بهترین نرم افزارهای امنیتی 2019 برای دستگاه‌های متصل به شبکه

امنیت فناوری اطلاعات در سطح تجاری به‌سرعت در حال متحول‌شدن است، اما آن چیزی که همیشه مورد توجه بوده محافظت از دستگاه‌های متصل به شبکه سازمانی است. نقض‌های امنیتی اغلب در سازمان‌های بزرگ رخ می‌دهد. این یک واقعیت انکارناپذیر است که نفوذگران اغلب به دنبال شکارهای بزرگ هستند، اما درعین‌حال از سایر طعمه‌های پیرامون خود چشم‌پوشی نمی‌کنند و کسب‌وکارهای متوسط و کوچک به همان اندازه سازمان‌های بزرگ در معرض خطر هستند. درست مثل یک موتور جست‌وجو همچون گوگل که دائم وب را برای سایت‌های جدید و به‌روزرسانی‌ها اسکن می‌کند، خرابکاران سایبری نیز در گوشه و کنار اینترنت می‌خزند تا شبکه‌های دارای نقص، سیستم‌عامل‌های ضعیف و هر نوع راه نفوذ دیگری را که بتوانند از آن سوءاستفاده کنند، پیدا کنند. نکته جالب‌توجه آن‌که در اغلب موارد تمام این فرآیندها بدون مداخله انسانی انجام می‌شود.

وظیفه مدیران فناوری اطلاعات در کسب و کارهای کوچک به اندازه وظیفه همتایانشان در سازمان‌های بزرگ خطیر است. به همین دلیل، مدیریت امنیتی دستگاه‌های متصل به شبکه در تمام سازمان‌ها از اهمیت بالایی برخوردار است. در مجموعه‌های محافظتی استاندارد نیاز است تا یک بک‌اند مبتنی بر سرور ایجاد شود، نرم‌افزار اسکن کردن روی همه دستگاه‌ها مستقر شود و مسئولیت دریافت به‌روزرسانی‌های ارائه‌شده پذیرفته شود. با استفاده از یک سرویس مدیریت‌شده این وظایف پیچیده و خسته‌کننده توسط ارائه‌کننده سرویس انجام می‌شود. تمام وظایف بک‌اند را فروشنده مدیریت می‌کند و کاربران به‌طور خودکار نرم‌افزار و به‌روزرسانی‌ها را روی دستگاه خود دریافت خواهند کرد. همه این‌ها در حالی انجام می‌شود که بخش فناوری اطلاعات سازمان گزارش کاملی از تمام استثنائات، مشکلات و تهدیدات دریافت می‌کند.
کاهش هزینه‌ها و سرعت بخشیدن به پیاده‌سازی و به‌روزرسانی محافظت در مقابل بدافزارها برای هر کسب‌وکاری حیاتی است. تا وقتی که از داده‌های ارزشمندی نگهداری می‌کنید برای مجرمان فرقی نمی‌کند که شرکت شما چقدر بزرگ است. از سوی دیگر، مجرمان سایبری می‌توانند با استفاده از سیستم‌های یک کسب‌وکار کوچک اعتماد کسب‌وکارهای بزرگ را جلب کنند. در چنین شرایطی بخشی از مسئولیت صدمه‌های وارده بر عهده کسب‌وکار کوچک خواهد بود.

انتخاب یک نرم‌افزار امنیتی مناسب برای محافظت از دستگاه‌های متصل به شبکه برای کسب‌وکارهای متوسط و کوچک امری ضروری است. محصولاتی که از ویژگی‌های متعدد و متنوع برخوردارند برای مدیران امنیتی سازمانی مناسب هستند. از سوی دیگر، نباید وقت و انرژی مدیران امنیتی سازمانی را صرف مدیریت این محصولات کنید. انتخاب یک نرم‌افزار امنیتی با کنسول مدیریتی مناسب و ساده با گزینه‌های بصری قابل‌فهم می‌تواند یک انتخاب شایسته باشد. داشبوردها باید یک ارزیابی جامع از وضعیت امنیتی شرکت ارائه دهند و زمانی که چیزی اشتباه است، یک راهکار سریع و آسان برای مواجه‌شدن، ارزیابی مسئله و حل آن ارائه کنند. گزارش‌ها باید مفید و آموزنده باشد. سیاست‌گذاری‌ها باید بر اساس بهترین شیوه‌ها از پیش پیکربندی‌شده باشد. برای یک مدیر امنیتی کسب‌وکارهای متوسط و کوچک که کارهای زیادی برای انجام دادن دارد، استفاده از قابلیت‌های هشداردهی و اعلان‌ها می‌تواند مقدار

زیادی از وقت را صرفه‌جویی کند.

