

# Privilegierte Zugriffe perfekt geschützt

Privileged-Access-Management-Lösungen (PAM) überwachen sämtliche Nutzeraktivitäten und verwalten den Zugang von Personen mit privilegierten Rechten auf die IT-Infrastruktur. Damit erhöht sich die Sicherheit im Netzwerk massiv.

**P**rivilegierte Anwender – sowohl eigene Mitarbeitende als auch externe Partner – haben Zugriff auf unternehmenskritische Ressourcen. In manchen Unternehmen werden die Konten solcher Nutzer nicht zentral verwaltet, Fernzugriffe nur ungenügend überwacht und womöglich sogar Benutzerkonten von mehreren Personen parallel genutzt. Dies wiegt umso schwerer, als es oftmals Monate oder sogar Jahre dauert, bis ein Missbrauch privilegierter Zugriffsrechte entdeckt wird.

## PAM schützt vor Angriffen aus dem privilegierten Bereich

Mit Privileged-Access-Management-Lösungen (PAM) können Unternehmen diesen Problemen begegnen. PAM überwacht sämtliche Zugriffe, zeichnet die User Sessions auf und unterstützt Sicherheit und Compliance durch stringentes Management privilegierter Benutzerkonten und deren Passwörter. Die derzeit wohl fortschrittlichste PAM-Lösung auf dem Markt heisst Fudo PAM und stammt vom ganz auf PAM spezialisierten Hersteller Fudo Security. Mithilfe von Machine Learning ist Fudo PAM in der Lage, das Verhalten der Nutzer zu analysieren und Verdächtiges in Echtzeit zu erkennen. Zusammen mit proaktivem Monitoring anhand von Musterabgleich, flexiblen Policies und automatisierten Aktionen ergibt sich ein bisher unerreichtes Niveau an Sicherheit.

## Drei Hauptfunktionen

Fudo PAM bietet ausgereiftes Session Monitoring: Die User Sessions werden in Echtzeit aufgezeichnet, bis hin zu einzelnen Tastaturanschlägen und Mausclicks – nützlich zur internen Dokumentation, für Schulungen und bei Gerichtsfällen. Per Live-Streaming beziehungsweise Session Collaboration können die Sitzungen gleichzeitig von Adminis-

tratoren mitverfolgt und begleitet werden. Damit entfallen unsichere Desktop-Sharing-Tools. Die proaktive Überwachungsfunktion erkennt Aktivitätsmuster und kann unerwünschte Sitzungen automatisch anhalten oder beenden, den Nutzer blockieren und den Systemadministrator warnen.

Bei der Aufzeichnung setzt Fudo PAM auf die Rohdaten, wobei alle gängigen Protokolle von SSH über RDP bis HTTPS unterstützt werden. Dies benötigt im Vergleich zu der bei anderen PAM-Lösungen üblichen Videoaufzeichnung markant weniger Speicherplatz und erlaubt es, den Session-Verlauf exakt nachzuvollziehen und vollständig zu durchsuchen.

Der **Secret Manager** von Fudo PAM generiert Passwörter mit anpassbarer Komplexität, speichert sie sicher und hält dabei Compliance-Vorgaben wie Passwortlänge und Passwortrotation ein. Ein zusätzlicher Application-to-Application-Passwortmanager deckt die direkten Verbindungen zwischen Anwendungen ab.

Die KI-basierte **Anomalie-Erkennung** erlaubt, dass Fudo PAM selbst kleinste Veränderungen im Nutzerverhalten während laufender SSH- und RDP-Verbindungen erkennt. Sobald verdächtige Ereignisse auftreten, benachrichtigt Fudo PAM den Systemadministrator. Beispiele sind etwa eine unerwartete Zunahme von Verbindungen oder Sessions, die länger als üblich dauern.

Eine weitere nützliche Funktion: Der Efficiency Analyzer misst die Produktivität der externen Dienstleister. Damit lässt sich das Aktivitätsniveau während der Dauer einer Session ermitteln.

## Schnell implementiert, flexibel betrieben

Die PAM-Lösung von Fudo Security wird in Form einer All-in-one-Appliance (Hard-

ware oder virtuell) implementiert und lässt sich innerhalb eines Arbeitstages installieren und aufsetzen. Fudo PAM arbeitet agentenlos: Weder auf den zu überwachenden Systemen noch auf Seiten des Anwenders muss eine zusätzliche Software installiert werden. Die Appliances werden zwischen den Nutzern und dem Unternehmensnetzwerk eingebunden und lassen sich individuell in vier Betriebsvarianten implementieren. So passt sich Fudo PAM dem Unternehmen an – und nicht umgekehrt.



## Fudo PAM: Die Highlights

- ▶ Agentenlose, appliancebasierte All-in-one-PAM-Lösung der nächsten Generation
- ▶ Umfassender Schutz für alle privilegierten Zugriffe
- ▶ Effiziente, sichere und compliancekonforme Passwortverwaltung
- ▶ Erhöhte Sicherheit durch Substitution von Benutzerkonten
- ▶ Proaktives Session Monitoring und Session Collaboration
- ▶ Platzsparende Session-Aufzeichnung anhand von Rohdaten
- ▶ Rasch implementiert, schnell amortisiert

## Kontakt:

**BOLL Engineering AG**

Jurastrasse 58, 5430 Wettingen

Tel. 056 437 60 60, info@boll.ch, www.boll.ch