سپارا
SPARA

SATRAP

# مدیریت دسترسی ممتاز

# Privileged Access Management

# 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 سامانه مدیریت دسترسی ممتاز (ساتراپ)

حساب‌های کاربری ممتاز به حساب‌هایی گفته می‌شود که کاربرانش دسترسی‌های ممتاز دارند. این دسترسی‌ها می‌تواند منجر به ایجاد تغییرات در سطوح کلان اجرایی روی برنامه‌ها و سیستم‌ها و همینطور سروکار داشتن با اطلاعات محرمانه شرکت شود. به همین دلیل این حساب‌ها و کاربرانش اهداف جذابی برای مجرمان سایبری هستند. هکرها با هدف قرار دادن کاربران و دزدیدن مشخصات کاربری‌شان (Credentials) سعی می‌کنند تا این دسترسی‌های ممتاز را در اختیار بگیرند.

تحقیقات نشان می‌دهد که بیش از ۸۰ درصد نقض داده‌ها ناشی از مشخصات کاربری به‌سرقت‌رفته یا به خطر افتاده است[1] و میانگین هزینه جهانی این اتفاق، ۴/۴۵ میلیون دلار عنوان شده.[2]

در نتیجه یکی از دغدغه‌های اصلی در سازمان‌ها، مدیریت دسترسی‌های ممتاز است.

**ساتراپ اسپارا** محصولی برای پیاده‌سازی مدیریت دسترسی ممتاز است که امکان پایش، کنترل و امن‌سازی دسترسی کاربران ممتاز به سامانه‌های حیاتی سازمان را فراهم می‌کند.

1- https://www.crowdstrike.com/cybersecurity-101/what-is-privileged-access-management/

2- https://www.ibm.com/reports/data-breach

## آمارهای جهانی

**٪۸۶**

از نقض داده‌ها به علت سواستفاده از مشخصات کاربری (Credentials) به‌سرقت‌رفته است. (Verizon)

**٪۷۱**

به‌صورت سال به سال، استفاده از مشخصات کاربری دزدیده‌شده یا به خطر افتاده افزایش داشته است. (IBM)

**۶۷۹،۶۲۱**
**دلار**

میانگین خسارت سرقت Credentialها در هر حادثه است.
(Ponemon Institute)

**۱۶/۹**
**میلیارددلار**

پیش‌بینی میزان ارزش بازار PAM تا سال ۲۰۳۰ است. (kbv research)

# ویژگی‌های محصول ساتراپ اسپارا

## ویژگی‌های اصلی

- مدیریت، کنترل و ممیزی بازه متعددی از نشست‌های راه دور کاربران
- پشتیبانی از پروتکل‌های SSH، RDP، VNC، Oracle database و MS SQL server
- مدیریت سامانه از طریق کنسول وب
- عدم نیاز به نصب عامل نرم‌افزاری در کلاینت و سرور (Agentless)
- امکان اتصال به سرورها از طریق کنسول وب، Transparent و Bastion
- سازگاری با استانداردهای PCI-DSS و FIPS140-2
- RemoteApp: ارائه نرم‌افزارهای کاربردی در یک محیط ایزوله و تحت نظارت (مرورگر، دسکتاپ، IDE و غیره)
- امکان پیاده‌سازی HA در انواع مختلف مدل‌های استقرار
- تجهیز تمام اپلیکیشن‌های مورداستفاده سازمان به احراز هویت چندگانه

# سایر ویژگی‌های ساتراپ

## ممیزی نشست‌ها

- مشـاهده برخط فعالیت‌های کاربر در نشسـت و اجبار به خاتمه در صـورت صلاحدید کاربر ممیز (4Eye Authentication)
- مشاهده فعالیت‌های کاربر در نشست‌ها به‌صورت فیلم
- مشاهده کلیه فعالیت‌های Keyboard و Clipboard در نشست‌های SSH، RDP و VNC
- مشاهده نام، حجم و Checksum فایل‌های منتقل‌شده در نشست‌های RDP
- امـکان Full-Text Search روی محتوای نشست‌ها و پخش فیلم نشست از زمان ظاهر شدن عبارت جستجوشده در صفحه بر اساس OCR
- امکان Global Full-Text Search روی محتوای تمام نشست‌ها
- نگهداری اطلاعات نشست‌ها (فیلم‌ها و لاگ‌ها) به‌صورت فشرده و با حجم کم (به‌صورت میانگین ۳۰ مگابایت بر ساعت برای هر نشست)
- عدم وجود محدودیت نرم‌افزاری روی تعداد نشست‌های قابل ذخیره و پخش در سامانه
- امکان فیلتر نشست‌ها بر اساس مبدا، مقصد، زمان نشست و غیره

