



APPLICATION
CONTROL

کنترل اجرای نرم افزار Application Control



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 محصول کنترل اجرای نرم افزار

با اینکه روش ها و نرم افزارهای مختلفی برای نظارت و کنترل امنیت، تبادل اطلاعات، جلوگیری از نفوذ و تکثیر بدافزارها وجود دارد اما همچنان راه های نفوذ برای انواع تهدیدها فراهم است. از آنجایی که آنتی ویروس ها امکان شناسایی و تشخیص تمام بدافزارهای جدید را ندارند؛ بنابراین استفاده از نرم افزاری که از روند اجرای فایل های غیرمجاز جلوگیری کند، اولویت و ضرورت دارد.

محصول بومی **کنترل اجرای نرم افزار اسپارا** به منظور افزایش میزان امنیت سیستم های موجود در شبکه شما طراحی و پیاده سازی شده است. EMS اسپارا با جلوگیری از اجرای فایل های آلوده، غیرمجاز و ناشناخته، کنترل سطح دسترسی به ۴۸ پسوند مهم ویندوز (فایل های اجرایی، جاوا، اسکریپت، پاورشل و غیره) و کنترل تجهیزات متصل به سیستم (کلاینت های شبکه و دستگاه های خودپرداز) امنیت شما را تامین می کند.

آمارهای جهانی

۱۲ میلیارد دلار

میانگین خسارت صنعت مالی و پرداخت به دلیل حملات سایبری بوده است. (IMF)

رتبه دوم

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

مهم ترین علل ضعف خودپردازها در حملات سایبری

– عدم استفاده از ویندوزهای به روز (استفاده از ویندوزهای XP و 7)

– عدم استفاده از نرم افزارهای امنیتی

– عدم استفاده از نرم افزارهایی که از اجرای فایل ها و اتصال دیوایس های

غیرمجاز جلوگیری کند

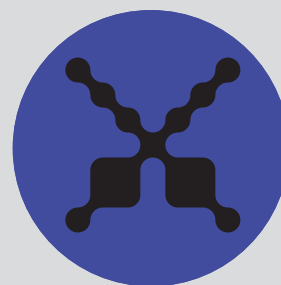
ویژگی‌های

Application Control

- نصب و فعال سازی نسخه کلاینت توسط پنل سرور
- جلوگیری از اجرای نرم افزارهای غیرمجاز و بخش های مهم ویندوز (مانند Telnet) حتی در محیط کاربرانی با سطح دسترسی Admin
- صدور مجوز نصب نرم افزار توسط یک Setup مطمئن
- کنترل تجهیزات متصل به سیستم (ماوس، کیبورد، فلش، موبایل و غیره)
- ارسال گزارش از شناسایی فایل های غیر مجاز و دیوایس های متصل به سیستم
- امکان گروه بندی سیستم ها
- حفاظت از امنیت سیستم در حال SafeMode و قطعی شبکه
- سیستم Self defence به منظور عدم فعالیت غیرمجاز کاربران
- اطلاع رسانی از روند دسترسی های غیرمجاز در قالب پیامک
- عدم اشغال منابع سیستم (CPU، RAM)

مقایسه راهکارهای امنیتی برای جلوگیری از اجرای انواع تهدیدات

Threat	Firewall	Antivirus	Application Control
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 Application Control در خودپردازها

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:

سایر محصولات مشابه	Application Control
در محیط Safemode غیرفعال هستند	در محیط Safemode فعال است و فرایند کنترل پالیسی را انجام می‌دهد
این قابلیت امکان‌پذیر نیست	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

