نگاهی به ترلیکس

راهکارهای امنیت نقاط پایانی و حفاظت از اطلاعات

در مقایسه با رقبا

شبکه گستر

امنیت شما | وظیفه ما

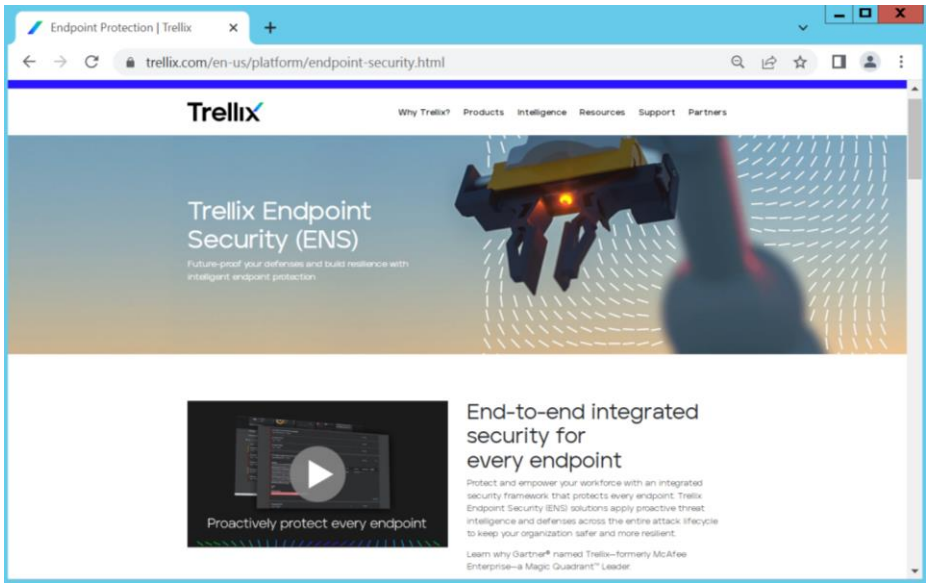
فهرست مطالب

درباره ترلیکس

در ماه مارس ۲۰۲۱ شرکت مک‌آفی (McAfee) خدمات و محصولات سازمانی خود را به مبلغ ۴ میلیارد دلار به شرکت اس‌تی‌جی (STG) واگذار کرد که منجر به ظهور شرکت جدید مک‌آفی اینترپرایز (McAfee Enterprise) شد. در ماه ژوئیه ۲۰۲۱ نیز، فایرآی (FireEye) از فروش محصولات این شرکت به اس‌تی‌جی به قیمت ۱.۲ میلیارد دلار خبر داد.

دو شرکت امنیتی مک‌آفی اینترپرایز و فایرآی در اواخر سال میلادی ۲۰۲۱ توسط اس‌تی‌جی در هم ادغام شدند. این دو از زمستان سال گذشته با نام جدید ترلیکس (Trellix)، فصلی نو را در دنیای امنیت فناوری اطلاعات رقم می‌زنند.

اس‌تی‌جی، یک شرکت خصوصی است که در سال ۲۰۰۲، توسط رومش تی ودهوانی (Romesh T. Wadhwani) تأسیس شد. رومش ودهوانی متولد کراچی است. در همان روزهای ابتدایی تولد، والدینش به هند نقل مکان کردند. وی مدرک کارشناسی را از مؤسسه IITB هند و کارشناسی ارشد و دکترای خود را در رشته مهندسی برق از دانشگاه کارنگی ملون دریافت کرده است. رومش ودهوانی، در حال حاضر عهده‌دار ریاست هیأت مدیره شرکت اس‌تی‌جی است. در سال ۲۰۲۲، مجله فوربز (Forbes)، نام او را در ردیف ۶۸۷ از فهرست ثروتمندترین افراد جهان قرار داد.



اس‌تی‌جی در حالی اقدام به خرید و ادغام دو ابر شرکت امنیتی مک‌آفی اینترپرایز و فایرآی و تشکیل شرکت ترلیکس نموده که اجرای مستمر حملات مخرب، پیچیده و گسترده، کسب‌وکار تبهکاران سایبری را پررونق‌تر از همیشه کرده است.

نگاهی به محصولات دو شرکت مذکور نشان می‌دهد که محصولات متنوع آنها در نقش مکمل یکدیگر موجب ظهور نسل جدیدی از راهکارها در حوزه‌های مختلف از جمله امنیت سرورها و نقاط پایانی، امنیت بسترهای رایانش ابری، جلوگیری از نشت داده‌ها (DLP) و مدیریت عملیات امنیتی خواهد شد. ضمن آن که توسعه راهکارهای به اصطلاح Extended Detection & Response – به اختصار XDR – با تمرکز بر روی فناوری‌های یادگیری ماشین و خودکارسازی از جمله برنامه‌های کلیدی شرکت جدید ترلیکس اعلام شده است.

در این گزارش، امکانات و قابلیت‌های محصولات امنیت نقاط پایانی ترلیکس در مقایسه با برخی ضدویروس‌های فعال در بازار ایران از نگاه گروه تحقیق و توسعه شرکت مهندسی شبکه گستر ارزیابی شده است.

مقایسه امکانات امنیت نقاط پایانی

	Trellix Complete Endpoint Protection	Bitdefender GravityZone Business Security Enterprise	AmnPardaz Padvish Ultimate	ESET Protect Complete	Kaspersky Endpoint Security for Business Adv.
کنسول تحت وب	✔	✔	-	✔	امکانات محدود
تعیین سطح دسترسی کاربران به کنسول مدیریت	✔	✔	✔	✔	✔
تقسیم بار میان چندین سرور[۱]	✔	✔	-	✔	✔
پشتیبانی از سیستم‌های عامل Windows	✔	✔	✔	✔	✔
پشتیبانی از سیستم‌های عامل Mac	✔	✔	✔	✔	✔
پشتیبانی از سیستم‌های عامل Linux	✔	✔	✔	✔	✔
تهیه نسخه پشتیبان از پایگاه داده	✔	-	✔	✔	✔
مدیریت نمایش اعلان‌ها	✔	✔	✔	✔	✔
پویش درایوهای اشتراکی	✔	✔	✔	✔	✔
پویش زمانبندی شده	✔	✔	✔	✔	✔
امکان پویش محضرخانه[۲] و حافظه	✔	✔	✔	✔	✔
قواعد دیواره آتش مبتنی بر نرم‌افزار یا بسته‌های شبکه	✔	✔	✔	✔	✔
دسته‌بندی قواعد دیواره آتش بر اساس بستر ارتباطی (Wired، Wireless یا Virtual)	✔	✔	-	-	-
اجازه برقراری ارتباط برنامه‌های مورد اطمینان در قواعد دیواره آتش به‌صورت خودکار	✔	✔	-	-	-
قابلیت تعریف قاعده براساس درهم‌ساز[۳] برنامه در دیواره آتش	✔	-	-	-	-
پویش ترافیک SSL	✔	✔	-	✔	-
زمانبندی دسترسی به وب	✔	✔	-	-	-
کنترل دسترسی به وب براساس محتوای سایت	✔	✔	-	-	✔
مسدودسازی یا مجاز نمودن دسترسی به سایت‌های مورد نظر سازمان	✔	✔	✔	✔	✔
درجه‌بندی امنیت لینک‌ها در نتایج جستجوی موتورهای جستجوگر	✔	✔	-	-	-
ضدبدافزار برای سرویس Exchange	✔	✔	✔	✔	✔

