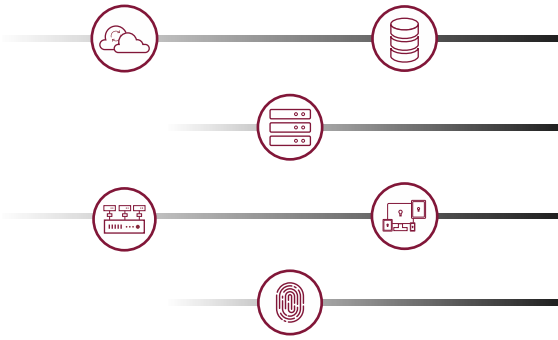
Datasheet

Sectona



عملکرد برقراری امنیت برای کاربر ویژه

افزایش در نقض امنیت در نتیجه سوءاستفاده از امتیازهای کاربری، در محیط امروزی قابل مشاهده است. سازمان ها در حال بررسی دلیل به کارگیری ابزارها و شیوه های امنیتی ضعیف از سوی ادمین ها و گروه های پشتیبانی هستند. امروزه، کسب وکارها اغلب به سختی می توانند کاربران را تحت تعاریف معمول یعنی کاربران داخلی و خارجی دسته بندی کنند. با تغییر حوزه کاربران، سرورها و اپلیکیشن ها، شاهد گذار در زیرساخت هستیم به اینصورت که وابستگی بیشتری بر مجازی سازی و پلتفرم های ابری می بینیم. شمار کاربران دوردست همواره در حال افزایش است؛ بنابراین مدیریت الزامات کاربری و سرعت به کارگیری فناوری نیز پیچیده تر می شوند .
و بدین ترتیب گروه های امنیتی برای تدارک دیدن راهبردهای انعطاف پذیر محافظت، چالش ایجاد می‌کند. اسپکترا پم با فراهم ساختن بهره‌وری مبتنی بر SSO به منظور دسترسی مدیریت، اتوماسیون گذرواژه برای حذف به اشتراک گذاری اطلاعات ورود، مدیریت کار ویژه در جهت کاهش اعطای امتیازهای اضافی و کنترل دستری‌س گرانولار همراه با قابلیت‌های مدیریت امتیاز سرور به منظور کنترل امتیازهای مربوط به دسترسی برای سازمان‌ها در هر اندازه‌ای چابکی به ارمغان می‌آورد. این راهکار در قالب یکپارچه‌سازی‌هایی با ابزارهای تایید چندعاملی، پلتفرم های مجازی‌سازی و ابری، راهکار تیکتینگ و سیستم‌های SEIM است .

مدیریت دسترسی ویژه در اسپکترا

میان امنیت و بهره‌وری کاربران دوردست با دسترسی ویژه، تعادل برقرار کنید

ادمین‌ها را چنان توانمند کنید تا به هر دستگاه یا هر شبکه‌ای که از قابلیت ساده و امن ورود یکباری برخوردار است، دسترسی داشته باشند. موارد استفاده این راهکار، این امکان را در اختیار شما قرار می‌دهند تا در سرتاسر دستگاه‌ها، با استفاده از مرورگری برگه‌ای (gnisworb debbat) مبتنی بر کلاینت، یا دسترسی مبتنی بر مرورگر برای کاربران سیار، بر نیازهای ادمین را تأمین کنید. با استفاده از سازوکارهای دسترسی امن چندگانه اسپکترا، میان نیاز به دسترسی به کاربران درونی و بیرونی از یکسو و دسته‌های حساب ویژه همراه با کانکتورهای از پیش طراحی شده و مجموعه قوانین از سوی دیگر، تعادل برقرار کنید.
ظرف چند ثانیه و با ارتقا دادن قابلیت sseccA ot yrevocsiD در سرتاسر eraWMV، XSE، ESXi، Active Directory و Cloud Resources می‌توانید به مدیریت قوانین و رویه‌ها بپردازید .

