- **حاکمیت سختگیرانه دسترسی**
- **کنترل مرکزی**
- **انطباق با مقررات**
- **اتوماسیون گردش کار هوشمند**
- **دید بیشتر**
- **مدیریت اعتبار آنلاین**
- **همبستگی عمیق رویداد**

دستاوردهای PAM360

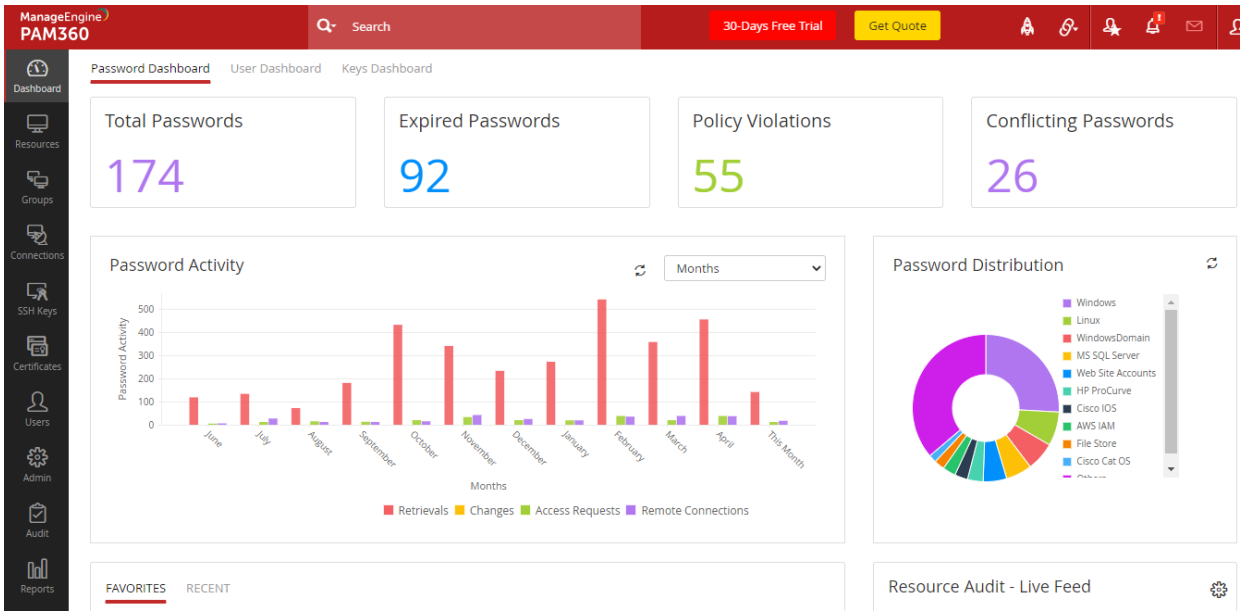
- مدیریت حساب ممتاز
- مدیریت کلید SSH
- مدیریت گواهی SSL / TLS
- DevOps و امنیت ابری
- ترفیع امتیاز به موقع
- تامین دسترسی از راه دور امن
- نظارت بر جلسه ممتاز
- تجزیه و تحلیل رفتار کاربر
- همبستگی ثبت وقایع آگاه از متن
- حسابرسی و گزارش گیری جامع

یک راه حل کامل دسترسی ممتاز برای شرکتها

PAM360یک راه حل تحت وب مدیریت دسترسی ادمینها (PAM) است که با تنظیم دسترسی به اطلاعات حساس ، از سازمان در برابر سو استفاده از مجوز ادمین دفاع می کند. از طریق حاکمیت قدرتمند دسترسی ممتاز ، روان سازی اتوماتیک گردش کار، تجزیه و تحلیل پیشرفته و یکپارچه سازی متناسب با خدمات مختلف فناوری اطلاعات ، PAM360شرکت ها را قادر می سازد راه های مختلفی از سیستم مدیریت فناوری اطلاعات خود را گرد هم آورده، استنتاج های معنی دار و روش های اصلاحی سریعتر را تسهیل کنند.

