Sectona

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

حساب‌های ویژه خواه در خود شرکت، در حالت عمومی، ابری یا بصورت 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 آی‌تی 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 نسبتا 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 سازمان دهند .

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

ما برای موارد استفاده ای همچون دسترسی دوردست گرفته تا مدیریت گذرواژه، به شما راهکارهایی ارائه می کنیم. این راهکارها شامل موارد زیر هستند :

- مدیریت گذرواژه و پایش جلسات با تأیید چندعاملی
- فروشندگان دورکار تحت سرپرستی و برخوردار از امنیت
- دسترسی از طریق مرورگر بصورت امن و ایزوله به اپلیکیشن های بحرانی تجاری
- دسترسی پایش شده و شفاف به ایستگاه های کاری برای کاربران دورکار
- به اشتراک گذاری 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 میان پلتفرمی سکتونا که با پم قدرت گرفته است، رویکرد دسترسی ویژه و از راه دور خود را به روزرسانی کنید.

ساخته شده برای به‌کارگیری‌های آنی

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

با ویژگی کشف یا discovery، به اتوماسیون بیشتری بپردازید

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

دسترسی میان‌پلتفرمی و بدون عامل (agent)

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

استفاده از حساب ویژه از راه دور به‌صورت ایزوله و امن

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

ویژگی‌های اصلی

• مدیریت خودکار گذرواژه

کافی است فرایند سه مرحله ای مدیریت خودکار گذرواژه (تغییر، صحه گذاری، جایگزینی) را برای حساب های کاربری محلی و ویژه دامنه در سرتاسر سیستم عامل، پایگاه داده، دستگاه های شبکه و منابع ابری فعال کنید

• 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) .

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 آی‌تی و اپلیکیشن‌ها دسترسی پیدا کنند

• تأیید چندعاملی

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

• مشارکت در جلسات ویژه

گروه‌های آی‌تی 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 .

• کشف دارایی‌ها و حساب‌های کاربری

با ایجاد زمان‌بندی برای کشف خودکار دارایی و حساب‌های کاربری، می‌توانید با بهره‌گیری از فهرست‌سازی از دارایی‌های ناشناخته آی‌تی و حساب‌های ویژه در دپارتمان فناوری اطلاعات، مدیریت پم را تسهیل کنید .

• وارسی کنترل‌ها و گزارش‌گیری

با دستیابی به بیش از یکصد گزارش خلاقانه ازجمله حقوق کاربری، تلاش‌های ناموفق برای ورود، فهرست دارایی‌ها و حساب‌ها، بهترین اقدامات برای تأمین امنیت دسترسی ویژه را در اختیار خود داشته باشید .

موارد مورد نیاز

اسپکترا یک راهکار سبک وزن پام و برخوردار از یک معماری مبتنی بر میکروسرویس است که می توان 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 رمزگذاری شده)AES ۲۵۶ یا RSA ۲۰۴۸(در درون اسپکترا والت)Spectra Vault) ذخیره می شوند. کاربران می توانند با بهره گیری از اسپکترا از روی هرگونه پلتفرم کاربر نهایی، سیستم عامل ویندوز، مک با هر مرورگری که از HTML5 پشتیبانی می کند، به دارایی های آی تی 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 دارایی های بیشتر آی تی و فعال سازی بیش از ۲۵جلسه همزمان، می توانید با هزینه اندکی به نسخه جدید Enterprise+ دست پیدا کنید. علاوه بر این، می توانید ویژگی های پیشرفته از جمله مدیریت گذرواژه اپلیکیشن به اپلیکیشن، طراحی گزارش خاص، زمان بندی گزارش، دیدن جلسه مستقیم، پیکربندی‌پیشرفته برای نمره دهی به ریسک، اتوماسیون کارهای ویژه، یکپارچه سازی های سازمانی همراه با میز سرویس وSIEM و مدیریت چندمستاجر(Multi-Tenant)، اعلان های بلادرنگ و کنترل بر مدیریت حساب خصوصی را نیز در اختیار داشته باشید؛ همگی با استفاده از نسخه Enterprise +. امکان پذیر است.

برای اطلاعات بیشتر با نمایندگان فروش ما تماس بگیرید.

Sectona