معرفی کسپرسکی

شرکت کسپرسکی در سال ۱۹۹۷ توسط یوجین کسپرسکی در کشور روسیه، و با هدف ارائه نرم‌افزارهای امنیتی ویژه سیستم‌های کامپیوتری تاسیس شد. اطلاعات تهدید عمیق و جامع این شرکت در کنار تخصص بالای کارشناسان آن در زمینه‌ی امنیت، دائماً به توسعه‌ی راهکارها و سرویس‌های نوآورانه‌ی امنیتی منجر می‌شود که از کسب‌وکارها، زیرساخت‌های حیاتی، دولت‌ها و مشتریان مختلف در سراسر جهان حفاظت می‌کنند. مجموعه‌ی جامع محصولات امنیتی این شرکت، علاوه بر راهکارهای پیشرو امنیت اندپوینت، تعداد زیادی از راهکارهای امنیتی تخصصی را نیز شامل می‌شود که با تهدیدات دیجیتال پیشرفته‌ی امروزی که همواره در حال تغییر و تکامل هستند، مبارزه می‌کنند. در حال حاضر بیش از ۴۰۰ میلیون کاربر توسط کسپرسکی محافظت می‌شوند و این شرکت به بیش از ۲۵۰،۰۰۰ مشتری سازمانی در سراسر دنیا کمک می‌کند از ارزشمندترین دارایی‌های خود حفاظت کنند. این شرکت جوایز پرشماری را از سایت‌های رتبه‌بندی و مقایسه‌ی آنتی‌ویروس دریافت کرده است. همان طور که پیش از این نیز اشاره شد، شرکت کسپرسکی راهکارها و سرویس‌های بسیار متنوعی را برای نیازهای مختلف و مشتریان متفاوت ارائه می‌کند. چند نمونه از محصولات این شرکت عبارتند از:

- Kaspersky Endpoint Security for Business
- Kaspersky Endpoint Security Cloud
- Kaspersky Endpoint Security Cloud Plus
- Kaspersky Endpoint Detection and Response
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Security for Internet Gateway
- Kaspersky Sandbox
- Kaspersky Anti Targeted Attack Platform
- Kaspersky Managed Detection and Response
- Kaspersky Embedded Systems Security

محصول آنتی‌ویروس سازمانی کسپرسکی، یا Endpoint Security for Business، یکی از محصولات قدرتمند این شرکت است که امکانات فراوانی را در اختیار سازمان‌ها قرار داده و سطح بی‌نظیری از امنیت را برای آن‌ها به ارمغان می‌آورد، و جوایز و گواهینامه‌های متعدد این محصول از معتبرترین مراجع ارزیابی مستقل نیز گواه این ادعاست. چند نمونه از جوایز این محصول در سال ۲۰۲۰ عبارتند از:

جایزه سالانه بهترین راهکار حفاظت از اندپوینت در سال 2020 از SE Labs

گواهینامه حفاظت پیشرفته از اندپوینت از NSS Labs، v.4

دریافت بالاترین درجه حفاظتی SE Labs (نمره AAA) در هر چهار سه‌ماهه‌ی سال ۲۰۲۰ و کسب بالاترین رتبه‌بندی در سه آزمون از چهار آزمون

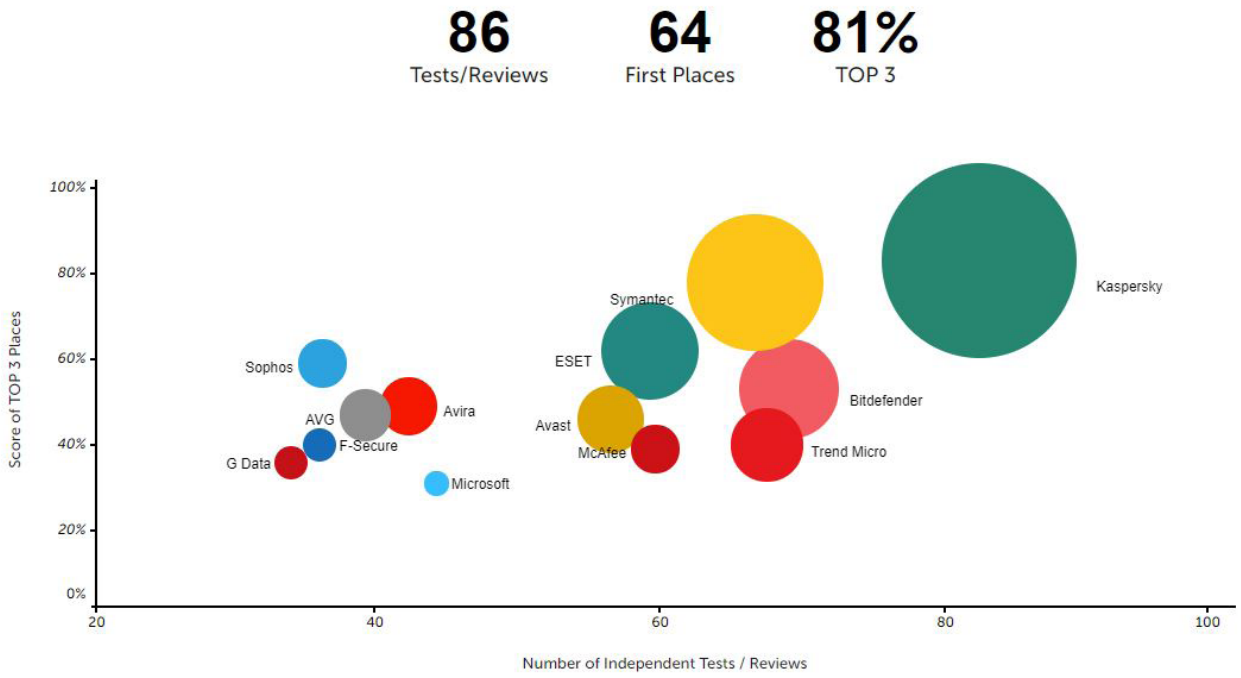
دریافت گواهینامه VB100 از VirusBulletin در فوریه و آپریل 2020

دریافت گواهینامه حفاظت در برابر تهدیدات پیشرفته از AV-Comperatives در نیمه‌ی اول و دوم ۲۰۲۰، با سطح بالای حفاظت در برابر حملات پیشرفته مانند تهدیدات فایل‌لس و اکسپلویت‌ها

کسب گواهینامه‌ی دوماهه AV-Test در تمامی دوماهه‌های سال 2020

دریافت گواهینامه امنیت کسب‌وکار از AV-Comperatives در نیمه‌ی اول و دوم ۲۰۲۰، با سطح بالای حفاظت در برابر تهدیدات واقعی با کمترین میزان تشخیص مثبت کاذب

در سال ۲۰۱۹ محصولات کسپرسکی در ۸۶ آزمون و بازبینی مستقل شرکت کردند. محصولات کسپرسکی در ۶۴ ارزیابی رتبه اول و در ۷۰ ارزیابی جزو سه محصول برتر قرار گرفتند. معیار TOP۳ جمع امتیاز به‌دست‌آمده توسط بیش از ۸۰ تامین‌کننده امنیتی شناخته‌شده در معتبرترین تست‌ها و بازبینی‌های مستقل را نشان می‌دهد. ارزیابی مداوم عملکرد چندین محصول در تست‌های مختلف، نسبت به یک بار ارزیابی در تنها یک تست، نتایج معنادارتر و قابل اطمینان‌تری را به دست می‌دهد. این نتایج را می‌توانید در نمودار زیر هم ببینید:



در ادامه‌ی این مقاله به بررسی Kaspersky Endpoint Security for Windows (که از این به بعد Kaspersky Endpoint Security نامیده می شود) خواهیم پرداخت.

