پاسخ‌گویی و تشخیص نقاط پایانی و امنیت

Endpoint detection and response and Security (EDR)

فهرست مطالب

۱ مقدمه

فناوری امنیت سایبری EDR[۱] (پاسخ‌گویی و تشخیص نقاط پایانی)، نیاز به نظارت و پاسخ‌گویی مستمر به تهدیدهای امنیتی پیشرفته را برآورده می‌کند. در اینجا فهرستی از مهم‌ترین فناوری‌های EDR قابل توجه، آمده است.

EDR یک فناوری امنیت سایبری است که نیاز به نظارت و پاسخ مستمر به تهدیدهای امنیتی را برآورده می‌کند. این فناوری زیرمجموعه‌ای از فناوری امنیت نقاط پایانی[۲] و بخش حساسی از وضعیت مطلوب امنیتی[۳] است. EDR با سایر بسترهای حافظت نقاط پایانی (EPP)[۴] مانند آنتی‌ویروس و ضدتروجان[۵] متفاوت است. آن‌ها تمرکز عمده خود را بر توقف خودکار تهدیدها در مرحله پیش از اجرا[۶] نگذاشته‌اند ولی EDR یک مشاهده و بینش درستی از نقاط پایانی[۷] را فراهم می‌کند تا به تحلیل‌گرها در جهت کشف، بررسی و پاسخ‌گویی به تهدیدات بسیار پیشرفته و حملات گسترده‌تر که در نقاط پایانی متعدد گسترش می‌یابند، مساعدت کند. با این وجود بسیاری از ابزارهای تشخیص و پاسخ‌گویی نقاط پایانی، EDR را با EPP ترکیب می‌کنند.

۲ گستردگی EDR

بازار EDR با دلیلی منطقی، به سرعت در حال رشد است. نقض‌های (breaches) امنیتی بیش از زمان‌های دیگر در حال افزایش است و اغلب از طریق نقاط پایانی، به شبکه راه می‌یابند. تنها چیزی که جهت رخنه و ورود مخفیانه موردنیاز است یک کاربر با اطلاعات کم در زمینه‌های امنیتی و افرادی که از آن‌ها سوءاستفاده کنند، است.

مطابق اعلام Gartner درآمد EDR در سال ۲۰۱۶ بیش از دو برابر شده و به ۵۰۰ میلیون دلار رسیده است. بیش از نیمی از این فروش کل متعلق به چهار شرکت -**Tanium**، **FireEye**، **CrowdStrike** و

---

[۱] Endpoint Detection and Response
[۲] Endpoint security
[۳] Optimal security posture
[۴] Endpoint protection platforms
[۵] Anti-malware
[۶] Pre-execution
[۷] Endpoint

Carbon Black- است. اما موارد دیگری نیز وجود دارند که ارزش ذکرکردن را دارند. در این مستند همچنین به بررسی Guidance، Symantec، Cyberreason، RSA، Cisco و Countertack خواهیم پرداخت.

Avivah Litan یک تحلیل‌گر Gatner گفته است: "ما انتظار داریم در ادامه، ثبات قابل‌توجهی در بازار امنیت نقاط پایانی اتفاق بیفتد. محصولات امنیت نقاط پایانی باید سطح اطلاعات و هشدارهایی که به کاربر می‌دهند و سطح داده‌ها را بالابرده و همچنین قابلیت‌های خود در پاسخ‌گویی و پاک‌سازی، به‌صورت خودکار درآورند."

علی‌رغم این ثبات، پیش‌بینی Gatner مبنی بر رشد پنجاه درصدی سالانه EDR، حداقل تا سال ۲۰۲۰ است. این امر موجب تمایز قابل‌توجه EDR نسبت به سایر حوزه‌های فناوری اطلاعات می‌شود که رشد سالانه آن‌ها تنها ۷ درصد است. عامل دیگر در رشد شدید EDR این واقعیت است که در مقایسه با تعداد تقریبی ۷۱۱ میلیون رایانه رومیزی، لپ‌تاپ و سایر دستگاه‌هایی که از نرم‌افزار استفاده می‌کنند، تنها بر روی ۴۰ میلیون نقاط پایانی، EDR نصب‌شده است.

