آشنایی با خدمات شرکت سامانه هوشمند فیدارنت:

شرکت سامانه هوشمند فیدارنت با رویکرد ارائه خدمات تخصصی در حوزه امنیت فناوری اطلاعات و ارتباطات در راستای برآورد نیازمندی های مهم و اساسی سازمان ها و ارگان ها در این حوزه، تأسیس گردید. شرکت سامانه هوشمند فیدارنت در زمینه های مختلف امنیت چون تست نفوذ و امن سازی شبکه، برنامه های کاربردی (Privilege access Management) PAM و سرویس های زیرساختی فعالیت دارد که با تیم پویا و متخصص در حال حاضر به صورت تخصصی با تست نفوذ و توسعه خدمات سرویس PAM که در حوزه ی سرویس های امنیتی سازمانها و شرکتهای معتبر هست را آغازنموده است و آمادگی پشتیبانی از خدمات رو دارد .

PRIVILEGE ACCESS MANAGEMENT

سرویس مدیریت دسترسی ممتاز سامانه هوشمند فیدارنت

PAM چیست؟

مدیریت دسترسی ممتاز یا ویژه (PAM – Privileged Access Management) یک بخش مهم از امنیت سایبری و مدیریت هویت است که روی کنترل، نظارت و حفاظت از حساب‌های کاربری با دسترسی ممتاز (privileged accounts) در سازمان‌ها تمرکز دارد. این حساب‌ها به کاربران، برنامه‌ها و سیستم‌های خودکار اجازه می‌دهند تا به داده‌های حساس و سیستم‌های حیاتی دسترسی پیدا کنند. به خاطر این سطح بالای دسترسی، حساب‌های ممتاز، اهداف اصلی برای حملات سایبری هستند.

PAMبا استفاده از همکاری بین افراد، فرآیندها و فناوری‌ها، هویت‌های دارای دسترسی ممتاز را مدیریت می‌کند. این سیستم امنیتی با محدود کردن تعداد کاربران دارای مجوزهای مدیریتی(administrative privileges) ، نظارت بر فعالیت‌های آن‌ها پس از ورود و افزودن لایه‌های حفاظتی بیشتر مانند احراز هویت چندعاملی(MFA) ، از سوءاستفاده و نفوذ جلوگیری می‌کند.

با اجرای least privilege principle یا اصل کمترین دسترسی، PAMدسترسی کاربران را به حداقل نیاز محدود می‌کند و از نشت داده‌ها و آسیب به سیستم‌ها جلوگیری می‌کند. همچنین، با نظارت مداوم بر فعالیت‌های کاربران ممتاز، جلوی سوءاستفاده از مجوزهای حساس گرفته می‌شود و ریسک‌های امنیتی کاهش پیدا می‌کند. به این ترتیب، PAMبه عنوان یک لایه حفاظتی مهم، امنیت کلی سازمان را افزایش می‌دهد.

حساب کابری ممتاز چیست؟

حساب‌های ممتاز دسترسی و مجوزهایی فراتر از حساب‌های عادی دارند و کاربران آن‌ها می‌توانند تغییرات مهمی در سیستم ایجاد کنند، که این امر ریسک‌های امنیتی بالاتری به همراه دارد. حساب‌های ویژه‌ای به نام «سوپر یوزر» یا «Root» در Unix/Linux و «Administrator» در ویندوز، دسترسی کامل به سیستم می‌دهند و به کاربران IT اجازه می‌دهند دستورات حیاتی را اجرا کرده و تغییرات سیستمی بزرگی ایجاد کنند. این

حساب‌ها امکان مدیریت فایل‌ها، نصب نرم‌افزار، حذف کاربران و داده‌ها، و تنظیم مجوزهای دسترسی را دارند. سوءاستفاده یا خطای کوچک در این حساب‌ها می‌تواند آسیب جدی به سیستم یا سازمان وارد کند .درmacOS ، به‌طور پیش‌فرض کاربران به سطح روت دسترسی دارند، اما برای امنیت بیشتر، توصیه می‌شود از حساب‌های غیرممتاز برای کارهای روزمره استفاده شود. در محیط‌های امن، کاربران بیشتر از حساب‌های غیرممتاز بهره می‌برند تا ریسک‌های مربوط به دسترسی‌های بیش از حد کاهش یابد.

مدیریت دسترسی ممتاز یا PAM چگونه کار می‌کند؟

راه‌حل مدیریت دسترسی ممتاز (PAM) به این شکل کار می‌کند که ابتدا حساب‌های حساس مانند مدیران سیستم و حساب‌های خدماتی را شناسایی می‌کند و سپس سیاست‌های امنیتی مناسب برای آن‌ها تعیین می‌شود. برای مثال، ممکن است سازمان تصمیم بگیرد که مدیران سیستم باید از احراز هویت چندعاملی (MFA) استفاده کنند یا رمز عبور حساب‌های خدماتی به‌طور خودکار تغییر کند .این سیستم به‌طور خودکار این سیاست‌ها را اجرا می‌کند و دسترسی کاربران را به مقدار و زمان لازم محدود می‌سازد. این رویکرد به این معناست که افراد فقط زمانی که نیاز دارند و به اندازه کافی به سیستم دسترسی پیدا می‌کنند. همچنین مدیریت دسترسی ممتاز فعالیت‌های حساب‌های ویژه را به‌صورت مداوم زیر نظر دارد و در صورت مشاهده رفتارهای غیرعادی هشدار می‌دهد. با ثبت دقیق تمام فعالیت‌ها، این سیستم به سازمان‌ها کمک می‌کند تا هم از نظر امنیتی و هم از نظر رعایت مقررات در امان باشند و گزارش‌های کامل و مفیدی از دسترسی‌ها تهیه کنند.

انواع حساب‌های کاربری ممتاز چیست؟

حساب‌های کاربری ممتاز، دروازه‌هایی به دنیای امکانات و دسترسی‌های گسترده‌تر در سیستم‌ها هستند. این حساب‌ها که به کاربران اجازه می‌دهند فراتر از محدودیت‌های حساب‌های معمولی عمل کنند، انواع مختلفی دارند که هر کدام با ویژگی‌ها و سطح دسترسی منحصر به فرد خود شناخته می‌شوند:

۱ .حساب‌های مدیر دامنه

حساب‌های مدیر دامنه (Domain Administrator) بالاترین سطح دسترسی را در یک شبکه دارند و به کاربران اجازه می‌دهند به تمام ایستگاه‌های کاری و سرورهای دامنه دسترسی کامل داشته باشند. این حساب‌ها مدیریت پیکربندی‌های سیستمی، کنترل حساب‌های مدیریتی (Administrator Accounts)و مدیریت عضویت در گروه‌های کاربری (Group Memberships) را بر عهده دارند. به دلیل دسترسی گسترده‌ای که ارائه می‌دهند، این حساب‌ها نقش کلیدی در امنیت و مدیریت شبکه دارند.

