پارا
SPARA

EMS

مدیریت صدور مجوز اجرای فایل

Execution Management System

درباره اسپارا

شـرکت راهـکار هوشـمند امن (اسـپارا) بـرای مقابله بـا تهدیدات پیچیده و پیشـرفته سـایبری به همراه جمعی از بهترین متخصصان کشـور اقدام به تولیـد و ارائه محصـولات نوین، خدمـات متنوع و راهکارهای جامع امنیت سایبری کرده است. از مهم‌ترین محصولات اسپارا می‌توان به XDR، EDR، PAM (Satrap) و EMS اشاره کرد. خدمات و راهکارهای امنیتی اسـپارا هم شامل طیف وسیعی از خدمـات ماننـد Threat Hunting، Pentest، SOC، Red Team Incident Response، مشاوره و آموزش می‌شود.

معرفی محصول مدیریت صدور مجوز اجرای فایل(EMS)

بـا اینکه روش‌هـا و نرم‌افزارهای مختلفی بـرای نظارت و کنترل امنیت، تبادل اطلاعات، جلوگیری از نفوذ و تکثیر بدافزارها وجود دارد اما همچنان راه‌های نفوذ برای انواع تهدیدها فراهم است. از آنجایی که آنتی‌ویروس‌ها امکان شناسـایی و تشخیص تمام بدافزارهای جدید را ندارند؛ بنابراین اسـتفاده از نرم‌افزاری که از روند اجرای فایل‌های غیرمجاز جلوگیری کند، اولویت و ضرورت دارد.

محصـول بومـی **مدیریت اجـرای فایـل اسـپارا (EMS)** به منظور افزایش میزان امنیت سیستم‌های موجود در شبکه شما طراحی و پیاده‌سـازی شده اسـت. EMS اسـپارا با جلوگیری از اجـرای فایل‌های آلـوده، غیرمجاز و ناشـناخته، کنترل سـطح دسترسـی به ۴۸ پسـوند مهم ویندوز (فایل‌های اجرایی، جاوا، اسـکریپت، پاورشل و غیره) و کنترل تجهیزات متصل به سیستم (کلاینت‌هـای شـبکه و دسـتگاه‌های خودپرداز) امنیت شـما را تامین می‌کند.

آمارهای جهانی

۱۲ میلیارد دلار

میانگین خسـارت صنعت مالـی و پرداخت به دلیل حملات سـایبری بوده است. (IMF)

رتبه دوم

در میزان خسارات مربوط به حوادث سایبری دنیا به صنعت مالی و پرداخت اختصاص دارد. (IBM)

مـهم‌تریـن عـلل ضعـف خودپـردازها در حـملات سـایبری

ـ عدم استفاده از ویندوزهای به‌روز (استفاده از ویندوزهای XP و 7)

ـ عدم استفاده از نرم‌افزارهای امنیتی

ـ عدم اسـتفاده از نرم‌افزارهایی که از اجرای فایل‌ها و اتصال دیوایس‌های غیرمجاز جلوگیری کند

ویژگی‌های سامانه EMS اسپارا

- نصب و فعال‌سازی نسخه کلاینت توسط پنل سرور
- جلوگیـری از اجرای نرم‌افزارهای غیرمجاز و بخش‌های مهم ویندوز (مانند Telnet) حتی در محیط کاربرانی با سطح دسترسی Admin
- صدور مجوز نصب نرم‌افزار توسط یک Setup مطمئن
- کنترل تجهیزات متصل به سیستم (ماوس، کیبورد، فلش، موبایل و غیره)
- ارسال گزارش از شناسایی فایل‌های غیر مجاز و دیوایس‌های متصل به سیستم
- امکان گروه‌بندی سیستم‌ها
- حفاظت از امنیت سیستم در حال SafeMode و قطعی شبکه
- سیستم Self defence به‌منظور عدم فعالیت غیرمجاز کاربران
- اطلاع‌رسانی از روند دسترسی‌های غیرمجاز در قالب پیامک
- عدم اشغال منابع سیستم (CPU، RAM)