این محصول با تکیه بر ماژول ها و تکنولوژی های مختلف، از رایانه در برابر انواع تهدیدات، حملات شبکه و فیشینگ به طور کامل محافظت می‌کند. در این محصول هر نوع تهدید توسط یک ماژول اختصاصی کنترل می شود. یکی از مزایای کلیدی این محصول، امکان فعال‌کردن، غیرفعال‌کردن و پیکربندی مستقل و جداگانه‌ی ماژول‌هاست که قدرت کنترل و انعطاف‌پذیری زیادی را در اختیار ادمین‌های شبکه و کارشناسان امنیت قرار می‌دهد. در ادامه به بررسی ماژول های کنترلی و حفاظتی محصول Endpoint Security کسپرسکی می پردازیم.

ماژول‌های کنترلی

Application Control

این ماژول فعالیت های کاربر در خصوص اجرای برنامه ها را مانیتور کرده و شروع به کار برنامه ها توسط کاربران را تنظیم می کند. ادمین می تواند این کار را از طریق انتخاب فایل نصبی برنامه، انتخاب از دسته‌بندی‌های[1] موجود در مرکز امنیت کسپرسکی، انتخاب از رجیستری کامپیوتر، انتخاب فایل MSI، انتخاب Metadata از فایل های موجود در یک فولدر، انتخاب مجوز[2] فایل ها از یک فولدر، انتخاب هش فایل و یا نوع درایورها انجام دهد. هر یک از موارد فوق تنظیمات جداگانه ای در پالیسی Endpoint Security دارند. درست مثل قوانین[3] فایروال، هر قانونی که در خط بالاتری باشد، اولویت اجرای بیشتری دارد.
قوانین موجود در این ماژول می توانند سه عملکرد کلی داشته باشند:

- **On**: به این معنی که از آن قانون وقتی Application Control فعال است، استفاده شود.
- **Off**: به این معنی است که این قانون در زمان فعال بودن Application Control غیرفعال است.
- **Test**: این وضعیت نشانگر این است که Endpoint Security به برنامه‌هایی که قوانین با آن‌ها مطابقت دارد اجازه فعالیت می دهد ولی گزارشات و اطلاعات مربوط به فعالیت این دسته از برنامه‌ها را در بخش گزارش ثبت می کند.

برای مثال ادمین مرکز امنیت کسپرسکی می تواند دسترسی تمام کاربران بجز ادمین ها را به نرم افزارهای مانیتورینگ شبکه مسدود کند.

Device Control

با استفاده از این ماژول می‌توان محدودیت هایی روی دستگاه های ذخیره سازی اطلاعات مثل هارد کامپیوتر، درایو های قابل حمل مثل فلش و هارد اکسترنال و درایورهای CD/DVD، تجهیزات انتقال داده مثل مودم و کارت شبکه، تجهیزات تبدیل‌کننده‌ی اطلاعات مثل پرینتر، دوربین (Webcam)، موبایل و رابط های بلوتوث اعمال کرد. این محدودیت می تواند بر اساس یک دستگاه و یا یک کاربر تنظیم شود. برای مثال یک فلش فقط توسط یک کاربر (در شبکه ی دامین) قابل استفاده باشد. همچنین می توان محدودیت هایی روی درگاه های ورودی Infrared، FireWire ، Serial،USB و PCMCIA نیز اعمال کرد.
در این ماژول می‌توان دستگاه خاصی را بر اساس مدل، ID و PID به لیست امن اضافه کرد. اگر چندین دستگاه با شناسه (ID) مشابه استفاده می کنید، می توان با استفاده از قابلیت mask در تنظیمات این ماژول، آنها را به لیست امن اضافه کرد.
اگر از چندین دستگاه با VID یا PID مشابه استفاده می کنید (به عنوان مثال دستگاه هایی از یک سازنده‌ی مشترک)، می توان با استفاده از mask و کاراکتر * آنها را به لیست امن اضافه کرد.

- در صورت نصب Endpoint Security روی کامپیوترهایی که از نسخه‌های Work Station ویندوز استفاده می‌کنند این ماژول در دسترس است؛ تنظیمات این ماژول روی سرورهای ویندوزی متفاوت است و محدودیت هایی برای اجرای آن وجود دارد.

Web Control

با استفاده از این ماژول می توان محدودیت هایی بر اساس محتوا، دسته بندی، آدرس وبسایت ها و یا هر سه روش برای گروه های متفاوت کاربران در بازه های زمانی دلخواه ایجاد کرد که به کاهش ترافیک و جلوگیری از هدررفت ساعات کاری کمک می-کند. برای مثال در زمان ساعت کاری هیچ کاربری نتواند سایت هایی مثل دیجیکالا و یا سایت های با محتوای فیلم را باز کند. همچنین می توان این ماژول را به نحوی تنظیم کرد که در زمانی که کاربر یا کاربرانی بخواهند از سایت خاصی بازدید کنند، دسترسی آن آزاد یا محدود باشد و یا هنگام بازکردن وبسایت، صرفا یک پیغام اخطار توسط کسپرسکی نمایش داده شود. همچنین می توان دسترسی به اینترنت توسط یک مرورگر را در زمان خاصی محدود کرد.

- این ماژول از پروتکل RTMP پشتیبانی نمی کند.

1 - Category
2 - Certificate
3 - Firewall Rules

Adaptive Anomaly Control

این ماژول در ابتدای کار از قوانین خاصی که توسط متخصصین شرکت کسپرسکی و بر اساس فعالیت های مخربی که قبلا شناسایی شده اند، برای ردیابی رفتارهای مشکوک در شبکه استفاده می کند که همراه با هر به‌روزرسانی Kaspersky Endpoint Security به‌روز می گردند.
سپس با استفاده از هوش مصنوعی خود، فعالیت های معمول کاربران یک شبکه را طی یک بازه ی زمانی خاص (معمولا دو هفته) فراگرفته و رویدادهای مشکوک را به مرکز امنیت کسپرسکی ارسال می کند. اگر در این زمان هیچ Rule یا قانونی در مرکز مدیریت کسپرسکی ایجاد نشود، این ماژول آن را مشکوک فرض خواهد کرد و کسپرسکی تمام اقدامات مربوط به آن قانون را مسدود می کند. اگر فعالیتی غیر از آنچه که کسپرسکی طی این زمان فراگرفته است توسط یک کاربر و یا سیستم صورت گیرد، آنرا کنترل و در نهایت مسدود می کند.
قوانینی که کسپرسکی طی این مدت فرا می گیرد در مخزن مرکز امنیت کسپرسکی به نام Triggering of rules in Smart Training state قابل مشاهده است. ادمین مرکز امنیت کسپرسکی می تواند این گزارشات را تجزیه و تحلیل کرده و در نهایت انتخاب کند که در زمان بروز هر فعالیت واکنش مرکز امنیت کسپرسکی چگونه باشد: مسدود یا مجاز.
زمان حالت فراگیری (Smart Training mode) می تواند افزایش یابد. اما اگر ادمین در این خصوص تنظیمی انجام ندهد، Endpoint Security مجدد در حالت Smart Training فعالیت می کند سپس این محدودیت زمانی مجدداً تنظیم خواهد شد و قوانین قبلی حذف می گردند.
برای مثال اگر فایلی هم‌نام یکی از فایل های اصلی سیستمی بود، مسدود می گردد. قوانین این ماژول در پالیسی های مرکز امنیت کسپرسکی قابل مشاهده و تنظیم هستند.

- این ماژول فقط در نسخه ی Advance و Total قابل استفاده است.

