AV comparatives

Independent Tests
of Anti-Virus Software

مقایسه توان شناسایی دقیق بدافزارها در

محصولات ضدویروس سازمانی

شبکه گستر

امنیت شما | وظیفه ما

موسسه AV-Comparatives در هر سال، در یکی از آزمون‌های خود با عنوان Business Test به بررسی محصولات ضدویروس سازمانی می‌پردازد.

این موسسه در اردیبهشت ماه ۱۳۹۷، نتایج آزمون سال ۲۰۱۸ محصولات ضدویروس سازمانی را در بخش‌های "محافظت در دنیای واقعی"[۱] و "محافظت در برابر بدافزارها"[۲] منتشر کرد.

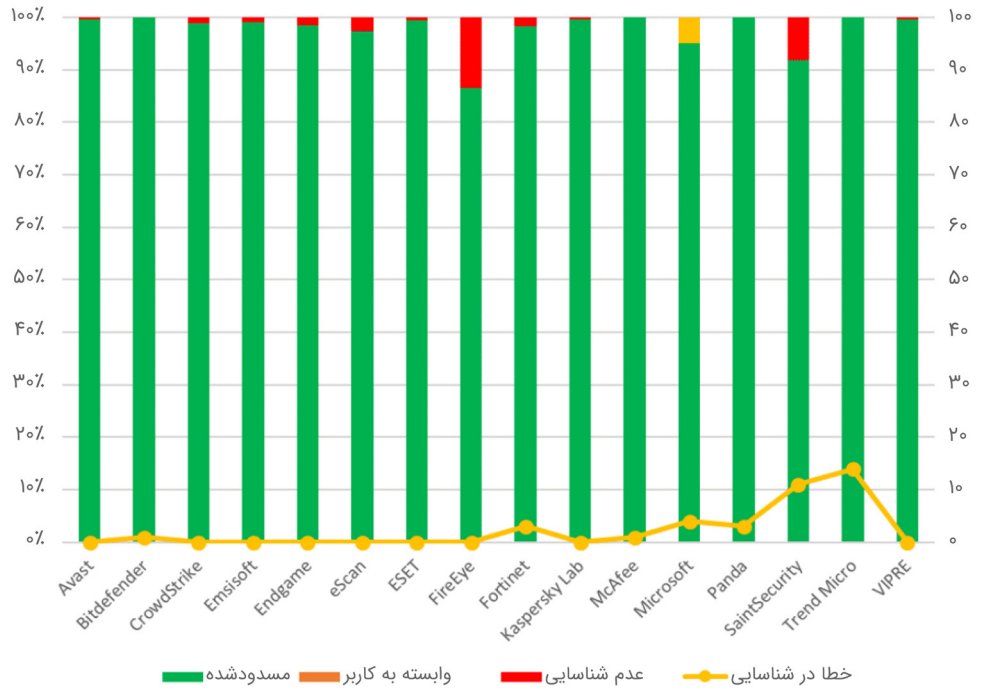
در این آزمون، محصولات زیر در بستر سیستم عامل Windows 10 RS3 b4-bit مورد بررسی قرار گرفته‌اند:

- Avast Business Antivirus Pro Plus 18.1 & 18.2
- Bitdefender Endpoint Security Elite 6.2
- CrowdStrike Falcon Prevent 4.0
- Emsisoft Anti-Malware 2018.2 & 2018.3
- Endgame Endpoint Security 2.5
- eScan Corporate 360 14.0
- ESET Endpoint Security 6.6
- FireEye HX Endpoint Threat Protection Platform 4.0
- Fortinet FortiClient with FortiGate & FortiSandbox 5.6
- Kaspersky Lab Endpoint Security 10.3
- McAfee Endpoint Security with Adaptive Threat Protection 10.5
- Microsoft Windows Defender for Enterprise 4.12
- Panda Endpoint Protection Plus 7.90
- Saint Security MAX Antivirus 1.0
- Trend Micro OfficeScan XG 12.0
- VIPRE Endpoint Security 10.1

محافظت در دنیای واقعی

"محافظت در دنیای واقعی" از جمله بخش‌های کلیدی در آزمون‌های AV-Comparatives به شمار می‌آید. در این بخش از تمام امکانات و قابلیت‌های ضدویروس برای مقابله با انواع تهدیدات، مشابه آنچه که هر روز در دنیای واقعی رخ می‌دهد، استفاده می‌شود. ضدویروس‌ها باید عملکرد بالایی نشان دهند، بدون آنکه درصد خطای زیادی داشته باشند و یا نیاز به دخالت مکرر کاربر باشد.

