



شناسایی و پاسخ به نقاط انتهایی

Endpoint Detection and Response



درباره اسپارا

ما در اسپارا امنیت را بازتعریف کرده ایم. راهکارهای ما با شناخت عمیق تهدیدهای امروز و فردا طراحی شده اند تا شما یک قدم جلوتر از خطر باشید. اسپارا فقط ارائه دهنده خدمات نیست، شریک استراتژیک شما در مسیر رشد ایمن و پایدار است. ما به همراه جمعی از بهترین متخصصان کشور محصولات نوین، خدمات متنوع و راهکارهای جامع امنیت سایبری را به سازمان ها ارائه می دهیم.

محصولات و خدمات ما:

PAM (Satrap) EDR IAP Isolator Platform MFA VPN

Blue Team Red Team Pentest Purple Team GRC

Application Control

اسپارا

معرفی سامانه شناسایی و پاسخ در نقاط انتهایی

یک شبکه از گروهی از دستگاه‌های کامپیوتری تشکیل شده که داده‌ها را مبادله می‌کنند و به هریک از این دستگاه‌ها نقطه پایانی (Endpoint) گفته می‌شود. به عبارت دیگر، نقطه پایانی هر دستگاهی است که به شبکه کامپیوتری متصل می‌شود. از طرف دیگر شرکت‌ها و کارمندان آن‌ها برای دسترسی روان‌تر به داده‌ها، هر روز بیشتر از گذشته شیوه‌ها را با یکدیگر ترکیب می‌کنند و افزایش روش‌های BYOD (دستگاه خود را بیاورید)، منجر به آسیب‌پذیری چندگانه نقاط انتهایی می‌شود.

ابزارهای امنیتی سنتی برای محافظت از این نقاط انتهایی، به دلیل ضعف‌هایی که دارند نمی‌توانند تهدیدات پیشرفته را شناسایی و متوقف کنند. در واقع آنتی‌ویروس‌ها و دیگر محصولات مشابه (EPP) که از روش‌های تشخیص و جلوگیری مبتنی بر امضا (Signature) استفاده می‌کنند، علی‌رغم الزامی بودنشان برای سازمان‌ها، به تنهایی نمی‌توانند در مواجهه با حملات APT، حملات بدون فایل، باج‌افزارهای پیشرفته و حملات فیشینگ کارایی داشته باشند.

محصول **شناسایی و پاسخ در نقاط انتهایی (EDR) اسپارا** با استفاده از روش‌های تحلیل رفتاری و تکنیک‌های تحلیل داده و با هدف افزایش امنیت در سطح نقاط انتهایی، بعد از جمع‌آوری و بررسی عمیق رویدادهای سیستمی، رفتارهای مخرب را تشخیص و گزارش می‌دهد.

آمارهای جهانی

+۳۶
میلیارد دلار

پیش‌بینی ارزش بازار جهانی امنیت نقاط انتهایی تا سال ۲۰۲۸ است. (Statista)

۳۱۷/۵۹
میلیون

تعداد اقدامات باج‌افزاری انجام‌شده در سراسر جهان در سال ۲۰۲۳ بوده است. (Statista)

۹۰٪

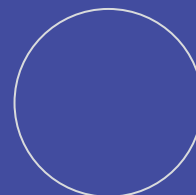
از حملات سایبری موفق از نقاط انتهایی آغاز شده‌اند. (IBM)

+۵
میلیون دلار

میانگین هزینه هر حمله باج‌افزاری در سال ۲۰۲۳ بوده است. (Fisher Philips)