ماژول های حفاظتی

ماژول های زیر ماژول های حفاظتی Kaspersky Endpoint Security for Windows هستند:

Behavior Detection

این ماژول اطلاعات مربوط به نحوه ی عملکرد برنامه ها در کامپیوتر را دریافت کرده و آن را در اختیار سایر ماژول ها حفاظتی قرار می دهد تا عملکرد آنها بهبود یابد. این مولفه بر اساس آنالیز BSS (Behavior Stream Signatures) یا توابع جریان رفتاری برنامه ها فعالیت می کند؛ اگر رفتاری مشابه فعالیت باج‌افزارها شناسایی کند، می تواند آن را حذف کند، فعالیت آن را متوقف کند و یا اطلاعات مربوط به فعالیت بدافزار را به لیست تهدیدات فعال در مرکز امنیت کسپرسکی (Active threat) اضافه کند. علاوه بر این، می تواند از پوشه های اشتراکی در برابر رمزگذاری خارجی محافظت کند و ارتباط را به میزان مدتی که ادمین تعیین کرده (بر حسب دقیقه)، مسدود کند.

Exploit Prevention

این ماژول، فعالیت برنامه های آسیب پذیر و فایل های اجرایی آن را کنترل می کند و اگر تشخیص دهد یک فایل اجرایی توسط شخص دیگری به‌جز کاربر اجرا شده است، آن را شناسایی و مسدود می کند. هم‌چنین تمام فعالیت های خارجی را که سعی در دسترسی به فعالیت های سیستمی (System Process) دارند، مسدود می کند. این ماژول به صورت پیشفرض فعال است.

Host Intrusion Prevention (HIPS) (پیشگیری از نفوذ به میزبان)

این ماژول بر اساس قوانینی که ادمین برای گروه های مختلف برنامه ها تنظیم می کند، از فعالیت و دسترسی برنامه هایی که ممکن است برای سیستم عامل و اطلاعات کاربر خطرناک باشند، جلوگیری می کند.
می توان این ماژول را به گونه ای تنظیم کرد که هر برنامه، دسترسی مشخصی به فایل های کاربر و منابع سیستم عامل داشته باشد. البته شایان ذکر است که ارتباط برنامه ها با شبکه توسط ماژول فایروال کنترل می شود.
زمانی که یک برنامه و یا یک process اجرا می شود، این ماژول میزان امنیت آن را با استفاده از پایگاه داده ی آنتی ویروس و- در صورت اتصال به اینترنت- پایگاه دادهی ابری کسپرسکی بررسی می کند و سپس در ۴ گروه به نام های امن (Trusted)، محدودیت کم (Low restricted)، محدودیت زیاد (High Restricted) و ناامن (Untrusted) قرار می دهد که هر کدام right یا مجوزهای مختص خودشان را دارند. دفعهی بعدی که برنامه فعالیت کند، Kaspersky Endpoint Security یکپارچگی (integrity) برنامه را بررسی کرده و اگر بدون تغییر باشد، ماژول از مجوزهای فعلی آن استفاده می کند در غیر این صورت تنظیمات و مجوزها به حالت اولیه برمی گردند و نیاز است مجدد تنظیم شود.
به عنوان مثال اگر یک نرم افزار بدون امضای دیجیتال در شبکه موجود باشد و ادمین آن را در گروه Trusted قرار داده باشد، پس از ارتقا و به‌روزرسانی، مجدداً به یکی از گروه های Restricted منتقل می شود.
- این ماژول از Audio stream نیز محافظت می کند ولی محدودیت هایی دارد.

Remediation Engine

این ماژول به Kaspersky Endpoint Security اجازه می دهد اقدامات انجام شده توسط بدافزار در سیستم عامل را خنثی کرده به حالت اول برگرداند. هنگام بازگرداندن فعالیت بدافزار در سیستم عامل، Kaspersky Endpoint Security انواع فعالیت های مخرب را کنترل می کند:
- **File activity**: فایل های مخربی که توسط بدافزار روی تمام دستگاه‌های ذخیره‌سازی (بجز درایورهای شبکه) ایجاد شده‌اند حذف می‌شوند و علاوه بر این، اگر برنامه‌ای توسط بدافزار آسیب دیده باشد و فایل‌هایی ایجاد کرده باشد، آن فایل‌ها نیز حذف می‌شوند. هم‌چنین فایل هایی را که توسط بدافزار اصلاح یا حذف شده اند بازیابی می کند.

ماژول می تواند فایلهای با پسوندهای زیر را بازیابی کند:

odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, .p7b, p7c, 1cd

این ماژول محدودیت هایی نیز دارد:

۱.فایل های دستگاه هایی که فقط File System با فرمت NTFS و FAT۳۲ دارند قابل بازیابی اند.
۲. امکان بازگردانی اطلاعات درایوهای شبکه و دیسک های CD/DVD وجود ندارد.
۳. امکان بازگردانی فایل هایی که با Encryption File System (EFS) رمزگذاری شده اند وجود ندارد.
۴.نمی تواند تغییرات فایل های هسته ی سیستم عامل را کنترل کند.
۵. تغییرات ایجاد شده روی فایل ها از طریق رابط شبکه را کنترل نمی کند (به عنوان مثال، اگر فایلی در یک پوشه مشترک ذخیره شده باشد و فرایند از راه دور از رایانه دیگری شروع شود).

- **Registry activity**: فقط کلیدهای رجیستری ایجاد شده توسط بدافزار را حذف می کند ولی کلیدهای رجیستری را که توسط بدافزار اصلاح یا حذف شده اند بازیابی نمی کند.
- **System activity**: پروسه هایی را که توسط بدافزار شروع شده‌اند و یا بدافزار در آنها نفوذ کرده است متوقف می کند ولی پروسه هایی را که توسط بدافزار متوقف شده اند فعال نمی کند.
- **Network activity**: فعالیت های شبکه ای بدافزار را مسدود می کند.

بازگردانی اقدامات به وسیله‌ی ماژول های File Threat Protection و Behavior Detection و نیز در زمان اجرای اسکن ویروس انجام می شود. این امر فقط روی فایل های مشخصی که توسط بدافزار دچار تغییر شده‌اند اثر می گذارد و تاثیری روی یکپارچگی سایر اطلاعات کاربر و سیستم عامل ندارد.

File Threat Protection

به صورت پیش‌فرض این ماژول حافظه‌ی RAM، تمام فایل های باز، ذخیره‌شده و فعال، اعم از فایل های درایوهای رایانه و درایوهای متصل به آن را اسکن می کند و با استفاده از پایگاه داده‌ی آنتی ویروس کسپرسکی، پایگاه داده‌ی ابری کسپرسکی (در صورت اتصال به اینترنت)، تجزیه و تحلیل امضای بدافزارها و هوش مصنوعی خود، از فایل ها و سرویس ها در برابر تهدیدات محافظت کرده و در صورت شناسایی بدافزار، آن را پاکسازی، حذف و یا مسدود می کند.

پیش از پاکسازی فایل، کسپرسکی یک نسخه ی پشتیبان از فایل تهیه می کند. اگر فایل با موفقیت پاکسازی شود این نسخه ی پشتیبان به صورت خودکار حذف می گردد و فایل در فولدر خود مجدد در دسترس قرار خواهد گرفت؛ در غیر این صورت فایل حذف خواهد شد. اگر کد مخربی در فایلی که جزو برنامه‌های Windows Store است شناسایی شود، بدون تهیه نسخه ی پشتیبان فوراً حذف خواهد شد.

- اگر چند فایل با نام یکسان و محتوای مختلف در یک پوشه به بخش Backup مرکز امنیت کسپرسکی منتقل شوند، فقط آخرین فایلی که به این بخش منتقل شده است، قابل بازیابی خواهد بود.