در این بخش از آزمون سال ۲۰۱۸، توان شناسایی محصولات در برابر ۶۲۰ نمونه تهدید مورد بررسی قرار گرفته که نتایج آن در نمودار زیر قابل مشاهده است.



۱ Real-World Protection
۲ Malware Protection

همچنین جزییات امتیازهای کسب شده در این بخش از آزمون در جدول زیر نمایش داده شده است.

	مسدودشده	وابسته به کاربر	عدم شناسایی	نرخ شناسایی [۲ / (وابسته به کاربر٪) + مسدودشده٪]	خطا در شناسایی
Bitdefender, McAfee	۶۲۰	-	-	۱۰۰٪	۱
Panda	۶۲۰	-	-	۱۰۰٪	۳
Trend Micro	۶۲۰	-	-	۱۰۰٪	۱۴
Avast, Kaspersky Lab, VIPRE	۶۱۸	-	۲	۹۹/۷٪	۰
ESET	۶۱۶	-	۴	۹۹/۴٪	۰
Emsisoft	۶۱۴	-	۶	۹۹/۰٪	۰
CrowdStrike	۶۱۳	-	۷	۹۸/۹٪	۰
Endgame	۶۱۰	-	۱۰	۹۸/۴٪	۰
Fortinet	۶۰۹	-	۱۱	۹۸/۲٪	۳
Microsoft	۵۸۹	۳۱	-	۹۷/۵٪	۴
eScan	۶۰۳	-	۱۷	۹۷/۳٪	۰
Saint Security	۵۶۹	-	۵۱	۹۱/۸٪	۱۱
FireEye	۵۳۶	-	۸۴	۸۶/۵٪	۰

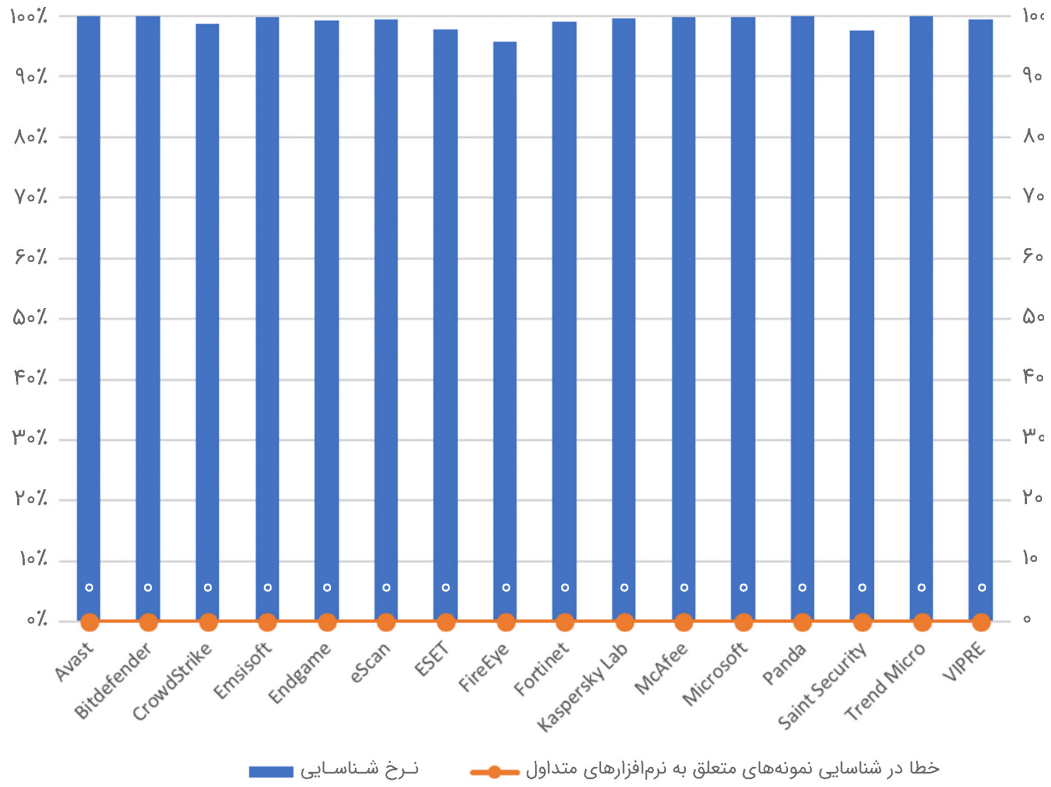
محافظت در برابر بدافزارها

در بخش "محافظت در برابر بدافزارها"، توانایی محصول در جلوگیری از آلوده شدن دستگاه در حین و پس از اجرای فایل‌های مخرب مورد ارزیابی قرار می‌گیرد. همچنین در این بخش از روش‌های مختلف رخنه همچون انتقال از ذخیره‌ساز قابل حمل، کپی شدن از پوشه‌های اشتراکی یا ذخیره از طریق ایمیل استفاده می‌شود.

