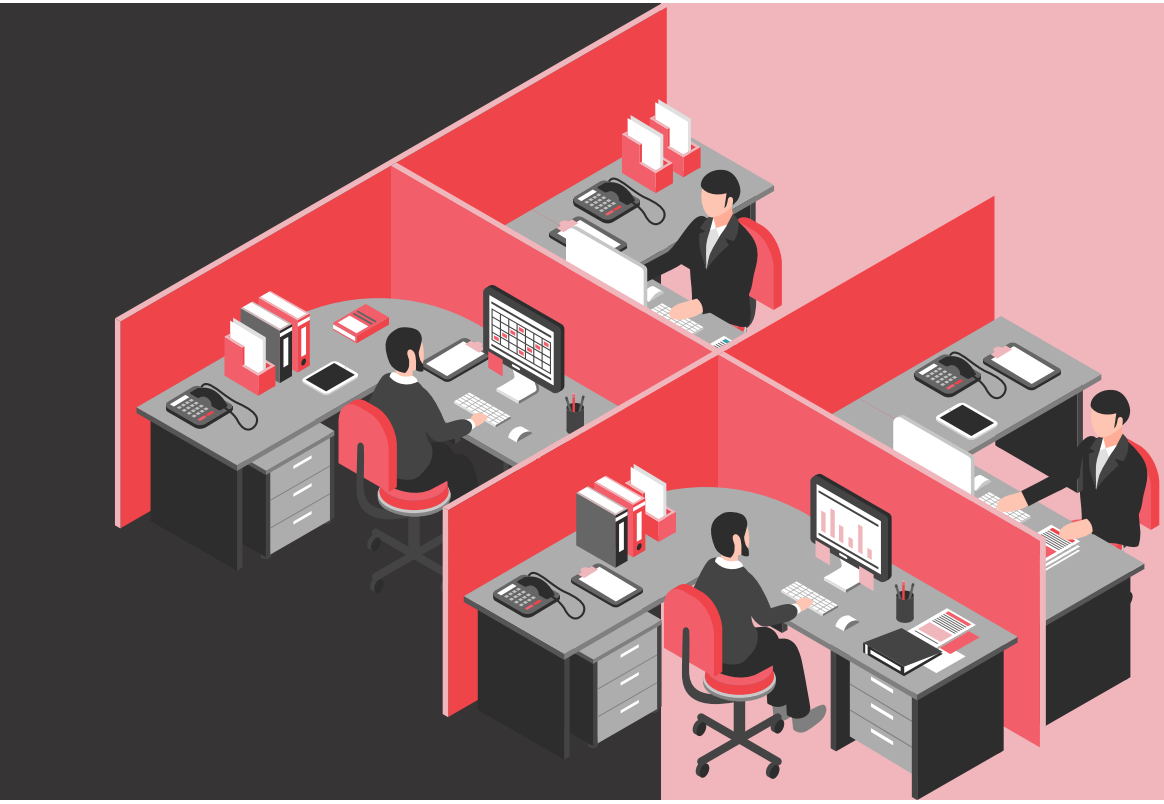
تهران، فلکه دوم صادقیه، بلوار آیت الله کاشانی، خ نجف زاده فروتن، خ اعتمادیان، پلاک ۴۲، واحد ۲ ▲ ۰۲۱ ۹۱۰۰۴۱۵۱