# کنترل محتوای نشست‌ها

ـ محدودسازی دستورهای مجاز و غیرمجاز واردشده توسط کاربر در قالب Regular Expression (متناسب با پروتکل استفاده‌شده)

ـ محدود کردن نوع کانال‌های مجاز در نشست‌های SSH (Port Forward, Exec, SFTP و غیره)

ـ محدود کردن نوع کانال‌های مجاز در نشست‌های RDP (Clipboard, File System و غیره)

ـ محدود کردن نوع دستورهای مجاز و جداول در نشست‌های Oracle (Select, Update و غیره)

# پایش‌پذیری

ـ داشبورد جامع پایش وضعیت سامانه

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

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

ـ ایجاد رخداد در صورت تغییر در وضعیت شاخص‌های سلامت سامانه

ـ امکان یکپارچه‌سازی با ابزارهای Monitoring

ـ عدم تغییر آدرس‌های IP مبدا و مقصد در حالت استقرار شفاف

ـ امکان آرشیو خودکار نشست‌ها در فضای ذخیره‌سازی تحت شبکه

ـ امکان حذف خودکار ویدیو نشست‌های قدیمی

# کنترل دسترسی

ـ امکان احراز هویت به چهار روش مختلف (Ask, Save Credential, PAM Credential, Ask Password)

ـ امکان احراز هویت کاربران با سامانه‌های مدیریت متمرکز کاربران ازجمله LDAP و Active Directory

- پشتیبانی از احراز هویت چندگانه در دسترسی کاربران

- احراز هویت کاربران با استفاده از کلید عمومی در نشست‌های SSH

ـ امکان نگاشت خودکار کلمات عبور سامانه‌های مقصد با استفاده از Password Vault و مخفی نگه داشتن آن‌ها از کاربران

ـ ارائه لیست سرورها و Credentials سرورهای مقصد که کاربر بعد از احراز هویت به آن‌ها دسترسی دارد

ـ امکان محدود کردن بازه‌های زمانی مجاز برای دسترسی کاربران (به دو صورت مطلق و روزانه)

ـ امکان حذف خودکار قواعد دسترسی که بازه‌های زمانی مجاز آن‌ها سپری شده است

ـ امکان محدود کردن دسترسی کاربران بر اساس آدرس IP مبدا، مقصد و گروه‌های کاربری

ـ کنترل متمرکز کلیدهای عمومی سرورهای SSH و RDP برای جلوگیری از حملات Man-in-the-middle

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

ـ امکان محدودسازی و جلوگیری از برنامه‌های اجرایی و اتصالات شبکه توسط کاربر در نشست‌های RDP

ـ امکان تعریف و اعمال درخواست تائیدیه دسترسی (Approval Workflow) تا ۱۰ سطح برای مدیریت جریان کاری دسترسی کاربران به سامانه‌های عملیاتی

## گزارش‌گیری

ـ امکان دریافت گزارش‌های تجمیعی از تعداد و مدت زمان نشست‌ها به تفکیک پروتکل، مبدا، مقصد و غیره

ـ امکان دریافت گزارش‌های تجمیعی از کانال‌های برقرارشده در نشست‌های RDP و SSH

ـ امکان دریافت گزارش‌های تجمیعی از نوع دستورهای واردشده و جداول پایگاه داده استفاده‌شده در نشست‌های Oracle

ـ امکان گزارش‌گیری پویا براساس سرور مبدا و مقصد

## رخدادنگاری

ـ امکان جستجو و ثبت کلیه رخدادهای سامانه به‌صورت متمرکز

ـ امکان ارسال رخدادهای سامانه در قالب Syslog برای 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