لازم به ذکر است که می‌توان ماژول File Thread Pro را به‌گونه‌ای پیکربندی کرد که در زمان‌های مشخص یا هنگام کار با برنامه‌های خاصی متوقف شود.

سه سطح امنیت Recommended، High و Low در این ماژول وجود دارد:

- **High**: زمانی که این سطح امنیتی انتخاب می شود، File Threat Protection دقیق ترین کنترل را روی تمام فایل-های باز، ذخیره‌شده و در حال اجرا، انجام می دهد. انواع فایل ها در همه ی هارددرایوها، درایوهای اکسترنال و درایوهای شبکه، آرشیوهای جدید، بسته های نصبی جدید و تمام فرمت های مایکروسافت آفیس را اسکن می کند.
- **Recommended**: این ماژول فقط فرمت های مشخصی از فایل های جدید و تغییر یافته را در همه‌ی هارددرایوها، درایوهای اکسترنال و درایوهای شبکه کامپیوتر و تمام فرمت های ماکروسافت آفیس در حالت Smart Mode اسکن می کند.
- **Low**: این حالت سریع ترین روش اسکن بوده و فقط فایل هایی با پسوند مشخص را که به تازگی ایجاد شده و یا تغییر یافته‌اند روی تمام هارددرایوها، درایوهای اکسترنال و درایوهای شبکه کامپیوتر اسکن می کند.

ادمین می تواند در هر زمان تنظیمات را تغییر دهد. علاوه بر مواردی که گفته شد، کسپرسکی از چند روش و تکنولوژی متفاوت برای این کار استفاده می کند.

روش Heuristic Analysis برای شناسایی تهدیدهایی ساخته شده است که با استفاده از اطلاعات فعلی پایگاه داده کسپرسکی قابل شناسایی نباشند. این روش، فایل هایی را که توسط ویروس های ناشناخته آلوده شده‌اند نیز شناسایی می کند و در سه حالت light، Medium و Deep قابل تنظیم است.

دو فناوری دیگر به نام های iSwift و iChecker نیز به Kaspersky Endpoint Security کمک می کنند تا اسکن فایل-ها را با سرعت بیشتری انجام دهد.

Web Threat Protection

این ماژول با استفاده از پایگاه داده‌ی ابری کسپرسکی، پایگاه داده ی آنتی‌ویروس کسپرسکی و آنالیز رفتاری، از دانلود فایل-های مخرب از اینترنت جلوگیری کرده و وبسایت های مخرب و فیشینگ را مسدود می کند. این ماژول ترافیک های HTTPS، HTTP و FTP و نیز URL و IP را اسکن می کند. می توان پورت یا پورت هایی را که توسط Kaspersky Endpoint Security نظارت می شوند انتخاب کرد. هم‌چنین می توان آدرس وبسایت های مشخصی را به لیست امن اضافه کرد تا ترافیک آن ها اسکن نشود.

Mail Threat Protection

این ماژول پیوست های ایمیل های ورودی و خروجی را برای شناسایی تهدیدات و لینک های مخرب و فیشینگ اسکن می کند. این ماژول به صورت پیش‌فرض در RAM کامپیوتر فعال بوده و کلیه پیام های دریافتی یا ارسال‌شده با استفاده از پروتکل های POP۳، SMTP، IMAP و NNTP و نیز Microsoft Office Outlook mail client را اسکن می کند.
می توان محدودیتی برای اسکن فایل هایی بیشتر از ظرفیت مد نظر و زمان اسکن پیوست ایمیل ها اعمال کرد. هم‌چنین می-توان ماژول را به گونه ای تنظیم کرد که در زمان شناسایی آلودگی و تهدید، آنرا غیرفعال و پاک کرده و یا مسدود کند.
برنامه های مخرب را ممکن است به صورت پیوست در ایمیل پنهان شده باشند. می توان فیلترکردن را براساس نوع پیوست ایمیل به نحوی تنظیم کرد تا فایل های مشخص‌شده به طور خودکار تغییر نام داده یا حذف شوند.

Network Threat Protection

این ماژول ترافیک ورودی شبکه را برای شناسایی حملات شبکه اسکن می کند. وقتی Kaspersky Endpoint Security یک حمله از طریق شبکه به کامپیوتر کاربر را تشخیص دهد، اتصال آن به کامپیوتر مهاجم در بستر شبکه را مسدود می کند. ادمین مرکز امنیت کسپرسکی می‌تواند مدت مسدودبودن ارتباط با کامپیوتر مهاجم را تغییر دهد. به صورت پیش‌فرض این زمان ۶۰ دقیقه است.
این ماژول آسیب پذیری های موجود در پروتکل ARP را نیز ردیابی کرده و از کامپیوتر در برابر حملات Mac spoofing محافظت می کند. نوع واکنش کسپرسکی به این حملات را می توان در سه حالت عدم ردیابی، نمایش اعلانات و یا مسدودسازی تنظیم کرد.
لیست حملاتی که توسط این ماژول شناسایی می شود، با هربار به‌روزرسانی پایگاه داده، به‌روز می شوند.

BadUSB Attack Prevention

برخی ویروس ها Firmware دستگاه های USB را به نحوی تغییر می دهند تا دستگاه USB به عنوان کیبورد شناسایی شود. در نتیجه، ویروس ممکن است دستوراتی را با بهره‌گیری از اختیارات حساب کاربر برای دانلود بدافزار به دستگاه هدف ارسال کرده و اجرا کند. این قابلیت از این روش حمله جلوگیری می کند.
هنگامی که یک دستگاه USB به رایانه متصل شده و توسط سیستم عامل به عنوان یک کیبورد شناسایی می شود، کسپرسکی یک کد تصادفی تولید کرده و از کاربر می خواهد کد عددی تولیدشده را با استفاده از کیبوردی که به تازگی متصل شده، وارد کند. این روش به عنوان مجوز کیبورد شناخته می شود.

اگر کد به درستی وارد شده باشد، کسپرسکی پارامترهای شناسایی (VID / PID) صفحه کلید و تعداد درگاهی را که به آن متصل شده است) در لیست کیبوردهای مجاز ذخیره می کند. پس از ثبت مجوز، هنگام اتصال دوباره‌ی کیبورد یا پس از راه‌اندازی مجدد سیستم عامل، دیگر نیازی به تکرار مرحله‌ی شناسایی کیبورد نیست. هنگامی که کیبورد مجاز به درگاه USB متفاوتی از کامپیوتر وصل شود، کسپرسکی مجددا یک درخواست برای صدور مجوز این کیبورد نشان می دهد. اگر کد سه بار اشتباه وارد شود، این USB مسدود می شود و با ریست سیستم عامل می توان مجدد عملیات دریافت مجوز را اجرا کرد.
این ماژول به صورت پیش‌فرض همراه با Kaspersky Endpoint Security for Windows نصب نمی شود. برای نصب آن می بایست قبل از نصب، ماژول را انتخاب کرد و یا پس از نصب، ماژول های نرم افزار کسپرسکی را تغییر داد.

AMSI Protection

ماژول Antimalware Scan Interface که به اختصار AMSI نامیده می شود، برای پشتیانی از رابط اسکن Antimalware ماکروسافت در نظر گرفته شده است. این ماژول به برنامه های third-party با پشتیبانی AMSI اجازه می-دهد تا اشیا (مثل اسکرپیت‌های PowerShell) را برای اسکن اضافی به Kaspersky Endpoint Security ارسال کرده و نتایج این اسکن را دریافت کنند. این ماژول فقط کار اسکن و شناسایی تهدید را انجام می دهد و نرم افزار third-party پس از دریافت اخطار، اجازه ی انجام اقدامات مخرب را نمی دهد.
لازم به ذکر است که برای هر برنامه سقف درخواست وجود دارد و اگر یک برنامه در یک بازه زمانی تعداد درخواستی بیش از حداکثر مجاز ارسال کند، ممکن است AMSI Protection درخواست‌های برنامه را رد کند. Kaspersky Endpoint Security اطلاعات مربوط به درخواست ردشده از برنامه ثالث را به سرور کسپرسکی ارسال می کند. البته می‌توان پیکربندی را به گونه‌ای انجام داد که هیچ‌کدام از درخواست‌های یک برنامه‌ی خاص رد نشوند.