www.liangroup.net ▲

Arcon



نرم افزار مدیریت سطح دسترسی Arcon

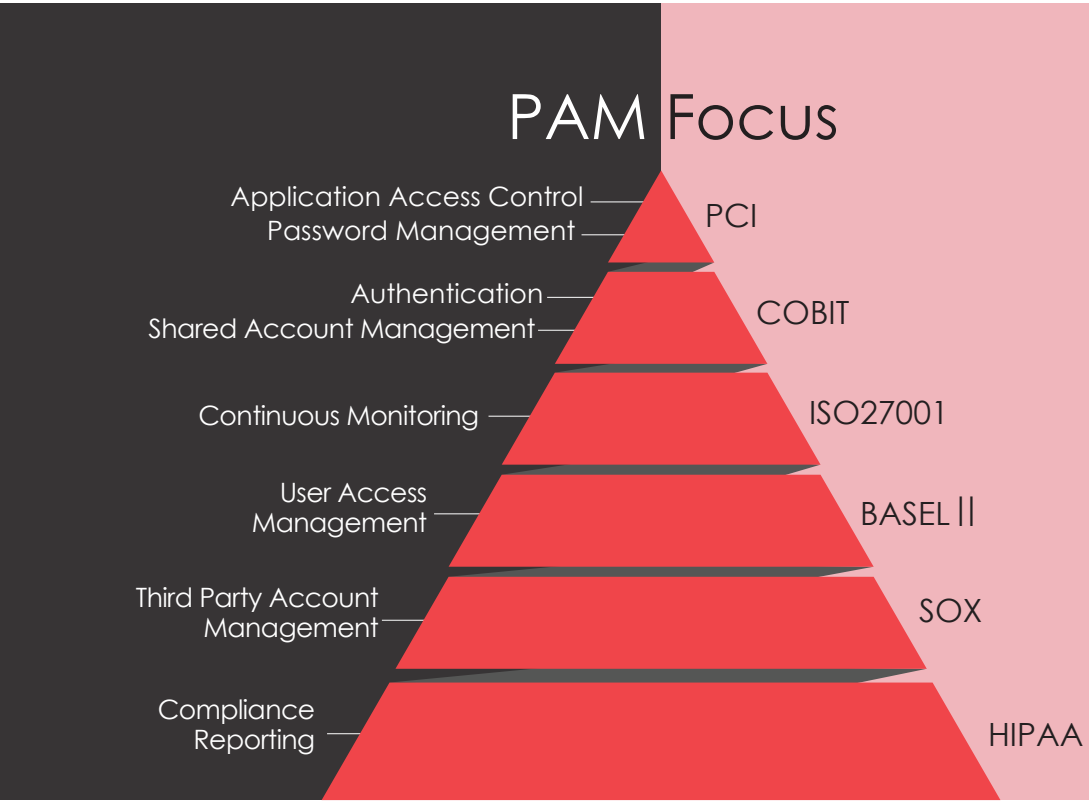
امروزه تامین امنیت فناوری اطلاعات و محافظت از دارایی‌های غیرملموس سازمانی از دغدغه‌های ویژه مدیران سازمان‌ها و شرکت‌ها به شمار می‌رود. یکی از مهم‌ترین نقطه‌های تامین امنیت فناوری اطلاعات سازمانی که خیلی کم به آن توجه شده است کنترل فعالیت کاربران با سطح دسترسی بالا می‌باشد، افرادی که سازمان بنا به ضرورت به آنها اعتماد کرده و دسترسی به حساس‌ترین و محرمانه‌ترین دارایی‌هایش را به ایشان واگذار نموده است. به منظور ایجاد بستری امن برای دسترسی مجاز و به موقع به سرویس‌ها و منابع شبکه، می‌بایست با در نظرگرفتن سطوح مختلف دسترسی و محرمانگی، امکان دسترسی به منابع شبکه را در اختیار کاربران ادمین قرار داد تا تمامی فعالیت‌ها ثبت و ضبط شده و حتی بتوان آنها را به صورت خودکار از کارهایی که نباید انجام دهند و یا می‌توانند برای سازمان پر ریسک باشند بر حذر داشت.