۲ .حساب‌های مدیر محلی

حساب‌های مدیر محلی (Local Administrator Accounts) دسترسی کاملی به یک دستگاه (مانند رایانه شخصی یا سرور) می‌دهند و برای مدیریت و نگهداری آن دستگاه استفاده می‌شوند. با این حساب‌ها می‌توان تنظیمات سیستم را تغییر داد، نرم‌افزار نصب کرد و مشکلات فنی را برطرف نمود. برخلاف حساب‌های مدیر دامنه که بر کل شبکه نظارت دارند، حساب‌های مدیر محلی تنها به دستگاه خاصی محدود می‌شوند. این حساب‌ها معمولاً برای انجام وظایف فنی و پشتیبانی ایجاد می‌شوند.

۳ .حساب‌های مدیر برنامه(Application Administrator Accounts)

حساب‌های مدیر برنامه دسترسی کاملی به یک نرم‌افزار خاص و داده‌های آن را در اختیار کاربران قرار می‌دهند. با استفاده از این حساب‌ها می‌توان تمام تنظیمات، پیکربندی‌ها و داده‌های برنامه را مدیریت کرد. این نوع حساب‌ها معمولاً برای مدیرانی که مسئولیت نگهداری از برنامه‌های حیاتی سازمان را بر عهده دارند، طراحی شده است و به آن‌ها امکان می‌دهد تا به صورت کامل روی برنامه نظارت و کنترل داشته باشند.

٤ .حساب‌های سرویس(Service Accounts)

حساب‌های سرویس (Service Accounts)برای اجرای خودکار وظایف مشخصی در سیستم‌عامل طراحی شده‌اند. این حساب‌ها بدون نیاز به دخالت مستقیم کاربر، کارهایی مانند اجرای سرویس‌ها، فرآیندهای پس‌زمینه و تعاملات بین برنامه‌ها را انجام می‌دهند. به دلیل دسترسی‌های خاصی که به منابع سیستم دارند، نقش مهمی در عملکرد صحیح و امن برنامه‌های مختلف ایفا می‌کنند. این حساب‌ها برای ایجاد ارتباط امن بین برنامه‌ها و سیستم‌عامل به کار می‌روند.

٥ .حساب‌های کاربری ممتاز تجاری(Privileged Business User Accounts)

حساب‌های کاربری ممتاز تجاری به کاربران اجازه می‌دهند تا به داده‌ها و منابع حساس سازمان دسترسی داشته باشند و عملیات مدیریتی مرتبط با حوزه مسئولیت خود را انجام دهند. سطح دسترسی این حساب‌ها بر اساس وظایف کاری هر کاربر تعیین می‌شود و می‌تواند شامل بخش‌های حساس سیستم یا داده‌های حیاتی سازمان باشد. به دلیل دسترسی گسترده این حساب‌ها، مدیریت و نظارت بر آن‌ها برای حفظ امنیت اطلاعات سازمان بسیار مهم است.

٦ .حساب‌های اضطراری(Emergency Accounts)

حساب‌های اضطراری برای مواقع بحرانی یا اختلال در سیستم‌ها طراحی شده‌اند. این حساب‌ها به کاربران غیر ویژه اجازه می‌دهند تا در شرایط خاص و محدود، به صورت موقت دسترسی مدیریتی به سیستم پیدا کنند. هدف از ایجاد این حساب‌ها، اطمینان از ادامه فعالیت‌های حیاتی سازمان در زمان بحران و امکان بازیابی سیستم است. استفاده از این حساب‌ها معمولاً با محدودیت‌هایی همراه است و تنها در شرایط اضطراری مجاز است.

ویژگی‌های کلیدی مدیریت دسترسی ممتاز چیست؟

مدیریت دسترسی ممتاز (PAM) ابزاری مهم برای سازمان‌ها است تا بتوانند دسترسی به منابع حساس و سیستم‌های حیاتی را کنترل کنند. با استفاده ازPAM ، سازمان‌ها می‌توانند خطر دسترسی‌های غیرمجاز و سوءاستفاده از حساب‌های کاربری با امتیازات بالا را کاهش دهند. ویژگی‌های کلیدی PAMعبارتند از:

۱ .مدیریت سشن‌های کاربران با دسترسی بالا

با استفاده از این ویژگی، امکان نظارت و ضبط دقیق بر فعالیت کاربران با دسترسی‌های حساس فراهم می‌شود. اطلاعات حاصل از این سشن‌ها به منظور انجام بررسی‌های آتی و بازرسی‌های موردنیاز، به صورت ایمن ذخیره می‌شود. این امر نه تنها به افزایش امنیت سیستم کمک می‌کند بلکه امکان بازبینی و تحلیل دقیق‌تر رویدادها را نیز فراهم می‌آورد.

۲ .صندوق امن برای رمزهای عبور

صندوق رمزهای عبور ممتاز، یک راهکار امن برای مدیریت و حفاظت از رمزهای عبور حساس است. با محدود کردن دسترسی به کاربران مجاز و اعمال نقش‌های مشخص، این ابزار امنیت اطلاعات را افزایش می‌دهد. همچنین، با اتوماسیون فرایند تغییر و به‌روزرسانی رمزهای عبور، از قوی بودن

و عدم افشای آن‌ها اطمینان حاصل می‌شود. این صندوق، ابزاری ضروری برای سازمان‌ها و افرادی است که به دنبال محافظت از اطلاعات حساس خود در برابر تهدیدات سایبری هستند.

۳ .تحلیل تهدیدات برای کاربران با دسترسی بالا

با این ابزار، می‌توان فعالیت‌های مشکوک یا غیرعادی کاربران را در سطحی عمیق‌تر بررسی کرد. این ابزار با دسترسی به اطلاعات کلیدی، به شناسایی زودهنگام تهدیدات سایبری کمک کرده و از نفوذ احتمالی جلوگیری می‌کند. به عبارت دیگر، این ابزار یک لایه امنیتی اضافی را برای حفاظت از سیستم‌ها فراهم می‌کند.