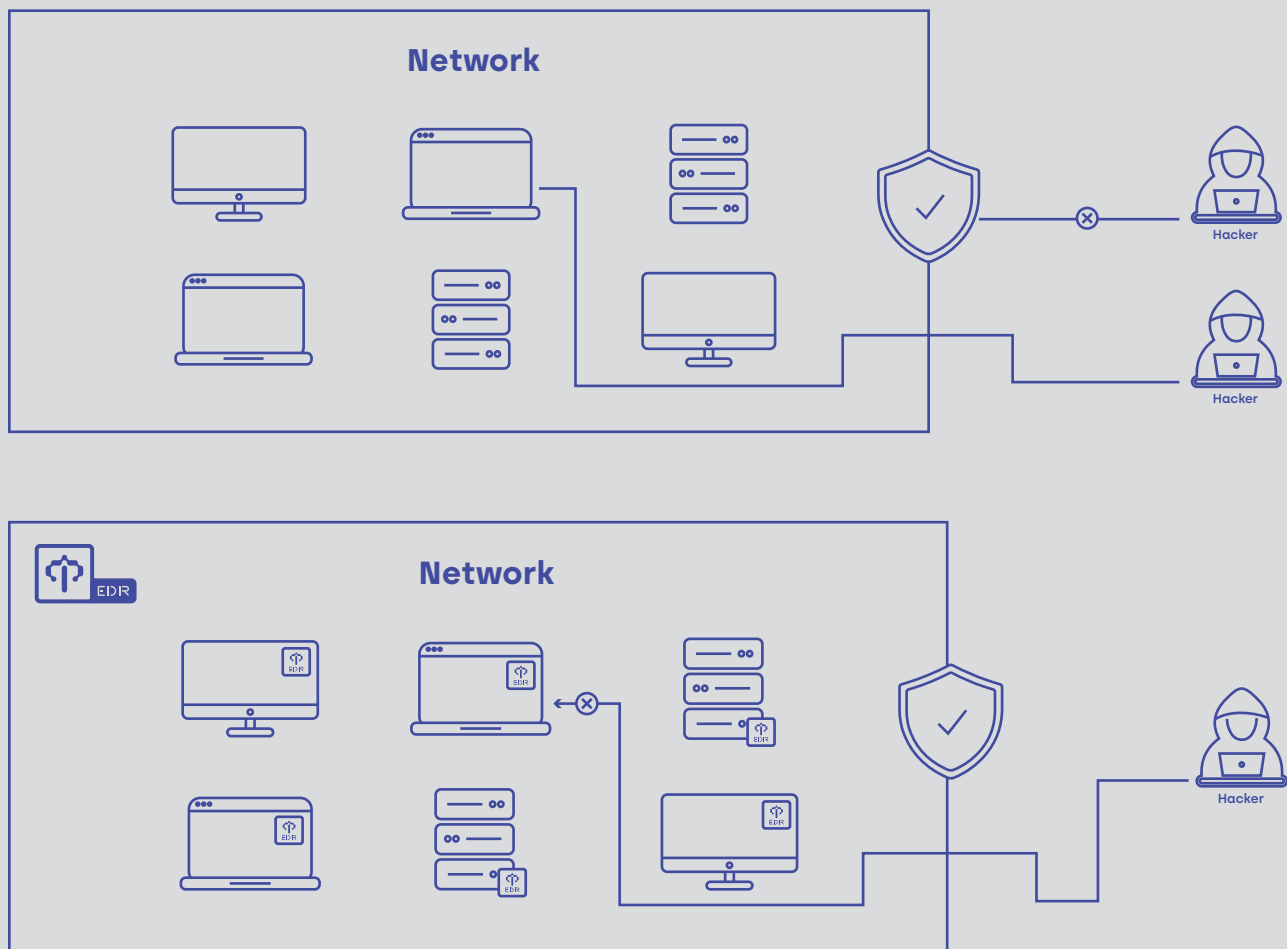
ویژگی‌های محصول EDR

- جمع‌آوری رویدادهای سیستم در سطح کرنل
- امکان پاسخ‌دهی به حملات از طریق ایزوله کردن سیستم یا از بین بردن فرآیندهای مخرب
- امکان اسکن سیستم براساس امضای بدافزارها
- بررسی مطابقت رایانه‌ها بر اساس استاندارد امنیتی مورد استفاده در سازمان
- محافظت در برابر حمله مهاجم به ایجنت EDR
- ایجاد ارتباط امن بین سرور و ایجنت با پروتکل‌های امنیتی به‌روز (TLS1.2)
- پیاده‌سازی الزامات امنیتی EDR اف‌تا
- امکان تشخیص حملات سایبری پیشرفته از طریق تشخیص رفتار (رفتارهای یک مرحله‌ای یا چند مرحله‌ای)
- امکان تشخیص رخدادهای امنیتی براساس تشخیص ناهنجاری با یادگیری ماشین
- استفاده از تکنولوژی‌های به‌روز موتور جستجو برای بررسی رویدادهای کل رایانه‌ها
- استفاده از تکنولوژی داکر برای راه‌اندازی و به‌روزرسانی سریع و راحت