## مدیریت کاربران

ـ امکان تعریف چند Directory برای کاربران

ـ امکان تعریف کاربران به‌صورت محلی در ساتراپ

ـ گروه‌بندی کاربران بر اساس گروه‌های تعریف‌شده در ساتراپ

ـ امکان تولید یک‌بار رمز (OTP) مدت‌دار برای کاربران به‌منظور ایجاد دسترسی موقت

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

ـ تخصیص نقش‌های مختلف به هر کاربر به‌صورت نامحدود

ـ محدود کردن نشست‌های قابل ممیزی بر اساس برچسب نشست برای هر کاربر

ـ محدود کردن نوع رخدادهای قابل مشاهده برای هر کاربر

ـ امکان اعمال قاعده پیچیدگی کلمات عبور برای کاربران محلی ساتراپ

ـ امکان تعریف Lockout Policy برای هر کاربر

ـ امکان تعریف و اعمال سیاست‌های Check-In/Out روی شناسه‌های کاربری

## مدیریت کلمات عبور

ـ امکان ذخیره امن کلمات عبور در Password Vault سامانه

ـ رمزنگاری کلمات عبور با الگوریتم AES -256

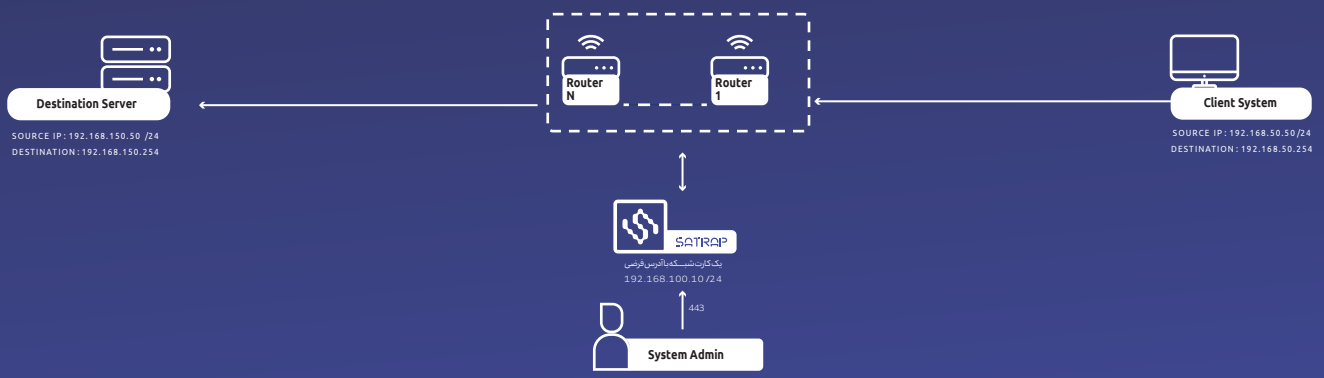
ـ عدم امکان دستیابی مدیر سامانه به کلمات عبور ذخیره‌شده در Password Vault

# انواع استقرار

سامانه مدیریت دسترسی ممتاز اسپارا بر اساس انتخاب کارفرما در دو حالت غیرشفاف و شفاف قابل استقرار است:

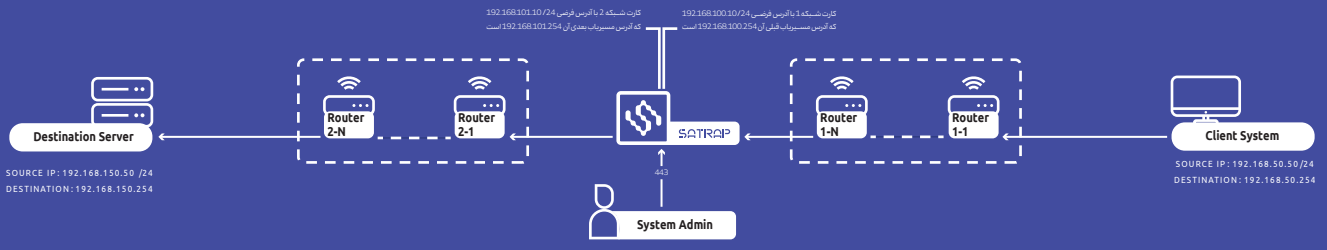
## استقرار غیرشفاف

کاربر برای اتصال به سـرور مقصد، ابتدا به آدرس سرور ساتراپ متصل شده و سپس در کنسول نمایش‌داده‌شده توسط ساتراپ، آدرس سرور مقصد را وارد می‌کند.



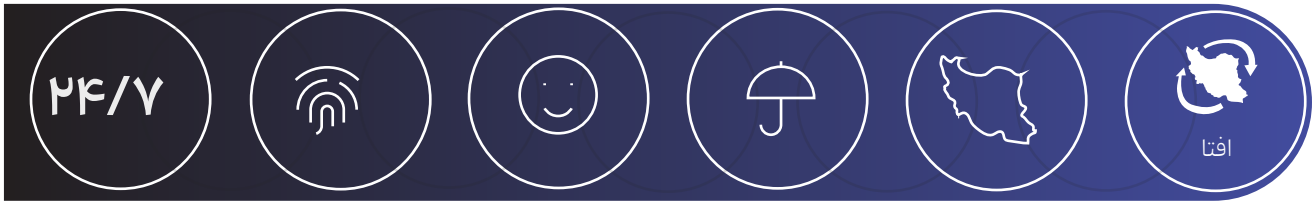

## استقرار شفاف

امکان مسیریابی ترافیک مربوط به دسترسی‌های ممتاز از مسیر سرور ساتراپ وجود دارد و کاربر هنگام اتصال، به‌صورت مستقیم آدرس سرور مقصد را وارد می‌کند. به‌علاوه می‌توان سامانه را به‌صورت ARP Proxy نیز در مدار قرار داد.