مقایسه راهکارهای امنیتی برای جلوگیری از اجرای انواع تهدیدات

Threat	Firewall	Antivirus	Whitelist Application(EMS)
Malware			
Trojan Horse	●	●	●
Worms	●	●	●
Downloader	●	●	●
Key Logger	●	●	●
Backdoor	●	●	●
Zero-day Viruses	○	○	●
Fake Anti-Viruses	○	○	●
Tools			
Proxy Software	○	○	●
Shareware	○	○	●
Threat Sources			
Internet	●	●	●
Network Share	●	●	●
USB drive	○	●	●
CDRom	○	●	●
Time Killers			
Games	○	○	●

عملکرد EMS در دستگاه‌های خودپرداز

هک دستگاه‌های خودپرداز و خروج اسکناس به روش‌های غیرمجاز افزایش بسیار زیادی داشته و به همین دلیل، نظارت بر امنیت این دستگاه‌ها اهمیت بالایی دارد. یکی از راه‌های حفظ امنیت، کنترل و بررسی انواع تجهیزاتی است که به خودپردازها و به‌طور کلی به سیستم متصل می‌شوند. در همین راستا محصول امنیتی EMS تفاوت‌های عمده‌ای با محصولات مشابه در محافظت از خودپردازها دارد:

ESM	سایر محصولات مشابه
در محیط Safemode فعال است و فرایند کنترل پالیسی را انجام می‌دهد	در محیط Safemode غیرفعال هستند
امکان فعال و غیرفعال کردن انواع ماوس و کیبورد متصل به دستگاه	این قابلیت امکان‌پذیر نیست
ارسال گزارش اتصال و انفصال تمام دیوایس‌های مجاز و غیرمجاز برای پنل سرور	این قابلیت امکان‌پذیر نیست

عملکرد EMS در کنترل سطح دسترسی انواع فایل‌ها

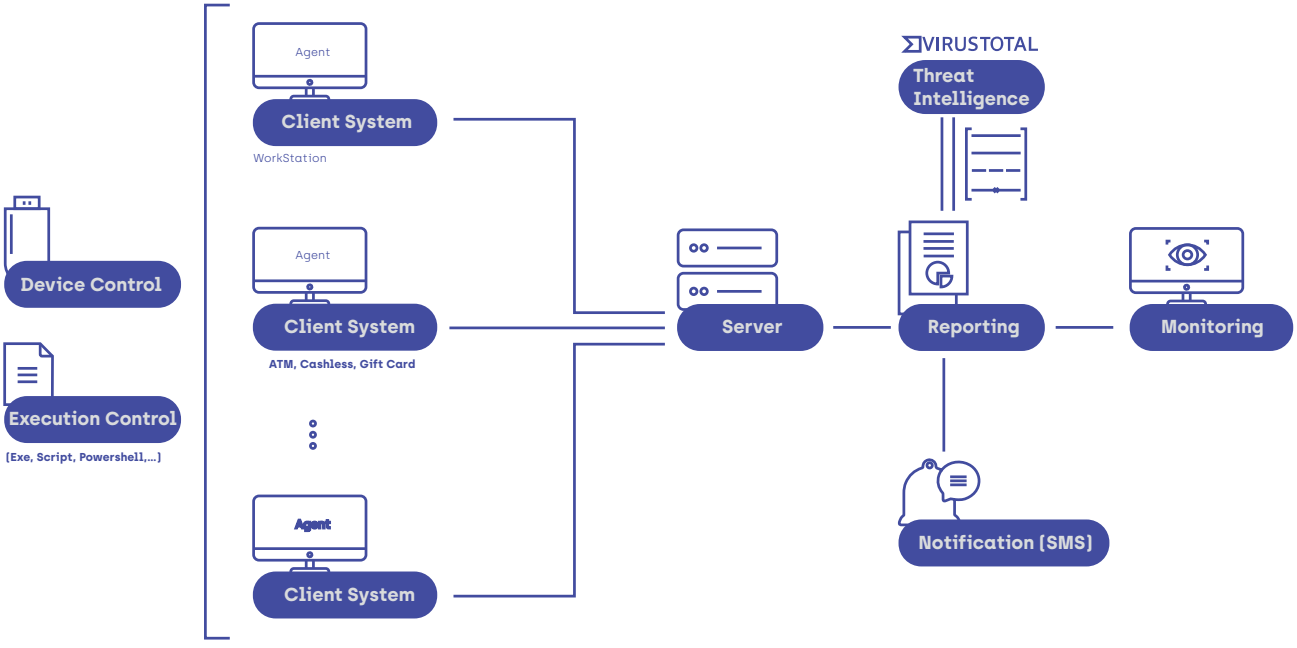
EMS اسپارا با قرار دادن سیستم‌های شبکه در یک محدوده تعریف‌شده، تنها به فایل‌هایی قابلیت اجرا می‌دهد که امضا (هش) آن‌ها در پنل مدیریت سرور معرفی شده باشند. در غیر این صورت به‌عنوان فایل غیرمجاز شناخته شده و از اجرای آن‌ها جلوگیری می‌شود. درواقع فایل‌های قابل اجرا روی سیستم‌های شبکه مشخص و تعریف شده‌اند و ورود فایل‌های اجرایی جدید تحت کنترل خواهد بود.