مدیریت گذرواژه و مدیریت کار را خودکارسازی کنید

ادمین‌ها، فروشندگان و گروه‌های پشتیبانی دوردست، اغلب نیاز دارند به خدمات و اپلیکیشن‌های دارای حساب‌های ویژه یا مدیریت‌نشده، دسترسی داشته باشند. ویژگی اسپکترا با عنوان tluaV drowssaP، برای مدیریت و وارسی دسترسی به حساب‌های تعاملی و همچنین حساب‌های مربوط به اپلیکیشن‌ها و حساب‌های کاربری غیرانسانی، بسیار مناسب هستند. ویژگی drowssaP detamotuA tnemeganaM این راهکار، به شما کمک می‌کند تا با یکپارچه‌سازی امن کانال‌های دسترسی در زیرساخت‌تان، سطح حمله به حساب‌های ویژه را کاهش دهید. ویژگی دیگر اسپکترا برای مدیریت کار با نام tnemeganaM ksaT نیز به خودکارسازی کارهای عادی می‌پردازد و با رهاسازی ادمین‌ها از کار قید و بند پیگیری جریان کار که لازم است هر بار برای دسترسی پیدا کردن به یک دارایی گرفتار آنها شوند، تسهیل می‌نماید. با تخصیص کار، خطای انسانی به کمترین میزان ممکن می‌رسد .

اثر بیشتر بر روی سرمایه‌گذاری‌تان

انعطاف‌پذیری را در مقیاس‌های مختلف بدون به مخاطره افتادن امنیت از طریق ماژول‌های مدیریتی یکپارچه برای دسترسی ویژه که برای تمام طرح‌های قیمتی طراحی شده‌اند، تجربه کنید .
بیش از صد کانکتور از پیش طراحی شده را ارتقا دهید و از SDKها برای توسعه هر کانکتور جدید استفاده کنید تا در خدمات جدید صرفه‌جویی به‌عمل بیاورید.
با استفاده از قابلیت‌های یکپارچه اسپکترا با نام High Availability و Disaster Recovery، در وقت و هزینه‌های خودتان صرفه‌جویی کنید.
این راهکار برای به‌کارگیری ساده طراحی شده و برای اخذ مجوز نیز گزینه‌های ساده‌ای دارد.

مزایای رقابتی

دسترسی میان‌پلتفرمی
با استفاده از هر مرورگر، هر دستگاه، کلاینت‌های نیتیو، ملزومات دسترسی پیشرفته، یا لندینگ سرور می‌توانید دسترسی پیدا کنید .

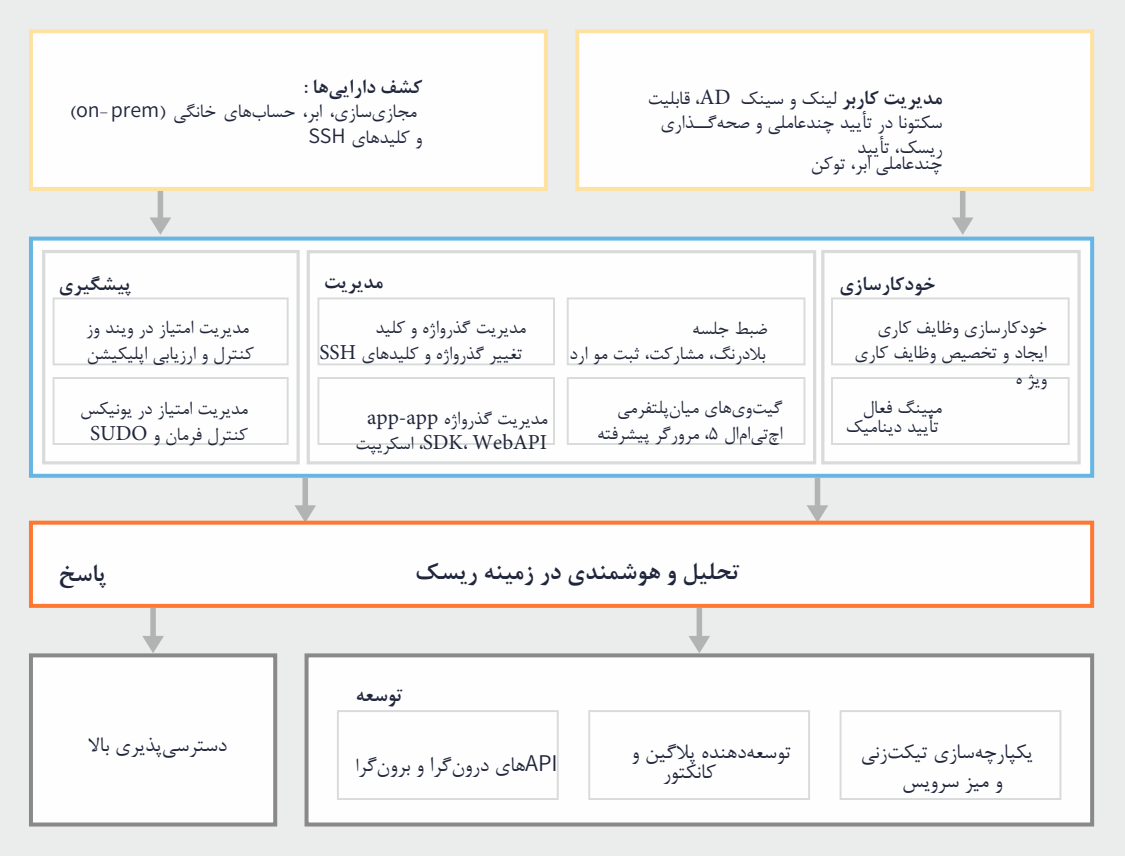
نمره دهی هوشمند به ریسک نمره دهی خودکار برای فعالیت هر جلسه که بر حسب نشانگرهای ریسک امنیتی دسته بندی شده باشند.