۱ Load Balancing
۲ Windows Registry
۳ Hash

	Trellix Complete Endpoint Protection	Bitdefender GravityZone Business Security Enterprise	AmnPardaz Padvish Ultimate	ESET Protect Complete	Kaspersky Endpoint Security for Business Adv.
ضدهرزنامه برای سرویس Exchange	-	✔	✔	✔	✔
ضدباج‌افزار	✔	✔	✔	✔	✔
کنترل نرم‌افزار بر اساس نام	✔	✔	✔	✔	✔
کنترل نرم‌افزار بر اساس درهم‌ساز (MD5 و SHA256)	✔	✔	-	-	✔
ارائه جزییات تغییرات اعمال‌شده در محضرخانه توسط فایل موردنظر	✔	-	-	-	-
اعمال قواعد براساس نام کاربر یا مکان دستگاه	✔	-	-	-	-
تعریف قواعد مجزا برای یک سیستم	✔	✔	-	✔	-
فناوری‌های یادگیری ماشینی	✔	✔	✔	✔	✔
بهره‌گیری از رایانش ابری	✔	✔	✔	✔	✔
امکان به‌روزرسانی برون‌خط[۴]	✔	✔	✔	✔	نیاز به ابزار جانبی سازنده
استثنا کردن فایل / پوشه از پویش شدن توسط ضدویروس	✔	✔	✔	✔	✔
تعیین واکنش به فایل‌های شناسایی‌شده	✔	✔	✔	✔	✔
تخصیص رمز عبور برای جلوگیری از حذف نرم‌افزار	✔	✔	✔	✔	✔
تخصیص رمز عبور برای محدود کردن دسترسی کاربر به تنظیمات	✔	✔	✔	✔	✔
کنترل سخت‌افزار	✔	✔	✔	✔	✔
محصول بهینه‌شده مجزا برای بسترهای مجازی	محصول مجزا (Trellix MOVE AV)	✔	✔	✔	✔
ارسال گزارش از طریق پست الکترونیکی	✔	✔	✔	✔	✔
نمایش ارتباطات تهدید در قالب گرافیکی	✔	✔	-	-	محصول مجزا (Kaspersky Optimum Security)
مدیریت اصلاحیه‌های امنیتی	-	افزونه	-	محصول مجزا (ESET Patch Management)	✔
راهکار برای دستگاه‌های همراه	-	✔	-	✔	✔
تعداد کاربران موتور پویشگر ضدویروس در سطح جهان	بیش از ۶۲۰ میلیون	بیش از ۵۰۰ میلیون	نامشخص	بیش از ۱۱۰ میلیون	بیش از ۴۰۰ میلیون
پایگاه داده مورد استفاده سرور مدیریت	SQL	MongoDB	SQLITE	MySQL یا SQL	MySQL یا SQL
خروجی گزارش‌ها	PDF، CSV، HTML، XML و Archive	PDF و CSV	HTML و XML	PDF، PS و CSV	PDF، HTML و XLS

[۴] Offline Update

مقایسه امکانات حفاظت از اطلاعات

	Trellix Complete Data Protection - Advanced	Symantec (Broadcom) Data Loss Prevention Core Solution	Safetica ONE Enterprise
کنسول مدیریت تحت وب	✔	-	✔
کنسول مدیریت یکپارچه با محصولات امنیت نقاط پایانی	✔	-	-
طبقه‌بندی[۵] اسناد و فایل‌ها با استفاده از برچسب‌زنی[۶]	✔	نیاز به محصول Symantec ICS	✔
کنترل سخت‌افزار	✔	نیاز به محصول Symantec EP	✔
تعریف کاربران با سطوح دسترسی مختلف جهت دسترسی به کنسول مدیریت	✔	✔	✔
قواعد کنترل دسترسی نرم‌افزارها به فایل‌های حاوی محتوای طبقه‌بندی شده	✔	✔	-
قواعد کنترل قرار گرفتن محتوای طبقه‌بندی شده در حافظه موقت[۷]	✔	✔	✔
قواعد کنترل قرار گرفتن فایل‌های طبقه‌بندی شده در ذخیره‌سازهای ابری	✔	✔	✔
قواعد کنترل ارسال فایل یا محتوای طبقه‌بندی شده از طریق سرویس ایمیل	✔	✔	✔
قواعد کنترل ارسال فایل‌های طبقه‌بندی شده از طریق ارتباطات شبکه‌ای	✔	✔	✔
قواعد کنترل قرار گرفتن فایل‌های طبقه‌بندی شده در مسیرهای اشتراکی	✔	✔	✔
قواعد کنترل چاپ اسناد طبقه‌بندی شده توسط چاپگرها	✔	✔	✔
قواعد کنترل تصویربرداری از صفحه نمایش	✔	✔	✔
محدود کردن دسترسی به فایل‌های ذخیره شده بر روی تجهیزات ذخیره‌ساز همراه	✔	✔	-
جلوگیری از ارسال فایل‌های مهم سازمان با استفاده از مرورگرها	✔	✔	-
جلوگیری از ارسال فایل‌ها توسط پودمان‌های شبکه	✔	✔	-
پویش دستگاه جهت شناسایی فایل‌های طبقه‌بندی شده بدون استفاده	✔	✔	✔
شناسایی فایل‌های طبقه‌بندی شده در حال استفاده	✔	✔	✔
برچسب‌زنی دستی فایل‌های طبقه‌بندی شده توسط کاربران مجاز تعیین‌شده	✔	-	-
شناسایی محتوای طبقه‌بندی‌شده از طریق کلیدواژه، لغت‌نامه و عبارات منظم تعیین‌شده	✔	✔	✔

[۵] Classification
[۶] Tagging
[۷] Clipboard

	Trellix Complete Data Protection - Advanced	Symantec (Broadcom) Data Loss Prevention Core Solution	Safetica ONE Enterprise
شناسایی محتوای طبقه‌بندی شده از طریق ویژگی‌های اسناد (نام نویسنده، عنوان سند و ...)	✔	-	-
ذخیره نمونه‌ای از فایل‌هایی که قواعد مرتبط با آنها توسط کاربر نقض شده، به‌عنوان مدرک[۸]	✔	✔	-
قابلیت تعریف تاییدیه‌های مختلف و واکنش‌های متفاوت برای هر تاییدیه	✔	✔	✔
تعیین ماژول‌های فعال سفیر DLP نصب شده بر روی ایستگاه‌های کاری	✔	✔	-
واکنش‌های جداگانه بر اساس محل دستگاه (داخل یا خارج از سازمان)	✔	✔	-
تعیین نحوه شناسایی متصل بودن به شبکه سازمان	✔	✔	-
فعال بودن در حالت Safe Mode	✔	-	-
سازوکار امنیتی Challenge-response در فرایند حذف سفیر از روی نقطه پایانی	✔	-	-
قابلیت غیرفعال نمودن سفیر DLP برای مدت زمان مشخص از طریق کنسول مدیریت	✔	-	-
ایجاد گزارش‌های جدید (غیر از گزارش‌های پیش‌فرض)	✔	-	-
سفارشی‌سازی گزارش‌های تعریف‌شده	✔	✔	✔
ارسال گزارش‌ها از طریق ایمیل در فواصل زمانی تعیین‌شده	✔	-	✔
ذخیره‌سازهای ابری پشتیبانی شده	Box, DropBox, Google Drive, iCloud, OneDrive, Syncplicity	OneDrive ،Google Drive Box و Dropbox	OneDrive ،Google Drive Box و Dropbox
پایگاه داده	SQL	Oracle	SQL
فرآیند نگهداری از پایگاه داده	آسان	پیچیده	آسان
خروجی گزارش‌ها	PDF ،CSV ،HTML ،XML و Archive	CSV و XML	PDF و XLS

^ Evidence

مقایسه بسته‌های ترلیکس

امکانات امنیتی در بسته‌های نرم‌افزاری	Trellix Endpoint Protection Essential	Trellix Endpoint Protection Advanced	Trellix Complete Endpoint Protection	Trellix Complete Data Protection	Trellix Complete Data Protection Advanced	Trellix MOVE AV
ابزار مدیریت متمرکز و یکپارچه محصولات | Central Management Console	✔	✔	✔	✔	✔	✔
ضدبدافزار، دیواره‌آتش، نفوذیاب و پایشگر سایت برای سرور و ایستگاه کاری | Endpoint Security	✔	✔	✔			
کنترل سخت‌افزار | Device Control	✔	✔	✔			
ضدبدافزار برای سرور پست الکترونیکی | Security for Email Servers		✔	✔			
ضدبدافزار برای محیط SharePoint | Security for Microsoft SharePoint		✔	✔			
کنترل برنامه‌ها و نرم‌افزارهای کاربردی | Application Control			✔			
حفاظت از دستگاه‌های ذخیره‌ساز NAS | Storage Protection			✔			
تبادل اطلاعات درباره تهدیدات و تحلیل یکپارچه | Threat Intelligence Exchange			✔			
به‌اشتراک‌گذاری اطلاعات بین محصولات امنیتی | Data Exchange Layer			✔			
رمزگذاری فایل‌ها و حافظه‌های قابل حمل | File & Removable Media Encryption				✔	✔	
رمزگذاری کامل دیسک | Drive Encryption				✔	✔	
حفاظت و جلوگیری از نشت داده‌ها | Data Loss Prevention					✔	
حفاظت از بسترهای مجازی | Virtual Environments AV						✔

جایگاه ترلیکس در ارزیابی‌های بین‌المللی

گارتنر (Gartner)

شرکت گارتنر[۹]، یکی از معتبرترین مؤسسات بین‌المللی ارزیابی محصولات فناوری اطلاعات است.

این شرکت به‌صورت دوره‌ای وضعیت رقبای موجود در هر زمینه از محصولات فناوری اطلاعات را با هم مقایسه کرده و نتیجه را به‌صورت نمودار "چهار بخشی" نشان می‌دهد که آن را "چهارگانه جادویی"[۱۰] می‌نامد.