استفاده از AMSI Protection برای اسکن پرونده‌های مرکب:
یک روش معمول برای پنهان‌کردن بدافزارها، جاسازی آن ها در پرونده های ترکیبی مانند بایگانی ها است. برای شناسایی بدافزارهایی که از این طریق پنهان شده‌اند، باید فایل مرکب را از حالت بسته خارج کنید که ممکن است اسکن را کُندتر کند. با استفاده از امکانات این ماژول می توان انواع فایل های مرکب را که باید اسکن شوند محدود کرد، تا سرعت اسکن افزایش یابد.

Firewall

این ماژول هنگام کار در اینترنت یا شبکه Local، ارتباطات غیرمجاز با کامپیوتر را مسدود می کند و فعالیت مرتبط با شبکه ی برنامه های موجود در کامپیوتر را کنترل می کند. با این کار می‌توانید از شبکه سازمان خود در برابر سرقت هویت و حملات دیگر محافظت کنید. این ماژول با کمک پایگاه داده‌ی آنتی‌ویروس، سرویس ابری Kaspersky Security Network و قوانین از پیش تعریف‌شده‌ی شبکه، از کامپیوتر محافظت می کند.

می توان قوانین یا Ruleهای شبکه را در سطوح زیر تنظیم کرد:

- **Network Packet Rules:**

این قوانین بر اساس شبکه، و بدون توجه به کاربرد آن محدودیت هایی را اعمال می کنند. این قوانین ترافیک ورودی و خروجی شبکه را بر مبنای پروتکل ها و پورت های خاص محدود می کنند. در کنسول مدیریت کسپرسکی قوانین از پیش تعیین شده‌ای وجود دارد که می توان از آنها استفاده کرد. هم‌چنین می توان قوانین جدیدی به این لیست اضافه کرد.

- **Application Network Rules:**

این قوانین، با توجه به ویژگی های پکت‌هایی که توسط برنامه ارسال یا دریافت شده است، محدودیت هایی برای فعالیت یک برنامه خاص در شبکه اعمال می کنند.

پیش‌تر توضیح دادیم که دسترسی کنترل‌شده‌ی برنامه ها به منابع سیستم عامل، پروسس‌ها و داده های شخصی توسط ماژول Host Intrusion Prevention با توجه به مجوزهای برنامه (application rights) فراهم می شود.

در اولین راه اندازی برنامه، فایروال اقدامات زیر را انجام می دهد:

۱. با استفاده از پایگاه داده ی آنتی‌ویروس، امنیت برنامه را بررسی می کند.

۲. میزان امنیت برنامه را در شبکه امنیت کسپرسکی (KSN) بررسی می کند.

۳. مشابه ماژول Host Intrusion Prevention، برنامه را در یکی از ۴ گروه امن (Trusted)، محدودیت کم (Low Restricted)، محدودیت زیاد (High Restricted) و یا نا امن (Untrusted) قرار می دهد.

۴. با توجه به گروهی که برنامه در آن قرار گرفته است، محدودیت‌هایی بر فعالیت برنامه در شبکه اعمال می کند.

- نمی توان یک نرم افزار را فقط در ماژول فایروال و یا ماژول پیشگیری از نفوذ میزبان (Host Intrusion Prevention) قرار داد و باید نرم افزار در هر دو ماژول در یک گروه یکسان قرار گیرد.
- قانونی که در لیست بالاتر باشد، اولویت بیشتری دارد.

- **Network Rules**

این قوانین بر اساس ۳ وضعیت شبکه عمومی، شبکه Local و شبکه ی امن نوشته می شوند.

اگر کاربر بخواهد به شبکه ی عمومی متصل شود، فایروال دسترسی به فایل‌ها و پرینترهای کامپیوتر را مسدود می-کند. هم‌چنین کاربران خارجی نمی توانند از طریق share Folder و به صورت ریموت به این کامپیوتر دسترسی داشته باشند. فایروال به صورت پیشفرض وضعیت شبکه ی عمومی را برای اینترنت در نظر می‌گیرد. شبکه ی محلی برای کاربرانی که دسترسی محدودی به فایل ها و پرینترهای یک رایانه (در شبکه LAN یا شبکه خانگی) دارند، استفاده می شود. در وضعیت شبکه ی امن نیز بر فعالیت های شبکه هیچ محدودیتی اعمال نمی شود.

به عنوان مثال، برنامه های موجود در گروه High Restricted به طور پیش‌فرض در هیچ‌کدام از وضعیت ها مجاز به فعالیت در شبکه نیستند.

اگر یک Network Rule برای یک برنامه اصلی مشخص شده باشد، پروسس‌های زیرمجموعه ی آن نیز مطابق با قانون شبکه‌ی برنامه اصلی اجرا می شوند. اگر هیچ قانون شبکه ای برای یک برنامه وجود نداشته باشد، پروسس‌های وابسته بر اساس access rule مربوط به trust group آن برنامه اجرا خواهند شد.

سایر قابلیت‌ها و تکنولوژی‌ها

علاوه بر ماژول هایی که معرفی کردیم، موارد دیگری نیز وجود دارند که در ادامه آنها را معرفی و بررسی خواهیم کرد.

Vulnerability & Patch Management

این ماژول با متمرکزکردن و خودکارکردن وظایف امنیتی و مدیریتی مثل ارزیابی آسیب پذیری، توزیع Patch و آپدیت، تهیه خودکار لیست منابع سخت افزاری و نرم افزاری و برنامه های کاربردی شبکه، تهیه اطلاعات لایسنس های موجود در شبکه و مکانیزم جلوگیری از دسترسی غیرمجاز از راه دور، خطرات امنیتی IT و پیچیدگی های آن را به حداقل می رساند. تمام این کارها توسط یک کنسول مدیریتی یکپارچه انجام می شود.

اسکن خودکار نرم افزارها امکان شناسایی سریع، اولویت بندی و اصلاح آسیب پذیری ها را فراهم می کند. اسکن آسیب پذیری را می-توان به صورت خودکار یا طی یک برنامه زمانی مشخص از طریق یک سیاست منعطف و واحد برای شناسایی آسیب‌پذیری های مایکروسافتی و غیرمایکروسافتی ارائه داد. تشخیص موثر آسیب پذیری باعث می‌شود مهم‌ترین آسیب پذیری ها اولویت‌بندی و رفع شوند. شدت آسیب‌پذیری توسط کارشناسان کسپرسکی و همچنین منابع فرعی تهدیدات ارزیابی می شود.

این ماژول می تواند نقش سرور WSUS (Windows Update) را ایفا کند. به‌روزرسانی ها و پچ‌ها می توانند به صورت خودکار در شبکه توزیع شوند ولی ادمین قبل از توزیع آنها در شبکه، می تواند آن‌ها را آزمایش کند تا مطمئن شود پس از نصب سیستم به درستی کار کند. هم‌چنین می تواند لیستی از پچ‌های قابل اجرا را به لیستی تاییدشده محدود کند. هم‌چنین با پشتیبانی Wake-on-LAN می توان توزیع را به زمان خاصی محدود کرد. در جهت کاهش استفاده از پهنای باند در سازمان هایی که دفاتر مختلفی دارند، در هر دفتر یک کامپیوتر به عنوان distribution point یا نقطه توزیع تعیین می‌شود تا به‌روزرسانی ها و پچ‌های لازم را دریافت کند و سایر کامپیوترها از طریق آن موارد لازم را دریافت کنند. نتیجه ی نصب پچ از طریق گزارش تولیدشده در مرکز امنیت کسپرسکی قابل بررسی است و نیازی نیست ادمین تک تک کامپیوترها را جداگانه بررسی کند. اطلاعات مربوط به اکسپلویت‌های موجود و تهدیدهای شناخته شده و CVE آنها نیز در این مرکز قابل مشاهده است.