امنیت بهبودیافته
الگوریتم های رمزگذاری ۲۵۶، - AES
RSA-۱۰۲۴ با FIPS ۱۴۰-۲
پشتیبانی و Salting گذرواژه های رمزگذاری شده.
قابلیت های هاردینگ خودکار لایه میزبان

مدیریت گذرواژه app-app
وب‌سرورها :
(آپاچی، IIS) ،
SDKها (جاوا، دات‌نت) ،
WebAPI

پشتیبانی، فایل‌های پیکربندی اپلیکیشن
مدیریت کاربر

استک)پُشته(معماری عملکردی اسپکترا پم



یکپارچه‌سازی

صحه‌گذاری و تأیید چندعاملی

صحه‌گذاری: Active Directory، صحه‌گذاری محلی سکتونا، IBM TivoepO ،yrotceriD iln LDAP، etnI elcarO ،DA eruzArnet Directory، Radius، Oauth

تأیید چندعاملی: تأیید سکتونا، RSA SecureID، MCom،ZE ،ouD ،nigolenO ،atkO ،ocsaV Safenet، Radius

کشف
مبتنی بر شبکه، کامپیوتر اکتیو دایرکتوری، منابع آژور، منبع SWA، سیستم‌عامل میهمان eraWMV، حساب‌های کاربری محلی (ویندوز، یونیکس، لینوکس، اوراکل، Db۲، MSSQL، MySQL، Sybase)

هدایت (فورواردینگ) SIEM & Log

سامانه‌های تیکت‌زنی

مین‌فریم‌ها
AS/۴۰۰، OS/۳۹۰، z/OS

دیگران
حساب‌های سرویس ویندوز (Windows Service Accounts)، سرویس‌های وابسته، فایل‌های پیکربندی، فایل‌های پیکربندی اپلیکیشن، Dell DRAC، HP iLo

SSO و واسط‌های دسترسی
واسط‌های معمول: RDP، SSH، SFTP، FTP، Telnet، HTTP/HTTPs
پایگاه داده‌ها: SQL Server Management Studio، MySQL Workbench، Toad، SQL Developer، PL-SQL Developers، SQLPlus، MySQL Administrator، Oracle Enterprise Manager، IBM Data Studio
مجازی‌سازی: vSphere Client، VMWare Remote Control، Hyper-V Manager
ابر: کنسول AWS، پرتال Azure
دستگاه شبکه: کنسول چک‌پوینت، FortiWeb، Cisco ASDM، Juniper Network Manager
ابزارهای از راه دور: Dameware، X۱۱، VNC
واسط CLI:
SecureCRT، TeraTerm، SmartTerm

مدیریت گذرواژه
سیستم عامل
ویندوزسرور ۲۰۰۳، ویندوز سرور ۲۰۰۸، ویندوز سرور ۲۰۱۲، ویندوز سرور ۲۰۱۶، MACOS، ویندوز ویستا، ویندوز ۸، ویندوز ۱۰، سولاریس، AIX، اوبونتو، RHEL، HP-UX، Debian، مک اواس

پایگاه‌های داده
MSQL ۲۰۰۰، MSSQL ۲۰۱۲، MSSQL ۲۰۱۴، MSQL ۲۰۱۶، DB۲، MySQL، MS Azure SQL، MariaDB، Oracle ۱۱g، Oracle ۹i، Oracle ۱۰g، PostgreSQL، Sybase

دستگاه‌های شبکه
IOS، Fortigate، F۵، چک‌پوینت، سیسکو Juniper، HP ProCurve، Palo Alto، Riverbed

مجازی‌سازی
VMWare ESX، VMWare ESXi، Microsoft Hyper-V

سرویس‌های دایرکتوری
Active Directory، Open LDAP، IBM Tivoli Directory، Oracle Internet Directory، Azure