# مزیت رقابتی ساتراپ اسپارا

## نسبت به رقبای داخلی




دارای مجوز افتا

تولید بومی و From scratch

پشتیبانی از پروتکل‌های Oracle و SQL server

رابط و تجربه کاربری به‌مراتب آسان‌تر

امکان شخصی سازی بر اساس نیاز سازمان‌ها

پشتیبانی ۲۴ ساعته

## نسبت به رقبای خارجی

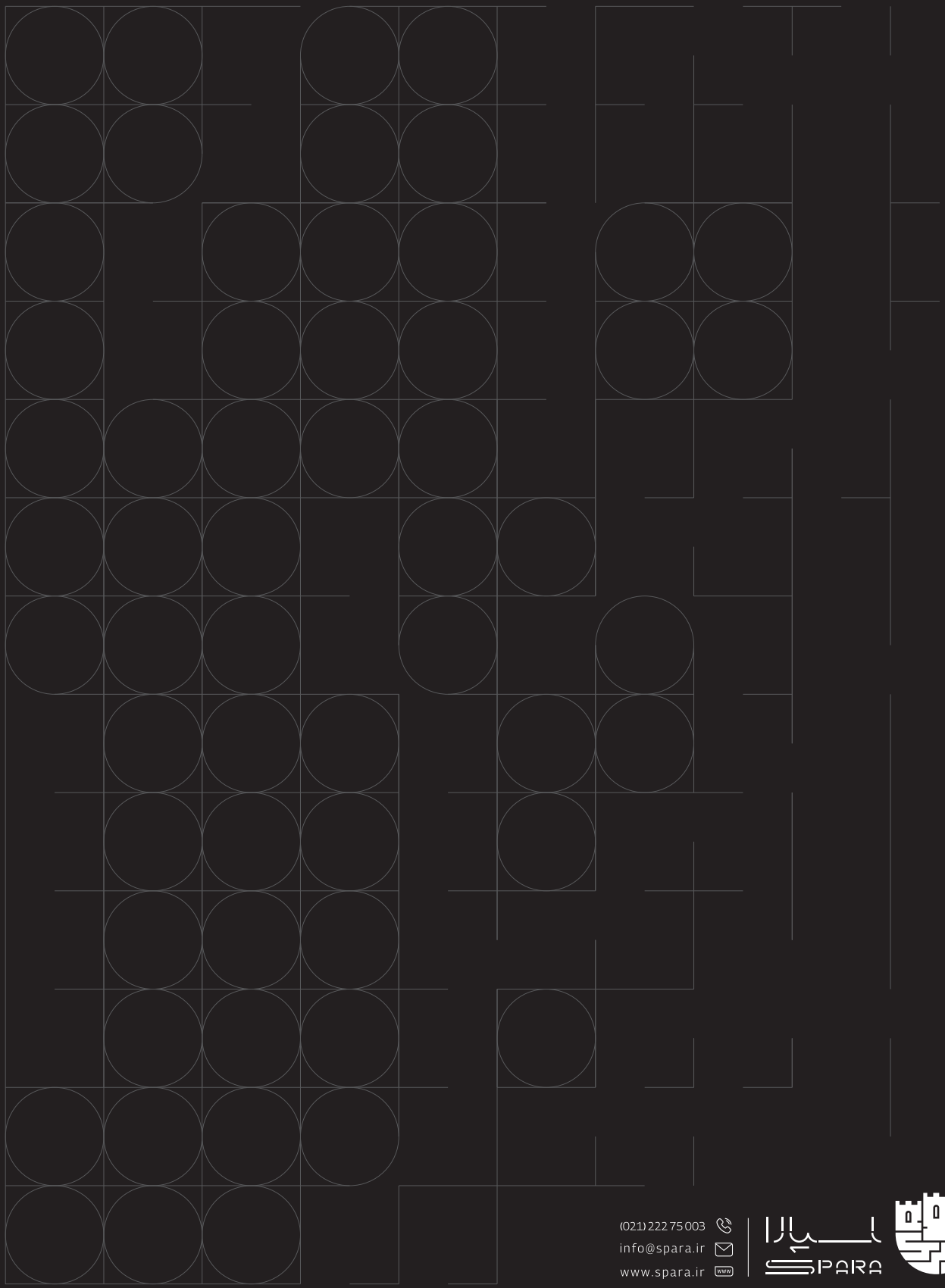

قیمت بسیار مناسب

توجه به امکانات محدود موجود به‌دلیل تحریم‌ها و استفاده از کتابخانه‌های متن باز

# مشتریان ساتراپ اسپارا







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

اسپارا
SPARA