برای بهینه سازی پیاده سازی سیستم عامل و صرفه جویی در وقت، Kaspersky Vulnerability & Patch Management، ایجاد و ذخیره و تهیه ی Clone از Image سیستم امن را خودکار و متمرکز می کند. تمام Imageها در یک مخزن ویژه نگهداری می شوند و در زمان پیاده سازی قابل دسترسی‌اند. پیاده سازی Imageهای مربوط به سیستم‌هایی که جزو کلاینت‌های شبکه هستند می تواند با استفاده از سرورهای PXE و برای ماشین های جدید بدون سیستم عامل با استفاده از تسک مخصوص Kaspersky Vulnerability & Patch Management انجام شود. Image سیستم عامل می تواند با روش های زیر اداره شود:

- اجرای یک اسکریپت یا نصب یک نرم‌افزار پس از نصب سیستم عامل
- ایجاد یک فلش Boot با Windows PE
- وارد کردن Image سیستم عامل از طریق یک بسته ی توزیع (Windows Imaging Format (WIM

این ماژول در محصولات زیر عرضه می گردد:

- بخشی از Kaspersky Total Security for Business
- بخشی از Kaspersky Endpoint Security for Business Advanced
- بخشی از Kaspersky Hybrid Cloud Security Enterprise
- یک Add-on برای Kaspersky Endpoint Security for Business Select
- به عنوان یک راه حل مستقل و هدفمند با لایسنس سالانه

در محصول Kaspersky Hybrid Cloud Security، نام این قابلیت Vulnerability Assessment است.

Mobile Threat Protection

دستگاه‌های تلفن همراه به کل اقدامات امنیتی، از حفاظت ضدبدافزار و VPN گرفته تا اقدامات ضد سرقت فیزیکی که شامل پاک‌کردن از راه دور اطلاعات، مکان‌یابی دستگاه سرقت‌شده و مسدودکردن دسترسی به آن است، نیاز دارند. دستگاه‌های موبایل به دلایل مختلفی هدف یک حمله سایبری قرار می گیرند:

- کاربران اطلاعات باارزش خود را در آن ذخیره می کنند،
- دائما در شبکه های اجتماعی فعالیت می کنند و اجرای فیشینگ روی آنها ساده تر است.
- پیکربندی نادرست نقاط عمومی دسترسی به اینترنت (Public Internet Access) این دستگاه ها را در معرض حملات شبکه‌ی مبتنی بر Wi-Fi قرار می دهد.
- حمله به داده های بانکی موجود در دستگاه های تلفن همراه یک هدف سودآور است.
- گسترش BYOD و شیوه های استفاده از همان دستگاه برای تجارت، کاربران تلفن همراه شرکتی را به یک هدف وسوسه‌کننده برای جاسوسی تجاری تبدیل می کند.

محصولات آزمایشگاه کسپرسکی از همه‌ی فناوری های پیشرفته‌ی حال حاضر برای مقابله با تهدیدات تلفن همراه استفاده می کنند. ابزارهای اصلی محافظت از دستگاه‌های تلفن همراه به شرح زیر هستند:

URL Filtering:

علاوه بر این که از دسترسی کاربر به لینک های مخرب جلوگیری می کند، Kaspersky QR Scanner اعتبار و امنیت URL را در کدهای QR به صورت آنلاین و از طریق Kaspersky KSN بررسی می کند.

Anti-Malware:

در دستگاه های iOS، علی‌رغم محافظت اپل از App Store و الزام نصب برنامه ها از طریق آن، همچنان آلودگی به بدافزار مشاهده می شود. سیستم عامل این دستگاه‌ها اجازه ی ساخت یک برنامه ی ضدبدافزار کلاسیک برای iOS را نمی دهد. به همین خاطر است که ترکیبی از رویکرد اپل در نظارت و کنترل App Store با محافظت در برابر دسترسی به URLهای آلوده و مخرب، یک استراتژی امنیت سایبری خوب برای iOS است.

در دستگاه های Android ، کاربران می توانند فایل ها را از منابع مختلف و بازارهای اپلیکیشن نصب کنند. Kaspersky Internet Security for Android هنگام اجرای Installer برنامه و پس از نصب، آن را اسکن می کند. به دلیل این که مکانیزم یادگیری ماشین استفاده‌شده در این محصول به منابعی فراتر از منابع یک موبایل نیاز دارد، استفاده از رویکرد ابری کسپرسکی یا همان KSN می تواند این امکان را در اختیار کاربران قرار دهد تا از آن برای شناسایی تهدیدات و آلودگی ها استفاده کنند.

VPN:

برنامه Kaspersky Secure Connection با ساخت یک VPN، از تلفن همراه در برابر حملات Wi-Fi hotspots Rogue محافظت می کند. VPN کسپرسکی می تواند به طور خودکار محافظت از VPN را در زمینه های حساسی مثل اتصال از طریق یک نقطه ی آسیب پذیر، دسترسی به URL یا استفاده از برنامه ای که داده های حساس دارد (مثل امور مالی و بانکی، شبکه های اجتماعی و خرید) فعال کند.

Anti-theft یا ضدسرقت:

این تکنولوژی این امکان را به کاربر می دهد تا در زمان سرقت دستگاه موبایل، از راه دور داده های موجود در آن را پاک کرده و دستگاه را به حالت اولیه کارخانه برگرداند. همچنین از طریق پورتال کسپرسکی می تواند به صورت ریموت از سارق عکس بگیرد تا در شناسایی او استفاده شود.

رمز عبور و محافظت از اطلاعات حساس:

برنامه Kaspersky Password Manager به کاربران امکان می دهد رمزهای عبور قوی را در سرویس های وب و برنامه هایی که استفاده می کنند فعال کنند. این باعث می شود کاربران به دلیل حمله به رمزهای عبور ضعیف دسترسی خود را از دست ندهند. این برنامه به طور خودکار اطلاعات مربوط به حساب کاربری (شامل رمز عبور) را در صفحات وب پر می کند و داده های کارت اعتباری، عکس های مهم و سایر اطلاعات حساس را ذخیره می کند.

امنیت برای تجارت (MTD):

+این تکنولوژی برای سازمان هایی که دستگاه موبایل شرکتی دارند، مناسب است و از آنها در سطح دستگاه، شبکه و برنامه با جلوگیری، شناسایی و ازبین‌بردن حملات محافظت می کند. Kaspersky Security for Mobile، به عنوان بخشی از Kaspersky Endpoint Security for Business، یک راه حل MTD برای محافظت از کاربر تلفن همراه شرکتی است. این تکنولوژی با Real-time antimalware protection ، فیلترکردن URL، تعیین سیاست امنیتی، نظارت و پاسخگویی به تخلفات، حذف داده ها از راه دور، شناسایی root و افزودن امنیت به سایر راه‌حل های موجود در زمینه ی مدیریت تلفن همراه (EMM) از دستگاه در برابر تهدیدات محافظت می کند.