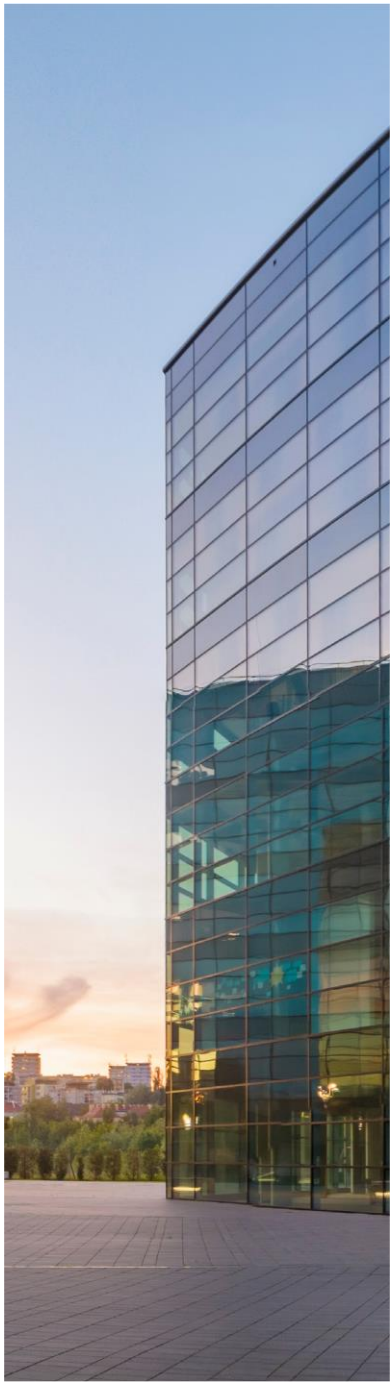
با نگاه به این نمودار می‌توان وضعیت شرک ت‌های فعال در یک زمینه خاص از فناوری اطلاعات را نسبت به همدیگر دانست. از آنجا که این نمودار، پارامترهایی را که بیشتر جنبه کیفی دارند، به شکل کمی درمی‌آورد، سالهاست که توسط شرکت‌ها و تحلیلگران برای ارزیابی بازار محصولات گوناگون فناوری اطلاعات مورد استفاده و استناد قرار می‌گیرد.

در نمودار "چهارگانه جادویی"، جایگاه هر شرکت براساس دو محور "پیش‌بینی نیاز بازار"[۱۱] و "توان پیاده‌سازی و اجرا"[۱۲] تعیین می‌گردد. برای تشخیص میزان هر یک از این دو متغیر، بر اساس نوع محصول تحت ارزیابی، عوامل متعددی تعریف می‌شود.

به‌عنوان مثال، برای تعیین میزان "پیش‌بینی نیاز بازار" از عواملی نظیر نوآوری، شناسایی نیازهای بازار - و عرضه محصول برای پاسخگویی به آنها - و استراتژی‌های معرفی محصول استفاده می‌شود. برای تعیین میزان "توان پیاده‌سازی و اجرا" نیز عواملی همچون رضایت مشتری و توانایی اجرایی شرکت به کار می‌رود.

در این نمودار شرکت‌ها در یکی از چهار گروه زیر دسته‌بندی می‌شوند:

- پیشگامان[۱۳] - این شرکت‌ها توانسته‌اند میان "پیش‌بینی نیاز بازار" و "توان پیاده‌سازی و اجرا" تعادلی قابل قبول برقرار کنند. قابلیت‌های محصولاتشان، آنها را بالاتر از رقبایشان قرار داده و بنابراین به نوعی پیشرو در بازار هستند.
- چالشگران[۱۴] - این گروه از شرکت‌ها هر چند از لحاظ "توان پیاده‌سازی و اجرا" دارای جایگاه نسبتاً بالایی هستند اما در مسیر صحیحی در بازار قرار ندارند.
- آینده‌اندیشان[۱۵] - این دسته از شرکت‌ها از رویکرد صحیحی در بازار برخوردارند؛ در عین حال "توان پیاده‌سازی و اجرا" آنها در حد قابل قبولی قرار ندارد.
- تازه‌کاران[۱۶] - این شرکت‌ها ممکن است در بخش کوچکی از بازار به موفقیت‌هایی دست یافته باشند اما توان رقابت با رقبای مطرح را ندارند.

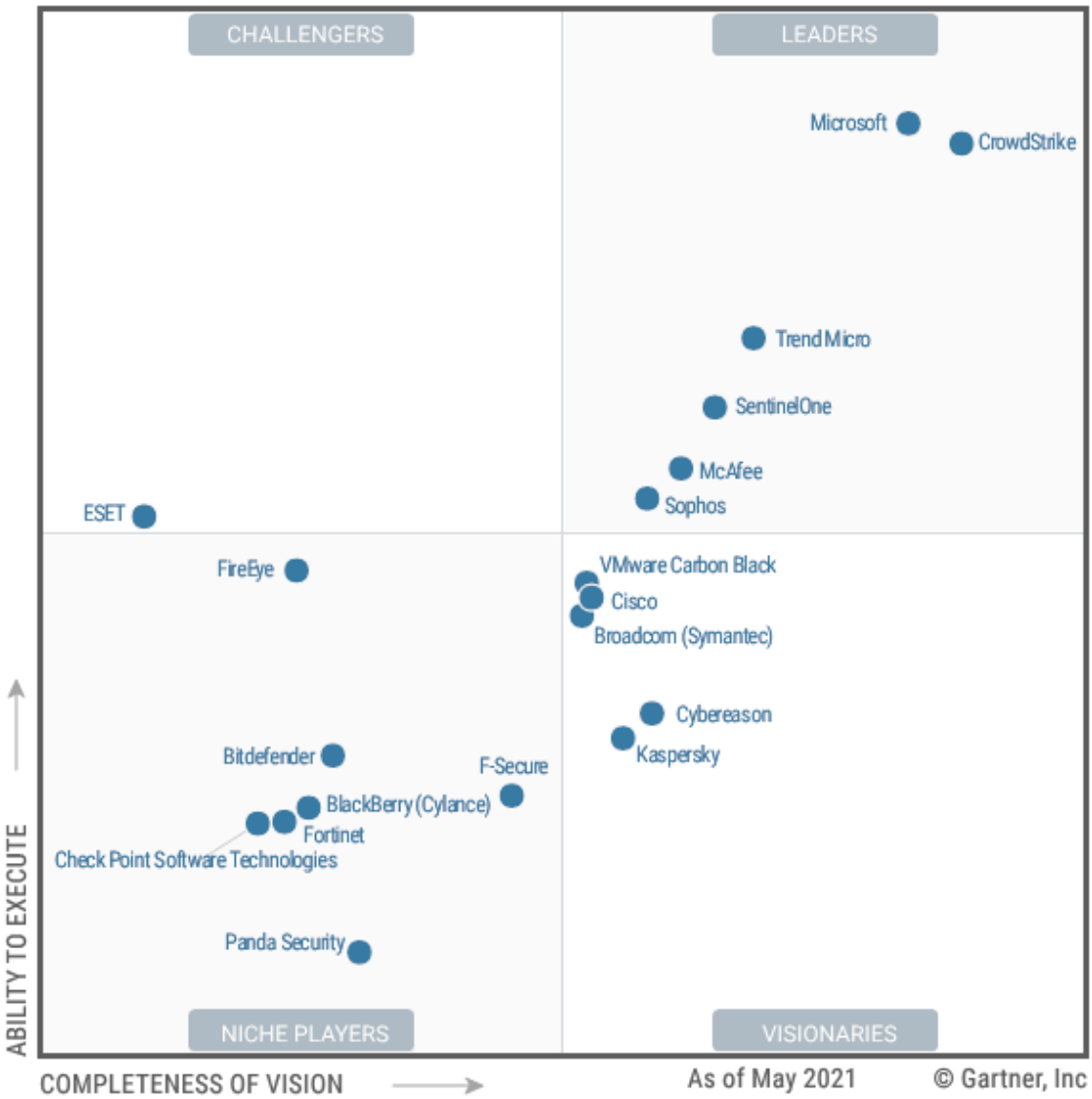


---

۹ Gartner, Inc
۱۰ Magic Quadrant
۱۱ Completeness of Vision
۱۲ Ability to Execute
۱۳ Leaders
۱۴ Challengers
۱۵ Visionaries
۱۶ Niche Players

در گزارشی که ۱۵ اردیبهشت ۱۴۰۰ منتشر شد گارتنر شرکت مک‌آفی را به‌عنوان یک شرکت "پیشگام" (Leader) در زمینه "محصولات حفاظت از نقاط پایانی"[۱۷] معرفی کرد.

نمودار زیر جدیدترین گزارش شرکت گارتنر در خصوص بازار محصولات EPP و وضعیت فعالان این زمینه را نشان می‌دهد.