arcon

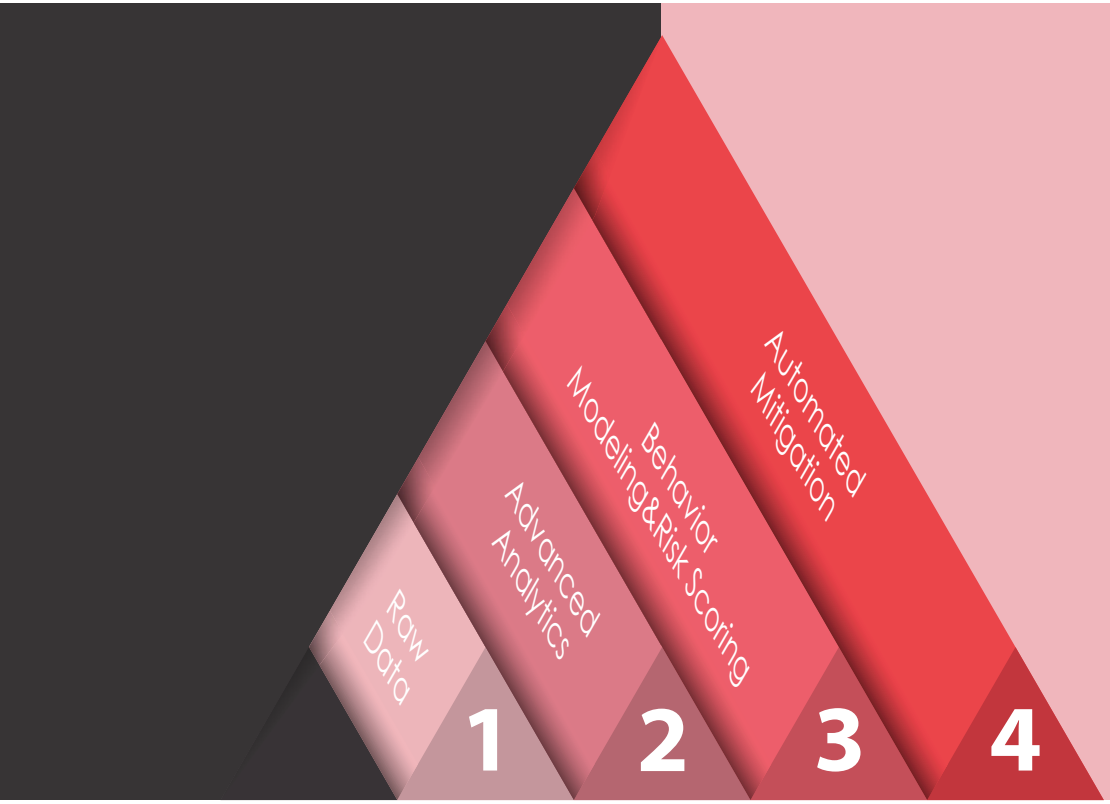
اهداف طرح

هدف از پیشنهاد طرح حاضر کنترل، مدیریت و نظارت بر عملکرد کاربران با سطح دسترسی بالا (کاربران ادمین) در سطح مرکز داده و شبکه سازمان‌ها به منظور کاهش مخاطرات امنیتی ناشی از فعالیت‌های مخرب یا اشتباهات سهوی نیروهای انسانی سازمان می‌باشد.

آمارها نشان می‌دهند که در سازمان‌های بزرگ، ریسک‌ها و تاثیر آسیب‌هایی که این افراد (افرادی که سازمان بنا به ضرورت به آنها اعتماد کرده و دسترسی به حساس‌ترین و محرمانه‌ترین دارایی‌هایش را به ایشان واگذار نموده است) به مجموعه وارد می‌کنند بسیار قابل تامل است. فارغ از اینکه علت و انگیزه چه می‌تواند باشد و یا اینکه حوادث رخ داده عمدی بوده‌اند یا سهوی، نتیجه و تاثیر بسیاری از وقایع غیرقابل جبران است. که سازمان بنا به ضرورت به آنها اعتماد کرده و دسترسی به حساس‌ترین و محرمانه‌ترین دارایی‌هایش را به ایشان واگذار نموده است) به مجموعه وارد می‌کنند بسیار قابل تامل است. فارغ از اینکه علت و انگیزه چه می‌تواند باشد و یا اینکه حوادث رخ داده عمدی بوده‌اند یا سهوی، نتیجه و تاثیر بسیاری از وقایع غیرقابل جبران است.