فناوری iChecker

فناوری iChecker، چک‌سام (Checksum) فایل های اسکن‌شده را محاسبه و ذخیره می کند. همان‌طور که میدانیم، چک‌سام با تغییر فایل تغییر می کند. این فناوری تغییرات فایل ها را بین دو بازه ی اسکن در نظر می‌گیرد، اگر چک‌سام تغییر کرده باشد، برنامه کسپرسکی فایل ها را برای یافتن ویروس بررسی می‌کند. این موضوع برای پیوست های ایمیل نیز صدق می کند. لازم به ذکر است اگر فایل به پوشه ی دیگری منتقل شود اسکن نمی شود چون چک‌سام آن تغییر نمی کند.
به دلیل این که اسکن چک‌سام فایل های بزرگ زمان زیادی نیاز دارد، این فناوری آن‌ها را اسکن نمی کند. هم‌چنین این فناوری فرمت های محدودی از جمله ZIP، CHM، COM، SYS، INF، TTF، LNK، DLL، exe و RAR را اسکن می کند.

فناوری iSwift

این فناوری مشابه فناوری iChecker است با این تفاوت که برای اسکن فایل های سیستمی NTFS استفاده می گردد. این فایل ها به هر شیئ شناسه ی متفاوتی اختصاص می دهند. این فناوری شناسه ی NTFS را با مقادیر موجود در پایگاه داده ی خود مقایسه کرده و در صورت عدم تطبیق، فایل برای شناسایی تهدیدات اسکن خواهد شد. این فناوری زمان اولین و آخرین اسکن اشیا را در نظر می‌گیرد و از اسکن هایی که در این میان انجام شده‌اند استفاده نمی کند. به دلیل این که این فناوری به محل ذخیره‌سازی نیز حساس است (Location-Based است)، اگر فایل در محل دیگری کپی شود، از ابتدا اسکن خواهد شد.

Disk and File Encryption

کسپرسکی ابزارهای یکپارچه‌ای برای رمزگذاری داده ها دارد که طبق سیاست‌های مرکز امنیت کسپرسکی (Policies) کار می-کنند. این سیاست‌ها می توانند برای میزبان‌های مختلف متفاوت باشند و داده های آن در قالب یک گزارش مشترک برای ادمین قابل مشاهده است.
رمزگذاری کامل دیسک یا (FDE Full Disk Encryption) از نشت اطلاعات در اثر سرقت لپتاپ یا هارد دیسک اکسترنال جلوگیری می کند. زمانی که دیسک رمزگذاری می شود، کاربران غیرمجاز نمی توانند از طریق آن boot شوند و یا داده های آن را بخوانند.
رمزگذاری در سطح فایل یا (FLE File-Level Encryption) از فایل ها در زمان انتقال در مسیرهای ناامن محافظت می کند. کاربرانی که طبق سیاست های مرکز امنیت کسپرسکی مجاز به دسترسی به این فایل ها هستند، می توانند آن ها را به صورت رمزگذاری‌نشده ببینند. در این نوع رمزگذاری، سیاست ها می‌توانند فایل را بر اساس پسوند یا مکان روی هارد رمزگذاری کنند. به محض اینکه فایل منطبق با این شرایط در رایانه شناسایی شود، رمزگذاری می شود.
برای دستگاه های قابل حمل مثل فلش که به کامپیوتر متصل هستند می توان سیاست‌های خاصی را تنظیم کرد. به عنوان مثال می توان تا زمانی که کاربر رمزگذاری روی دستگاه یا فایل های خاصی که در آن وجود دارند را قبول نکرده، دستگاه را مسدود کرد.

رمزگذاری شفاف

روند رمزگذاری با روال کاری یک کاربر معمولی تداخلی ندارد و برای برنامه ها شفاف است. یعنی وقتی کاربر در سیستم عامل احراز هویت شود، داده‌ها از دید برنامه‌ها رمزگذاری‌نشده هستند. فیلتر رمزگذاری، داده ها را بین برنامه ها و دیسک ها انتقال می دهد. این فیلتر، داده هایی را که از دیسک به سمت برنامه ها می آیند رمزگشایی کرده و داده هایی را که از سمت برنامه به دیسک می آیند، رمزگذاری می کند. داده ها بلافاصله در زمان خواندن/نوشتن رمزگذاری می شوند و هیچ داده ای بدون رمزگذاری روی دیسک ذخیره نمی شود.
برای برخی از برنامه ها، رمزگذاری نباید به این شفافیت باشد. به عنوان مثال، راهکارهای پشتیبان گیری که یک کپی از یک دیسک رمزگذاری‌شده را ذخیره می کنند تا آن را در جای دیگر نگه دارند، نباید داده های پشتیبان را بدون رمزگذاری ذخیره کنند. بنابراین برنامه پشتیبان گیری باید دیسک را در حالت رمزگذاری‌شده کپی کند. در این مورد و سایر موارد مشابه، ادمین می‌تواند transparent encryption یا رمزگذاری شفاف را برای برنامه ای خاص غیرفعال کند.
مکانیز رمزگذاری دیسک (FDE)تمام دیسک های موجود روی یک کامپیوتر را رمزگذاری می کند. این قابلیت از رمزگذاری انواع دیسک مثل HDD، SSD، Flash-Drive پشتیبانی می کند. برای دستگاه های SSD، ماژول FDE تعداد چرخه های خواندن/نوشتن را کاهش می دهد تا باعث افزایش طول عمر درایو شود. در صورتی که پردازنده کامپیوتر از AES-NI پشتیبانی کند، FDE از شتابدهی سخت‌افزاری رمزگذاری نیز پشتیبانی می کند. هم‌چنین از UEFI Secure Boot یا فناوری محافظت‌کننده از کامپیوتر هنگام بوت حفاظت می کند و تضمین می کند که فقط نرم‌افزار مورد اعتماد بارگیری شود و سیستم‌عامل و نرم‌افزار بدون هیچ‌گونه تداخل در فرایندهای دیگر به درستی شروع به کار می کنند.
فیلتر رمزگذاری دیسک را با کلید دیسک رمزگذاری و رمزگشایی می کند. برای هر دیسک یک کلید جداگانه ایجاد می شود و در سه نسخه رمزگذاری‌شده روی آن ذخیره می شود. حتی اگر دیسک آسیب دیده باشد و یک نسخه اصلی از بین رفته باشد، با نسخه دیگری می توان به دیسک دسترسی داشت. اگر هر سه نسخه اصلی دیسک آسیب دیده باشد می توان با نسخه ذخیره‌شده در مرکز امنیتی کسپرسکی دسترسی به دیسک را بازیابی کرد. برای انجام این کار هنگامی که یک disk key ایجاد می شود، کپی آن به طور ایمن به مرکز امنیتی کسپرسکی ارسال می شود. کلیدها هرگز بدون رمزگذاری بر روی دیسک ذخیره نمی شوند. disk key ذخیره‌شده در دیسک پس از احراز هویت کاربر در دسترس فیلتر رمزگذاری قرار می گیرد. کاربر می‌تواند با رمز عبور ، رمز USB یا کارت هوشمند احراز هویت کند. پس از احراز هویت موفقیت‌آمیز، سیستم عامل می‌تواند از دیسک رمزگذاری‌شده بوت شود.
در حین رمزگذاری دیسک، کاربران می توانند طبق معمول کار کنند، کامپیوتر را به حالت Sleep ببرند یا آن را خاموش کنند. وقتی کامپیوتر دوباره روشن شود، رمزگذاری از سر گرفته می شود. این فرآیند هم‌چنین در برابر خرابی هایی مثل قطع برق و خرابی سیستم عامل مقاوم است. طراحی رمزگذاری Failsafe تضمین می کند که تمام داده ها در نهایت رمزگذاری می شوند.

