule for access to devices

+ Add Edit X Delete

Access schedule	Status	Read	Write
Business hours	On	☐	☐

Schedule editor

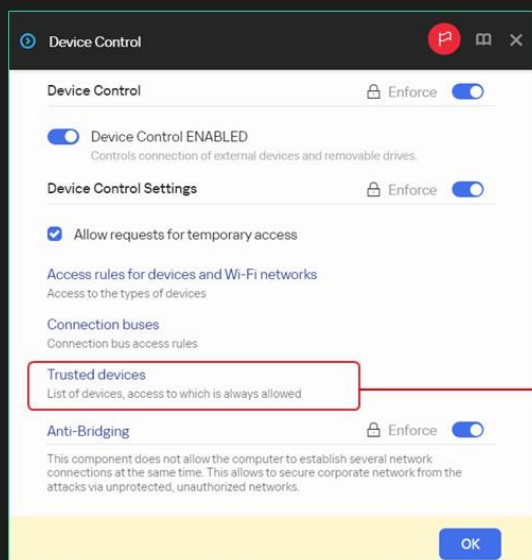
Name: Business hours

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Mo Tu We Th Fr Sa Su

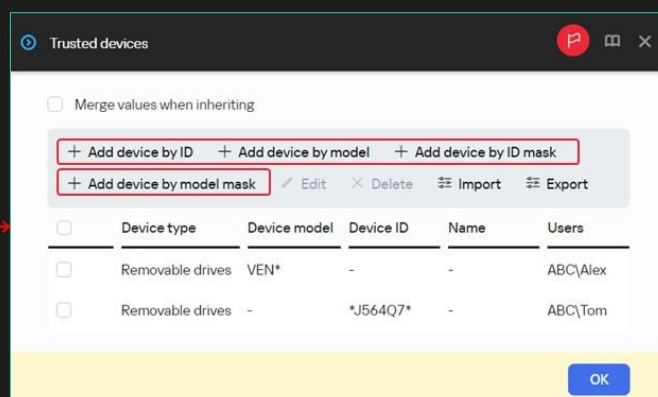
For storage devices, you can flexibly set up a rule with a schedule for a particular user, taking into account types of file operations

Trusted devices



A trusted device can be specified by:

- Device ID
- Device model
- Mask of device ID
- Mask of device model



اگر شرکت درایوهای قابل جابجایی دارد که باید همیشه و همه جا مجاز باشند، ممکن است ارزش داشته باشد که آنها را قابل اعتماد کنید.

دستگاه‌های قابل اعتماد در سیاست امنیتی کسپرسکی اندپوینت، در Device Control | دستگاه‌های قابل اعتماد، مشخص شده‌اند. برای اینکه اطلاعات مربوط به یک دستگاه در یک سیاست قابل دسترسی باشد، ابتدا دستگاه را به رایانه‌ای که کسپرسکی اندپوینت سکیوریتی روی آن نصب شده و مؤلفه Device Control فعال است، متصل کنید. سپس منتظر بمانید تا رویداد اتصال به سرور مدیریت برسد.

یک دستگاه قابل اعتماد را می‌توان با موارد زیر مشخص کرد:

- Device ID -
- Device model -
- Mask of device ID -
- Mask of device model -

دو گزینه اول به شما امکان می‌دهند دستگاهی را که می‌خواهید قابل اعتماد کنید انتخاب کنید. شناسه یا مدل آن به لیست اضافه می‌شود. سرور مدیریت باید دستگاه را در پایگاه داده خود داشته باشد. اگر سرور مدیریت از این دستگاه خاص بی‌اطلاع باشد، نمی‌توانید آن را قابل اعتماد کنید.

