



Apadana PAM

سامانه مدیریت دسترسی کاربران ممتاز

پایش، کنترل و ثبت دقیق تمامی دسترسی‌های ممتاز به دارایی‌های حیاتی سازمان با امنیت، شفافیت و کنترل کامل، بدون نیاز به نصب ابزار جانبی روی سیستم کاربر.

SECURE · COMPLIANT · IN CONTROL

Apadana PAM چیست؟

Apadana PAM راه حل جامع مدیریت دسترسی کاربران ممتاز (Privileged Access Management) است که پایش، کنترل و ثبت دقیق تمامی دسترسی های ممتاز به دارایی های حیاتی سازمان را ممکن می سازد؛ اینکه «چه کسی، به چه منبعی، در چه زمانی و با چه سطح دسترسی ای» متصل شده است. Apadana PAM دسترسی امن به سرورها، تجهیزات شبکه، پایگاه های داده و برنامه های کاربردی سازمان را تنها از طریق مرورگر وب و بدون نیاز به ابزار جانبی روی سیستم کاربر فراهم می کند.

حلقه مفقوده امنیت سایبری سازمان ها

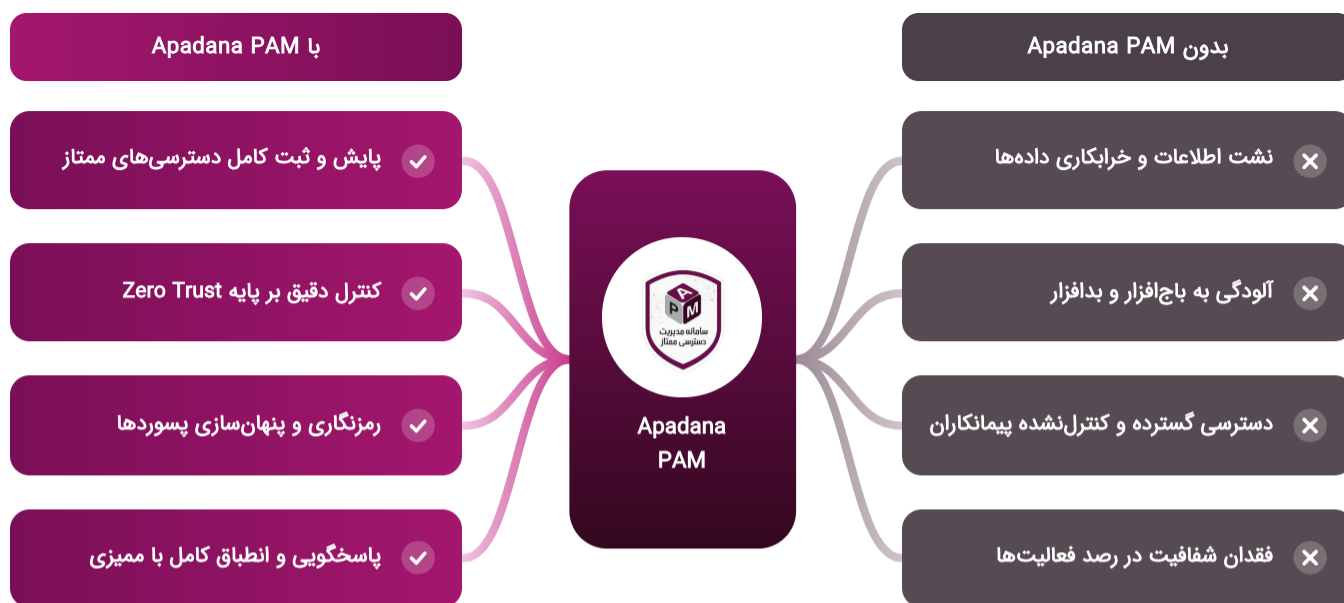
حساب های کاربری ممتاز به دلیل سطح دسترسی بالا، اهداف جذابی برای مجرمان سایبری اند و وجود پیمانکاران متعدد با دسترسی گسترده، این ریسک را دوچندان می کند.

۶۳%

نشت داده شامل سوءاستفاده از هویت ممتاز (Gurukul)

۸۰%

نشت داده با واسطه حساب های ممتاز (Verizon ۲۰۲۰)



Apadana PAM این حلقه مفقوده را تکمیل می کند: **پایش، کنترل و ثبت متمرکز** تمامی دسترسی های ممتاز، در یک بستر یکپارچه و قابل ممیزی. ✓

ویژگی‌ها و قابلیت‌های کلیدی

مجموعه‌ای از قابلیت‌های سامانه Apadana PAM که کنترل، پایش و امنیت دسترسی‌های ممتاز را در یک بستر یکپارچه فراهم می‌کند.