نحوه عملکرد EDR

محصول EDR اسپارا به عنوان یکی از محصولات مهم در صنعت امنیت، با مدل سازی رفتارهای سطح سیستم در تمامی رایانه های شبکه دید جامعی از اتفاقات شبکه به مدیران امنیت می دهد و در کاهش زمان کشف، بررسی و پاسخ دهی به حملات بسیار تاثیرگذار است. این محصول با بهره مندی از تکنولوژی های روز، به عنوان یکی از نمونه های داخلی موفق به شمار می رود. بسیاری از مشتریان دولتی و سازمانی برای تامین امنیت خود به اسپارا اعتماد کرده اند و EDR تا کنون در تامین نیازهای این سازمان ها در حوزه امنیت نقاط انتهایی موفق عمل کرده است.





منابع مورد نیاز



ایجنت محصول EDR اسپارا از سیستم‌های عامل Win7SP1 و بالاتر پشتیبانی می‌کند. اگر مایل به استفاده از نسخه درون سازمانی (On-Permise) محصول هستید، نیاز به یک ماشین با چنین خصوصیتی دارید:

Minimum System Requirements:

CPU: 8 Core

RAM: 32 GB

Storage: 1 TB SSD (3 Month)

این خصوصیات برای حدود 5K EPS (که برای حدود ۱۰۰۰ کلاینت در نظر گرفته شده) مناسب است.

Recommended System Requirements:

CPU: 16 Core

RAM: 128 GB

Storage: 3TB SSD (3 Month)

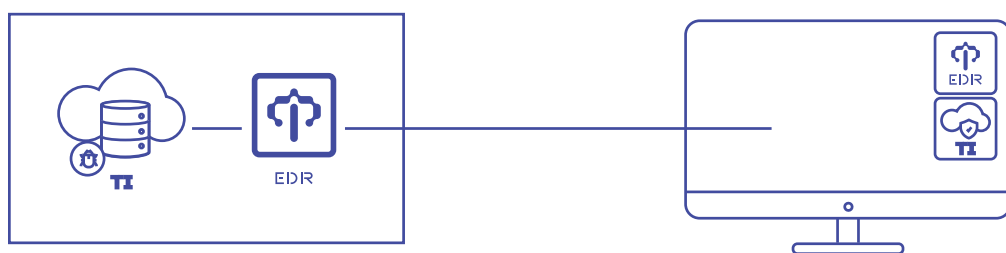
این خصوصیات برای حدود 15K EPS (که برای حدود ۵۰۰۰ کلاینت در نظر گرفته شده) مناسب است.

مراحل اجرا و پیاده سازی

راه اندازی سرور	نصب ایجنت در نقاط انتهایی
- با استفاده از ابزار docker و در محیط container انجام می‌شود. - سرویس docker image توسط تیم اسپارا و در داخل ایران راه اندازی شده است. - به روز رسانی سرور در هر زمانی و از طریق دریافت آخرین نسخه docker image امکان پذیر است.	- تیم اسپارا فایل نصبی با فرمت MSI را در اختیار کارفرما قرار می‌دهد. - این فایل با هر ابزار مدیریت دارایی مورد استفاده سازمان، نصب و راه اندازی می‌شود. - قابلیت استقرار از راه دور توسط ابزارهای استقرار تیم پشتیبانی اسپارا وجود دارد.

سامانه هوش تهدید

سامانه‌های هوش تهدید که با عنوان «TI» شناخته می‌شود، زیرساخت‌هایی ابری متشکل از داده‌های پیش‌پردازش‌شده‌ای از حملات اخیر و تهدیدات حال حاضر جهان هستند. این داده‌ها به سامانه‌های EDR کمک می‌کند تا از دانش و داده‌های جدیدترین حملات جهان آگاه شود و روش‌های مقابله با آن‌ها را در اختیار داشته باشند. استفاده از سامانه TI در کنار سامانه EDR قابلیت‌های حفاظتی را دو چندان می‌کند.