٤ .دسترسی با حداقل نیاز

با محدود کردن دسترسی کاربران به تنها موارد ضروری، سطح امنیت به میزان زیادی ارتقا داده می‌شود. این رویکرد، ضمن جلوگیری از سوءاستفاده‌های احتمالی، ریسک‌های ناشی از دسترسی‌های بیش از حد را کاهش داده و از اطلاعات حساس سازمان محافظت می‌کند. با این روش، کاربران تنها به آنچه برای انجام وظایف خود نیاز دارند دسترسی خواهند داشت و این امر، کنترل دقیق‌تری بر محیط سیستم و داده‌ها را فراهم می‌کند.

٥ .یکپارچه‌سازی هویت در سیستم‌های مختلف

این ویژگی با تمرکز بر مدیریت یکپارچه هویت کاربران در سیستم‌عامل‌های مختلف (UNIX ، Linux، (Macو همگام‌سازی آن‌ها با Active Directory، فرآیندهای احراز هویت و کنترل دسترسی را بهبود بخشیده است. با ایجاد یک چارچوب امنیتی واحد، سازمان‌ها قادر خواهند بود تا

دسترسی کاربران به منابع مختلف را به‌صورت کارآمدتری مدیریت کرده و امنیت کلی زیرساخت خود را افزایش دهند. در این راستا، کاربران تنها با استفاده از یک هویت واحد می‌توانند به تمام منابع مورد نیاز خود دسترسی پیدا کنند و در نتیجه، مدیریت هویت و دسترسی‌ها به شکلی ساده‌تر و یکپارچه‌تر انجام می‌شود.

٦ .مدیریت متمرکز دسترسی‌ها

مدیریت متمرکز دسترسی‌ها در یک پلتفرم، به سازمان‌ها امکان می‌دهد تا با کنترل دقیق‌تر بر دسترسی کاربران، امنیت و کارایی سیستم خود را افزایش دهند. این رویکرد یکپارچه، ضمن جلوگیری از دسترسی‌های غیرمجاز، فرآیندهای مدیریتی را ساده کرده و بهینه‌سازی عملکرد کلی را به دنبال دارد.

بهترین روش‌ها برای مدیریت دسترسی ویژه چیست؟

در زمان برنامه‌ریزی و اجرای راه‌حل مدیریت دسترسی ممتاز(PAM) ، رعایت برخی از بهترین روش‌ها می‌تواند به بهبود امنیت و کاهش ریسک‌های سازمان کمک کند. این روش‌ها به شما کمک می‌کنند تا پیاده‌سازی بهتری داشته باشید و از منابع حیاتی خود به‌طور مؤثرتری محافظت کنید:

١ .درخواست احراز هویت چند عاملی

احراز هویت چند عاملی با افزودن یک لایه امنیتی اضافی، حفاظت از حساب‌های کاربری را تقویت می‌کند. این روش با درخواست تأیید مجدد هویت کاربر از طریق یک دستگاه دیگر، مانع از دسترسی افراد غیرمجاز به اطلاعات شخصی و حساس می‌شود. به این ترتیب، امنیت حساب‌ها به طور زیادی افزایش پیدا می‌کند.

۲ .خودکارسازی، کلید امنیتی پایدار

خودکارسازی اقدامات امنیتی، راهکاری مؤثر برای کاهش خطاهای انسانی و افزایش کارایی است. با شناسایی خودکار تهدیدات، سیستم به سرعت دسترسی‌ها را محدود کرده و از وقوع اقدامات مخرب جلوگیری می‌کند. این رویکرد، تضمین‌کننده امنیتی مستمر و بدون نیاز به دخالت دستی است.

۳ .حذف حساب‌های کاربری غیرفعال مدیران محلی

حذف حساب‌های کاربری مدیران غیرفعال از سیستم‌های ویندوز، یک اقدام ضروری امنیتی است .این حساب‌ها به دلیل دسترسی گسترده به سیستم و شبکه، در صورت سوءاستفاده، می‌توانند خطرات جدی برای امنیت اطلاعات ایجاد کنند. با حذف این حساب‌ها، از دسترسی‌های غیرمجاز جلوگیری کرده و سطح امنیت شبکه را ارتقا می‌دهیم.

٤ .تشخیص و پیشگیری از فعالیت‌های غیرمجاز

نظارت دقیق بر فعالیت‌های کاربران با دسترسی‌های ویژه، از طریق تعیین معیارهای رفتاری نرمال، به تشخیص سریع هرگونه تغییر غیرعادی کمک می‌کند. این تغییرات ممکن است نشانه‌ای از تهدیدات امنیتی باشند. با شناسایی و مقابله با این تهدیدات، امنیت سیستم افزایش یافته و ریسک‌های احتمالی کاهش می‌یابد.

۵ .دسترسی به‌موقع

دسترسی به‌موقع (Just-in-Time Access) روشی برای افزایش امنیت و کنترل دسترسی‌هاست. با این روش، دسترسی‌ها فقط در زمان نیاز و به میزان موردنیاز اعطا می‌شوند. این کار با اعمال اصل حداقل دسترسی و دسته‌بندی کاربران بر اساس سطح اعتماد و مجوزها، به کاهش ریسک‌های امنیتی و بهبود مدیریت سیستم کمک می‌کند. به عبارت دیگر، JITبه شما امکان می‌دهد تا دسترسی‌ها را دقیق‌تر کنترل کرده و فقط در مواقع ضروری افزایش دهید.

٦ .اجتناب از دسترسی نامحدود ممتاز

برای ارتقای امنیت سیستم، به جای اعطای دسترسی‌های نامحدود، استفاده از رویکرد دسترسی به‌موقع (Just-in-Time Access) و دسترسی به‌اندازه کافی (Just-enough Access) توصیه می‌شود. این روش به کاربران تنها در زمان نیاز و برای انجام وظایف مشخص، دسترسی‌های لازم را می‌دهد. با این کار، از ایجاد دسترسی‌های اضافی جلوگیری شده و ریسک سوءاستفاده‌های احتمالی کاهش می‌یابد.