[۱۷] Endpoint Protection Platforms – به اختصار EPP

همچنین در آخرین بررسی انجام شده توسط گارتنر، شرکت امنیتی مک‌آفی موفق به کسب جایگاه "پیشگام در حوزه "محصولات سازمانی پیشگیری از نشت اطلاعات" شده است.

نمودار زیر آخرین "چهارگانه جادویی" شرکت گارتنر را در بخش بازار "محصولات سازمانی پیشگیری از نشت اطلاعات"[۱۸] و وضعیت فعالان این حوزه را نمایش می‌دهد.

[۱۸] Enterprise Data Loss Prevention

ای‌وی-کامپرتیوز (AV-Comparatives)

مؤسسه ای‌وی-کامپرتیوز[۱۹] بر اساس آزمون‌های مختلفی که هر سال بر روی انواع محصولات ضدویروس انجام می‌دهد، ارزیابی بیطرفانه و منصفانه‌ای را بعمل آورده و این محصولات را رتبه‌بندی می‌کند. ترلیکس در تمامی آزمون‌های Business Security، موفق به کسب معتبرترین نشان این مؤسسه در این حوزه، یعنی Approved Business Security شده است. بخشی از توضیحات ای‌وی-کامپرتیوز در گزارش جولای این مؤسسه در خصوص Trellix Endpoint Security در زیر قابل مطالعه است:

Trellix Endpoint Security (ENS) is a comprehensive security solution designed for enterprise networks of all sizes. The ePolicy Orchestrator management console offers flexible options for efficient management of the endpoint protection software.

Key Features

Customizable Dashboard: The dashboard and reporting can be tailored to display relevant endpoint status information for each user.

Deployment Flexibility: The console offers a variety of deployment options, including cloud-based, on-premises hosting, and Amazon hosting.

Management Console: The ePolicy Orchestrator console is easily accessed through the primary navigation menu located at the top left of the main dashboard.

Real Protect: Through machine learning classification, threats are detected in real time, and behavior classification continually evolves to identify future attacks. Endpoints are restored to the last known good state, preventing infections and reducing administrative burdens.

Adaptive Scanning: The system intelligently skips scanning trusted processes and gives priority to suspicious processes and applications during scanning.

Endpoint Client Deployment: Client agent packages can be created on the Product Deployment page. The installer file can be distributed via a web link, manually executed, or deployed through a systems management product.

Proactive web security: This feature ensures safe browsing by providing web protection and filtering for endpoints.

Hostile network attack blocking: The integrated firewall utilizes reputation scores based on GTI to safeguard endpoints against botnets, DDoS attacks, advanced persistent threats, and suspicious web connections. During system startup, the firewall only allows outbound traffic, providing protection when endpoints are not connected to the corporate network.

Antimalware protection: Trellix protects, detects, and corrects malware quickly with an antimalware engine that works across multiple devices and operating systems.

---

[۱۹] AV-Comparatives GmbH

ای‌وی-تست (AV-Test)

در آزمون‌های مؤسسه ارزیابی ای‌وی-تس ت[۲۰] محصولات ضدبدافزار در سه بخش "حافظت"[۲۱]، "کارایی"[۲۲] و "قابلیت استفاده"[۲۳] مورد ارزیابی قرار می‌گیرند.

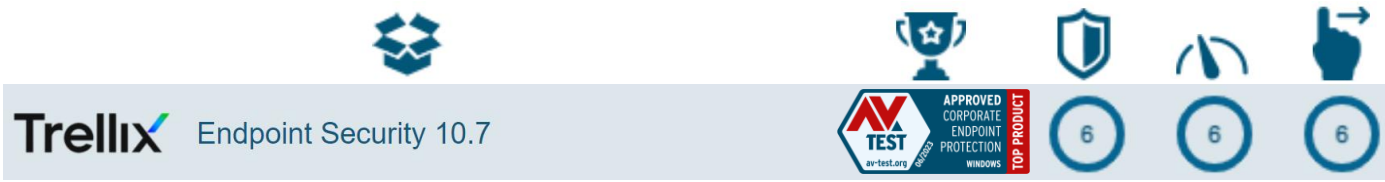
در جمع‌بندی سالانه این مؤسسه معتبر، ترلیکس موفق به کسب نشان "بهترین کارایی در سال ۲۰۲۱"[۲۴] شد.

Trellix/FireEye demonstrated excellent performance in all the tests in 2021. In the category of Performance, the overall findings not only far exceeded the industry average but also topped the charts of the comparative tests. That is why Trellix/FireEye also deserved the Performance Award. The AV-TEST Institute wishes every success to FireEye and McAfee (corporate sector) in their merging to form the new company Trellix.

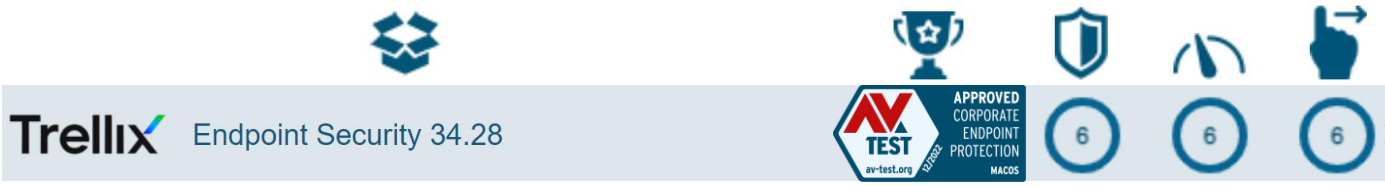
---

[۲۰] AV-TEST GmbH
[۲۱] Protection
[۲۲] Performance
[۲۳] Usability
[۲۴] ۲۰۲۰ Best Performance

در آزمون ژوئن ۲۰۲۳ مؤسسه AV-Test در حوزه محصولات سازمانی تحت Windows، نرم‌افزار Trellix Endpoint Security موفق به کسب بالاترین امتیاز (۶ از ۶) در هر سه بخش Protection، Performance و Usability شد.



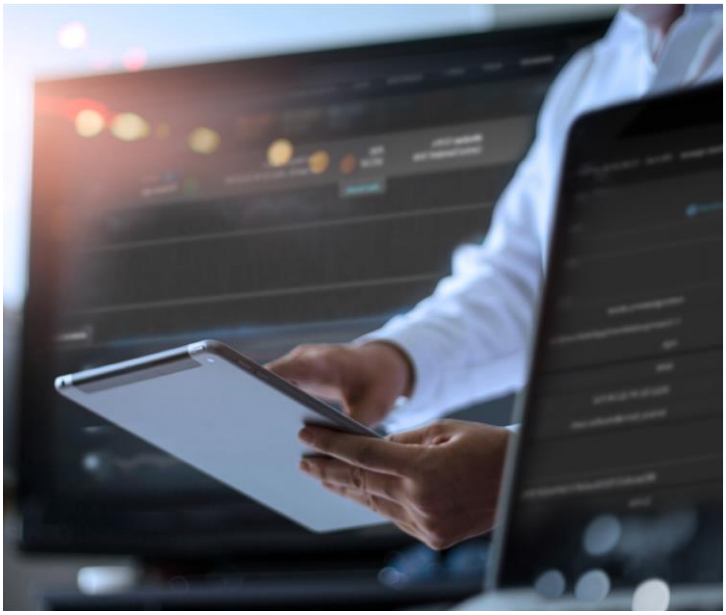
در آزمون دسامبر ۲۰۲۲ مؤسسه AV-Test در حوزه محصولات سازمانی تحت macOS هم، نرم‌افزار Trellix Endpoint Security موفق به کسب بالاترین امتیاز (۶ از ۶) در هر سه بخش Protection، Performance و Usability شد.



رادیکاتی (Radicati)

شرکت رادیکاتی[۲۵]، در هر سال به بررسی وضعیت شرکت‌های عرضه‌کننده فناوری در بازار و قابلیت‌های محصولات آنها پرداخته و جایگاه آنها را در چهارگانه[۲۶] خود تعیین می‌کند. این چهارگانه از بخشهای زیر تشکیل شده است:

- بازیگران اصلی[۲۷] - "بازیگران اصلی"، علاوه بر داشتن چشم‌اندازی مشخص برای آینده، دارای محصولاتی با قابلیت‌های گسترده و عملکرد مناسب هستند. این شرکت‌ها با فناوری و چشم‌انداز راهبردی خود، تعیین‌کننده سمت‌وسوی بازار هستند. کسب این جایگاه مستلزم تلاش فراوان و تداوم نوآوری است. بسیاری از "بازیگران اصلی" حضور در بخش‌های "متخصصین" و یا "پیشروان" را تجربه کرده‌اند.
- پیشروان[۲۸] - این شرکت‌ها، فناوری پیشرفته و برتری را در برخی از راهکارهای خود ارائه می‌کنند؛ اما لزوما موفق به کسب امتیاز برای همه امکانات و عملکردهای مورد نیاز برای قرارگیری در جایگاه "بازیگران اصلی" نشده‌اند. "پیشروان" بالقوه این توان را دارند که با یک فناوری یا روش جدید، وضعیت بازار را دگرگون کنند. ارتقا به جایگاه "بازیگران اصلی" برای این شرکت‌ها، با گذشت زمان محتمل‌تر از شرکت‌های حاضر در بخش‌های "متخصصین" و "بازیگران کهنه‌کار" است.