Manageengine PAM360محافظت قدرتمند ۳۶۰ درجه برای انعطاف پذیری سایبری در عصر دیجیتال

https://www.manageengine.com/pam360



چرا از PAM استفاده کنیم؟

مدیران سازمانی برای اطلاع از عملکرد ادمین های خود در سازمان نیاز به نظارت دقیق بر رفتار آنها با سیستم ها ، سرویس ها و سرور ها را دارند.
شرکت ManageEngine محصولی به نام PAM360 دارد که می تواند رابط بین تمامی سرور ها و سرویس ها با ادمین ها باشد، به طوری که ادمین ها ابتدا به محیط نرم افزار PAM لاگین می کنند و به واسطه نرم افزار PAM به سرور ها و سرویس های خودشان دسترسی پیدا می کنند و در حقیقت Privileged Access Management دسترسی را به آن ها خواهد داد.
ابتدا کل دارایی هایی که باید نظارت شوند به نرم افزار اضافه شده سپس دارایی ها در اختیار تمامی ادمین ها قرار می گیرد.
این نرم افزار می تواند اتصال بصورت RDP , VNC , SSH را پشتیبانی کرده و به طیف گسترده ای از سیستم عامل ها ، دیتا بیس ها و سرویس ها و ... متصل شود.
همچنین می توان به عنوان Password Management (مدیریت پسورد) هم از این نرم افزار استفاده کرد بدین صورت که رمز عبور ها در آن ذخیره و با متد بسیار جالبی در اختیار بقیه قرار می دهد. و امکان انتقال فایل بین جلسات (Session) مختلف را دارد.
به سادگی به اکتیو دایرکتوری متصل می شود , احراز هویت دو مرحله ای و ضبط تمامی جلسات نیز قابل دسترسی می باشد.

بازنشانی رمز عبور از راه دور برای انواع منابع سفارشی: برای منابعی که به انواع منبع فوق تعلق ندارند ، PAM360 تنظیم مجدد رمز عبور از راه دور را از طریق پلاگین های سفارشی تسهیل می کند که می تواند از طریق هر کد زبان یا اسکریپتی مانند Java، C، Rust، PowerShell، Bash ، و غیره این پلاگین ها را می توان از رابط PAM360 برای انجام بازنشانی رمز عبور اجرا کرد. همچنین می توانید مجموعه ای از دستورات SSH را برای تنظیم مجدد رمز ورود هر منبع مبتنی بر SSH هنگامی که از رابط PAM360 اجرا می شود، فرموله کنید.

ترکیب ماژول های مختلف امنیتی IT در یک کنسول واحد

برای تقویت بیشتر طرح PAM خود ، شرکت ها می توانند از طریق ادغام های متنی ، ویژگی های مهم سایر راه حل های امنیتی ManageEngine را در نمونه PAM360 بگنجانند. با این حال ، این قابلیت در حال حاضر به کاربران نیاز دارد تا مجوزهای جداگانه ای برای راه حل های مربوطه داشته باشند.

پیشنهادات کلیدی از طریق ادغام با سایر محصولات ManageEngine:

- تجزیه و تحلیل رفتار کاربر ممتاز (ManageEngine Analytics Plus)
- حسابرسی دسترسی ممتاز برای درخواستهای خدمات (ManageEngine ServiceDesk Plus)
- قابلیت های ارتقا امتیاز به موقع (ManageEngine ADManager Plus)
- همبستگی ثبت نقطه پایانی برای ممیزی های جلسه ممتاز (آنالیز کننده رویداد LogE ManageEngine)
- تجزیه و تحلیل رفتار کاربر و نهاد مبتنی بر ML (ManageEngine Log360 UEBA)
- قابلیت مدیریت رمز عبور سلف سرویس و قابلیت های ورود به سیستم (ManageEngine ADSelfService Plus)

ماژولها

خزانه اعتبارنامه Enterprise credential vault

شبکه ها را اسکن کرده و دارایی های مهم را کشف می کند تا به طور خودکار حساب های ممتاز را در یک خزانه امن قرار دهد که در نتیجه آن مدیریت متمرکز ، رمزگذاری AES-256 و مجوزهای دسترسی مبتنی بر نقش را ارائه می دهد.

دسترسی از راه دور امن

به کاربران ادمین اجازه می‌دهد مستقیما با یک کلیک ارتباط با میزبان های از راه دور را بدون نیاز به ایجنت یا برنامه جانبی و یا افزونه های مروگر ها آغاز کند.اتصالات تونل از طریق دروازه های رمزگذاری شده و بدون رمز عبور برای محافظت حداکثری قابل انجام است.