۷ .کنترل دسترسی بر اساس فعالیت

دسترسی فقط به منابعی داده شود که فرد واقعاً از آنها استفاده می‌کند، و این بر اساس فعالیت‌ها و استفاده‌های قبلی او تنظیم می‌شود. این کار باعث می‌شود که دسترسی‌های غیرضروری داده نشود و تنها دسترسی‌های لازم به کاربران اختصاص پیدا کند .

مزایای استفاده از PAM چیست؟

مزایای استفاده از مدیریت دسترسی ممتاز (PAM) عبارتند از:

۱ .کاهش سطح حمله

مدیریت دسترسی ممتاز (PAM) با محدود کردن امتیازات کاربران و نقاط دسترسی، سطح حملات سایبری را به طور قابل توجهی کاهش می‌دهد. این رویکرد پیشگیرانه، با ایجاد یک چارچوب امنیتی مقاوم، در برابر تهدیدات داخلی و خارجی از دارایی‌های سازمان محافظت می‌کند و ریسک‌ها را به حداقل می‌رساند PAM .با کاهش مسیرهای ورود مهاجمان، سطوح دفاعی سازمان را تقویت کرده و یک لایه امنیتی قوی ایجاد می‌کند.

۲ .بهبود عملکرد عملیاتی

مدیریت دسترسی ممتاز (PAM) با محدود کردن دسترسی کاربران به حداقل سطح مورد نیاز، عملکرد عملیاتی را بهبود می‌بخشد. این امر از بروز خطاهای انسانی و اختلال در سیستم جلوگیری کرده و باعث افزایش کارایی و بهره‌وری تیم‌ها می‌شود. باPAM ، محیط IT بهینه‌تر شده و تیم‌ها می‌توانند بدون وقفه روی فعالیت‌های اصلی کسب‌وکار تمرکز کنند.

۳ .کاهش نفوذ و گسترش بدافزار

مدیریت دسترسی ممتاز (PAM) به‌عنوان یک محافظ قوی در برابر بدافزارها عمل می‌کند. با پیاده‌سازی اصل حداقل دسترسی، PAMاجازه نمی‌دهد که کاربران به امتیازات غیرضروری دسترسی پیدا کنند و این کار مانع از اجرای نرم‌افزارهای مخرب می‌شود. این روش نه تنها از ورود بدافزارها به سیستم‌ها جلوگیری می‌کند، بلکه مانع از گسترش آن‌ها در شبکه نیز می‌شود.

٤ .آسان‌تر کردن رعایت قوانین و حسابرسی

PAMبا محدود کردن دقیق دسترسی‌ها، رعایت قوانین را تسهیل کرده و مسئولیت‌پذیری را افزایش می‌دهد. این رویکرد، ضمن ایجاد محیطی امن‌تر و ساده‌تر، سازمان را با استانداردهای صنعتی همسو کرده و به الزامات قانونی پاسخ می‌دهد PAM .با ارائه دید شفاف از حقوق دسترسی، فرهنگ رعایت قوانین را تقویت کرده و حسابرسی را ساده‌تر می‌کند.

چالش‌های استفاده از PAM چیست

PAMبا وجود مزایا، با چالش‌هایی نیز همراه است. درک این چالش‌ها، به سازمان‌ها کمک می‌کند تا در پیاده‌سازی و استفاده از PAM موفق‌تر باشند:

١ .تأثیر منفی محدودیت‌های شدید دسترسی بر بهره‌وری کارکنان

وقتی دسترسی‌های مدیریتی، بیش از حد محدود یا پیچیده باشد، می‌تواند باعث کاهش بهره‌وری کارکنان شود. مثلاً اگر کارکنان نتوانند به اطلاعات یا ابزارهای لازم برای کارشان دسترسی پیدا کنند، کارشان مختل می‌شود. از طرف دیگر، اگر کارکنان دسترسی بیشتری از نیازشان داشته باشند، مثلاً

با حساب‌های ادمین وارد سیستم شوند، این موضوع می‌تواند امنیت سازمان را به خطر بیندازد و آن را در معرض حملات هکری یا بدافزارها قرار دهد.

۲ .دسترسی‌های مدیریتی باقی‌مانده پس از خروج کارکنان

حساب‌های مدیریتی، کاربران و دارایی‌های فراموش‌شده می‌توانند راهی مخفی برای نفوذ هکرها باشند. برای جلوگیری از این مشکل، باید همه حساب‌های مدیریتی، کاربران و دارایی‌ها به دقت شناسایی و نظارت شوند. اگر این کار به خوبی انجام نشود، حساب‌های قدیمی و فراموش‌شده بدون شناسایی باقی می‌مانند و هکرها می‌توانند از این راه‌های ناشناخته برای دسترسی به سیستم‌های سازمان استفاده کنند. مثلاً وقتی یک کارمند از شرکت می‌رود، باید دسترسی‌های مدیریتی او غیرفعال شود. اما گاهی این دسترسی‌ها باقی می‌مانند و امکان سرقت یا خرابکاری در اطلاعات حساس را فراهم می‌کنند.

۳ .اشتراک‌گذاری دسترسی‌های مدیریتی در تیم‌های IT

وقتی کارکنان اطلاعات دسترسی مدیریتی را با هم به اشتراک می‌گذارند، ممکن است مشکلاتی در حسابرسی و رعایت قوانین پیش بیاید.
به‌خصوص در تیم‌های IT ، افراد معمولاً برای راحتی کار از یک حساب مدیریتی مثل ادمین ویندوز استفاده می‌کنند. این موضوع شاید کار آن‌ها را ساده‌تر کند، اما وقتی بخواهند مشخص کنند چه کسی مسئول یک کار خاص بوده، مشکل ایجاد می‌شود. این مسئله می‌تواند امنیت، حسابرسی و رعایت مقررات را برای سازمان دشوار کند.

٤ .مدیریت غیرمتمرکز حساب‌های مدیریتی

مدیریت غیرمتمرکز دسترسی‌ها می‌تواند باعث ایجاد مشکلات امنیتی شود. در سازمان‌ها، ممکن است هر بخش، به روش خودش اطلاعات دسترسی را مدیریت کنند و این کار حفظ امنیت را سخت می‌کند. در محیط‌های IT ، صدها یا حتی هزاران حساب مدیریتی وجود دارد و کنترل همه این حساب‌ها برای افراد دشوار است. به همین دلیل، کارکنان ممکن است برای راحتی از یک نام کاربری و رمز عبور در چند حساب استفاده کنند. این کار خطرناک است، چون اگر یکی از این حساب‌ها هک شود، بقیه حساب‌هایی که از همان اطلاعات استفاده می‌کنند هم در معرض خطر قرار می‌گیرند.