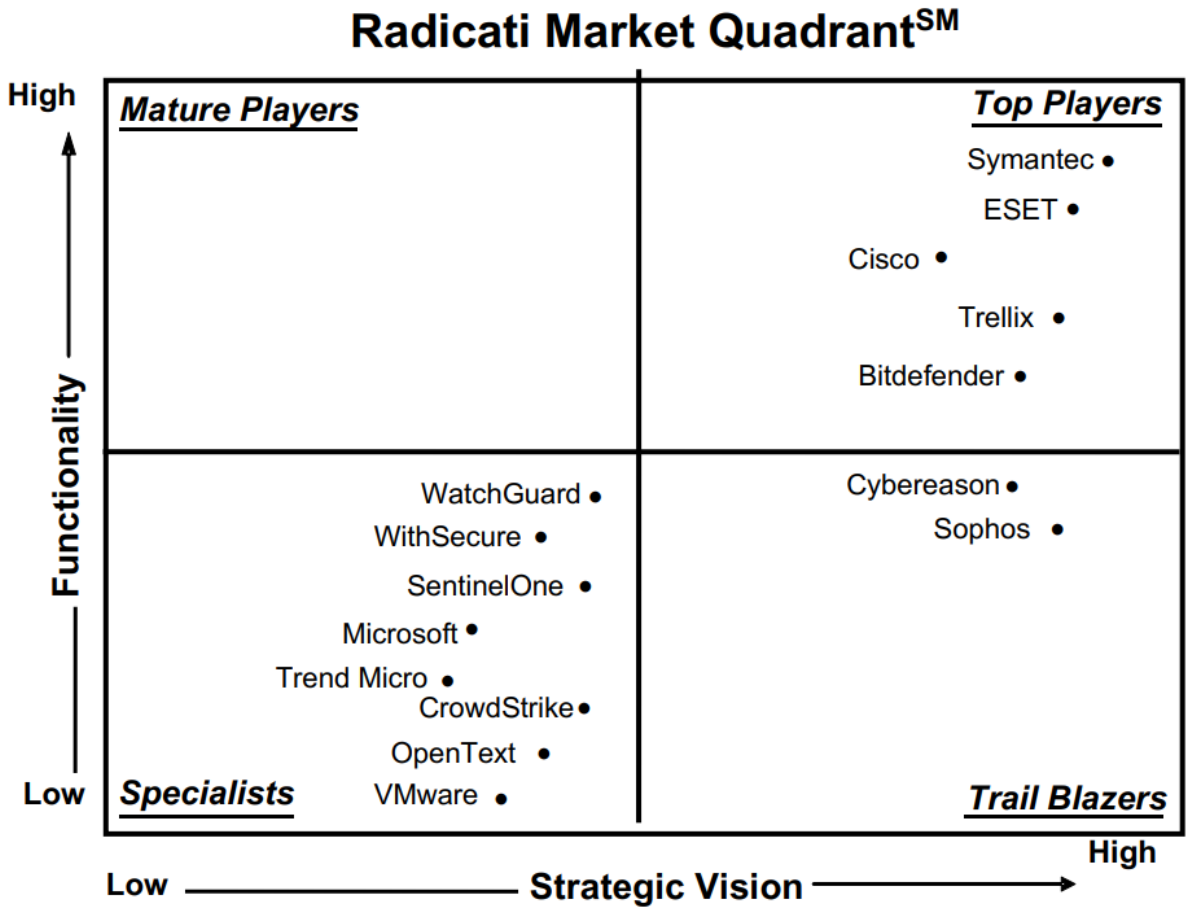
- متخصصین[۲۹] – شرکت‌های حاضر در این بخش خود به دو دسته زیر تقسیم می‌شوند:
  - بازیگران نوظهور[۳۰] – شرکت‌هایی که به‌تازگی در صنعت شناخته شده‌اند؛ اما در عین حال برای کسب جایگاه بالاتر لازم است که برخی از جنبه‌ها از راهکار خود را بهبود داده و ضمن حفظ راهبرد، فناوری خود را توسعه دهند.
  - پیشکسوتان[۳۱] – شرکتهایی که راهکارهای مناسبی برای نیازهای پایه مشتریان خود عرضه می‌کنند. نقطه اتکای این شرکت‌ها، مشتریان وفاداری است که از قابلیت‌های محصولات آنها همواره رضایت دارند.
- بازیگران کهنه‌کار[۳۲] – شرکت‌های بزرگ و صاحب‌نامی که اگر چه ممکن است امکانات و قابلیت‌های قدرتمندی ارائه کنند اما نوآوری در آنها سیری نزولی داشته و دیگر اثرگذاری گذشته را در بازار ندارند.

---

۲۵ Radicati Group
۲۶ Quadrant
۲۷ Top Players
۲۸ Trail Blazers
۲۹ Specialists
۳۰ Emerging Players
۳۱ Established Vendor
۳۲ Mature Players

Radicati Endpoint Security عنوان یکی از گزارش‌های این شرکت است. در گزارش مذکور، قابلیت‌های برند، در حوزه امکانات توزیع، پشتیبانی از بسترها و سیستم‌های عامل مختلف، شناسایی بدافزار، توانایی حذف ضدویروس‌های دیگر، یکپارچگی با پودمان‌هایی همچون Active Directory، دیواره آتش، پالایش نشانی‌های URL، ارزیابی وضعیت نصب اصلاحیه‌های امنیتی و توزیع آنها، گزارش‌دهی، امنیت وب و ایمیل، کنترل دستگاه، رمزگذاری، کنترل دسترسی به شبکه، حفاظت از دستگاه‌های همراه، جلوگیری از نشت اطلاعات، مدیریت و راهبری، دارا بودن قرنطینه امن و شناسایی به همراه واکنش مورد بررسی قرار می‌گیرد.

جایگاه شرکت‌های مطرح در حوزه "امنیت نقاط پایانی" برای سال ۲۰۲۳ میلادی در چهارگانه رادیکاتی در نمودار زیر به تصویر کشیده شده است.



بخشی از توضیحات رادیکاتی در گزارش Endpoint Security سال ۲۰۲۳، در زیر قابل مطالعه است:

Trellix is a cybersecurity company founded in 2022 when a consortium led by Symphony Technology Group (STG) acquired and merged McAfee Enterprise and FireEye. Trellix offers security solutions, threat intelligence and services that protect business endpoints, networks, servers, the Cloud and more. Trellix is privately held.

Trellix's endpoint security portfolio delivers a broad range of defenses, including advanced defense capabilities needed for zero-day threats, while also integrating and working with third party solutions and native OS security controls.

Trellix provides advanced threat defenses, like pre-execution and post-execution machine learning analysis and advanced analytics for file-less based attacks.