همچنین می‌توانید شناسه یا مدل دستگاه را با استفاده از یک ماسک با علامت‌های * یا ? مشخص کنید. در این حالت، مهم نیست که دستگاه برای سرور مدیریت شناخته شده باشد یا خیر، مادامی که مدیر از آن مطلع باشد. می‌توانید شناسه دستگاه را در مدیریت دستگاه ویندوز در قسمت مشخصات دستگاه پیدا کنید. به نظر می‌رسد چیزی شبیه به این باشد:

USBSTOR\DISK&VEN_&PROD_USB_FLASH_DRIVE&REV_1.01\574B17001160&0

هنگام اضافه کردن یک ماسک، می‌توانید بخشی از شناسه را با * یا ؟ جایگزین کنید تا آن را برای چندین دستگاه قابل اجرا کنید. این کار زمانی مفید است که یک شرکت دستگاه‌های زیادی با شناسه‌های مشابه داشته باشد که باید به آنها اعتماد کرد. اضافه کردن یک دستگاه بر اساس مدل نیز می‌تواند در این مورد مفید باشد اگر همه دستگاه‌ها از یک فروشنده و از یک نوع باشند.

۴. Web Control

در این بخش، مؤلفه Web Control را بررسی می‌کنیم که به ما امکان می‌دهد دسترسی کاربر به منابع موجود در اینترنت را تنظیم کنیم.

Why Web Control is necessary and how it works

70

It filters access to the internet according to the internal corporate policy

Scans HTTP and HTTPS traffic regardless of the browser used

What is checked:

- Website address (URL)
- Website contents:
 - Content category – games, adult content, job search, social networks, etc.
 - Type of downloaded files – video, photo, audio, executable files and others
- Who opens the site or downloads a file – you can set up rules for different users
- When the site is opened – you can set up a schedule

هدف از Web Control، فیلتر کردن دسترسی به اینترنت طبق سیاست داخلی شرکت است. معمولاً برای مسدود کردن شبکه‌های اجتماعی، موسیقی، ویدیو، ایمیل‌های وب غیرشرکتی و غیره در ساعات کاری استفاده می‌شود. اگر کاربری سعی کند چنین سایتی را باز کند، بسته به تنظیمات موجود در سیاست، می‌توان اعلانی مبنی بر مسدود شدن دسترسی یا هشدار در مورد یک سایت نامطلوب نمایش داد.

Web Control مشابه سیستم‌های کنترل مختلف عمل می‌کند. مدیر مجموعه‌ای از قوانین مسدود کردن و اجازه دادن را ایجاد می‌کند. ویژگی‌های این قوانین شامل آدرس‌ها یا نوع محتوا، حساب‌های کاربری، زمان‌بندی و اقدام است. ترافیک HTTP و HTTPS اسکن می‌شود.

پیکربندی Web Control

Configure Web Control

Kaspersky Endpoint Security for Windows (12.1.0)

High protection level.

General Event configuration Application settings Revision history Policy profiles

Advanced Threat Protection

Essential Threat Protection

Security Controls

Detection and Response

Data Encryption

Local Tasks

General settings

Application Control
Monitors startup of applications by users.

Device Control
Controls connection of external devices and removable drives.

Web Control
Controls users' access to web resources.

The default rule can:

- Always allow everything (Denylist)
- Deny everything (Allowlist)

Order matters: the first matching rule is applied

By default, nothing is blocked, because the default rule allows everything

Web Control

Enforce ☒

☒ Web Control ENABLED
Controls users' access to web resources.

Web Control Settings ☒ Enforce

Rule List

+ Add × Delete ^ Move up v Move down

≡ Import ≡ Export ≡ Filter

☐	Rule name	State	Actions
☐	Social networks	☒ Active	Block

Default rule

☒ Allow all except the rules list

☐ Deny everything except the rules list

Web Control در سیاست امنیتی کسپرسکی اندپوینت پیکربندی شده است. ترتیب اهمیت دارد: اولین قانون منطبق اعمال می‌شود.

دو قانون پیش‌فرض وجود دارد که بسته به حالت عملیات انتخاب شده اعمال می‌شوند:

- همه را به جز لیست قوانین مجاز کنید - حالت لیست ممنوعه.
- همه چیز را به جز لیست قوانین ممنوع کنید - حالت لیست مجاز.