از خصوصیات و رقابت بارز سرویس PAM شرکت سامانه هوشمند فیدلرنت درمقایسه به بهترین ابزارهای PAM دنیا طبق جدول زیر اعلام میگردد.

در دنیای امروز، دسترسی امن به منابع سازمانی از هر نقطه و هر دستگاهی ضروری است. راهکارهای دسترسی از راه دور (Remote Access Solutions - RAS) به سازمان‌ها این امکان را می‌دهند که به کاربران خود دسترسی امن و کنترلی به دسکتاپ‌ها، برنامه‌ها و داده‌ها را از طریق اینترنت ارائه دهند. در این مقاله، چهار راهکار PAM محبوب یعنی FID-PAM ، Wallix، Teleport , ARCON را با هم مقایسه می‌کنیم. این مقایسه بر اساس قابلیت‌ها، ویژگی‌ها، مزایا و معایب هر راهکار انجام می‌شود.

در ادامه، توضیحات بیشتری در مورد هر یک از قابلیت‌های ذکر شده در جدول ارائه می‌کنیم:

نحوه ارائه دسترسی:

Invisible Mode: در این حالت، کاربران به طور مستقیم به دسکتاپ‌ها یا برنامه‌های راه دور متصل می‌شوند و هیچ واسطه‌ای بین آنها وجود ندارد. این روش امن‌ترین روش است، اما می‌تواند برای مدیریت پیچیده‌تر باشد.

Portal Mode: در این حالت، کاربران از طریق یک پورتال وب به دسکتاپ‌ها یا برنامه‌های راه دور متصل می‌شوند. این روش مدیریت آسان‌تری را ارائه می‌دهد، اما به اندازه Invisible Mode امن نیست.

Gateway Mode: در این حالت، کاربران از طریق یک سرور واسط به دسکتاپ‌ها یا برنامه‌های راه دور متصل می‌شوند. این روش تعادل خوبی بین امنیت و قابلیت مدیریت ارائه می‌دهد.

Bastion Mode: در این حالت، کاربران ابتدا به یک سرور Bastion امن متصل می‌شوند و سپس از طریق آن به دسکتاپ‌ها یا برنامه‌های راه دور متصل می‌شوند. این روش امن‌ترین روش است، اما پیچیده‌ترین روش برای مدیریت نیز می‌باشد.

پروتکل‌های تحت پوشش:

راهکارهای PAM از پروتکل‌های مختلفی برای انتقال داده بین کاربران و منابع راه دور پشتیبانی می‌کنند. رایج‌ترین پروتکل‌ها عبارتند از:

RDP (Remote Desktop Protocol): این پروتکل برای دسترسی به دسکتاپ‌های ویندوز استفاده می‌شود.

RDP Gateway: این پروتکل RDP را از طریق یک سرور واسط امن ارائه می‌دهد.

SSH (Secure Shell): این پروتکل برای دسترسی به سرورهای لینوکس و یونیکس استفاده می‌شود.

Telnet: این پروتکل برای دسترسی به دستگاه‌های شبکه مبتنی بر متن استفاده می‌شود.

VNC (Virtual Network Computing): این پروتکل برای به اشتراک‌گذاری دسکتاپ‌ها در زمان واقعی استفاده می‌شود.

Http(s): این پروتکل برای دسترسی به برنامه‌های وب استفاده می‌شود.

پشتیبانی از دیتابیس:

برخی از راهکارهای PAM می‌توانند به طور مستقیم به دیتابیس‌ها متصل شوند و به کاربران امکان می‌دهند تا از راه دور به آنها دسترسی داشته باشند. این قابلیت برای سازمان‌هایی که از دیتابیس‌ها برای ذخیره داده‌های حساس استفاده می‌کنند، مفید است.

پشتیبانی از پروتکل‌ها با Jump Server:

Jump Serverها سرورهای واسطه‌ای هستند که به کاربران امکان می‌دهند به طور امن به چندین دستگاه یا برنامه راه دور متصل شوند. برخی از راهکارهای PAM از App Sharing در Jump Serverها پشتیبانی می‌کنند که به کاربران امکان می‌دهد برنامه‌ها را بدون نیاز به نصب آنها بر روی دستگاه خود اجرا کنند.

ممیزی و ضبط نشست‌ها:

راهکارهای PAM می‌توانند نشست‌های کاربران را ممیزی و ضبط کنند که به سازمان‌ها امکان می‌دهد فعالیت کاربران را ردیابی کنند و در صورت بروز مشکل، شواهدی داشته باشند.

نظارت چهارچشمی:

نظارت چهارچشمی به دو یا چند کاربر اجازه می‌دهد تا به طور همزمان به یک دسکتاپ یا برنامه راه دور متصل شوند. این قابلیت برای آموزش یا ارائه پشتیبانی از راه دور مفید است.

قابلیت‌های کنترلی:

راهکارهای PAM طیف گسترده‌ای از قابلیت‌های کنترلی را ارائه می‌دهند که به سازمان‌ها امکان می‌دهد دسترسی کاربران به منابع راه دور را محدود کنند. این قابلیت‌ها شامل Blacklisting/Whitelisting برنامه‌ها و دستورات، محدود کردن انتقال فایل، اعمال Time Policy، ایجاد Access Control Listها، محدود کردن IPهای کاربران و ... می‌شود.

مدیریت حساب‌های کاربری:

راهکارهای PAM با Active Directory، LDAP و سایر دایرکتوری‌های سازمانی ادغام می‌شوند تا مدیریت حساب‌های کاربری را آسان‌تر کنند. این قابلیت‌ها شامل احراز هویت کاربران، مدیریت رمز عبور، تنظیم مجدد رمز عبور از راه دور و ... می‌شود.

احراز هویت:

راهکارهای PAM از Single Sign On (SSO)، احراز هویت چند عاملی (MFA) و سایر روش‌های احراز هویت برای ایمن‌تر کردن دسترسی به منابع راه دور پشتیبانی می‌کنند.

مدیریت دارایی‌ها:

راهکارهای PAM می‌توانند برای مدیریت دارایی‌های سازمانی، مانند دستگاه‌ها، برنامه‌ها و کاربران، استفاده شوند. این قابلیت‌ها شامل Import اطلاعات از فایل‌های CSV، ادغام با Active Directory/LDAP، کشف خودکار دستگاه‌ها، کشف حساب‌ها و ... می‌شود.