مطلب پیشنهادی

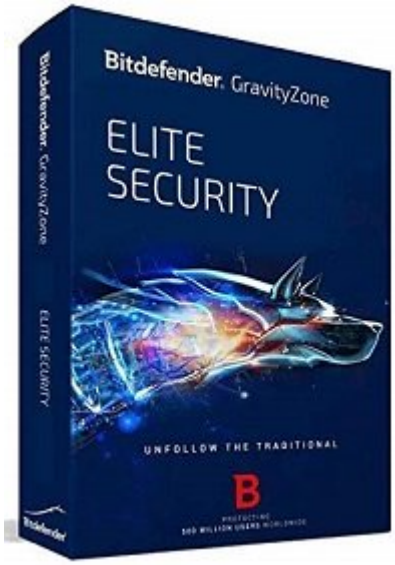
به‌کارگیری همزمان ضدویروس و ضدبدافزار
MalwareBytes ایده‌آل‌ترین مکمل برای ضدویروس دیفندر ویندوز 10 است

برای کارمندانی که دائم در حال سفر هستند باید امکاناتی در نظر گرفته شود. بعضی از این نرم‌افزارها شامل یک شبکه خصوصی مجازی هستند که اجازه می‌دهد در زمان سفر به‌طور امن به وبگردی بپردازند. سایر ابزارهای کاربردی نیز می‌توانند شامل ابزار مدیریت کلمات عبور و کدگذاری داده‌ها باشند که در برخی از این نوع نرم‌افزارهای امنیتی گنجانده شده است.
چالش پیش روی کسب‌وکارهای کوچک و متوسط این است که محصولی را انتخاب کنند که بتواند علاوه بر تهدیدات شناخته‌شده رفتارهای نامتعارف و شناخته‌نشده را شناسایی کند. برای این منظور، برخی از محصولات محافظتی شکلی از یادگیری ماشین اضافه‌شده به موتور ضدبدافزار خود را معرفی کرده‌اند که می‌تواند در زمان وقوع یک حمله سایبری رفتار آن را پیش‌بینی کرده و یک منبع و راهکار مناسب را برای برخورد با آن پیدا کند. این فناوری می‌تواند حملات مبتنی بر اسکریپت را که در گذشته قابل شناسایی نبودند، پیدا کند.
متاسفانه اسکنرهای بدافزار به‌اندازه کافی حساس نیستند که بتوانند تنها با استفاده از تنظیمات پیش‌فرض خود این‌گونه تهدیدات را پیدا کنند و از سوی دیگر، افزایش سطح حساسیت در این نرم‌افزارها گاهی اوقات روی عملکرد کاربران تاثیر منفی می‌گذارد. پیدا کردن یک سطح تعادل مناسب می‌تواند چالش‌برانگیز باشد و نتیجه آن در کوتاه‌مدت باعث نارضایتی کاربران خواهد شد. باید بر اساس میزان اهمیت داده‌های خود و سطح عملکرد سیستم‌ها یک راه‌حل مناسب را انتخاب کنید.
پرسشی که به ذهن خطور می‌کند این است که چه سطحی به‌اندازه کافی خوب است؟ پاسخ این پرسش از کاربری به کاربر دیگر متفاوت است و به نیازهای خاص، فرآیندهای سفارشی و عوامل خطر بستگی دارد. اما بدون شک، اینترنت روز به روز خطرناک‌تر می‌شود و در اختیار داشتن یک سیستم دفاعی مناسب برای کسب‌وکار مهم و حیاتی است.