به طور پیش فرض، از قانون جهانی مجاز کردن همه استفاده می شود و هیچ چیز مسدود نمی شود.

قوانین Web Control

Web Control rules

Rule

Rule name

Social networks

Status

☒ Active
☐ Inactive

Action

☐ Allow
☒ Block
☐ Warn

Content of the filter

☒ By content categories
☐ By types of data

Content categories

Types of data

Addresses

Each rule has the following attributes:

- Rule status
- Action
- Filtering type
- List of addresses
- Users
- Schedule

Rule

Addresses

☒ Apply to all addresses
☐ Apply to individual addresses and/or groups

+ Add Edit Delete

Address

No data

Users

☒ Apply to all users
☐ Apply to individual users and / or groups

+ Add Delete

User or group

No data

Rule schedule

Always

OK Cancel

هر قانون دارای یک نام و ویژگی های زیر است:

— وضعیت قانون:

- فعال
- غیرفعال

به عنوان مثال، می توان یک قانون را برای اهداف آزمایشی ایجاد کرد. اگر قانون در حال حاضر استفاده نمی شود، می توانید آن را به جای حذف غیرفعال کنید.

— اقدام:

- اجازه دادن
- مسدود کردن
- هشدار دادن
- نوع فیلتر:
- بر اساس دسته بندی محتوا

- بر اساس انواع داده‌ها
- پارامتر اختیاری. همچنین می‌توانید از دسته‌بندی‌های از پیش تعریف شده ایجاد شده توسط متخصصان کسپرسی استفاده کنید.
- لیست آدرس‌ها:
- اعمال بر همه آدرس‌ها
- اعمال بر آدرس‌ها و/یا گروه‌های فردی
- کاربران:
- اعمال بر همه کاربران
- اعمال بر کاربران و/یا گروه‌های فردی
- شما می‌توانید قوانین مختلفی را برای کاربران مختلف به صورت انعطاف‌پذیر پیکربندی کنید. به عنوان مثال، منابع انسانی می‌تواند از لینک‌دین بازدید کند، اما همه کارمندان دیگر نمی‌توانند.
- برنامه:
- می‌توانید دوره زمانی اعمال قانون را مشخص کنید، به عنوان مثال، فقط ساعات کاری.

۵. Adaptive Anomaly Control :

در این بخش، مؤلفه Adaptive Anomaly Control را بررسی می‌کنیم که به ما امکان می‌دهد رفتارهای غیرمعمول برنامه‌ها را در رایانه‌های کاربران ردیابی و مسدود کنیم.

Adaptive Anomaly Control

84

This component is designed to detect and block abnormal application behavior

The component monitors activity on the computer for several weeks and sends information about the matched rules to the Administration Server

To detect abnormal behavior, Adaptive Anomaly Control uses a set of rules distributed with the databases

The administrator must process an event: either confirm that the activity is abnormal or add it to exclusions if the activity is legitimate

Non-typical behavior is not always malicious; for this reason, the Adaptive Anomaly Control component works in Smart mode by default

Learning takes place independently on each computer for each rule, meaning that learning will be completed sooner in one place and later in another

Adaptive Anomaly Control شامل مجموعه‌ای از الگوهای فعالیت (روش‌های اکتشافی) است که همراه با پایگاه‌های داده آنتی‌ویروس به‌روزرسانی می‌شوند.

این الگوها رایج‌ترین رفتارهای مشخصه بدافزار را توصیف می‌کنند که ممکن است نشان‌دهنده تلاش‌های احتمالی برای به خطر انداختن امنیت باشند.

با این حال، برخی از این فعالیت‌ها ممکن است برای یک رایانه خاص یا گروهی از رایانه‌ها قانونی باشند. به عنوان مثال، اجرای PowerShell از برنامه دیگری یک اتفاق کاملاً عادی در رایانه یک مدیر یا توسعه‌دهنده است. اسکریپت‌های PowerShell مبهم نیز ممکن است برای خودکارسازی وظایف مختلف در یک شرکت استفاده شوند.