گزارش‌گیری:

راهکارهای PAM طیف گسترده‌ای از گزارش‌ها را ارائه می‌دهند که به سازمان‌ها امکان می‌دهد انواع فعالیت کاربران به نمایش بزارند

قابلیت‌های دسترس‌پذیری:

قابلیت‌های دسترس‌پذیری برای اطمینان از در دسترس بودن مداوم راهکار PAM برای کاربران و برنامه‌های کاربردی ضروری است .این قابلیت‌ها شامل موارد زیر می‌شود:

امکان تهیه نسخه پشتیبان: راهکار PAM باید از تهیه نسخه پشتیبان منظم از داده‌ها و پیکربندی‌ها پشتیبانی کند تا در صورت بروز مشکل بتوان آنها را بازیابی کرد.

امکان تعریف:Backup Schedule کاربران باید بتوانند برنامه زمان‌بندی تهیه نسخه پشتیبان را به دلخواه خود تنظیم کنند.

پشتیبانی از:High Availability راهکار PAM باید از High Availability برای اطمینان از در دسترس بودن مداوم در صورت خرابی یک سرور پشتیبانی کند.

امکان آرشیو نشست‌ها: راهکار PAM باید از آرشیو نشست‌های کاربران برای بررسی‌های بعدی پشتیبانی کند.

مدیریت سلسله مراتبی:

مدیریت سلسله مراتبی به سازمان‌های بزرگ با چندین زیرمجموعه امکان می‌دهد تا راهکار PAM را به طور موثر مدیریت کنند .این قابلیت‌ها شامل موارد زیر می‌شود:

مدیریت سلسله مراتبی سامانه به صورت آبشاری: این قابلیت به مدیران در سطوح مختلف سازمانی امکان می‌دهد تا به سطوح پایین‌تر دسترسی داشته باشند و آنها را مدیریت کنند.

ماژول گزارش ساز: این ماژول به مدیران امکان می‌دهد تا گزارش‌های سفارشی از فعالیت کاربران و عملکرد راهکار PAM ایجاد کنند.

مدیریت متمرکز لاگ‌ها: این قابلیت به مدیران امکان می‌دهد تا لاگ‌های تمام سرورهای PAM را از یک مکان مرکزی مدیریت کنند.

مشاهده وضعیت فعال بودن سامانه ها: این قابلیت به مدیران امکان می‌دهد تا وضعیت فعال بودن تمام سرورهای PAM را در یک نگاه مشاهده کنند.

سامانه تیکتینگ و درخواست اتصال با تایید مدیر بالادستی:

این قابلیت به کاربران اجازه می‌دهد تا برای دسترسی به منابع راه دور درخواست ارسال کنند و مدیران بالادستی آنها باید این درخواست‌ها را تأیید کنند .این قابلیت می‌تواند به افزایش امنیت و کنترل دسترسی کمک کند.

نحوه لایسنس گذاری سیستم:

راهکارهای PAM با مدل‌های لایسنس‌دهی مختلفی ارائه می‌شوند، مانند دائمی، سالانه یا مبتنی بر اشتراک .سازمان‌ها باید مدلی را انتخاب کنند که به بهترین وجه با نیازها و بودجه آنها مطابقت داشته باشد.

ملاحظات دیگر:

علاوه بر قابلیت‌هایی که در جدول مقایسه ذکر شده است، عوامل دیگری نیز وجود دارد که سازمان‌ها باید هنگام انتخاب راهکار PAM در نظر بگیرند، مانند:

قیمت: قیمت راهکار PAM می‌تواند بسته به قابلیت‌ها، مدل لایسنس‌دهی و تعداد کاربران متفاوت باشد.

سهولت استفاده: راهکار PAM باید برای کاربران و مدیران آسان باشد.

پشتیبانی: ارائه دهنده راهکار PAM باید پشتیبانی خوب و خدمات مشتری ارائه دهد.

مقایسه فنی راهکارهای دسترسی از راه دور FID-PAM , Teleport , ARCON , Wallix

مقایسه فنی

1. نحوه ارائه دسترسی به کاربران ممتاز و پیمانکاران

FID-PAM : - پشتیبانی از Invisible Mode ، Portal Mode (HTML 5 Gateway)، Gateway Mode، Port Forward Mode.

Wallix :-پشتیبانی از Bastion Mode و Portal Mode با استفاده از Wallix Access Manager.

ARCON: -پشتیبانی از Gateway Mode.

Teleport:-تنها پشتیبانی از Portal Mode (HTML 5 Gateway).

2. پروتکل‌های تحت پوشش بدون سرور واسط (Jump Server)

FID-PAM : - پشتیبانی از RDP ، RDP Gateway، SSH، Telnet، VNC، Http(s)، MS-SQL، SCP/SFTP.

Wallix :-پشتیبانی از RDP ، RDP Gateway، SSH، Telnet، VNC، Http(s)، SCP/SFTP.

ARCON: -پشتیبانی از RDP ، RDP Gateway، SSH، Telnet، VNC، Http(s)، MS-
SQL، Oracle، PostgreSQL، MySQL، MongoDB، Kubernetes، SCP/SFTP.

Teleport: -پشتیبانی از RDP ، SSH، PostgreSQL، MySQL، MongoDB، Kubernetes، SCP/SFTP.

3. ممیزی کامل نشست‌های کاربران ممتاز

FID-PAM -پشتیبانی از ضبط فعالیت‌های کاربران به صورت ویدئویی، ثبت کیستروک، مانیتور کردن فرآیندها و اپلیکیشن‌ها، ثبت لاگ‌های فرمان، پخش فعالیت‌ها از طریق وب و تبدیل لاگ فعالیت‌ها به فرمت‌های عمومی مانند .M4V همچنین دارای قابلیت.OCR Real-Time

Wallix -پشتیبانی از موارد مشابه FID-PAM با قابلیت تبدیل به فرمت‌هایM4V ، AVI، MKVو.WebM. OCR On-Demand

ARCON -مشابهWallix ، با تبدیل به فرمت‌هایM4V ، AVIو WMV و وابستگی به سرویس OCR ثالث.