مروری بر بهترین نرم‌افزارهای امنیتی برای محافظت از دستگاه‌های متصل به شبکه

قبل از معرفی محصولات کاربردی دفاع از تجهیزات شبکه ذکر این نکته ضروری است که قیمت‌ها بر مبنای قیمت‌های ارائه‌شده از سوی خرده‌فروشی‌های جهانی در این مقاله درج شده‌اند.

Bitdefender GravityZone Elite

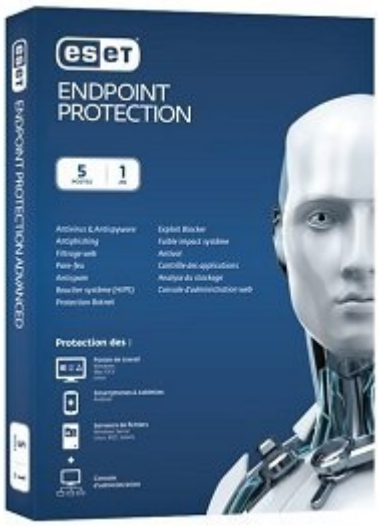


- امتیاز: 4.5
- قیمت خرده‌فروشی: 81 دلار
- مزایا: توانایی فوق‌العاده در شناسایی تهدیدات ناشناخته، ابزارهای مدیریت سیاست‌گذاری کارآمد، تحلیلگر Sandbox، داشبورد قابل سفارشی‌سازی، نمایش اقدامات صورت گرفته در یک حمله.
- معایب: عدم امکان بازگشت به حالت اولیه بعد از مواجه شدن با خسارات باج‌افزار.
- نتیجه: این نرم‌افزار امنیتی در فهرست مقایسه پلتفرم‌های امنیتی سطح تجاری با قابلیت‌هایی همچون شناسایی دقیق تهدیدات امنیتی حتی نمونه‌های ناشناس، امکانات سفارشی‌سازی بالا و محافظت در برابر بدافزارها همچنان صدرنشینی خود را حفظ کرده است.

مطلب پیشنهادی

آموزش نصب و استفاده از توتال سکیوریتی بیت دیفندر

ESET Endpoint Protection Standard



- امتیاز: 4.5
- قیمت خرده‌فروشی: 165 دلار
- مزایا: قدرت شناسایی تهدیدات فوق‌العاده، امکان مدیریت از راه دور ساده، توانایی تشخیص نفوذ قدرتمند، ابزار کارآمد برای پیگیری‌های قانونی.
- معایب: تشخیص حملات فیشینگ در این نرم‌افزار به نسبت ضعیف است. هیچ گزینه سندباکس دستی در آن وجود ندارد.
- نتیجه: کسب‌وکارهای کوچکی که به دنبال یک راهکار امنیتی موثر با قیمتی قابل‌قبول هستند باید به ESET Endpoint Protection نگاهی بیندازند. این پلتفرم مخاطبان کسب‌وکارهای کوچک و متوسط را هدف گرفته و در آزمایش‌های انجام‌گرفته ثابت کرده که با کمی مشکل در شناسایی حملات فیشینگ از عهده این کار برمی‌آید.

F-Secure Protection Service for Business

- امتیاز: 4
- قیمت خرده‌فروشی: 39 دلار
- مزایا: قابلیت شناسایی عالی بدافزار و اجرای اسکریپت‌های مخرب، امکان به‌روزرسانی نرم‌افزار در مقابل تهدیدات شناخته شده، شبکه خصوصی مجازی به‌عنوان بخشی از تجهیزات F-Secure Freedome.
- معایب: گزارش‌دهی می‌توانست بهتر انجام شود، سرعت کمتر نسبت به سایر محصولات معرفی‌شده.
- نتیجه: این نرم‌افزار امنیتی اقدامات پایه اعلام‌شده از طرف این شرکت را در زمینه حفظ امنیت تجاری ارائه می‌کند. این نرم‌افزار در گزارش‌دهی و مواجه‌شدن با اجرای اسکریپت‌های مخرب ضعف‌هایی دارد اما در مجموع یک راهکار قابل‌قبول را برای افزایش سطح امنیت سیستم در خود تعبیه کرده است.

