ISOLATOR
PLATFORM

جداسازی ایمن

Isolator Platform

درباره اسپارا

ما در اسپارا امنیت را بازتعریف کرده‌ایم. راهکارهای ما با شناخت عمیق تهدیدهای امروز و فردا طراحی شده‌اند تا شما یک قدم جلوتر از خطر باشید. اسپارا فقط ارائه‌دهنده 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 سازمان‌ها ارائه می‌دهیم.

محصولات و خدمات ما:

PAM (Satrap) EDR IAP Isolator Platform MFA VPN

Blue Team Red Team Pentest Purple Team GRC

Application Control

آمارهای جهانی

۲۷۷ روز

میانگین زمانی است که سازمان‌ها می‌توانند نقض داده‌ها را شناسایی و آن را کنترل کنند. مرورگرها یکی از رایج‌ترین مسیرها برای نفوذ مجرمان سایبری به شبکه است. (IBM)

رایج‌ترین تهدیدها

فیشینگ، باج‌افزار، تزریق SQL و Cross-site scripting جزو رایج‌ترین تهدیدهای امنیتی حوزه وب هستند. (Fortinet)

۳/۴ میلیون

ایمیل فیشینگ به‌صورت روزانه در سال ۲۰۲۳ ارسال شده است. (Slunk.com)

٪۷۰

از موارد نفوذ به سیستم شامل بدافزار بوده و ۳۲ درصد از این بدافزارها از طریق وب توزیع می‌شوند. (CheckPoint)

بیش از ۹۶۳ هزار

سایت فیشینگ در سه‌ماهه اول سال ۲۰۲۴ در سراسر جهان شناسایی شده است. (Statista)

معرفی جداسازی ایمن

سازمان‌ها هرچقدر که پیشرفته باشند و در هر ابعاد و اندازه‌ای هم که باشند باز هم ممکن است قربانی حملات بدافزاری و باج‌افزاری شوند و نمونه‌های این اتفاق هم کم نیست. به همین دلیل برای محافظت از خودتون نباید به مکانیسم‌های شناسایی قدیمی و ناکارآمد اعتماد کنید و صرفا به آن‌ها متکی باشید.

تحقیقات بسیاری نشان می‌دهد که هیچ فایروال یا ابزار محافظت از نقاط انتهایی (Endpoint) وجود ندارد که بتواند به طور صددرصدی جلوی یک هکر یا مهاجم سایبری مصمم را بگیرد و به همین دلیل محصولات و ابزارهای اختصاصی وجود دارد که تمرکزشان را برای حفظ امنیت بخش‌های مختلف سازمان قرار داده‌اند.

یکی از این بخش‌ها، فضای اینترنت و خطرات مرتبط با این حوزه است. **راهکار جداسازی ایمن اسپارا**، می‌تواند تهدیدهای مربوطه را به‌طور امنی برای شما کنترل کند. در این ابزار، تمام تعاملات مربوط به فضای وب در کانتینرهای Docker و در یک محیط ایزوله اجرا می‌شوند و تنها یک رندرینگ رابط کاربری (Rendering User Interface) یکپارچه برای کاربر ارسال می‌شود و از آنجایی که محتوای وب هرگز به‌صورت مستقیم با نقطه پایانی کاربر در تعامل نیست، سازمان شما در برابر تهدیدهای سایبری موجود محافظت می‌شوند و داده‌های شما ایمن خواهند ماند.

به‌طور کلی ابزار جداسازی اینترنت جز ضروری زیرساخت امنیت سایبری یک سازمان است که به محافظت در برابر تهدیدهای مختلف و محافظت از داده‌ها وسیستم های حساس کمک می‌کند. برای سازمان‌ها بسیار مهم است که روی چنین ابزارهایی سرمایه‌گذاری و امنیت و حریم خصوصی دارایی‌های دیجیتالشان را تضمین کنند.

مهم‌ترین دلایل اهمیت راهکار جداسازی ایمن اسپارا برای سازمان

ـ محافظت در برابر بدافزارها: یکی از بزرگترین تهدیدات سایبری، خطر آلودگی به بدافزار از طریق وب‌سایت‌ها یا لینک‌های مخرب است. راهکار جداکننده اینترنت به جداسازی فعالیت‌های اینترنتی در یک محیط امن کمک و درنتیجه از نفوذ بدافزار به شبکه و سیستم‌های سازمان جلوگیری می‌کند.

ـ حریم خصوصی و امنیت داده‌ها: با جداسازی سشن‌های مرورگر وب، سازمان‌ها می‌توانند از داده‌های حساس خود محافظت و از دسترسی غیرمجاز یا نشت داده‌ها جلوگیری کنند. این کار، برای تمامی صنایع به‌ویژه آن‌هایی که با اطلاعات محرمانه سروکار دارند، بسیار مهم است.

ـ دفاع در برابر حملات فیشینگ: حملات فیشینگ جزو تهدیدهای رایج سایبری است که می‌تواند کارکنان را فریب دهد تا اطلاعات حساس را فاش یا نرم‌افزارهای مخرب را دانلود کنند. راهکار جداکننده اینترنت و اپلیکیشن اسپارا می‌تواند با جداسازی وب‌سایت‌های فیشینگ و مسدود کردن دسترسی به آن‌ها، از این حملات جلوگیری کند.