تفاوت EDR با محصولات EPP

محصولات EPP مانند آنتی‌ویروس در مقایسه با سامانه‌های EDR اهداف مشابه دارند اما نیازهای متفاوتی را پوشش می‌دهند. محصولات EPP با تشخیص فایل‌ها و عملکردهای مخرب از طریق رویکردهای مبتنی بر امضا، نسبت به جلوگیری از رفتارهای مخرب اقدام و با جلوگیری از اجرای فایل‌های مخرب، امنیت سیستم را حفظ می‌کنند. به عبارت دیگر آنتی‌ویروس می‌تواند جلوی بدافزار را بگیرد اما مشخص نمی‌کند که این بدافزار به چه طریق وارد شبکه شده و گسترش پیدا کرده است.

در مقابل سامانه‌های EDR با رویکرد تحلیل رفتار با فرض وجود مهاجم در شبکه اقدام به شکار تهدیدات سایبری می‌کند. رویکرد سامانه‌های EDR مکمل رویکرد محصولات EPP است. درواقع EPP ها اولین خط دفاعی سازمان در مقابل حملات هستند و EDR دومین لایه محافظتی سازمان به‌شمار می‌رود. حملاتی که توسط EPP ها قابل کشف نیستند با رویکرد تحلیل رفتاری EDR کشف می‌شوند یا به تحلیل گرانگرمیتی قابلیت‌هایی برای شکار این تهدیدات ارائه می‌دهند. یک استراتژی امنیت دفاعی موثر در یک سازمان، از رویکرد جلوگیری (EPP) و رویکرد کشف و شکار (EDR) به‌طور همزمان استفاده می‌کند.

در جدول زیر برخی تفاوت‌های دو محصول EDR و EPP عنوان شده است:

EPP	EDR
تمرکز روی جلوگیری از تهدید است	تمرکز روی شناسایی تهدید است
شناسایی تهدید منفعل	شناسایی تهدید فعال
دید محدود نسبت به فعالیت نقاط انتهایی	جمع‌آوری داده‌های رویداد از نقاط انتهایی
ارائه سطح اولیه‌ای از جلوگیری از تهدید	امکان پاسخ‌دهی و مهار سریع حملات
تمرکز بر محافظت از هر نقطه انتهایی به‌صورت ایزوله	فراهم کردن داده‌ها و زمینه برای حملاتی که چندین نقطه انتهایی را در بر می‌گیرد
استفاده از رویکردهای مبتنی بر امضا	استفاده از رویکرد تحلیل رفتار

تفاوت EDR با SIEM

علی‌رغم شباهت‌های بسیار زیاد این دو محصول از بعضی ابعاد، در محل استفاده و کارکرد دو تفاوت اصلی دارند:

تفاوت در کشف حملات

- سامانه‌های EDR دقت کشف حملات را بالا می‌برد
- سامانه‌های EDR باعث کاهش میزان False positive هشدارها و هزینه عملیات می‌شود
- EDR قابلیت‌های بالاتری نسبت به SIEM در زمینه تحلیل و واکنش داده‌های نقاط انتهایی دارد
- EDR ابزار دفاع قدرتمندتری نسبت به SIEM در مقابل حملات سطح نقاط انتهایی است

تفاوت در قابلیت‌های پاسخ‌دهی به حملات

SIEM	EDR
ذاتاً قابلیت پاسخ‌دهی به حملات را ندارند و متکی به محصولات دیگری مانند SOAR هستند	با قابلیت‌های مختلف محدودسازی، از گسترش حمله جلوگیری می‌کند
—	محدوده تحت شعاع حمله را کاهش می‌دهد
—	با در اختیار داشتن ابزارهای بررسی عمیق به تحلیل‌گر امنیتی در شناسایی نقطه شروع و ریشه حمله کمک می‌کند
در نهایت استراتژی بهینه این است که شناسایی تهدیدات سمت نقاط انتهایی به EDR سپرده شود و لاگ‌های سامانه‌های EDR برای جمع‌بندی به SIEM ارسال شود.	