مدیر به Adaptive Anomaly Control دستور می‌دهد که کدام فعالیت برای یک رایانه خاص معمول است و کدام نیست. به همین دلیل است که این مؤلفه ابتدا به طور پیش‌فرض به مدت دو هفته در حالت آموزش (حالت هوشمند) کار می‌کند. در این مدت، فعالیت‌ها را رصد می‌کند، مدیر را در مورد آنها مطلع می‌کند و این مدیر (و نه مؤلفه) است که تصمیم می‌گیرد که آیا یک فعالیت خاص برای رایانه طبیعی است یا خیر.

آموزش در حالت هوشمند برای هر قانون در هر رایانه به طور مستقل انجام می‌شود، به این معنی که در برخی رایانه‌ها زودتر و در برخی دیگر دیرتر تکمیل می‌شود.

۵.۱ پیکربندی Adaptive Anomaly Control :

کامپوننت Adaptive Anomaly Control به طور پیش‌فرض نصب و فعال شده است، اما در ابتدا در حالت هوشمند کار می‌کند. Adaptive Anomaly Control در سیاست امنیتی Kaspersky Endpoint پیکربندی شده است. از ویژگی‌های کامپوننت، می‌توانید گزارش‌ها و لیست قوانین آن را باز کنید.

قوانین Adaptive Anomaly Control

Adaptive Anomaly Control از قوانینی (الگوهای فعالیت) استفاده می‌کند که همراه با پایگاه‌های داده آنتی‌ویروس ارائه می‌شوند، به این معنی که قابل به‌روزرسانی هستند. این قوانین چندین دسته را پوشش می‌دهند:

- فعالیت برنامه‌های اداری
- استفاده از ابزار مدیریت ویندوز (WMI)
- فعالیت موتورهای اسکریپت و چارچوب‌ها
- فعالیت غیرعادی برنامه

هنگامی که مدیر، قوانین را باز می‌کند، پیامی مبنی بر نیاز به تأیید به‌روزرسانی‌ها وجود دارد. این تأیید نسبتاً اطلاعاتی است و بر عملکرد کامپوننت تأثیری ندارد. با این حال، مدیر فقط پس از کلیک بر روی دکمه تأیید به‌روزرسانی‌ها می‌تواند یک استثنا به یک قانون اضافه کند.

اگر بعداً یک قانون جدید اضافه شود، پیام تأیید به‌روزرسانی دوباره ظاهر می‌شود تا توجه مدیر را جلب کند.

قوانین دارای تنظیمات زیر هستند: وضعیت روشن/خاموش، حالت عملکرد هوشمند/مسدود/اعلان، و موارد استثنا. می‌توانید حالت مسدود کردن یا اعلان را برای هر قانون مشخص کنید. به طور پیش‌فرض، حالت هوشمند فعال است.

Configure Adaptive Anomaly Control

85

Kaspersky Endpoint Security for Windows (12.1.0)

High protection level.

General Event configuration Application settings Revision history Policy profiles

Advanced Threat Protection

Essential Threat Protection

Security Controls

Detection and Response

Data Encryption

Local Tasks

General settings

Application Control

Monitors startup of applications by users.

Device Control

Controls connection of external devices and removable drives.

Web Control

Controls users' access to web resources.

Adaptive Anomaly Control

This component detects and blocks abnormal behavior of applications.

File Integrity Monitor

Tracks actions performed with the specified files and folders that may indicate a security breach on the protected device.

Log Inspection

Monitors the integrity of the protected environment based on the Windows Event Log inspection results.

By default, Adaptive Anomaly Control is enabled and works in Smart mode

Adaptive Anomaly Control

Enforce ☒

☒ Adaptive Anomaly Control ENABLED

This component detects and blocks abnormal behavior of applications.

Reports

Report on Adaptive Anomaly Control rules state

Report on triggered Adaptive Anomaly Control rules

Rules

Enforce ☒

Rules

The process is fully automated and does not require manual set up of the applications, however, it is possible to set up the rules that comply with the company's security policy