با فعال‌سازی نسخه کلاینت این محصول، فایل‌های .Exe و .Scr و .Com تحت نظارت و کنترل قرار می‌گیرند و اجازه سطح دسترسی به ۴۵ پسوند مهم دیگر (مانند فایل‌های DLL، اسکریپت، رجیستری، پاورشل، Jar و غیره) در ویندوزهای کلاینت اختیاری خواهد بود. سطح دسترسی به هریک از این پسوندها نیز در سه حالت زیر قابل انتخاب و اعمال است:

Nothing_

Monitoring_

Restriction_



کنترل تجهیزات متصل به سیستم توسط EMS

ارزش افزوده دیگر EMS اسپارا برای شما، کنترل دیوایس‌های متصل‌شده به سیستم و دستگاه‌های خودپرداز است. کنترل دیوایس‌ها (اتصال و انفصال) بر اساس انتخاب نوع دیوایس در پنل سرور و در سه بخش زیر قابل انتخاب و اعمال است:

- Mouse and Keyboard
- Storage Devices
- Bluetooth and WiFi and Mobile Tethering

در صورت غیرفعال شدن حافظه‌های جانبی مانند فلش‌ها، تنها فلش‌هایی که سریال آن‌ها به پنل سرور معرفی شده باشند مجوز استفاده خواهند داشت. همچنین در صورتی که پالیسی مربوط به دیوایس‌های ماوس و کیبورد غیرفعال باشد، با اتصال فلش‌هایی که سریال آن‌ها به سامانه معرفی شده است، ماوس و کیبورد فعال شده و با خروج (قطع) فلش مجاز، پالیسی غیرفعال شدن دیوایس‌ها به‌صورت خودکار اعمال می‌شود.

پیش‌نیازهای استفاده از محصول EMS اسپارا

پیش‌نیاز شبکه:

باز بودن یک پورت دلخواه شبکه جهت ارتباط بین سرور و کلاینت و بالعکس

پیش‌نیاز کلاینت نرم‌افزار:

پشتیبانی از ویندوزهای ۳۲ و ۶۴ بیتی:

WindowsXP(SP3)
Windows 7
Windows 10
Windows 10LTSC

پیش‌نیاز سرور:

عنوان	توضیحات	
حجم هارددیسک	Hard Disk: 300 GB حداقل شامل دو درایو باشد (۱۰۰ گیگابایت برای درایو ویندوز تخصیص داد شود)	
ویندوز موردنیاز (نسخه ۶۴ بیتی)	Microsoft Windows Server 2019 |2016 |2012	
مشخصات CPU & RAM برای پاسخگویی به ۱۰۰۰ سیستم کلاینت مشخصات CPU & RAM برای پاسخگویی به ۳۰۰۰ سیستم کلاینت مشخصات CPU & RAM برای پاسخگویی به ۵۰۰۰ سیستم کلاینت یا بالاتر	CPU: 4 Core CPU: 6 Core CPU: 8 Core	RAM :16 GB RAM :24 GB RAM :32 GB

