

برقراری امنیت ضروری برای دسترسی‌های ویژه و از راه دور با سکتونا

حساب‌های ویژه خواه در خود شرکت، در حالت عمومی، ابری یا به‌صورت ویژه، در همه جا هستند. این حساب‌ها به شکل‌های مختلفی وجود دارند: حساب‌های محلی، حساب‌های سرویس، حساب‌های دامین و حساب‌های اپلیکیشن. با نگاهی به گذشته، شاهد نقض‌های اطلاعاتی مشهوری در زمینه ریسک‌های فاجعه‌بار همراه با مدیریت ویژه ولی ضعیف گذرواژه هستیم. مشکل حساب‌های ویژه فراتر از مدیریت گذرواژه‌هاست. خیلی مهم است که برای حالت‌هایی همچون دسترسی نیروهای دورکار، دسترسی به تمامی دارایی‌های بحرانی آی تی مدیریت شوند.

نیاز برای مدیریت دسترسی ویژه، سیر تکاملی خود را پیموده و به یک الزام جدی برای سازمان‌هایی با هر اندازه و مقیاس تبدیل شده است. با توجه به اینکه سازمان‌ها نیازها و اولویت‌های نسبتاً متفاوتی دارند، یک راهکار کلی نمی‌تواند برای سازمان‌هایی با اندازه متوسط به‌منظور دستیابی به فواید مدنظر مناسب باشد. نسخه جدید سکتونا با نام Privileged Access Management Standard+ در جهت کمک به ایمن‌سازی سازمان‌های با اندازه متوسط در برابر هرگونه ریسک مرتبط با حساب‌های ویژه، مجموعه ابزارها و کارکردهای مناسبی به‌همراه دارد. این نسخه به سازمان‌ها کمک می‌کند تا به ارزش ارتقای سکتونا پام پی ببرند و به امنیت دسترسی به حساب‌های ویژه خود سر و سامان دهند.

موارد اصلی استفاده پیرامون دسترسی ویژه و دسترسی کاربران دورکار، شامل موارد زیر است:

ما برای موارد استفاده‌ای همچون دسترسی دور دست گرفته تا مدیریت گذرواژه، به شما راهکارهایی ارائه می‌کنیم. این راهکارها شامل موارد زیر هستند:

- مدیریت گذرواژه و پایش جلسات با تأیید چندعاملی
- فروشندگان دورکار تحت سرپرستی و برخورد از امنیت
- دسترسی از طریق مرورگر بصورت امن و ایزوله به اپلیکیشن‌های بحرانی تجاری
- دسترسی پایش‌شده و شفاف به ایستگاه‌های کاری برای کاربران دورکار
- به‌اشتراک‌گذاری و مشارکت در جلسات ویژه بدون حضور کلاینت
- دسترسی ویژه بدون VPN

خیلی مهم است که دسترسی کاربران دورکار از یک پلتفرم یکپارچه به دارایی‌های زیرساخت حیاتی، مدیریت و محافظت شود. با فناوری نسل جدید و میان‌پلتفرمی سکتونا که با پام قدرت گرفته است، رویکرد دسترسی ویژه و از راه دور خود را به‌روزرسانی کنید.



استفاده از حساب ویژه از راه دور به‌صورت ایزوله و امن

مجموعه پام بدون VPN یا قابل یکپارچه شدن با VPN به شکل میان‌پلتفرمی برای ایزوله کردن تمامی جلسات ویژه کاربری



دسترسی میان‌پلتفرمی و بدون عامل (agent)

رویکرد نوین در مقیاس سازمانی برای فراهم ساختن امکان دسترسی از هر سیستم‌عامل، هر مرورگر بدون نیاز به پلاگین یا عامل



با ویژگی کشف یا discovery، به اتوماسیون بیشتری بپردازید

ویژگی ذاتی و توانمند کشف هیبریدی و گروه‌بندی مبتنی بر خصوصیت (attribute)، باعث مدیریت ساده‌تر پام شده و زمان مورد نیاز برای فراهم کردن دسترسی را نیز کاهش می‌دهد



ساخته شده برای به‌کارگیری‌های آنی

میکروسرویس‌هایی که به‌صورت شهودی ایجاد شده‌اند و راهکارهای سبک‌وزن همراه با بسته‌هایی که برای به‌کارگیری سریع‌تر و ساده‌تر، تنها با یک کلیک نصب می‌شوند

ویژگی‌های اصلی

• پایش جلسه

افزایش میزان دید تمامی فعالیت‌های کاربران ویژه روی سرورها، پایگاه داده، ایستگاه‌های کاری و دستگاه‌های شبکه از طریق موتور ضبط جلسات که لاگ‌ها را ثبت می‌کند؛ از جمله نام‌های کاربری، آدرس‌های آی‌پی و مهر زمانی (timestamp).