ـ الزامات رگولاتوری: بسیاری از صنایع ملزم به ایمن کردن شبکه‌ها و داده‌های خودشان هستند. با پیاده‌سازی این راهکار، سازمان‌ها بهتر می‌توانند این الزامات را برآورده و از جریمه‌های پرهزینه جلوگیری کنند.

ـ افزایش بهره‌وری: راهکار جداکننده اینترنت و اپلیکیشن اسپارا می‌تواند بهره‌وری کاربر را با اجازه دادن به کارمندان برای دسترسی ایمن به اینترنت بدون ترس از به‌خطر انداختن امنیت سازمان، بهبود بخشد.

ISOLATOR PLATFORM

مهم‌ترین ویژگی‌های Isolator Platform

- مدیریت، کنترل و ممیزی بازه متعددی از نشست‌های راه دور کاربران
- مدیریت سامانه‌ها و اتصال‌ها به وب اپلیکیشن‌ها از طریق کنسول وب
- امکان پیاده‌سازی Highly Available (HA) در انواع مختلف مدل‌های استقرار
- تجهیز تمام اپلیکیشن‌های مورداستفاده سازمان به احراز هویت چندگانه

سایر ویژگی‌ها

ممیزی نشست‌ها

ـ مشاهده برخط فعالیت‌های کاربر در نشست و اجبار به خاتمه در صورت صلاحدید کاربر ممیز

(4Eye Authentication)

ـ مشاهده فعالیت‌های کاربر در نشست‌ها به‌صورت فیلم

ـ نگهداری اطلاعات نشست‌ها (فیلم و لاگ) به‌صورت فشرده و با حجم کم (به‌صورت میانگین ۳۰

مگابایت بر ساعت برای هر نشست)

ـ عدم وجود محدودیت نرم‌افزاری روی تعداد نشست‌های قابل ذخیره و پخش در سامانه

ـ امکان فیلتر نشست‌ها براساس مبدا، مقصد، زمان نشست و غیره

کنترل محتوای نشست‌ها

ـ محـدود کردن انـواع فایل‌های قابـل انتقال به اپلیکیشـن یا از اپلیکیشن

پایش‌پذیری

ـ داشبورد جامع پایش وضعیت سامانه

ـ پایش خـودکار صحت عملکرد اجزا و سرویس‌های سـامانه در قالب شاخص‌های سلامت سامانه

ـ پایش وضعیت منابع سامانه (پردازنده، حافظه، دیسک و غیره)

ـ ایجـاد رخداد در صورت تغییر در وضعیت شـاخص‌های سلامت سامانه

ـ امکان یکپارچه‌سازی با ابزارهای Monitoring

ـ امکان آرشـیو خودکار نشسـت‌ها در فضای ذخیره‌سازی تحت شبکه

ـ امکان حذف خودکار ویدیو نشست‌های قدیمی

گزارش‌گیری

ـ امـکان دریافـت گزارش‌هـای تجمیعـی از تعـداد و مـدت زمان نشست‌ها به تفکیک پروتکل، مبدا، مقصد و غیره

ـ امکان گزارش‌گیری پویا براساس سرور مبدا و مقصد

کنترل دسترسی

ـ امـکان احراز هویت کاربران با سـامانه‌های مدیریت متمرکز کاربران ازجمله LDAP و Active Directory

ـ پشتیبانی از احراز هویت چندگانه در دسترسی کاربران

ـ ارائـه لیسـت سرورهـا و Credentials سرورهای مقصد که کاربر بعد از احراز هویت به آن‌ها دسترسی دارد

ـ امـکان محدود کـردن بازه‌های زمانی مجاز برای دسترسـی کاربران (به دو صورت مطلق و روزانه)

ـ امکان حـذف خودکار قواعد دسترسـی کـه بازه‌های زمانی مجاز آن‌ها سپری شده است

ـ امکان محدود کردن دسترسـی کاربران بر اسـاس آدرس IP مبدا، مقصد و گروه‌های کاربری

ـ امکان تعریف مقادیر ثابت برای گروه‌های آدرس IP، بازه‌های زمانی، الگوهای داده و ارجاع به آن‌ها در قواعد دسترسی

ـ امـکان تعریـف و اعمـال درخواسـت تائیدیـه دسترسـی (Approval Workflow) بـه‌صورت سلسـله مراتبـی بـرای مدیریـت جریـان کاری دسترسـی کاربـران بـه سـامانه‌های عملیاتی

ـ امکان تعریف چند Directory برای کاربران

ـ امکان تعریف کاربران به‌صورت محلی در PAM (ساتراپ اسپارا)

ـ گروه‌بنـدی کاربـران براسـاس گروه‌های تعریف‌شـده در PAM (ساتراپ اسپارا)