ارتقاء آنی سطح دسترسی کاربر

کنترل های به موقع بر روی حساب های دامنه خود انجام دهید و فقط درصورت نیاز کاربران، امتیازات بالاتر برای آنها اختصاص دهید. مجوزهای حساب را به صورت خودکار پس از یک دوره مشخص لغو کرده و گذرواژه ها را برای امنیت بیشتر بازنشانی کنید.

نظارت بر نشست های ادمین

با قابلیت سایه زدن بر جلسه ، بر فعالیت کاربر ادمین نظارت کرده و به کنترل دوگانه دسترسی ادمین دست یابید. جلسات را رکورد کنید آنها را بهیلهای ویدیویی به منظور حسابرسی های تحقیقاتی بایگانی کنید.

تحلیل رفتار کاربران ادمین

استفاده از هوش مصنوعی و یادگیری ماشین برای تشخیص فعالیت غیر معمول کاربران ادمین. ادمین های خود را از نظر فعالیت های بالقوه مضر که ممکن است بر کسب و کار تاثیر بگذارد ، از نزدیک کنترل کنید.

Context-aware event correlation

برای افزایش دید و آگاهی از موقعیت ، داده های دسترسی ادمین را با گزارش وقایع کاربر نقطه پایان تلفیق کنید. نقاط کور را در حوادث امنیتی از بین ببرید و با شواهد موافق تصمیمات هوشمندانه بگیرید.

حسابرسی و انطباق

به طور گسترده تمام وقایع مربوط به عملیات حساب ادمین را به عنوان محتوای متنی زمینه ضبط کرده و به سرورهای SNMP خود هدایت کنید. با گزارش های داخلی برای راهنمایی های اساسی، همیشه برای ممیزی های انطباق آماده باشید.

گزارش گیری جامع

بر اساس طیف وسیعی از گزارش های بصری و قابل زمانبندی در مورد دسترسی و داده های فعالیت کاربر ، تصمیمات شغلی آگاهانه اتخاذ کنید. می توانید گزارش های دلخواه خود را با ترکیب مجموعه جزییات خاص از مسیرهای حسابرسی به منظور دستیابی به وظایف امنیتی ایجاد کنید.

محافظت از DevOps

امنیت رمز عبور را در خط لوله DevOps خود ادغام کنید و سیستم عامل های ادغام و تحویل مداوم خود را در برابر حملات مبتنی بر اعتبار محافظت کنید بدون اینکه در کارایی مهندسی به خطر بیفتید.

یکپارچه سازی سیستم تیکت

گردش کار تایید دسترسی خود را برای حسابهای ادمین با استفاده از اعتبار سنجی شناسه تیکت تقویت کنید. فقط برای تایید وضعیت تیکت ، برای درخواستهای خدمات که نیاز به دسترسی ادمین دارند ، بازیابی اعتبارنامه مجاز است.

مدیریت کلید SSH

دستگاه های SSH را در شبکه خود پیدا کرده و کلیدها را برشمارید. با یک کلیک جفت کلید SSH جدید را در کاربر نهایی مرتبط ایجاد و استقرار دهید. سیاستهای دقیق را برای چرخش خودکار دوره ای کلید اعمال کنید.

امنیت اطلاعات کاربری

ارتباطات ما بین برنامه های خود را با استفاده از رابط های برنامه کاربردی ایمن که نیاز به رمزگذاری سخت افزار اعتبار را رفع میکند ، تمیز کنید. بک دور های سرورهای مهم خود را ببندید و مهاجمان را از خود دور نگه دارید.

مدیریت SSL certificate

با محافظت کامل از گواهینامه های SSL و هویت های دیجیتال خود از نام تجاری آنلاین خود محافظت کنید. قابلیت یکپارچگی با شرکتهای های معروف صدور گواهی مانند Digicert، GoDaddy و Let's Encrypt فراهم شده است.

درباره: ManageEngine بخش مدیریت فناوری اطلاعات شرکت Zoho است. شرکت های بزرگ و در حال ظهور - از جمله ۹ سازمان از هر ۱۰ سازمان - Fortune 100برای اطمینان از عملکرد بهینه زیرساخت های فناوری اطلاعات خود ، از جمله شبکه ها ، سرورها ، برنامه ها ، دسک تاپ و موارد دیگر ، به ابزار مدیریت IT در زمان واقعی Manageengine اعتماد می‌کنند.

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir
www.arka.ir
arka رایان سامانه آرکا