روش تحقیق این بخش از مراحل زیر تشکیل شده است:

- پیش از اجرا، نمونه در معرض پویش موسوم به بلادرنگ[۱] (در صورت فراهم بودن این قابلیت) محصول قرار می‌گیرد.
- در صورت شناسایی نشدن در مرحله قبل، نمونه بر روی سیستم اجرا می‌شود. در این مرحله محصول قادر به برقراری ارتباط با اینترنت / ابر خود و بهره‌گیری از قابلیت‌هایی همچون رفتارشناسی می‌باشد.
- در صورتی که محصول موفق به شناسایی بدافزار نشده یا تمامی خرابکاری‌های اعمال شده توسط بدافزار را در مهلت تعیین شده به حالت قبل باز نگرداند، امتیاز منفی به آن تعلق خواهد گرفت.

در این بخش، از ۱۴۷۰ بدافزار جدید استفاده شده که نتایج آن در نمودار زیر ارائه شده است.



۱ On-access Scan

جزییات امتیازهای کسب شده در بخش "محافظت در برابر بدافزارها" نیز در جدول زیر نمایش داده شده است.

	مسدودشده	خطا در شناسایی نمونه‌های متعلق به نرم‌افزارهای متداول
Avast, Bitdefender, Panda, Trend Micro	۱۰۰٪	۰
Microsoft	۹۹/۹٪	۰
Emsisoft, McAfee, Kaspersky Lab	۹۹/۷٪	۰
eScan, VIPRE	۹۹/۵٪	۰
Endgame	۹۹/۳٪	۰
Fortinet	۹۹/۰٪	۰
CrowdStrike	۹۸/۸٪	۰
ESET	۹۷/۸٪	۰
Saint Security	۹۷/۶٪	۰
FireEye	۹۵/۹٪	۰

خطا در شناسایی

یکی از عوامل تاثیرگذار در هر دو بخش فوق واکنش به یک فایل سالم به عنوان فایل مخرب است. در حقیقت هر "خطا در شناسایی"[1] در این بخش‌ها امتیازی منفی برای محصول تلقی می‌شود. ضمن اینکه به‌منظور ارزیابی دقیق‌تر قابلیت شناسایی، بخشی از روش تحقیق این آزمون به بررسی تعداد "خطا در شناسایی" اختصاص داده شده و به همین جهت در فرآیند آزمون از برنامه‌های غیرتجاری و فایل‌های غیرمتداول نیز استفاده شده است. نتیجه این بخش از جمله مواردی است که باید به‌طور خاص مد نظر سازمان‌هایی که به‌نحو گسترده‌ای از برنامه‌های بومی استفاده می‌کنند قرار بگیرد.

نتایج حاصل شده در این بخش در جدول زیر نمایش داده شده است.

	خطا در شناسایی نمونه‌های متعلق به نرم‌افزارهای غیرمتداول
Avast, Bitdefender, Emsisoft, eScan, ESET, FireEye, Fortinet, Kaspersky Lab, McAfee, VIPRE	بسیار کم (صفر تا ۱۰)
Saint Security	کم (۱۱ تا ۵۰)
Endgame, Microsoft	زیاد (۵۱ تا ۱۰۰)
CrowdStrike, Panda, Trend Micro	بسیار زیاد (۱۰۱ تا ۵۰۰)

۱ False Positive

اتـــاق خـبـــر

newsroom.shabakeh.net

مـرکـز آمـــوزش

events.shabakeh.net

خدمات پس از فروش و پشتیبانی

my.shabakeh.net

تـارنـمـای شـرکت

www.shabakeh.net

درباره ما

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تاسیس شد. این شرکت یکی از باسابقه‌ترین شرکتهای فعال در حوزه امنیت فناوری اطلاعات است. با بیش از ۲۵ سال تجربه موفق در عرضه محصولات و خدمات امنیت شبکه، شرکت شبکه گستر افتخار خدمات‌دهی به هزاران شرکت و سازمان در بخش‌های مختلف کشور را دارد و مجری بزرگترین پروژه‌های نصب و نگهداری نرم‌افزارهای ضدبدافزار و سخت‌افزارهای دیواره آتش در کشور بوده است.

شبکه گستر

شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲-۰۲۱

info@shabakeh.net www.shabakeh.net