Teleport -پشتیبانی از ضبط فعالیت‌ها به صورت ویدئویی، بدون پشتیبانی از ثبت کیستروک، مانیتور کردن فرآیندها و اپلیکیشن‌ها و لاگ‌های فرمان.

.4 سیاست‌های کنترلی و اعمال محدودیت

FID-PAM -پشتیبانی از Black/Whitelisting اپلیکیشن‌ها و فرمان‌ها، کنترل انتقال فایل، سیاست‌های زمانی، لیست‌های کنترل دسترسی، محدودیت‌های IP کلاینت، سرور محلی TACACS و امکان ایجاد پروفایل‌های پیش‌فرض.

Wallix -مشابه FID-PAM ، اما بدون سرور محلی.TACACS

ARCON -مشابه.Wallix

Teleport -پشتیبانی محدود به Black/Whitelisting اپلیکیشن‌ها و فرمان‌ها، کنترل انتقال فایل و سیاست‌های زمانی.

.5 مدیریت حساب‌های کاربری و ماژول احراز هویت

FID-PAM - پشتیبانی از Active Directory/LDAP ، چند دامنه، تأمین کننده هویت محلی، مخزن گذرواژه، مدیریت و تنظیم گذرواژه، اتصال مبتنی بر کلید و گواهی دیجیتال، رمزنگاری داده‌ها، SSO، MFA و Credential Mapping.

Wallix -مشابه FID-PAM با نیاز به استفاده از Wallix Authenticator برای MFA.

ARCON -مشابه Wallix.

Teleport -پشتیبانی از Active Directory/LDAP ، SSO، MFA و محدودیت در Credential Mapping.

.6 مدیریت دارایی‌ها

FID-PAM -، Wallix، ARCON پشتیبانی از مدیریت دستی، واردات از فایل CSV ، Active Directory/LDAP و کشف خودکار.

Teleport: -پشتیبانی از مدیریت دستی و Active Directory/LDAP.

.7 گزارش گیری، هشداردهی و رخدادنماها

FID-PAM -، Wallix، ARCON: پشتیبانی از ارسال ایمیل هشدار، تهیه گزارش اپلیکیشن‌های اجرا شده، ارسال امن رویدادها به Syslog Server، گزارش‌گیری از عملکرد کاربران، پشتیبانی ازSNMP Trap ، گزارش‌سازی دستی و زمان‌بندی شده و یکپارچه‌سازی با سامانه‌های تیکتینگ.

Teleport: -پشتیبانی از ارسال ایمیل هشدار، تهیه گزارش اپلیکیشن‌های اجرا شده و ارسال امن رویدادها به.Syslog Server

8. قابلیت‌های دسترس‌پذیری، پشتیبان‌گیری و بازیابی

FID-PAM -، Wallix، ARCON: پشتیبانی از تهیه نسخه پشتیبان دستی و خودکار، تعریف برنامه پشتیبان‌گیری، پشتیبانی از High Availabilityو آرشیو نشست‌های ذخیره شده.

Teleport: -مشابه موارد فوق بدون پشتیبانی از آرشیو نشست‌های ذخیره شده.

9. مدیریت آبشاری برای سازمان‌های دارای زیرمجموعه‌های توزیع شده

FID-PAM -پشتیبانی از مدیریت سلسله‌مراتبی سامانه، گزارش‌سازی، مدیریت متمرکز لاگ‌ها و مشاهده وضعیت سامانه‌ها.

Wallix -، ARCON، Teleport: عدم پشتیبانی.

.10 نحوه لایسنس گذاری سیستم

FID-PAM -دائمی یا سالانه، بدون محدودیت در تعریف کاربر و تجهیزات، محدودیت در نشست‌های همزمان.

Wallix -لایسنس دائمی، محدودیت در تعریف کاربر و تجهیزات، محدودیت در نشست‌های همزمان.

ARCON -لایسنس سالانه، بدون محدودیت در تعریف کاربر و تجهیزات، محدودیت در نشست‌های همزمان.

TeleportOpen Source/Enterprise -، بدون محدودیت در تعریف کاربر و تجهیزات، محدودیت در نشست‌های همزمان.

نتیجه گیری

هر یک از این راهکارها مزایا و معایب خاص خود را دارند. انتخاب مناسب‌ترین راهکار بسته به نیازهای خاص سازمان شما، سطح امنیتی مورد نیاز، تعداد کاربران، و نحوه مدیریت و کنترل دسترسی‌ها دارد. در جدول زیر خلاصه‌ای از قابلیت‌های کلیدی هر یک از این راهکارها آورده شده است تا به شما در تصمیم‌گیری کمک کند.

این جدول به شما کمک می‌کند تا راهکار مناسب برای نیازهای خود را بر اساس ویژگی‌ها و قابلیت‌های هر سیستم انتخاب کنید.

جدول مقایسه نسخه فیدارنت FID-PAM در مقابل نسخه های برتر دنیا

FID-PAM – Wallix - ARCON- Teleport – PAM360

موضوع	PAM360	Wallix	ARCON	Teleport	FID-PAM
نحوه ارائه دسترسی به کاربران ممتاز و پیمانکاران	✓	✓	✗	✗	✓
Portal Mode (HTML 5 Gateway)	✓	نیاز به استفاده از Wallix Access Manager	✗	✗	✓
Gateway Mode	✓	✗	✓	✗	✓
Bastion Mode	✗	✓	✗	✗	✗
Port Forward Mode	✓	✗	✗	✗	✗
پروتکل‌های تحت پوشش بدون سرور	✓	✓	✓	✓	✓

واسط (Jump Server)					
RDP Gateway	✓	✓	✓	✗	✓
SSH	✓	✓	✓	✓	✓
Telnet	✓	✓	✓	✗	✓
VNC	✓	✓	✓	✗	✓
Http(s)	✓	بدون لاگ ویدئویی	با استفاده از ایجنت سمت کلاینت	✗	✓
MS-SQL	✓	✗	با استفاده از ایجنت سمت کلاینت	✗	✓
ORACLE	✓	✗	با استفاده از ایجنت سمت کلاینت	✗	✗
PostgreSQL	✓	✗	با استفاده از ایجنت سمت کلاینت	✓	✓