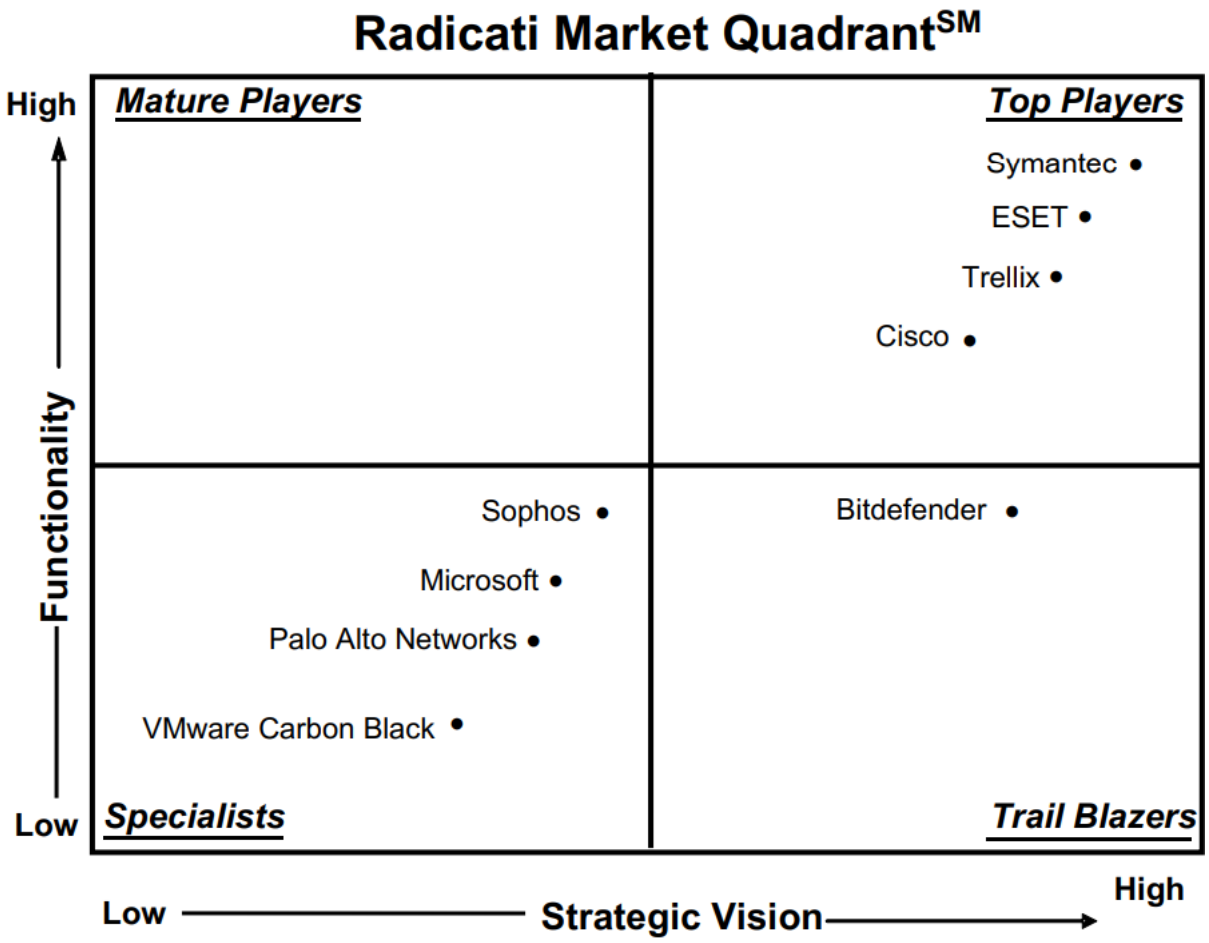
Trellix ePolicy Orchestrator is a powerful, single management console that allows administrators to create and manage policies across most Trellix security solutions.

Trellix's Endpoint Security provides a framework which enables IT to easily view, respond to, and manage the threat defense lifecycle.

Trellix Threat Intelligence Exchange secures systems in real time by operationalizing threat intelligence data and delivering protection to all points in the enterprise as new threats emerge. It leverages Data Exchange Layer (DXL) to instantly share threat data to all connected security systems, including third-party solutions.

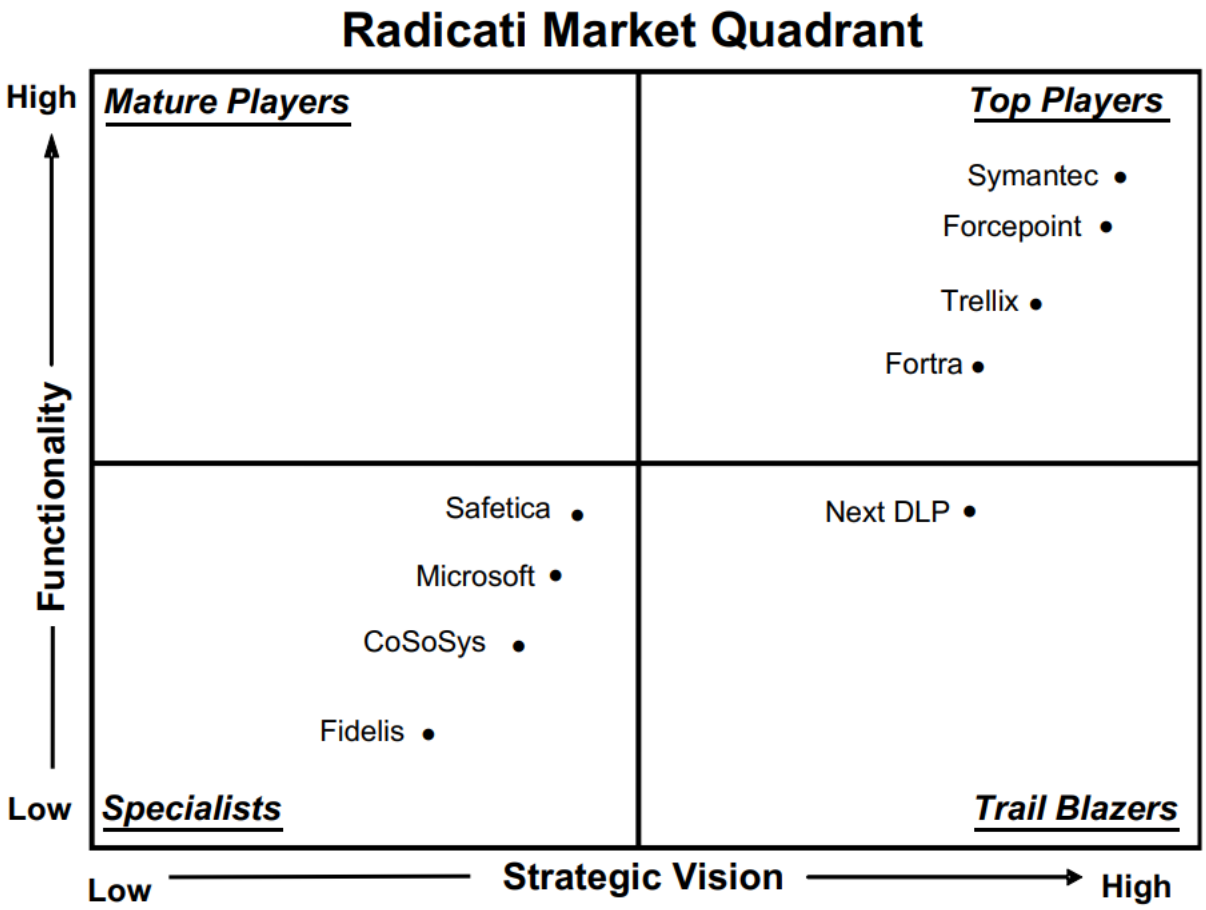
Trellix Application Control prevents zero-day attacks by blocking execution of unauthorized applications leveraging threat intelligence and custom rules. It uses inventory search and predefined reports to quickly find and fix vulnerabilities, compliance, and security issues in the customer environment. Trellix Application Control lets administrators combine rules based on file name, process name, parent process name, command line parameters, and username for enhanced protection.

Radicati Advanced Persistent Threat (APT) Protection عنوان گزارش دیگر رادیکاتی است که در آن عملکرد راهکارهای امنیتی در مقابله با تهدیدات روز-صفر و پیچیده و ماندگار مورد ارزیابی و بررسی قرار می‌گیرد. جایگاه شرکت‌های مطرح در حوزه "حفاظت از تهدیدات پیشرفته و ماندگار" برای سال ۲۰۲۳ میلادی در چهارگانه رادیکاتی در نمودار زیر به تصویر کشیده شده است.



Radicati Data Loss Prevention، عنوان یکی دیگر از گزارش‌های این شرکت است. در گزارش مذکور، منظور از Data Loss Prevention، تجهیزات، نرم‌افزارها، سرویس‌های مبتنی بر رایانش ابری و راهکارهای ترکیبی است که امکان نظارت و مدیریت داده‌های الکترونیکی را با هدف کمک به سازمان در جلوگیری از به اشتراک گذاشته شدن اطلاعات غیرمجاز فراهم می‌کنند. از این راهکارها برای حفاظت از داده‌های غیرفعال[۳۳]، داده‌های در حال استفاده[۳۴] و داده‌های در حرکت[۳۵] بهره گرفته می‌شود. علاوه بر آن، این راهکارها دارای قابلیت معروف به آگاه-از-محتوا[۳۶] بوده که بدان معناست که آنها قادر به درک محتوای مورد حفاظت در سطحی فراتر از تشخیص ساده کلیدواژه‌ها هستند. در گزارش رادیکاتی بر روی راهکارهای موسوم به Full DLP تمرکز شده که قادر به حفاظت از داده‌های غیرفعال، در حال استفاده و در حرکت بوده و از محتوای داده‌های مورد حفاظت آگاه هستند.

جایگاه شرکت‌های مطرح در حوزه "پیشگیری از نشت اطلاعات" برای سال ۲۰۲۳ در چهارگانه رادیکاتی در نمودار زیر به تصویر کشیده شده است.