SFTP

SSH

RDP-Gateway

RDP

HTTP(S)

Telnet

VNC

SCP

پروتکل‌های پشتیبانی‌شده

دسترسی امن از یک بستر واحد

قابلیت Virtual Apps

اجرای امن برنامه‌های گرافیکی سازمان از طریق مرورگر وب، بدون نصب هیچ نرم‌افزاری روی سیستم کاربر.



۰۲

کنترل انتقال فایل و کلیپ‌برد

محدودسازی و ثبت کامل کانال‌های انتقال داده در هر نشست، برای جلوگیری از نشت اطلاعات.



۰۱

مدیریت پیشرفته کاربران

تعریف کاربر محلی یا Active Directory، Import از CSV، گروه‌بندی و تعریف نقش (Role).



۰۴

احراز هویت چندعاملی (MFA)

پشتیبانی از توکن سخت‌افزاری، پیامک، TOTP و HOTP برای ورود ایمن کاربران.



۰۳

ضبط و بازپخش نشست‌ها

ثبت خودکار تصویر هر نشست، قابل بازبینی و تبدیل به فایل استاندارد ویدیویی.



۰۶

مشاهده زنده نشست‌ها

نظارت هم‌زمان بر چند نشست فعال و قطع فوری نشست در صورت فعالیت غیرمجاز.



۰۵

فیلترینگ پیشرفته فرامین

کنترل دستورات مجاز با Regexp و Command، Control، منطبق با هر پروتکل.



۰۸

جست‌وجوی OCR در نشست‌ها

امکان جست‌وجوی پیشرفته در متن و فرامین ثبت‌شده نشست‌های SSH و RDP.



۰۷

نمای کلی قابلیت‌های تخصصی

لایه دوم قابلیت‌های Apadana PAM، امنیت اعتبارنامه‌ها، انطباق و یکپارچگی با اکوسیستم امنیتی سازمان را کامل می‌کند.



✓ **بدون نیاز به نصب نرم‌افزار جانبی** تمامی قابلیت‌های فوق بدون نصب ایجنت روی سیستم کاربران یا سرورها در دسترس است.



Apadana PAM چه ارزشی برای سازمان شما دارد؟

افزایش امنیت سایبری سازمان

با ایجاد لایه‌های میانی مجازی بین کاربر و منابع حیاتی، سطح حمله سازمان (Attack Surface) کاهش یافته و نفوذ عوامل بیرونی به‌طور چشمگیری محدود می‌شود.



کنترل دقیق دسترسی‌ها

دسترسی هر کاربر به‌دقت بر اساس اصل Zero Trust و حداقل دسترسی لازم تعریف می‌شود؛ از سرور و شبکه گرفته تا برنامه‌های کاربردی حساس.



کاهش ریسک نشت اطلاعات

کنترل کانال‌های انتقال فایل و کلیپ‌برد، به‌همراه ذخیره‌سازی رمزنگاری‌شده پسوردها، ریسک نشت داده و اعتبارنامه‌ها را به حداقل می‌رساند.



ثبت، پایش و پاسخگویی کامل

ضبط تصویری نشست‌ها، لاگ فرامین اجراشده و ارسال رخدادها به SIEM سازمان، امکان ممیزی کامل و انطباق با الزامات امنیتی را فراهم می‌کند.



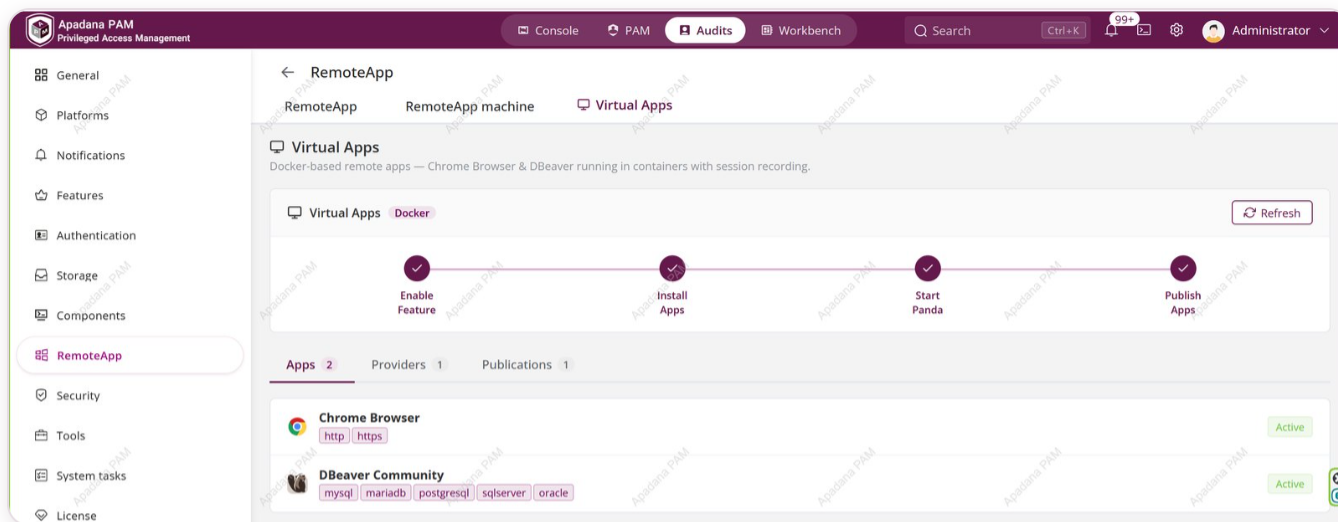
محدود کردن تعداد کاربران دارای دسترسی به عملکردهای مدیریتی، امنیت سیستم را به‌طور چشمگیری افزایش می‌دهد.