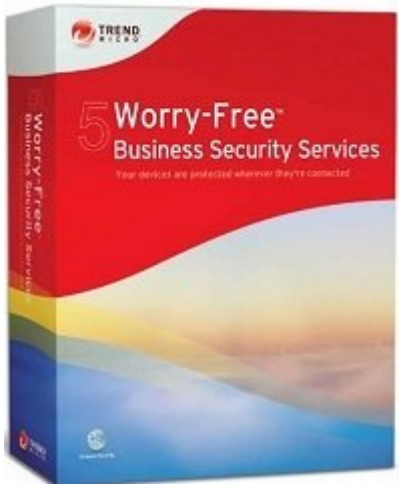
Symantec Endpoint Protection Cloud

- امتیاز: 4
- قیمت خرده‌فروشی: 4 دلار
- مزایا: محافظت عالی در برابر همه نوع تهدیدات امنیتی، سهولت در استفاده و ناوبری، قابلیت‌های مدیریتی قابل‌قبول برای دستگاه موبایل.
- معایب: کمبود امکانات ضدفیشینگ، عدم امکان گزارش‌گیری.
- نتیجه: این نرم‌افزار یک محصول امنیتی فوق‌العاده است، اما نقاط ضعف کمی هم دارد که از آن جمله می‌توان به کمبود امکانات ضدفیشینگ و عدم امکان گزارش‌گیری اشاره کرد.

Kaspersky Endpoint Security Cloud

- امتیاز: 3
- قیمت خرده‌فروشی: 300 دلار
- مزایا: سیستم شناسایی بدافزار و ویروس تهاجمی، محافظت قدرتمند از شبکه، شناسایی سریع حملات فیشینگ.
- معایب: داشبورد بی‌رونق و خسته‌کننده، ماژول گزارش‌گیری نه‌چندان درست، محدودیت‌های جست‌وجو در رویدادهای حسابرسی.
- نتیجه: این نرم‌افزار امنیتی در سیستم‌های محافظتی سرآمد است، اما در کنسول مدیریت ابر خود چندان موفق ظاهر نشده است. این سیستم محافظتی در زمینه ماژول گزارش‌گیری به اصلاحات نیاز دارد.

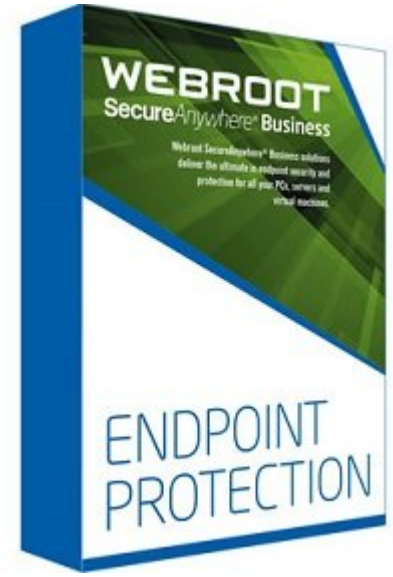
Trend Micro Worry-Free Business Security Services



- امتیاز: 3.5
- قیمت خرده‌فروشی: 75 دلار
- مزایا: شناسایی تهدیدات باینری و اسکریپت‌نویسی شده در حد قابل قبول، مدیریت کدگذاری داخلی، امکان شناسایی حملات فیشینگ، مدیریت دستگاه ساده، بهبود وضعیت تشخیص سو استفاده.
- معایب: هنوز برخی از انواع حملات مخفی را نادیده می‌گیرد.
- نتیجه: Trend Micro با نرم‌افزار Worry-Free Business Security Services امکانات قابل‌توجهی را در اختیارتان قرار می‌دهد. این محصول از اغلب شبکه‌های تجاری در برابر اکثر تهدیدات استاندارد بدافزار محافظت می‌کند، هر چند هنوز با برخی از انواع حملات مخفی مشکل داشته و آن‌ها را نادیده می‌گیرد. با پشتیبانی قابل‌قبول از پلتفرم‌های موبایل و حتی دفاع در برابر برخی باج‌افزارها، یک مجموعه امنیتی قدرتمند