[۳۳] Data at Rest
[۳۴] Data in Use
[۳۵] Data in Motion
[۳۶] Content-aware

بخشی از توضیحات رادیکاتی در گزارش Radicati Data Loss Prevention سال ۲۰۲۳، در زیر قابل مطالعه است:

> *Trellix DLP Endpoint controls data transfers that happen on endpoints via applications, removable storage devices, web, email, clipboard, screen capture, network sharing, as well as cloud. It can block, alert, notify, encrypt, quarantine, and perform other actions on sensitive data on an endpoint. DLP Endpoint provides Web Post support for Google Chrome browser. It is available for both Macs and PCs.*
>
> *Trellix Device Control manages and controls the copying of data to removable media and storage devices, such as USB drives, CDs, DVDs, Bluetooth, imaging equipment, and more. Transfers can be blocked based on content, context, or device type. It is available for both Macs and PCs.*

فارستر (Forrester)

شرکت فارستر[۳۷]، مک‌آفی را در حوزه "Data Security Portfolio"، به‌عنوان یک "بازیگر قدرتمند"[۳۸] معرفی می‌کند.

McAfee builds on a device to cloud data security approach, with an open architecture.

McAfee supports a Zero Trust approach with a range of capabilities across data, endpoint, and cloud security, in addition to security analytics. In data security, strengths include security data analytics, encryption, manageability of operations, and integrations.

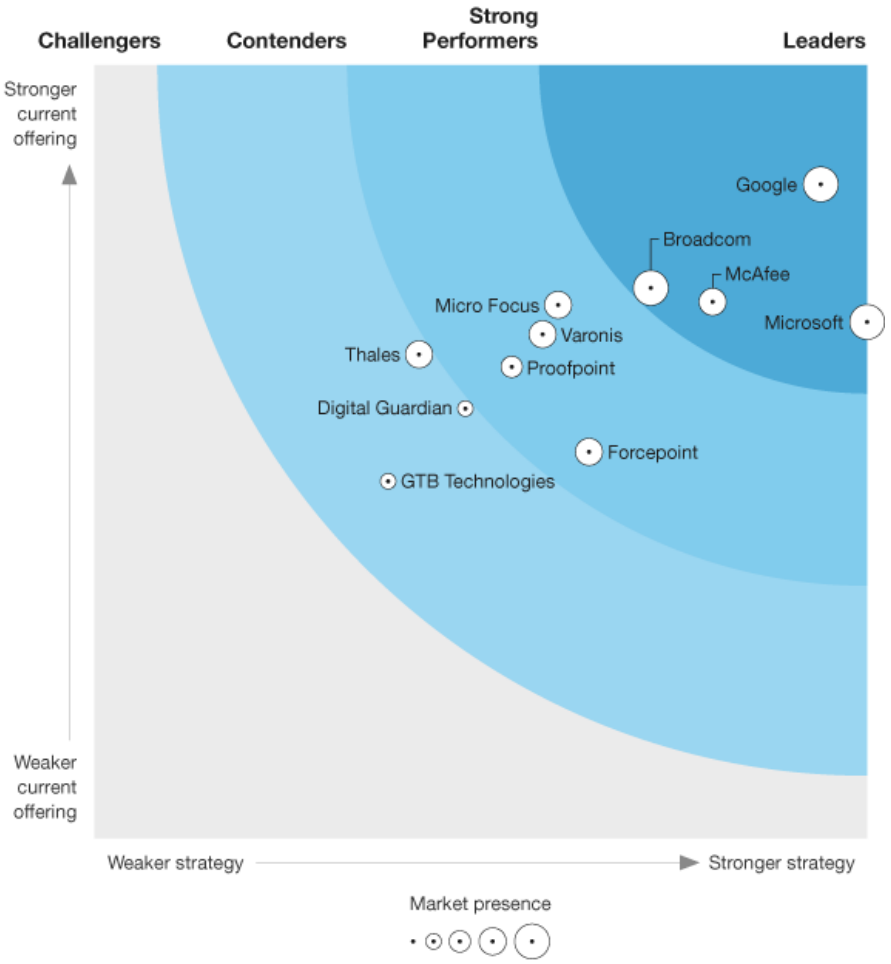
Customers have positive feedback regarding ePO for management and improvements with support. McAfee is a good fit for buyers seeking to centralize management of data protection policies and incident management.

The Forrester Wave: Data Security Portfolio Vendors, Q2 2019

---

[۳۷] Forrester Research, Inc
[۳۸] Strong Performer

همچنین این شرکت، در ارزیابی سه‌ماهه دوم سال ۲۰۲۱، مک‌آفی را در حوزه راهکارهای "Unstructured Data Security Platforms"، به‌عنوان یک "پیشگام" معرفی کرد.



McAfee Data Protection brings together a portfolio of product offerings a wide range of products including DLP, Drive Encryption, Native Encryption, and File and Removable Media Protection.

It serves a wide range of enterprise and midmarket clients, with heavy focus on supporting security and data protection in the cloud.

McAfee supports a Zero Trust approach with a range of capabilities across data, endpoint, and cloud security and a rich set of integrations.

Customer references noted its ease of deployment and management, integrations, and breadth of capabilities (in particular, capabilities for supporting remote work and cloud use). Security buyers looking for centralized management of data protection policies across their environment, cloud security, and incident management from devices to cloud should consider McAfee a strong option.

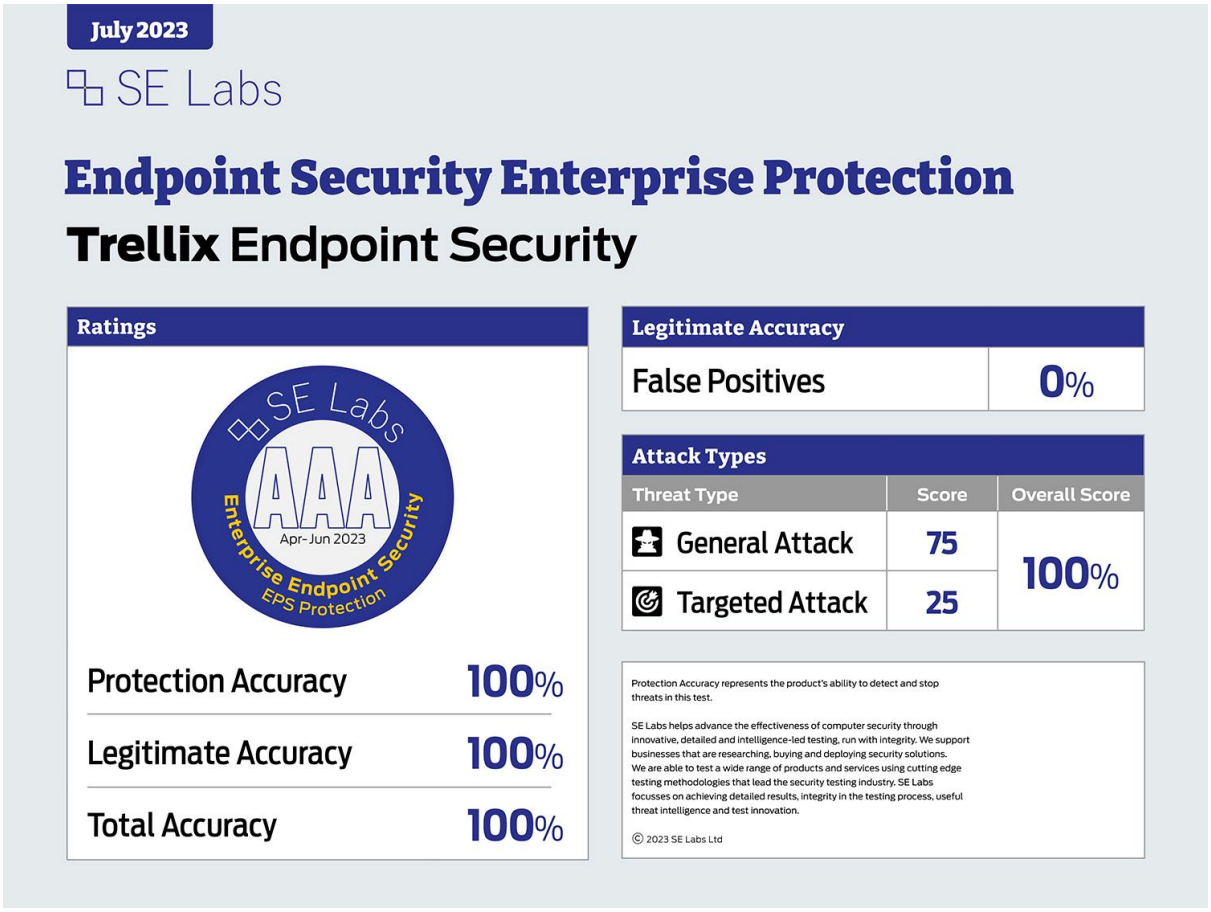
The Forrester Wave: Unstructured Data Security Platforms, Q2 2021

اس‌ای لبز (SE Labs)

شرکت اس‌ای لبز[۳۹]، یک شرکت خصوصی مستقل است که محصولات و خدمات امنیتی را ارزیابی می کند. آزمایشگاه اصلی آن در ویمبلدون، جنوب لندن واقع شده است. نتایج ارزیابی Trellix Endpoint Security در حوزه Small Business Protection در زیر نمایش داده شده است.