MySQL	✓	✕	با استفاده از ایجنت سمت کلاینت	✓	✓
MongoDB	✕	✕	با استفاده از ایجنت سمت کلاینت	✓	✓
Kubernetes	✕	✕mo	با استفاده از ایجنت سمت کلاینت	✓	✓
SCP / SFTP	✓	✓	✓	✓	✓
Monitoring	✕	✕	✕	✕	✓
پروتکل‌های تحت پوشش با سرور واسط (Jump Server)	بدون محدودیت	بدون محدودیت	بدون محدودیت	بدون محدودیت	بدون محدودیت

ممیزی کامل نشست‌های کاربران ممتاز	✓	✓	✓	✓	✓
Keystroke	✓	✓	✓	✗	✓
File Transfer	ارائه نسخه اصلی فایل	✓	✓	✗	✓
Process & App Monitor	✓	✓	✓	✗	✓
Command Log	✓	✓	✓	✗	✓
Replay Activity Player	Web-Based	Web-Based	Web-Based	Web-Based	Web-Based
Convert Activity Log to General Format	M4V	M4V-AVI-MKV-WebM	M4V-AVI-WMV	✗	M4V

Real-Time OCR	✓	On-Demand	وابسته به سرویس OCR ثالث	✕	✓
نظارت چهارچشمی	On-Line View	✓	✓	✓	✓
Force Stop Session	✓	✓	✓	✓	✓
Suspend Session	✕	✓	✓	✕	✓
قابلیت Full-Text Search	OCR	Full Screen Built-in OCR	Title Bar & Windows Built-in OCR (Action-Based/Optimized)	وابسته به سرویس OCR ثالث	OCR
Keystroke & Commands	✓	✓	✓	✕	✓
App & Process	✓	✓	✓	✕	✓
File Transfer	✓	✓	✓	✕	✓

سیاست‌های کنترلی و اعمال محدودیت	Blacklisting/Whitelisting of Applications	✓	✓	✓	✓
Blacklisting/Whitelisting of commands	✓	✓	✓	✗	✓
File Transferring	✓	✓	✓	✗	✓
Time Policy	✓	✓	✓	✗	✓
Access Control List	✓	✓	✓	✗	✓
Client IP Restriction	✓	✓	✓	✗	✓
SNMP Service Support	✓	✓	✓	✗	✓
Fail2Band	✓	✗	✗	✗	✓
Integrate With other APP	✗	✗	✗	✗	Anti-Virus ClamAv

Local TACACS Server	✓	✕	✕	✕	✓
TOTP Support	✓	✓	✕	✕	✓
پروفایل‌های پیش‌فرض برای اعمال محدودیت	✓	✓	✓	✓	✓
Load balancing	✓	✓	✕	✕	✓
مدیریت حساب‌های کاربری و ماژول احراز هویت	Active Directory/LDAP Integration	✓	✓	✓	✓
Multi-Domain Support	✓	✓	✓	✓	✓
Local Identity Provider	✓	✓	✓	✓	✓
Password Vault	✓	✓	✓	✕	✓

Password Management	✓	✓	✓	✗	✓
Remote Password Reset	✗	✓	✓	✗	✗
تعریف و مدیریت و اختصاص کلید رمز به کاربران جهت اتصالات SSH مبتنی بر کلید	✓	✓	✓	✓	✓
تعریف و مدیریت و اختصاص Certificate به کاربران جهت اتصالات مبتنی بر گواهی دیجیتال	✓	✓	✓	✓	✓

رمزنگاری داده‌های موجود در Password Vault مبتنی بر توکن سخت‌افزاری	✓	✗	✗	✗	✗
Single Sign On (SSO)	✓	✓	✓	✓	✓
MFA	✓	نیاز به استفاده از Wallix Authenticator	✓	✓	✓
Credential Mapping	✓	✓	✓	✗	✓
Account Discovery	✓	✓	✓	✗	✓
Self-Service Page	✗	✗	✓	✗	✗

مدیریت دارایی‌ها	✓	✓	✓	✓	✓
Import from CSV File	✓	✓	✓	✗	✓
Active Directory / LDAP	✓	✓	✓	✓	✓
Auto-Discovery	✓	✓	✓	✗	✓
Authentication Method	Local, Active Directory, LDAP, Destination Server	Local, Active Directory, LDAP, RADIUS, Destination Server	Local, Active Directory, LDAP, RADIUS, Destination Server	Local, LDAP, SAML	Local, Active Directory, LDAP, RADIUS, Destination Server
گزارش گیری، هشداردهی و رخدادنماها	✓	✓	✓	✓	✓

تهیه گزارش اپلیکیشن‌های اجرا شده توسط کاربر و ارسال آن به Syslog Server	✓	✓	✓	✗	✓
ارسال امن رویدادهای سیستم به Syslog Server	✓	✓	✓	✓	✓
گزارش‌گیری از عملکرد کاربران در قالب فایل CSV	✓	✓	✓	✗	✓
پشتیبانی از SNMP Trap	✓	✓	✓	✗	✓
گزارش‌سازی دستی و زمان‌بندی شده با	✓	✓	✓	✗	وابسته به ابزار BI

امکان سفارشی‌سازی قالب، فرمت‌های مختلف و ارسال ایمیل					
یکپارچه‌سازی با سامانه‌های تیکتینگ رایج	✓	✓	✓	✓	✓
پشتیبان‌گیری و بازیابی	✓	✓	✓	✓	✓
امکان تعریف برنامه زمان‌بندی برای تهیه نسخه پشتیبان	✓	✓	✓	✓	✓
پشتیبانی از High Availability	✓	✓	✓	✓	✓

آرشیو کردن نشست‌های ذخیره شده	✓	✓	✓	✗	✓
مدیریت آبشاری برای سازمان‌های دارای زیرمجموعه‌های توزیع شده	✓	✓	✗	✗	✓
سامانه تیکتینگ و درخواست اتصال با تایید مدیر بالادستی	✗	✓	✓	✓	✓
نحوه لایسنس‌گذاری سیستم	لایسنس دائمی یا سالانه، بدون محدودیت در تعریف کاربر و	✓	لایسنس محدود، محدودیت در تعریف کاربر و تجهیزات،	لایسنس سالانه، با محدودیت در تعریف کاربر و تجهیزات و	لایسنس سالانه، بدون محدودیت در تعریف کاربر و

	تجهیزات، محدودیت در تعداد نشست‌های همزمان		محدودیت در تعداد نشست‌های همزمان	محدودیت در تعداد نشست‌های همزمان	تجهیزات، بدون محدودیت در تعداد نشست‌های همزمان