مزایای استفاده از محصول EMS اسپارا

فراهم کردن بستری
امن‌تر جهت خروج
اسکناس از خودپرداز

یک لایه امنیتی مجزا و
مکمل نرم‌افزارهای
امنیتی

یکپارچه‌سازی نسخه‌های
نرم‌افزارهای کاربردی در
سیستم‌های شبکه

غیرفعال شدن
نسخه‌های متفاوت از
یک نرم‌افزار

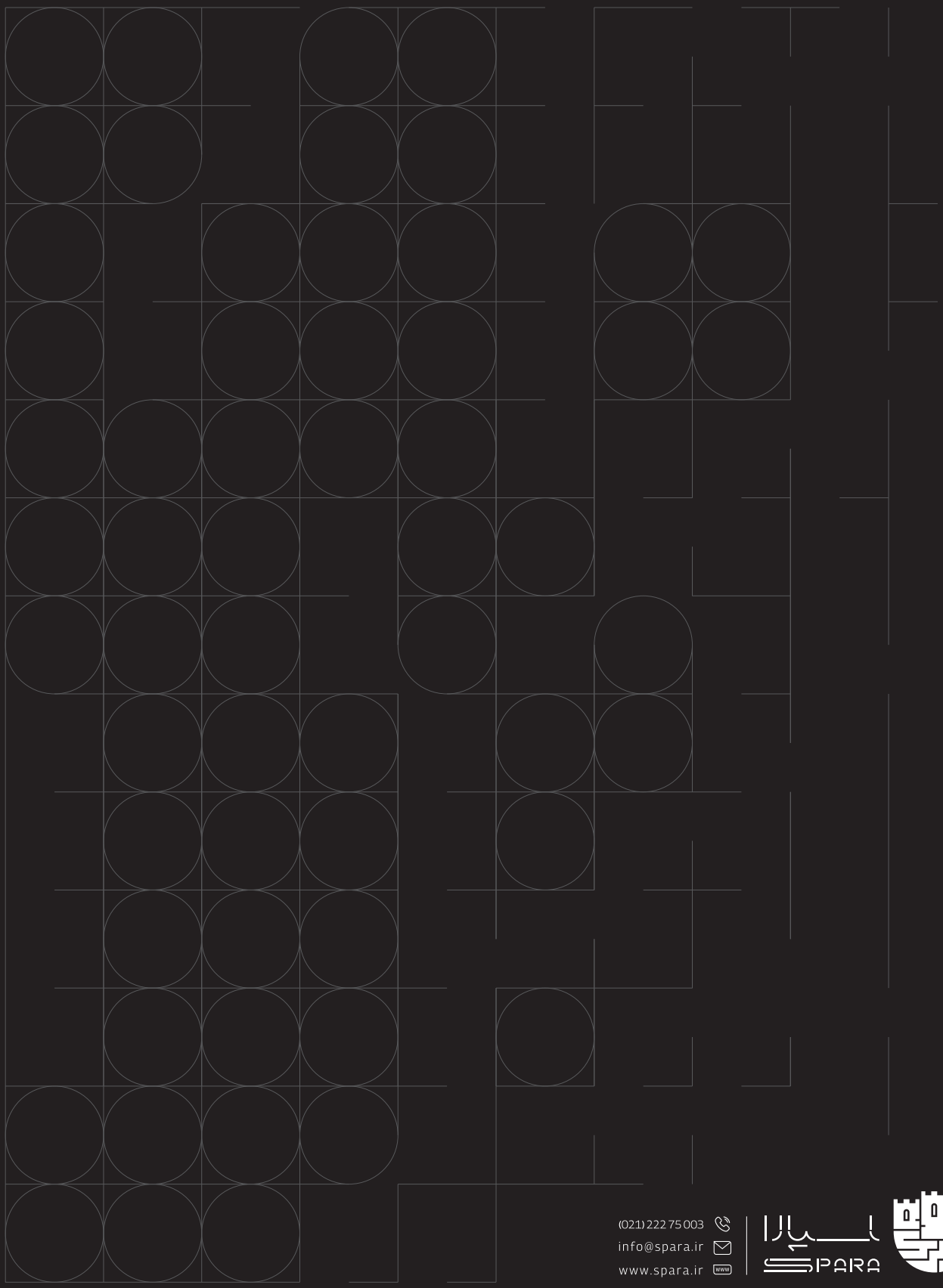
ارسال پیامک هشدار در
صورت بروز مشکلات
امنیتی

قابلیت بررسی انواع
فایل‌های غیرمجاز
شناسایی‌شده با ده‌ها
آنتی‌ویروس برتر دنیا

نظارت و کنترل بر روند
اجرای فایل‌ها و اتصال
دیوایس‌ها

سامانه‌ای متمرکز جهت
واکنش سریع در مقابله
با حملات سایبری

مشتریان اسپارا



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

اسپارا
SPARA