۳ ویژگی‌های اغلب راه‌حل‌ها (محصولات) EDR

ویژگی‌های اغلب راه‌حل‌های EDR، عبارتند از:

- توانایی تشخیص و جلوگیری از فرآیندهای بهره‌برداری پنهان که پیچیده‌تر از یک امضا یا الگوی ساده هستند.
- هوشمندی تهدید[۸]
- قابلیت مشاهده نقاط پایانی، شامل برنامه‌های کاربردی، پردازش‌ها و ارتباطات جهت تشخیص فعالیت‌های مخرب و ساده‌سازی پاسخ‌گویی به حوادث امنیتی.
- خودکارسازی هشدارها و همچنین پاسخ‌های تدافعی مانند پایان‌دادن به فرآیندهای خاص در زمانی که یک حمله تشخیص داده می‌شود.
- قابلیت جرم‌شناسی، چون که زمانی که یک مهاجم وارد می‌شود، نیاز به توانایی تفحص عمیق در فعالیت‌های آن برای درک حرکات آن و حداقل کردن اثرات منفی آن، وجود دارد.

[۸] Threat intelligence

- جمع‌آوری داده برای ایجاد مخازن لازم برای تجزیه‌وتحلیل‌ها.

۴ ده محصول (شرکت) برتر EDR

در اینجا به ۱۰ محصول برتر EDR که ارزش بررسی دارند، می‌پردازیم. Gatner در گزارش خود با عنوان "چشم‌انداز رقابتی: ابزارهای EDR" هر یک از این فروشندگان را به‌عنوان ده ارائه‌کننده برتر، برحسب سهم بازار معرفی کرده است. این مستند همچنین ویژگی‌های متفاوات موردنیاز جهت محصولات EDR که در اینجا بررسی‌شده‌اند را نیز مطرح کرده است.

در ادامه خلاصه‌ای از محصولات EDR را بیا شده است و در انتهای این مستند نیز جدولی، جهت مقایسه ویژگی‌های محصولات EDR، آمده است.

۴-۱ امنیت نقاط پایانی FireEye

FireEye به سازمان‌های با ۲۵۰ تا ۳۵۰.۰۰۰ نقاط پایانی سرویس‌دهی می‌کند و همچنین با یک محصول امنیت شبکه نقاط پایانی با نام CloudHX در حال نفوذ به بازار شرکت‌های کوچک‌تر است. این شرکت بیش از ۱۰۰۰ متخصص دارد که به حوادث پاسخ می‌دهند و در زمینه حملات تحقیقات انجام می‌دهند. ابزارهای اسکن شبکه آن به توان عملیاتی بیش از ۱۰۰۰ Mbps تقویت‌شده‌اند [۱].

۴-۲ Carbon Black Cb Response

Carbon Black مفتخر به تأمین بخش امنیت شبکه آژانس اطلاعات مرکزی (CIA)[۹] و آژانس امنیت ملی (NSA)[۱۰] بوده و بدون محدودیت در مقیاس‌پذیری، به ازای هر کلاستر ۱۵۰.۰۰۰ نقاط پایانی را پشتیبانی می‌کند. این EDR را می‌توان به‌عنوان نرم‌افزار و یا در فضای ابر و با اشتراک سالیانه از ۳۰ دلار به ازای هر نقاط پایانی، مورداستفاده قرار داد [۱].

[۹] Central Intelligence Agency
[۱۰] National Security Agency

۳-۴ Guidance Software EnCase Endpoint Security

EnCase بخش عمده‌ای از ۵۰۰ شرکت برتر آمریکا را به‌عنوان مشتری خود دارد. این EDR قابلیت مقیاس‌پذیری از ده الی صدها هزار گره را دارد و همچنین برای ایمن‌کردن دستگاه‌های ATM، POS و دستگاه‌های صنعتی، استفاده‌شده است [۱].

۴-۴ Cybereason Total Enterprise Protection

Cybereason توسط متخصصان هوش سایبری کشوری و برای شرکت‌های با اندازه‌های مختلف و تخصص کم در امنیت اطلاعات راه‌اندازی شد. این EDR محدودیتی در تعداد نقاط پایانی پشتیبانی‌شده ندارد و می‌تواند ۸ میلیون پرسش را در هر ثانیه، پردازش کند [۱].