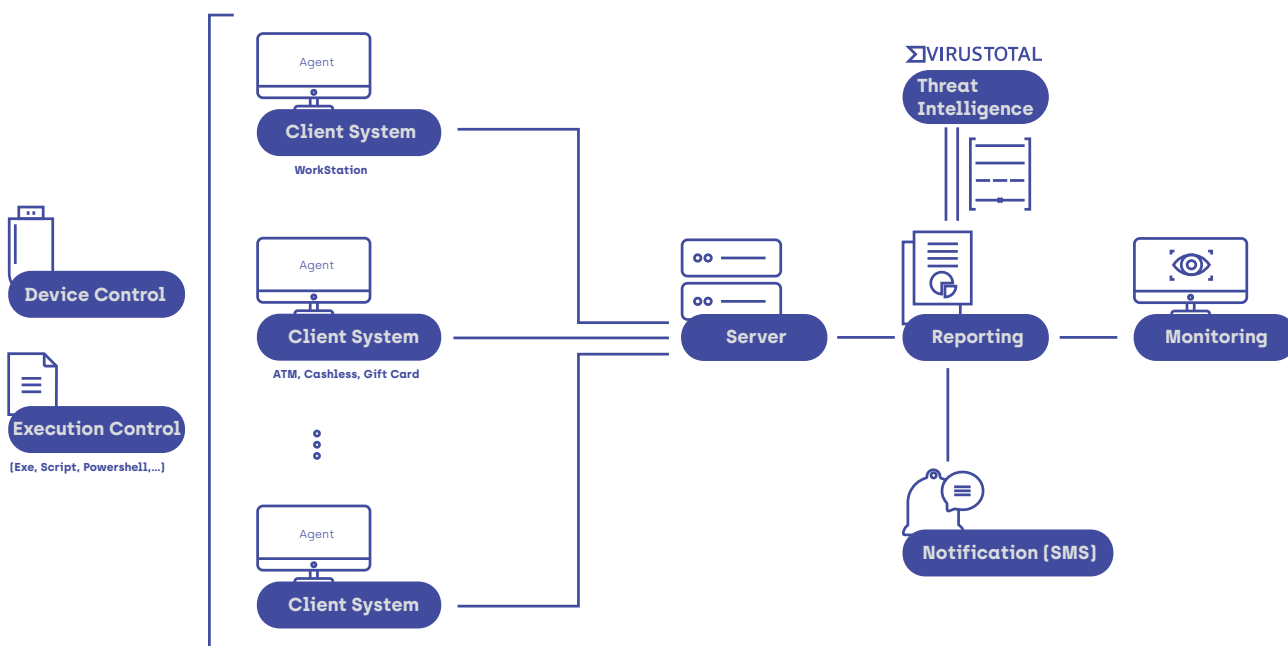
عملکرد Application Control در کنترل سطح دسترسی انواع فایل‌ها

این محصول اسپارا با قراردادن سیستم‌های شبکه در یک محدوده تعریف شده، تنها به فایل‌هایی قابلیت اجرا می‌دهد که امضا (هش) آن‌ها در پل مدیریت سرور معرفی شده باشند. در غیر این صورت به عنوان فایل غیرمجاز شناخته شده و از اجرای آن‌ها جلوگیری می‌شود. در واقع 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 Application Control

ارزش افزوده دیگر این محصول اسپارا برای شما، کنترل دیوایس‌های متصل شده 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 به صورت خودکار اعمال می‌شود.

پیش نیازهای استفاده از Application Control

پیش نیاز شبکه:

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

پیش نیاز کلاینت نرم افزار:

پشتیبانی از ویندوزهای ۳۲ و ۶۴ بیتی:

WindowsXP(SP3)

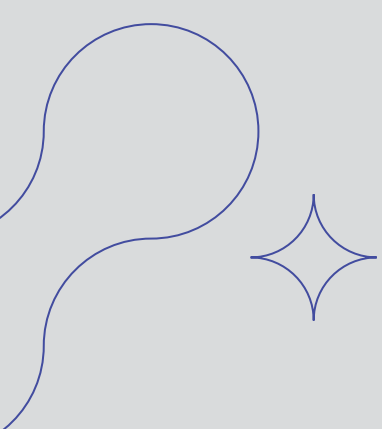
Windows 7

Windows 10

Windows 10LTSC

پیش نیاز سرور:

عنوان	توضیحات
حجم هارد دیسک	Hard Disk: 300 GB حداقل شامل دو درایو باشد (۱۰۰ گیگابایت برای درایو ویندوز تخصیص داد شود)
ویندوز مورد نیاز (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	RAM :16 GB CPU: 4 Core RAM :24 GB CPU: 6 Core RAM :32 GB CPU: 8 Core