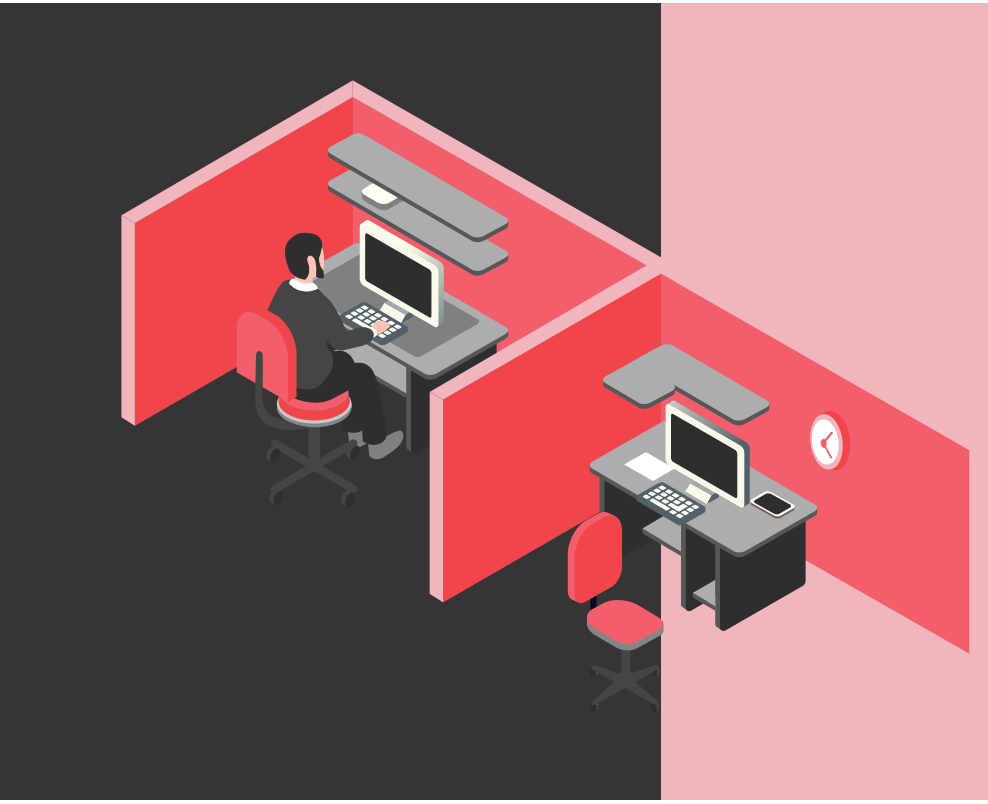
arcon



Privileged Accounts چیست؟

Privileged Accounts کاربران ارشد با بالاترین دسترسی در سیستم‌ها، دیتا بیس ها و تجهیزات شبکه هستند که با مجوز به تجهیزات و سیستم‌های بسیار حساسIT سازمان دسترسی دارند. این اکانت‌ها با دادن Privileged به کاربران دیگر ، آنها را کنترل می‌کنند. پیمانکاران، اپراتورهای نرم‌افزارهای راهبردی، مدیران شبکه‌ها و سیستم‌های اطلاعاتی، همگی به عنوان نمونه‌هایی از Privileged User ها هستند. این افراد به دلیل موقعیت شغلی یا تخصصشان، به صورت روزمره، به منابع اطلاعاتی ویژه‌ای دسترسی دارند، می‌توانند اطلاعات را کپی‌برداری کنند و در اختیار افراد غیرمجاز قرار دهند و یا مقادیر اطلاعات را به‌دور از چشم مسئولین تغییر دهند. تغییری که حتی ممکن است زمینه‌ساز تخلفاتی مانند اختلاس شود. در فرآیندهای IT پروسه‌ای به نام مدیریت تغییرات وجود دارد که در بیشتر تغییرات به‌دلایل مختلف کاربران با Privileged تغییراتی غیر از آنچه که میبایست انجام شود، انجام می‌دهند که باعث تاثیراتی غیر مطلوب در کارکرد کلی می‌گردد.