دسترسی به پرونده‌های رمزگذاری‌شده (FLE)

• دسترسی با Kaspersky Endpoint Security

وقتی کاربر در سیستم عامل احراز هویت می شود، طبق سیاست های رمزگذاری برنامه های موجود در رایانه که از طرف کاربر اجرا می شوند به پرونده های رمزگذاری‌شده دسترسی پیدا می کنند. برای دسترسی به پرونده های رمزگذاری‌شده توسط سایر کاربران، Agent Endpoint Security کلیدهای رمزگشایی مورد نیاز را از مرکز امنیتی کسپرسکی درخواست می کند. به عنوان مثال، اگر یک فایل ایمیل از طریق کاربر دیگری رمزگذاری شده باشد، Agent گیرنده یک کلید را از مرکز امنیتی کسپرسکی درخواست می کند و دریافت می کند (اگر سیاست ها اجازه دسترسی به آن را بدهند). این کلید برای دسترسی به این فایل و سایر فایل های رمزگذاری شده در همان دیسک منطقی همان کاربر کار می کند. این کلید Cache می‌شود بنابراین با هر بار دریافت فایلی که در همان دیسکِ همان کاربر رمزگذاری شده است، نیازی به درخواست کلید جدید نیست.

در صورت عدم اتصال به اینترنت، گیرنده می تواند از طریق تبادل کلید ایمن استاندارد پاسخ به چالش (standard challenge-response secure key) از طریق کانال های باز از مرکز امنیتی کسپرسکی یک کلید دریافت کند.

- **دسترسی بدون Kaspersky Endpoint Security**

اگر سیاست های رمزگذاری مجاز باشد، کاربران می توانند دستگاه‌های خود را پیکربندی کنند، بنابراین با استفاده از مجوز گذرواژه، می توان به پرونده های رمزگذاری‌شده در این دستگاه ها در رایانه های بدون Kaspersky Endpoint Security دسترسی پیدا کرد. هنگامی که کاربران چنین دستگاهی را با Kaspersky Endpoint Security پیکربندی می کنند:

- برنامه Kaspersky Portable File Manager در دستگاه کپی می شود، کلیدهای دسترسی فایل را به صورت ایمن ذخیره می کند و فایل ها را رمزگذاری / رمزگشایی می کند.
- کاربر برای دسترسی به فایل های این دستگاه رمز عبور ایجاد می کند.

وقتی کاربر دستگاهی را متصل می کند و در Portable File Manager مجوز ایجاد می کند، فایل‌های رمزگذاری‌شده برای خواندن و ویرایش در دسترس قرار می گیرند. هم‌چنین کاربران می توانند فایل‌های جدید را در دستگاه رمزگذاری کنند. این امکان وجود دارد که کاربر بدون نیاز به رمزگذاری مجدد کل دیسک مجازی، بتواند رمز عبور خود را تغییر دهد.

تکنولوژی Sandbox

Sandbox سیستمی برای شناسایی بدافزار است که یک شیئ مشکوک را در یک ماشین مجازی (VM) با سیستم عامل کاملاً ویژه اجرا می کند و با تجزیه و تحلیل رفتار آن، فعالیت مخرب آن را تشخیص می دهد. اگر شیئ در سیستم عامل مجازی اقدامات مخرب انجام دهد، Sandbox آن را به عنوان بدافزار شناسایی می کند. ماشین‌های مجازی از زیرساخت‌های واقعی سازمان/شرکت جدا شده اند.

چند سال پیش آزمایشگاه کسپرسکی یک Sandbox ویژه ی خود ایجاد کرد. این Sandbox بخشی از دو پلتفرم Kaspersky Anti-Targeted Attack یا به اختصار KATA و Kaspersky Lab Threat Intelligence است. این تکنولوژی برای دسته-بندی و شناسایی فایل ها و URLها در جهت ایجاد الگوریتم ها و قوانین تشخیص بدافزار مفید است. Sandbox امکانات زیر را دارد:

- مبتنی بر مجازی‌سازی سخت‌افزاری است که آن را سریع و پایدار می‌کند.
- تبادلات پردازش های کاوشگر با سیستم عامل را کنترل می کند و در موارد مشکوک، بررسی آن عمیق تر می شود.
- VM برای سیستم عامل ویندوز و سیستم عامل اندروید امکان‌پذیر است.
- exploit را از زمان اولیه فعالیتش شناسایی می کند.

انواع اشیای قابل اجرا

- **ویندوز:** تمام فایل ها. برای مثال MS Office files.*، .NET ، *.dll ، exe و PDF
- **اندروید:** APK (DEX)
- **URLها:** از طریق شناسایی رویدادهای Adobe Flash execution، JavaScript، Download و غیره.

موارد جمع‌آوری شده توسط Sandbox

- Application execution logs
- Memory dumps
- Loaded modules dumps
- Changes in file system, registry
- Network traffic (PCAP files)
- Screenshots (for easier audit and manual analysis, if needed)
- Artifacts of exploit activity

ممکن است وقتی بدافزار بفهمد در Sandbox در حال اجراست، فعالیت مخرب خود را انجام ندهد، خود را از دیسک پاک کند یا فعالیتش را خاتمه دهد. sandbox پردازنده و RAM را کنترل می کند اما عملکرد فرایند، حافظه، کتابخانه های سیستم روی دیسک و حافظه را تغییر نمی دهد و هیچ اثری از نظارت باقی نمی گذارد. این تکنولوژی دائما در حال ارتقا می باشد.

قابلیت Data Export via Syslog

می توان از پروتکل Syslog برای ارسال رویدادهای رخ داده در سرور مدیریت و سایر برنامه های کسپرسکی نصب شده در دستگاه-های شبکه به سیستم‌های SIEM توسط مرکز امنیت کسپرسکی استفاده کرد. مرکز امنیت کسپرسکی از سیستم های QRadar، ArcSight و Splunk نیز پشتیبانی می کند.

قابلیت OS & third-party software installation

علاوه بر پیاده‌سازی نرم افزارهای کمپانی کسپرسکی از طریق مرکز امنیت کسپرسکی، می توان سایر نرم افزارها و به‌روزرسانی آن‌ها را نیز نصب کرد. این قابلیت در نسخه ی Advanced و Total وجود دارد.
تا اینجا ماژول ها و تکنولوژی هایی را که کسپرسکی Endpoint Security for Business Workstations از آن‌ها برای تامین امنیت کامپیوترها استفاده می کند معرفی کردیم. این ماژول ها در نسخه های مختلفی ارائه می شوند و شما با توجه به نیاز و بودجه سازمان می توانید نسخه ی مناسب خود را تهیه کنید.

محصولات سازمانی کسپرسکی برای اندپوینت تحت عنوان Kaspersky Endpoint Security For Business و در سه نسخه-ی Select،Advanced و Total در بازه های زمانی یک‌ساله، دوساله و سه ساله به فروش می رسند. جدول زیر سه نسخه ی سازمانی را با یکدیگر مقایسه می کند:

	Select	Advanced	Total
Defense for PC, Linux, Mac, Android, iOS	✓	✓	✓
Defense for application and terminal servers		✓	✓
Defense for web gateways and email servers			✓
Mobile Threat Defense	✓	✓	✓
Application, Web & Device Controls for PCs	✓	✓	✓
Vulnerability Assessment, Behavior Detection, Exploit Prevention, Remediation Engine	✓	✓	✓
Environment variable permissions and HIPS	✓	✓	✓
Data export via Syslog	✓	✓	✓
Kaspersky Sandbox and Kaspersky EDR Optimum integration	✓	✓	✓
Web, Email threat protections and controls for servers		✓	✓
Adaptive Anomaly Control and Patch Management		✓	✓
Encryption and OS-built-in encryption management		✓	✓
SIEM integration, OS & third-party software installation		✓	✓
Inbound and outbound content filtering			✓
Anti-spam protection at gateway level			✓
Web traffic security and web controls at gateway level			✓