• مدیریت خودکار گذرواژه

کافی است فرایند سه‌مرحله‌ای مدیریت خودکار گذرواژه (تغییر، صحت‌گذاری، جایگزینی) را برای حساب‌های کاربری محلی و ویژه دامنه در سرتاسر سیستم‌عامل، پایگاه داده، دستگاه‌های شبکه و منابع ابری فعال کنید.

ویژگی‌های اصلی

• مدیریت جلسات هیبریدی

قابلیت‌های میان‌پلتفرمی را ارتقا دهید تا تمامی کاربران ویژه (از جمله کاربران دورکار که به سیستم‌های بسیار ویژه دسترسی دارند) از طریق مرورگر از روی هر سیستم‌عامل یا هر پلتفرم، بصورت امن و ایزوله به سیستم‌های بحرانی آتی‌تی و اپلیکیشن‌ها دسترسی پیدا کنند

• تأیید چندعاملی

با استفاده از تأیید چندعاملی (MFA) ذاتی و به‌منظور ایمن‌سازی دسترسی مدیریتی کاربران داخلی و کاربران آتی‌تی بیرونی، لایه امنیتی را بهبود دهید

• مشارکت در جلسات ویژه

گروه‌های آتی‌تی را توانمند کنید تا بصورت امن از طریق مرورگر و بدون نیاز به کلاینت یا پلاگین، در جلسات ویژه شرکت کنند و آنها را به‌اشتراک بگذارند. همچنین، وابستگی به ابزارهای مشارکتی طرف سوم که آسیب‌پذیر هستند را کاهش دهید.

موارد مورد نیاز

اسپکترا یک راهکار سبک‌وزن پام و برخوردار از یک معماری مبتنی بر میکروسرویس است که می‌توان از آن بر روی یک پلتفرم ویندوز (فیزیکی، ماشین مجازی یا روی ابر) استفاده کرد. با ارتقای Microsoft SQL برای پایگاه داده، تمامی اطلاعات حساس در یک فرمت رمزگذاری‌شده (AES ۲۵۶ یا RSA ۲۰۴۸) در درون اسپکترا والت (Spectra Vault) ذخیره می‌شوند. کاربران می‌توانند با بهره‌گیری از اسپکترا از روی هرگونه پلتفرم کاربر نهایی، سیستم‌عامل (ویندوز، مک، یونیکس) و با هر مرورگری که از اچ‌تی‌ام‌ال ۵ پشتیبانی می‌کند، به دارایی‌های آتی‌تی دسترسی پیدا کنند. این دسترسی با استفاده از ارتباط تک‌درگاهی تسهیل‌شده از هر ماشین کاربر نهایی به اپلیکیشن اسپکترا برای تانلینگ امن، برقرار می‌شود.

هر زمان که لازم است، نسخه جدیدتری در اختیار داشته باشید

برای مدیریت دسترسی به کاربران بیشتر، یا ضمیمه کردن دارایی‌های بیشتر آتی‌تی و فعال‌سازی بیش از ۲۵ جلسه همزمان، می‌توانید با هزینه اندکی به نسخه جدید Enterprise+ دست پیدا کنید. علاوه بر این، می‌توانید ویژگی‌های پیشرفته از جمله مدیریت گذرواژه اپلیکیشن به اپلیکیشن، طراحی گزارش خاص، زمان‌بندی گزارش، دیدن جلسه مستقیم، پیکربندی به‌تفرض‌رای نمره‌دهی به ریسک، اتوماسیون کارهای ویژه، یکپارچه‌سازی‌های سازمانی همراه با میز سرویس و MEIS و مدیریت چندمت‌سأجر (tnaneT-itluM)، اعلان‌های بلادرنگ و کنترل بر حساه‌یو‌ی‌ها را نیز در اختیار داشته باشید؛ همگی با استفاده از نسخه Enterprise+.

برای اطلاعات بیشتر با [نمایندگان فروش](#) ما تماس بگیرید.