مزایای رقابتی

Application Control اسپارا



غیرفعال شدن
نسخه‌های متفاوت از
یک نرم‌افزار



یکپارچه‌سازی نسخه‌های
نرم‌افزارهای کاربردی در
سیستم‌های شبکه



یک لایه امنیتی مجزا و
مکمل نرم‌افزارهای
امنیتی



فراهم کردن بستری
امن‌تر جهت خروج
اسکناس از خودپرداز



سامانه‌ای متمرکز جهت
واکنش سریع در مقابله
با حملات سایبری



نظارت و کنترل بر روند
اجرای فایل‌ها و اتصال
دیوایس‌ها



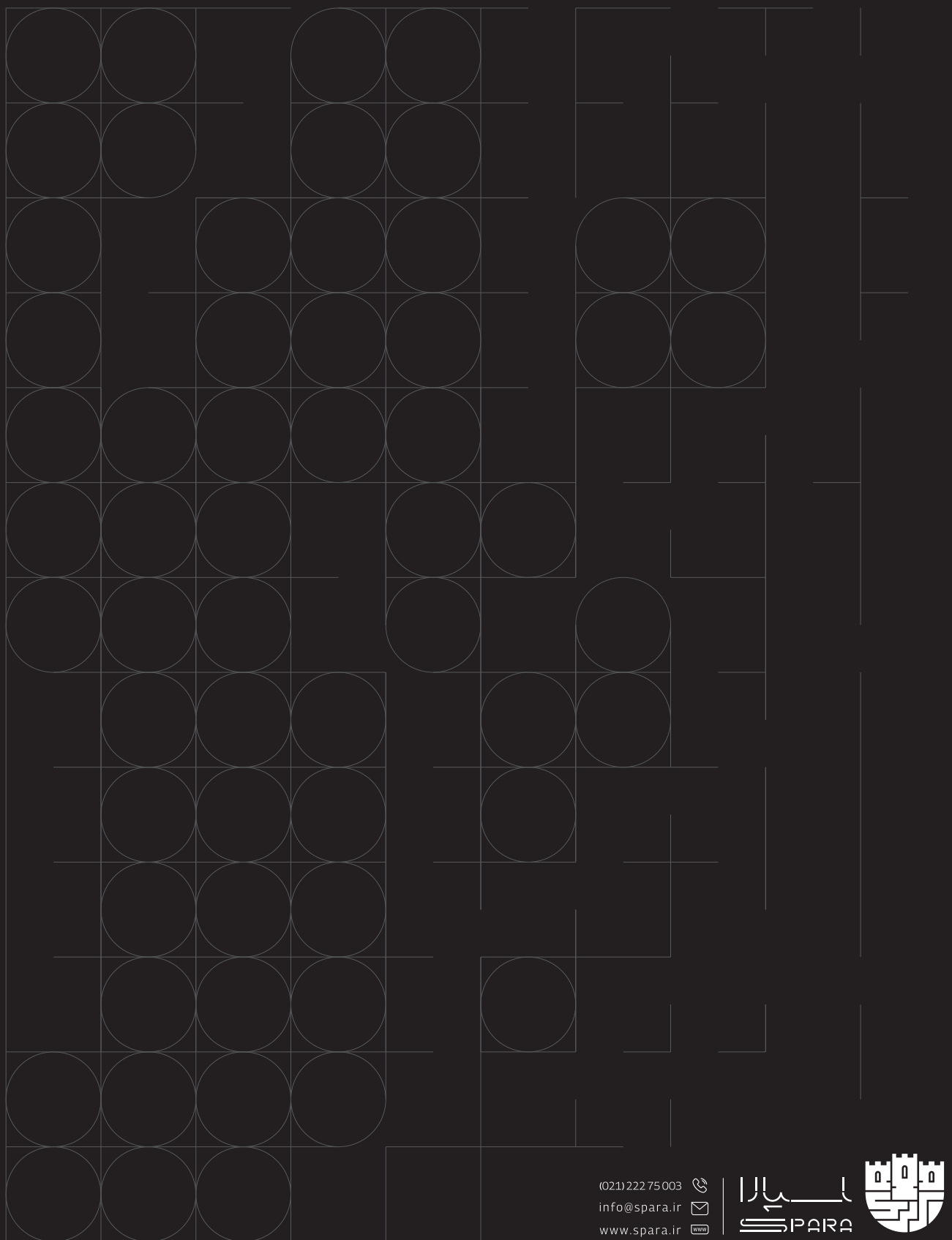
قابلیت بررسی انواع
فایل‌های غیرمجاز
شناسایی شده با ده‌ها
آنتی‌ویروس برتر دنیا



ارسال پیامک هشدار در
صورت بروز مشکلات
امنیتی

مشتریان اسپارا





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