۵-۴ Symantec Endpoint Protection

Symantec تقریباً تمامی تهدیدات پیشرفته را متوقف می‌کند و افزونه EDR شرکت، بررسی و پاسخ‌گویی به حوادث را نیز اضافه می‌کند. این محصول، قابلیت مقیاس‌پذیری الی صدها هزار گره را دارد و توسط بزرگ‌ترین شبکه هوشمندی تهدید دنیا، پشتیبانی شود [۱]

۶-۴ RSA NetWitness Endpoint

NetWitness بیش از ۳۰۰ شاخص رفتاری ارائه می‌کند که کاربران می‌توانند آن‌ها را شخصی‌سازی (تنظیم) کنند. این EDR از تحلیل‌های رفتاری، یادگیری ماشین و هوشمندی تهدید جهت تشخیص و اولویت‌بندی تهدیدها، بهره می‌برد [۱].

۷-۴ Cisco Advanced Malware Protection for Endpoints

ویژگی **Cisco AMP**، قابلیت تشخیص سریع و کسب رکورد صددرصد امتیاز جهت تشخیص تروجان و اکسپلویت از آزمایشگاه‌های NSS، است. چهارده تکنیک تشخیص یکپارچه آن می‌تواند حدود ۲۰ میلیارد تهدید را در روز، مسدود کنند [۱].

۸-۴ Tanium

Tanium EDR، ۴۰۰ میلیون دلار سرمایه از شرکت‌های سرمایه‌گذاری سطح بالا را در اختیار دارد و در سال گذشته فروش خود را دو برابر کرد. معماری این محصول بدون نیاز به زیرساخت‌های اضافی می‌تواند تا میلیون‌ها نقاط پایانی گسترش یابد. ۱۲ مورد از ۱۵ بانک برتر دنیا، مشتری‌های این محصول هستند [۱].

۹-۴ CrowdStrike Falcon Insight

Falcon Insight یک پلت‌فرم مبتنی بر ابر است که روزانه بیش از ۳۰ میلیارد حادثه در نقاط پایانی را از میلیون‌ها حس‌گر استفاده‌شده در ۱۷۶ کشور جمع‌آوری و تحلیل می‌کند [۱].

۱۰-۴ CounterTack Endpoint Threat

CounterTack از یک همکاری استراتژیک با پلت‌فرم‌های تجزیه‌وتحلیل درون‌حافظه‌ای SAP's HANA برای انجام میلیاردها اسکن در ثانیه بهره می‌برد. CounterTack ترکیبی از تحلیل رفتاری، یادگیری ماشین و تکنیک‌های اعتباری (reputational) برای مقابله با تهدیدات بهره می‌برد [۱].

راه‌حل‌ها (محصولات) برتر EDR

شرکت	مورد استفاده	معیارها	هوشمندی	نحوه تحویل	قیمت
FireEye	از ۲۵۰ تا ۳۰۰۰۰۰ نقاط پایانی، فضای ابری برای SMB	بیش از ۱۰۰۰ محقق، توان عملیاتی Mbps ۱۰۰۰	تشخیص تهدید خودکار و مقابله با تهدیدات شناخته‌شده و شناخته‌نشده	ابر یا دستگاه	از ۳۰ دلار به ازای هر نقاط پایانی شروع و بر اساس ابزارها به قیمت آن اضافه می‌شود
Carbon Black	تمامی بازارها و با وسعت‌های متفاوت را شامل می‌شود، اما مهم‌ترین کاربرد در صنایع با ریسک بالا	تا ۱۵۰.۰۰۰ نقاط پایانی در هر کلاستر، بدون محدودیت در تعداد کلاسترها	موتور تجزیه‌وتحلیل ابری تدافعی فعالیت‌های مخرب را شناسایی می‌کند	نرم‌افزار یا ابر	از ۳۰ دلار به ازای هر نقاط پایانی در سال آغاز می‌شود
Guidance Software	سازمان‌های بزرگ	قابل مقیاس گذاری تا صدها هزار گره	هشدار و پاسخ خودکار، اعتبارسنجی، اولویت‌بندی و پاسخ به حوادث	نرم‌افزار	از ۵۷.۹۹۵ دلار برای ۲۰۰۰ گره برای یک مجوز دائمی آغاز می‌شود
Cybereason	سازمان‌ها با	قابلیت پردازش ۸ میلیون سؤال در	یادگیری ماشین و	فضای ابری یا	از ۵۰ دلار به ازای هر نقاط