[۳۹] SE Labs Ltd

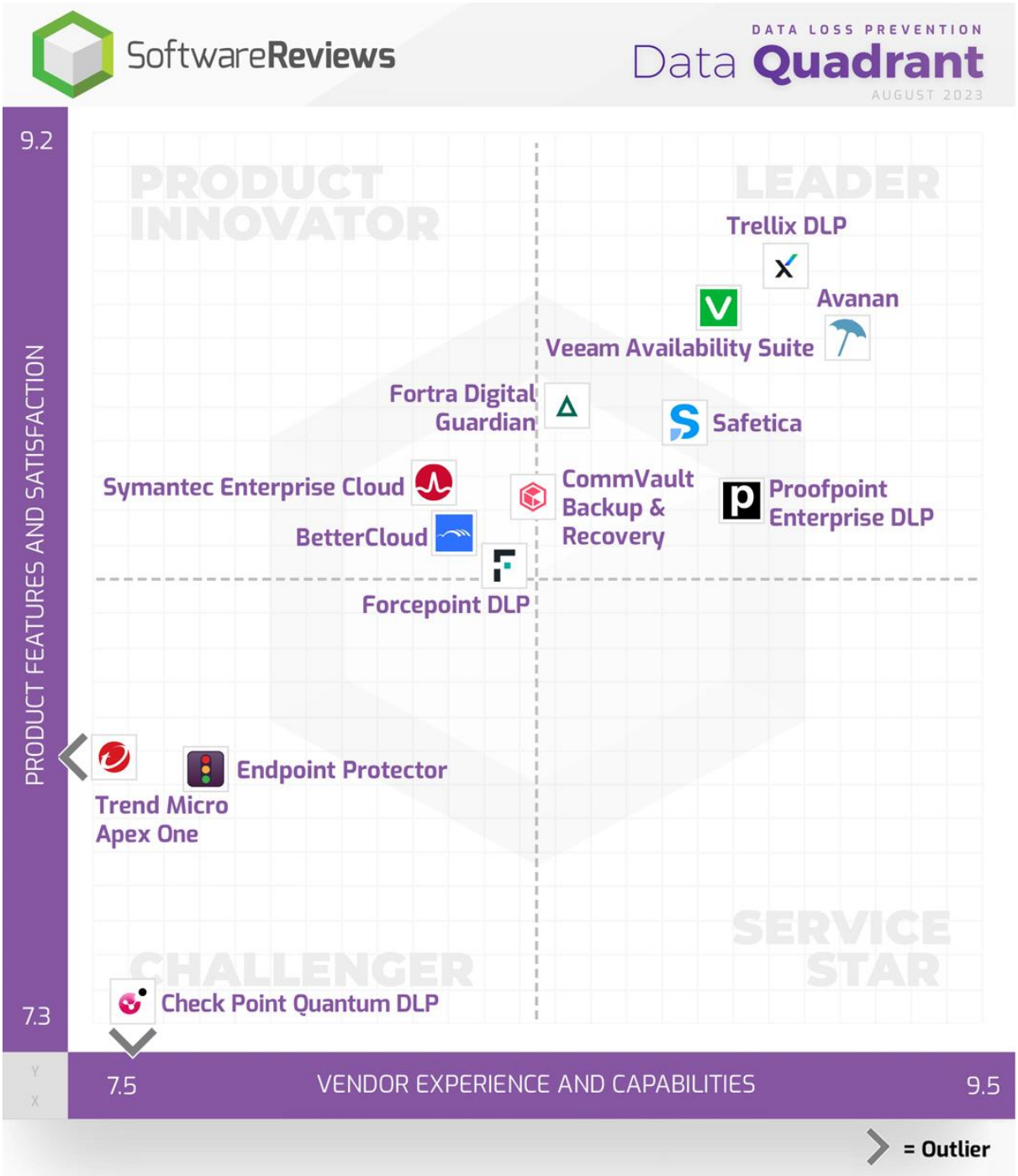
نتایج بررسی و ارزیابی Trellix Endpoint Security در حوزه Enterprise Protection نیز در زیر ارائه شده است.



Trellix Endpoint Security در تمامی بخش‌ها موفق به کسب امتیاز کامل و بالاترین نشان اس‌ای لبز، یعنی AAA شده است.

سافت‌ور ریویوز (SoftwareReviews)

در سال ۲۰۲۳، سایت SoftwareReviews.com در مربع چهارگانه Data Quadrant خود، راهکار Trellix DLP را جایگاه Leader قرار داد.



درباره شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است.

در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (سازنده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International، به‌تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای سازمانی ضدویروس McAfee ادامه داد. اخیراً بخش خدمات و محصولات سازمانی McAfee به همراه شرکت FireEye توسط گروه سرمایه‌گذاری STG خریداری و در هم ادغام شدند و اکنون این دو غول امنیت فناوری اطلاعات تحت نام Trellix در حال گذار و یکپارچه‌سازی محصولات دو شرکت تحت نام جدید هستند.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این

نقل‌وانتقال، شرکت مهندسی شبکه گستر با همکاری شرکت Sophos، فعالیت خود را در این زمینه ادامه داد و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید.

از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به‌عنوان نماینده توزیع (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee سابق، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

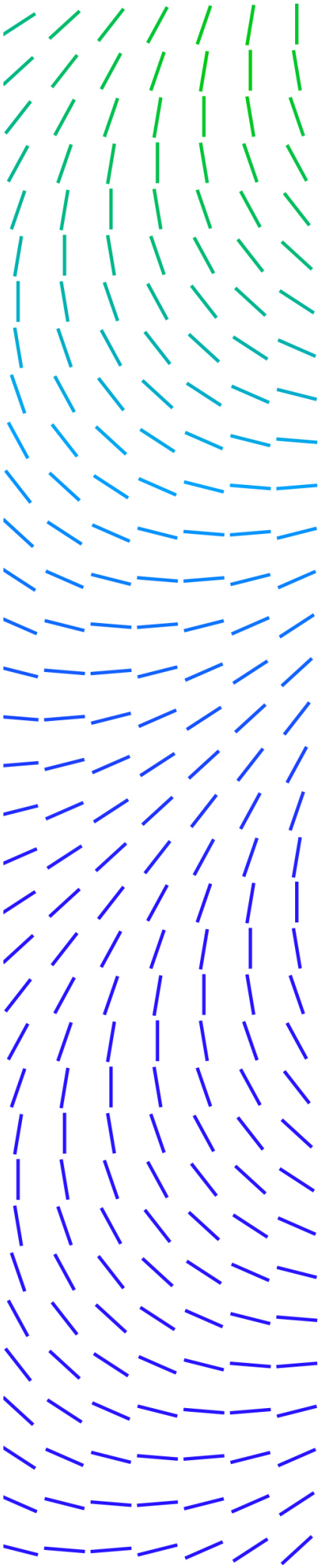
سال ۱۴۰۰ برخی ملاحظات ملی و بین‌المللی و همچنین جایگاه ثابت شرکت Kaspersky در بین دیگر شرکت‌های ضدویروس رده اول جهان، آغازگر توجه شبکه گستر به این شرکت امنیتی بوده است. اکنون شرکت مهندسی شبکه گستر در قالب همکاری رسمی، محصولات و خدمات شرکت Kaspersky نیز را به کاربران ایرانی ارائه می‌نماید.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور می‌باشد.

شرکت مهندسی شبکه گستر، از ابتدای تأسیس، گواهینامه احراز صلاحیت و طبقه‌بندی از شورای عالی انفورماتیک کشور را کسب کرده است. با حفظ استانداردهای مورد لزوم و افزایش سوابق و فعالیت ها، علاوه بر ارتقاء رتبه این شرکت در طبقه‌بندی شورایعالی انفورماتیک، تعداد بخش‌های تخصصی که شرکت مهندسی شبکه گستر مجاز به فعالیت در آنها می‌باشد نیز افزایش یافته است.

همچنین شرکت مهندسی شبکه گستر دارای پروانه فعالیت از مرکز راهبردی افتای ریاست جمهوری و سازمان فناوری اطلاعات در حوزه ارائه خدمات فنی افتا می‌باشد.

این شرکت همکاری نزدیکی با مرکز راهبردی افتای ریاست جمهوری در تهیه اخبار و هشدارهای امنیتی در حوزه فناوری اطلاعات دارد.



شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶ خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار	۰۲۱ – ۴۲۰۵۲
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net

SLS-775-07