معماری یکپارچه، دروازه واحد دسترسی

Apadana PAM به عنوان یک دروازه متمرکز (Gateway) میان کاربران و دارایی‌های حیاتی سازمان شامل سرورها، تجهیزات شبکه، پایگاه‌های داده و برنامه‌های کاربردی قرار می‌گیرد. تمامی ترافیک دسترسی از طریق این بستر عبور کرده، پایش، ثبت و کنترل می‌شود؛ بدون آنکه منابع داخلی به طور مستقیم در معرض شبکه کاربر قرار گیرند.



نحوه عملکرد Virtual Apps



● محیط مدیریت Virtual Apps در Apadana PAM انتشار مرورگر Chrome و کلاینت DBEaver به صورت کانتینری، همراه با ضبط نشست.



نمایش زنده و ضبط شده

انتقال تصویر با VNC، ضبط کامل و قابل ممیزی.



اجرا در کانتینر ایزوله

راه اندازی مستقل و جدا از سایر نشست‌های فعال.



درخواست از مرورگر

فراخوانی برنامه گرافیکی از پورتال وب، بدون نصب نرم افزار.

Apadana PAM در عمل

نمونه‌ای از سناریوهای رایج استفاده از سامانه در سازمان‌های دولتی و خصوصی:

پایش نشست‌های دسترسی از راه دور

آگاهی کامل از تمام اتفاقات یک نشست راه‌دور با فیلم ضبط‌شده، لاگ فرامین و امکان مداخله لحظه‌ای در صورت فعالیت مشکوک.



دسترسی امن و محدود پیمانکاران

ارائه پورتال اختصاصی به پیمانکاران با دسترسی محدود به سرورها و تجهیزات تعیین‌شده مناسب پروژه‌های بزرگ با همکاری تیم‌های برون‌سازمانی.



کاهش ریسک نشت اطلاعات

کنترل کامل کانال‌های انتقال فایل و کلیپ‌برد به همراه گزارش دقیق از محتوای منتقل‌شده در طول هر نشست.



حفاظت از پسوردهای حساس سازمان

ذخیره رمزنگاری‌شده پسورد سرورها و تجهیزات، بدون افشا به کاربر و با ورود خودکار توسط سامانه در زمان اتصال.



دسترسی امن به برنامه‌های گرافیکی حساس

استفاده از مرورگر Chrome و کلاینت پایگاه‌داده DBeaver از طریق Virtual Apps، بدون نصب نرم‌افزار جانبی روی سیستم کاربر.



در تمامی سناریوهای فوق، هیچ نرم‌افزاری روی سیستم کاربر یا سرور نصب نمی‌شود و دسترسی صرفاً از طریق پورتال وب Apadana PAM انجام می‌گیرد.





درباره امن افزار گستر آپادانا

امن افزار گستر آپادانا، ارائه دهنده برتر خدمات امنیت اطلاعات، با تمرکز بر طراحی و پیاده سازی راهکارهای بومی مدیریت دسترسی و امنیت زیرساخت، در کنار سازمان های دولتی و خصوصی است. Apadana PAM حاصل تجربه این تیم در حوزه مدیریت دسترسی ممتاز و پاسخی به نیاز واقعی سازمان های ایرانی برای کنترل، پایش و حفاظت از دارایی های حیاتی است.

تماس با ما

وبسایت
amnafzar.net

ایمیل فروش
Sales@amnafzar.net

یزد
۰۳۵-۳۸۳۰۴۲۷۰ | ۳۸۳۰۴۲۷۱

تهران
۰۲۱-۹۱۰۹۴۲۷۰ | ۸۸۰۵۳۰۸۱

دفتر یزد
خیابان مطهری، مرکز فناوری اقبال، واحد ۲۳

دفتر تهران
یوسف آباد، نبش خیابان ۴۲، پلاک ۴، واحد ۷

اسکن کنید

برای دسترسی سریع به اطلاعات تکمیلی محصول Apadana PAM و ارتباط مستقیم با تیم فروش، این کد را با دوربین گوشی خود اسکن کنید.



جهت دریافت اطلاعات تکمیلی، دمو محصول یا برگزاری جلسه فنی،
خوشحال می شویم با تیم ما تماس بگیرید.