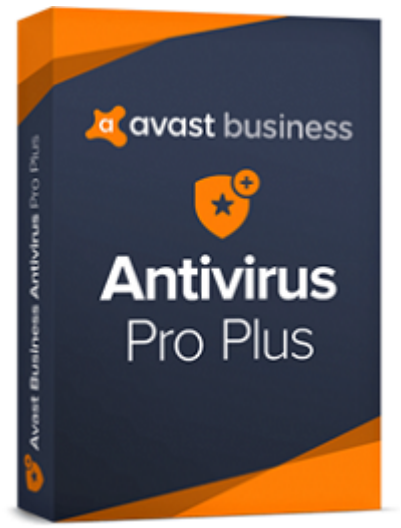
را در اختیار خواهید داشت.

Webroot SecureAnywhere Business Endpoint Protection



- امتیاز: 3.5
- قیمت خرده‌فروشی: 150 دلار
- مزایا: شناسایی حملات مبتنی بر مرورگر در سطحی بسیار بالا، توانایی بازگرداندن تغییرات اعمال شده از طرف باج‌افزار، شناسایی فایل‌های باینری مخرب، از کار انداختن سریع حملات مبتنی بر سند.
- معایب: در زمینه اقدامات دفاعی برای حملات مبتنی بر اسکریپت کمبود دارد. مقابله با حملات فیشینگ به ارتقای بیشتر نیاز دارد. به محض این‌که اسکریپت یا اپلیکیشن مهاجم به دسترسی مدیریتی دست پیدا کرد، این محصول با شکست مواجه می‌شود.
- نتیجه: این نرم‌افزار امنیتی در مقابل بدافزارهای استاندارد عالی عمل می‌کند، اما آزمایش‌های انجام شده روی این محصول نشان داد که در مقابل حمله‌های پیچیده مثل حمله‌های اسکریپت‌نویسی شده جدیدتر با مشکل مواجه می‌شود. اما در مجموع Webroot با ابزارهای فوق‌العاده‌ای که دارد ارزش امتحان کردن را خواهد داشت.

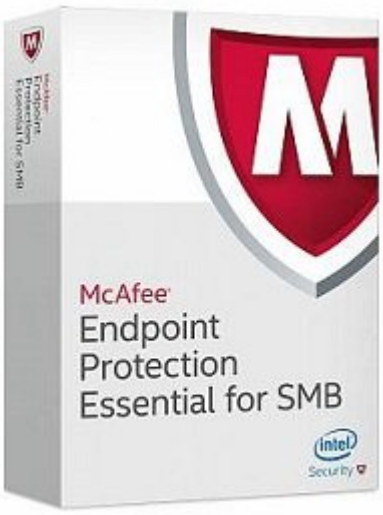
Avast Business Antivirus Pro Plus



امتیاز: 3.5
قیمت خرده‌فروشی: 60 دلار

مزایا: نصب و پیکربندی راحت، توانایی قابل‌قبول در تشخیص فایل‌های ناشناخته، قابلیت‌های کاربردی اضافی از قبیل شبکه خصوصی مجازی، قابلیت جلوگیری از حملات باج‌افزار.
معایب: داشبورد بیش‌ازحد ساده‌شده، فاقد ویژگی‌های گزارش‌گیری خوب.
نتیجه: این نرم‌افزار امنیتی با وجود سادگی، سطح محافظتی قابل قبولی را برای تهدیدات ناشناخته ارائه می‌کند. هر چند در گزارش‌گیری و پشتیبانی از دستگاه‌های موبایل کمی ضعیف عمل کرده است.