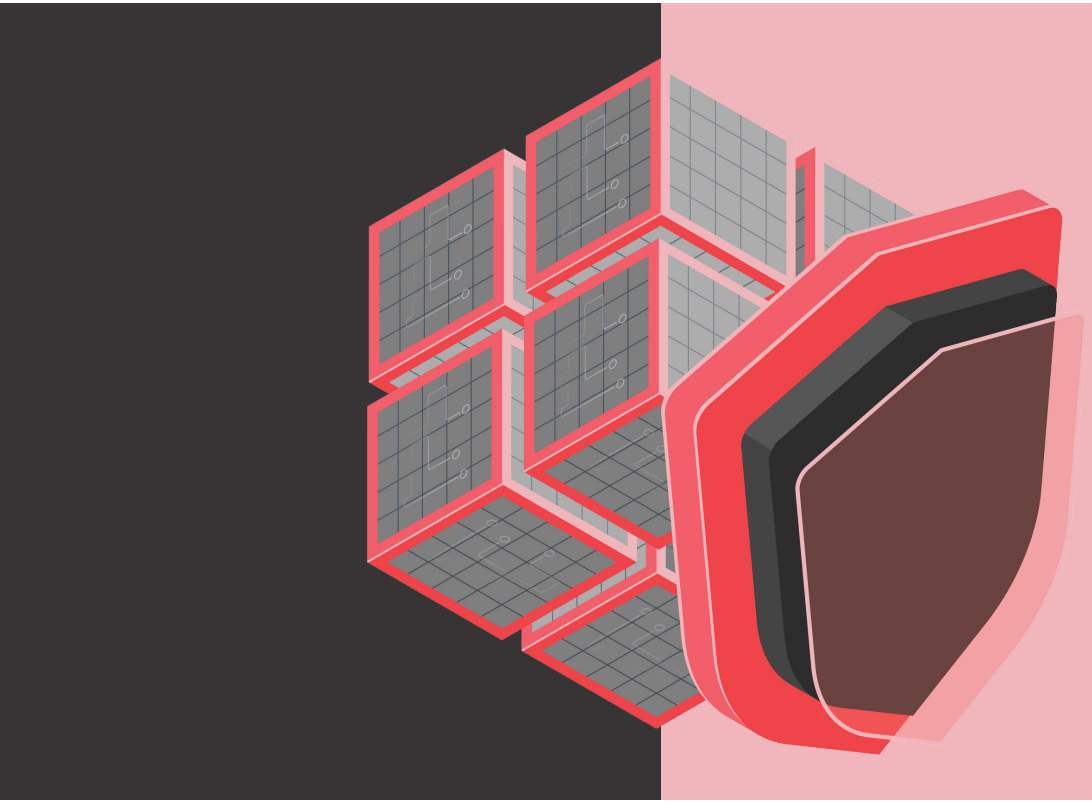
Arcon



Privileged Access Management چیست؟

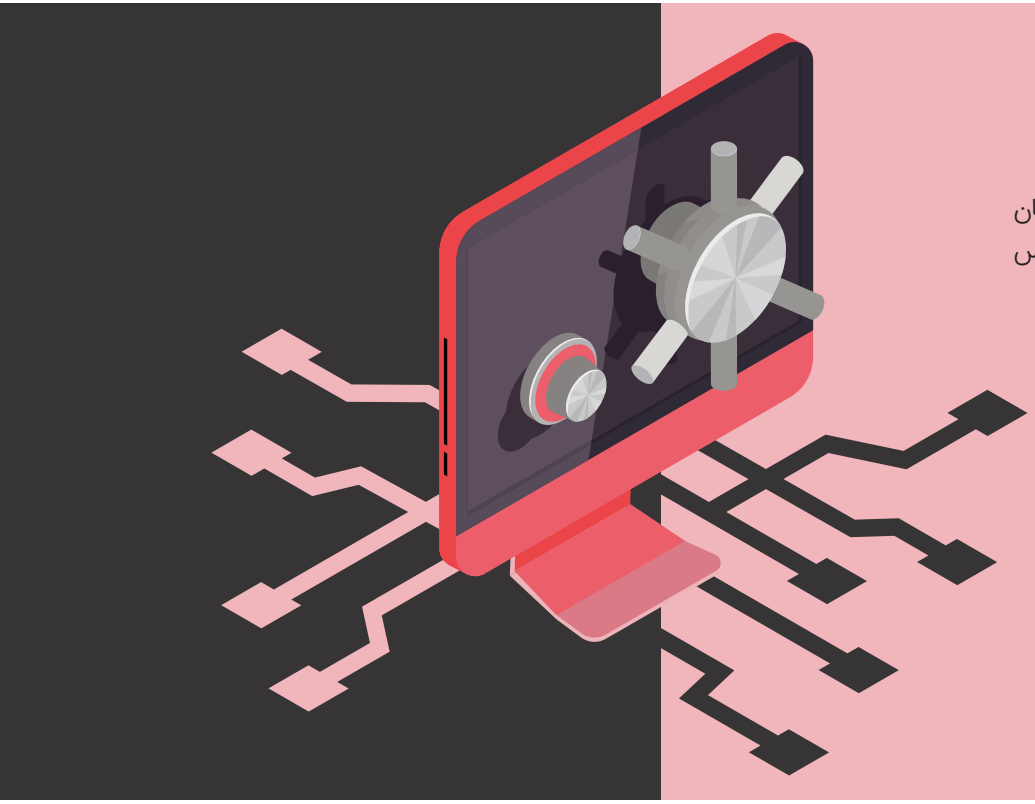
کاربرانی که سطح دسترسی بالا (Privileged) دارند می‌توانند دسترسی به منابع حیاتی سازمان داشته باشند. بنابراین، مانیتور کردن و کنترل کردن دسترسی‌های کاربرانی که سطح دسترسی بالا دارند بسیار حیاتی است. مهاجمین معمولا برای دسترسی و سرقت اطلاعات محرمانه و سوء استفاده از اطلاعات محرمانه نیاز به مجوزهای با Privilaged دارند که این مجوزها معتبر هم باشند. Privilaged Access Management راهکاری است که گروه‌های مدیریت ریسک سازمان‌ها و مدیریت امنیت سازمان‌ها را قادر می‌سازد، به دقت تمامی فعالیت‌های کاربرانی که سطح دسترسی بالا دارند را نظارت و سیاست‌های مد نظرشان را جهت ارایه دسترسی‌های آنها اعمال کنند. این سیاست‌ها می‌توانند بر اساس سیاست‌های بهینه و استاندارد شده جهانی نیز (مانند: GDPR, SOX, ISO27001, SWFT CSCF, PCI/DSS) باشد. در حقیقت با پیاده سازی راهکار PAM می‌توانید تعیین کنید چه کسی، چرا، چه زمانی و به چه میزانی به منابع سازمانی شما دسترسی داشته باشد. از آنجایی که پیشگیری همیشه بهتر و کم هزینه‌تر از چاره‌جویی‌های زمان حادثه است؛ راه کار Arcon PAM می‌تواند ریسک‌های این بخش را به طور کامل پوشش دهد. راهکار Arcon مانند یک ربات هوشمند به صورت بی‌وقفه و با خروجی‌های غیرقابل انکار، بر جزئی‌ترین فعالیت کاربران سطح بالا، نظارت کرده و با استفاده از سیاست‌های امنیتی، مدیران سازمان را قادر به کنترل‌ها و اقدامات پیشگیرانه می‌نماید.