	هراندازه‌ای	ثانیه بدون محدودیت در مقیاس‌پذیری	تجزیه‌وتحلیل	نرم‌افزار در محل	پایانی قبل از تخفیف حجمی آغاز می‌شود
Symantec Endpoint Protection with EDR	٪۲۵ تمامی موارد استفاده در جهان و ۳۵۰.۰۰۰ مشتری	قابل مقیاس پذیری تا صدها هزار گره	AI و بزرگ‌ترین شبکه هوشمندی تهدید	دستگاه‌های فیزیکی یا مجازی	از ۴۰ دلار به ازای هر نقاط پایانی در سال آغاز می‌شود
RSA NetWitness Endpoint	قوی‌ترین در شرکت‌های مالی، خدمات بهداشتی، دولتی، انرژی و مخابراتی	بیش از ۳۰۰ شاخص رفتاری قابل شخصی‌سازی	موتور تجزیه‌وتحلیل مبتنی بر رفتار و یادگیری ماشین	.....	قیمت‌گذاری به ازای هر نقاط پایانی
Cisco AMP for Endpoints	قوی در بازارهای افقی پر ریسک	بیشترین امتیاز از آزمایشگاه‌های NSS، مسدودسازی ۲۰ میلیارد تهدید در روز	هوش تطبیقی، تشخیص و پاسخ خودکار	فضای ابر، فضای ابر خصوصی یا دستگاه‌های در محل	قیمت‌گذاری بر اساس طول اشتراک و تعداد نقاط پایانی‌ها است
Tanium	سازمان‌های بزرگ	میلیون‌های نقاط پایانی و قابلیت مشاهده در ۱۵ ثانیه بر تمام نقاط پایانی‌ها	گردش کار خودکار جمع‌آوری داده و اقدامات اصلاحی	دستگاه، ماشین مجازی یا سرور مستقل	شرکت قیمت‌ها را اعلام نمی‌کند
CrowdStrike	سازمان‌های بزرگ	بیش از ۳۰ میلیارد اتفاق در روز از میلیون‌ها حس‌گر در ۱۷۶ کشور	APIها و تغذیه برای یکپارچه‌سازی با SIEM، IDS و پلتفرم‌های هوش تهدیدی	فضای ابری	قیمت‌گذاری بر اساس طول اشتراک
CounterTack	از SMBها تا شرکت‌های سرمایه‌گذاری	توانایی انجام میلیاردها اسکن در ثانیه	از طریق مشارکت استراتژیک با SAP	پلتفرم یا ابر	۱۴۰۰۰ دلار به ازای هر اشتراک دائمی، ۷۵۰۰

					دلار به ازای اشتراک یک‌ساله

منابع:

[۱]https://assetform.esecurityplanet.com/controller?asset=۲۳۶۲۷۸۰۱۰&srvid=۹۵۹۸۰&vkey=۴۱۹۰۳۱۰&io=۱۱۱۱۱&qset=CONTACTFORM_HQB&formHQB=y&domain=www.esecurityplanet.com&typage=https://www.esecurityplanet.com/products/fireeye-endpoint-security-edr.html&CCID=۲۰۳۹۹۶۵۰۲۰۴۶۵۴۸۰۴&QTR=ZZf۲۰۱۸۰۵۲۹۱۶۲۹۴۲۰Za۲۰۳۹۹۶۵۰Zg۲۵۵Zw۰Zm۰Zc۲۰۴۶۵۴۸۰۴Zs۹۴۷۷ZZ&CLK=۲۸۲۱۸۰۸۱۱۰۵۵۵۳۲۳۹۷&WT.qs_dlk=W۲۶sfQrIhEQAAFZQEw۴AAACn