McAfee Endpoint Protection Essential for SMB



- امتیاز: 3
- قیمت خرده‌فروشی: 30 دلار
- مزایا: محافظت خوب در برابر بدافزار و ویروس، محیطی کاربرپسند، انبوهی از گزینه‌ها، امکانات گزارش‌گیری فوق‌العاده.
- معایب: ناوبری ePO (سرنام ePolicy Orchestrator) کمی گیج‌کننده است. گزینه‌های تنظیماتی بیش از اندازه برای کسب‌وکارهای کوچک، سطح عملکرد ضعیف در مقابل حملات فیشینگ.
- نتیجه: این نرم‌افزار امنیتی یک سیستم محافظتی مناسب برای دستگاه‌های شما است، اما تنظیمات آن برای کاربران پیچیده و زمان‌بر است. با کمی ساده‌سازی این محصول بیشتر مورد توجه کسب‌وکارهای کوچک خواهد بود.

Panda Security Adaptive Defense 360

- امتیاز: 3.5

- قیمت خرده‌فروشی: 68 دلار
- مزایا: رابط کاربری خوش‌ساخت، پیکربندی و پیاده‌سازی راحت، قدرت فوق‌العاده در شناسایی بدافزارهای شناخته‌شده، برخورداری از گروهی از تحلیلگران فعال برای تجزیه‌وتحلیل حملات ناشناس.
- معایب: عدم شناسایی برخی از سو استفاده‌های ناشناخته، حالت Hardening بیش‌ازحد محدودکننده، قابلیت‌های ضد فیشینگ ضعیف، فراهم نبودن امنیت کافی از سمت تنظیمات پیش‌فرض.
- نتیجه: این نرم‌افزار امنیتی وظیفه محافظت از کاربران را در برابر بدافزارهای شناخته‌شده (حتی باج‌افزار) به‌خوبی انجام می‌دهد. اما برای انجام این کار بیشتر از سایر رقبای خود به محدود کردن کاربران نیاز دارد.

GFI LanGuard Review

- امتیاز: 4.5
- قیمت خرده‌فروشی: 0 دلار
- مزایا: نصب ساده و سریع، رابط کاربری و چرخه کاری بصری، گزارش‌گیری جامع شامل مقررات گزارش‌های خاص.
- معایب: پیش‌نمایش‌های گزارش روی صفحه‌نمایش به‌صورت نادرست قالب‌بندی شده و خواندن آن غیرممکن است.
- نتیجه: این نرم‌افزار امنیتی یک اسکنر امنیت شبکه قدرتمند است که به ابزارهای ارزیابی آسیب‌پذیری و مدیریت وصله مجهز شده است. رابط کاربری گردش کار محور آن به‌خوبی طراحی‌شده، اما پیش‌نمایش‌های گزارش روی صفحه‌نمایش ضعیف طراحی‌شده است.

Kaspersky Small Office Security

- امتیاز: 2.5
- قیمت خرده‌فروشی: 113 دلار
- مزایا: شامل مدیریت کلمات عبور، کدگذاری فایل، پشتیبان‌گیری و بازیابی. پیکربندی از پیش تنظیم‌شده برای محافظت حداکثری، ضد بدافزاری برجسته و محافظ قدرتمند در برابر آدرس‌های اینترنتی مخرب و حملات فیشینگ، کنسول مدیریتی ساده به همراه قابلیت‌های تجاری، قابلیت بازگشت به وضعیت قبل از تخریب باج‌افزار.
- معایب: فقدان مدیریت مبتنی بر سیاست‌گذاری، گزارش‌گیری و گزینه‌های پیاده‌سازی که بسیاری از سازمان‌ها وجود آن را ضروری می‌دانند.
- نتیجه: این نرم‌افزار امنیتی خود را به‌عنوان یک راهکار امنیتی برای کسب‌وکارهای کوچک معرفی کرده است. اما با وجود قدرت محافظتی بالا از برخی قابلیت‌های مدیریتی، گزارش‌گیری و سایر امکانات مورد نیاز کاربران تجاری محروم مانده است.

تاریخ انتشار:

29 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/16031/%D8%A8%D9%87%D8%AA%D8%B1%DB%8C%D9%86-%D9%86%D8%B1%D9%85-%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-2019-%D8%A8%D8%B1%D8%A7%DB%8C-

%D8%AF%D8%B3%D8%AA%DA%AF%D8%A7%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AA%D8%B5%D9%84-%D8%A8%D9%87-%D8%B4%D8%A8%DA%A9%D9%87