Arcon



شرکت Arcon محصولی در این حوزه تولید کرده است که همیشه در حال توسعه و اضافه کردن ویژگی‌های منحصر به فرد می‌باشد.(Arcon | Privileged Access Management (PAM یک راه‌حل جامع است که لایه‌های امنیتی بیشتری را برای محافظت از سیستم‌های بحرانی سازمانی و اطلاعات محرمانه ارائه می‌دهد. این راه‌حل به ما در کاهش تهدیدات داخلی و پیشرفته سایبری کمک خواهد کرد. با Arcon که مجموعه از ویژگی‌های پیشرفته یک راه حل PAM را برای شما فراهم می‌کند، شما می‌توانید از تجزیه تحلیل، هشدار تهدیدات بصورت Real Time و جلوگیری از دسترسی غیر مجاز به سیستم‌ها و تجهیزات IT سازمان کمک بگیرید.

Arcon



با پیاده سازی راهکار PAM با قابلیت‌های پایش، رصد و اقدامات پیشگیرانه، امکان پوشش دادن ریسک‌هایی که سازمان از جانب کاربران Privileged متحمل می‌شود، فراهم می‌گردد. همچنین این محصول قابلیت سفارشی سازی بر اساس نیاز مشتری را داشته و از خدمات پشتیبانی تولید کننده و نماینده رسمی مجرب در محل مشتری برخوردار است.

از مهم‌ترین ویژگی‌هایی که برای انتخاب یک PAM باید مورد توجه قرار دهید می‌توان به موارد زیر اشاره نمود:

- کامل بودن (ارائه تمام ماژول‌های مورد نیاز با قابلیت‌های کامل توسط یک برند)
- گستردگی (امکان یکپارچه سازی با تمامی سرورها، سرویس‌ها و تجهیزات موجود در شبکه)
- پشتیبانی (امکان ارائه پشتیبانی مستقیم و رفع نیازهای اپلیکیشن‌های محلی)
- عدم تحریم
- قیمت مناسب
- سهولت استفاده و توسعه

Aarcon

قابلیت‌های کلیدی

- Dual Factor
- Single Sign On
- AD Bridging
- Session Recording
- PEDM
- Virtual
- S.M.A.R.T.Audit
- Access Control
- One Admin
- Password Vault