مزایای رقابتی EDR اسپارا



راه اندازی سرویس
بدون نیاز به
Reboot
Down-Time



دقت بالای ارسال
هشدار و میزان
False Positive
پایین



ارائه دید جامع از
تمام فعالیت های
سیستم های
انتهاپی



افزایش سرعت
بررسی تهدیدات



دانش فنی تیم در
پیاده سازی
آزمون های نفوذ و
شبیه سازی
حملات



بهبود شکار
تهدیدات با ارائه
داده های زمینه ای
از حملات



افزایش سرعت
پاسخ دهی به
حملات



استفاده از پایگاه
داده ای از حملات و
داده های پردازش
شده

مشتریان EDR اسپارا



وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران



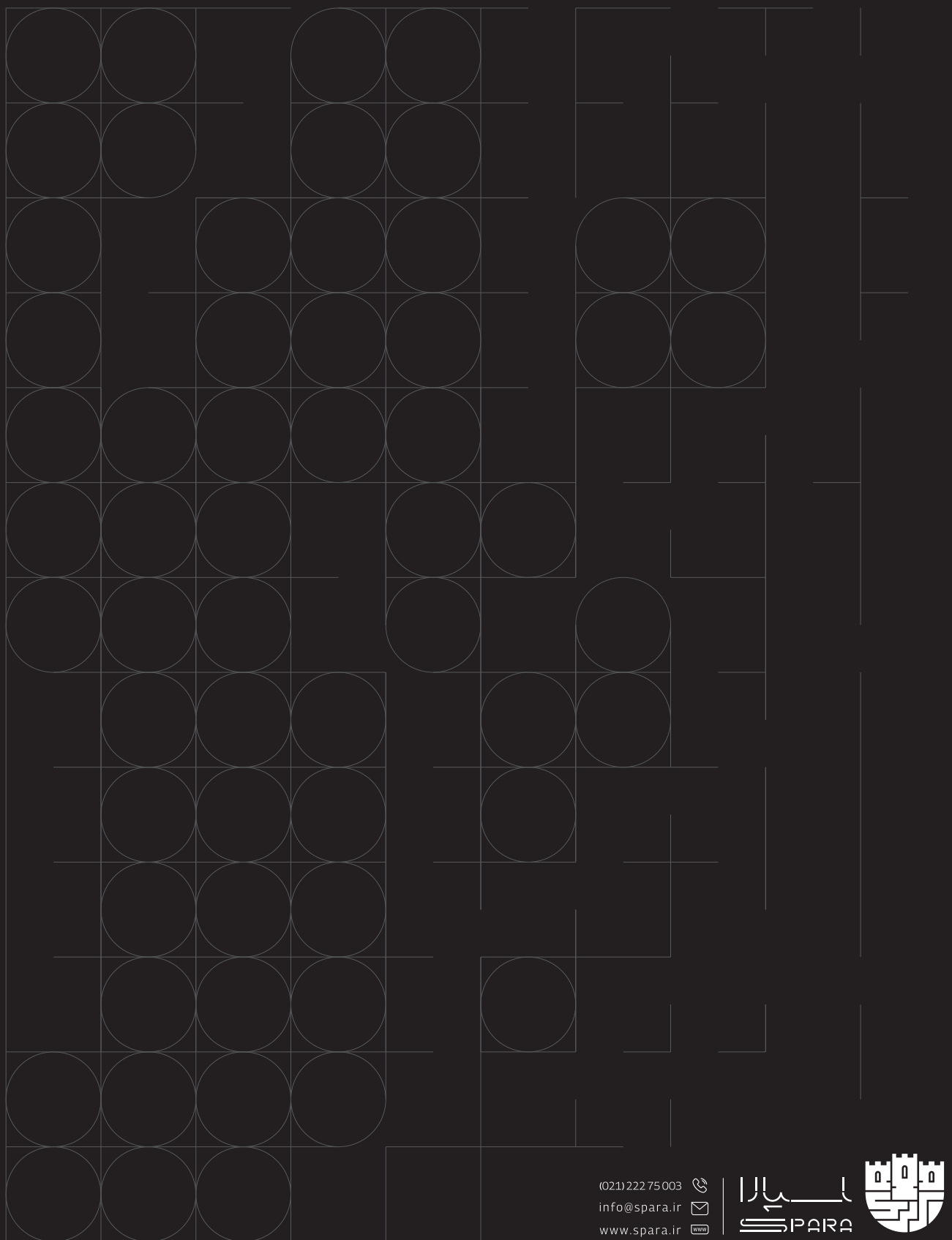
پایگاه اطلاع رسانی پشتیبانی پاد



پست بانک ایران



MIDHCO



(021) 222 75 003
info@spara.ir
www.spara.ir