ـ تخصیص نقش‌های مختلف به هر کاربر به‌صورت نامحدود

مزایـــای رقـابتـــی
Isolator Platform

تولید بومی و From scratch

رابط و تجربه کاربری به‌مراتب آسان‌تر

امکان شخصی‌سازی بر اساس نیاز سازمان‌ها

پشتیبانی ۲۴ ساعته

مبتنی بر تکنولوژی Container

مدیریت کلمات عبور

ـ امکان تولیـد یک‌بارمز (OTP) مدت‌دار بـرای کاربران به‌منظور ایجاد دسترسی موقت

ـ محدود کردن آدرس‌های IP مجاز برای ورود به کنسول وب برای هر کاربر

ـ امکان اعمـال تمام قواعد پیچیدگی کلمات عـبور برای کاربران محلی PAM

رخدادنگاری

ـ امـکان جسـتجو و ثبـت کلیـه رخدادهای سـامانه بـه‌صورت متمرکز

ـ امـکان ارسـال رخدادهـای سـامانه در قالـب Syslog بـرای سامانه‌های SIEM

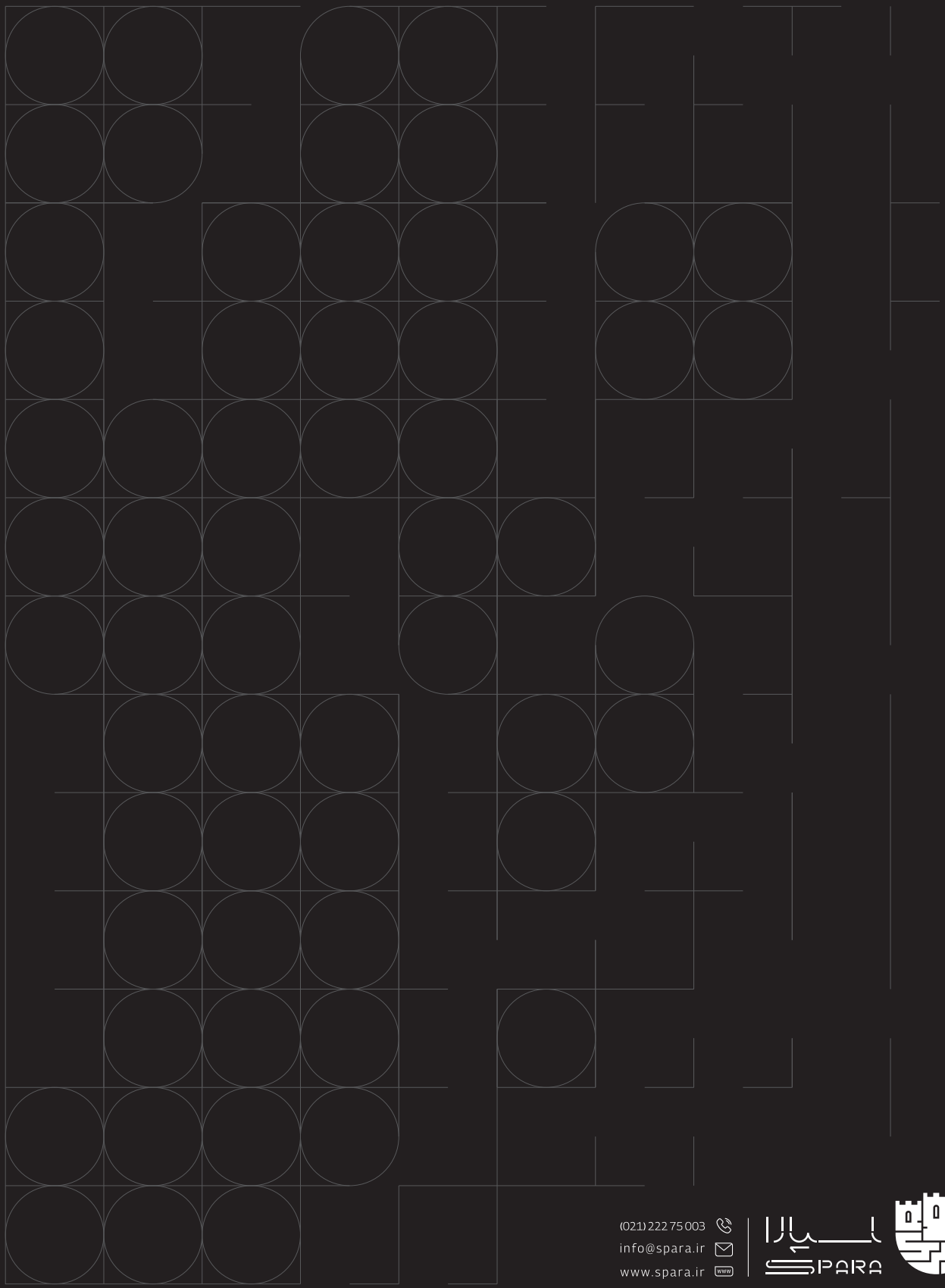
ـ امکان نگهداری و آرشیو رخدادها به‌صورت نامحدود

یکپارچه‌سازی

ـ یکپارچه‌سازی کاربران و امکان احراز هویت با LDAP

ـ امکان ایجاد انواع تغییرات در سامانه با استفاده از API

مشتریان اسپارا



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

اسپارا
SPARA