Privileged Access Management
WALLIX SaaS REMOTE ACCESS (SaRA)

Sicherer Zugriff ohne VPN, ohne gemeinsame Passwörter und ohne Sicherheitskompromisse!

Die meisten Unternehmen verlassen sich bei der Durchführung von Remote-Aufgaben, die einen privilegierten Zugriff auf ihr IT- oder OT-Netzwerk erfordern, auf externe Dienstleister. Die Hälfte von ihnen hat keine Übersicht über die Zugriffe Dritter auf ihr Netzwerk und nur wenig bis gar keine Kontrolle über die einzelnen digitalen Fernzugriffe.

WALLIX SaaS Remote Access (SaRA) hilft dabei, die neuen Zugangsanforderungen zu erfüllen. Externen Dienstleistern, die auf von WALLIX Bastion verwaltete kritische Infrastrukturen zugreifen müssen, wird ein sicherer Zugang bereitgestellt.

Features

Ende-zu-Ende-Sicherheit

- Vollständige Trennung des Verzeichnisses für externe Anbieter (Just-in-Time-Bereitstellung ohne Hinzufügen von Identitäten zum Unternehmens-AD)
- Kontinuierliche Einhaltung der Sicherheitsrichtlinien des Unternehmens
- Übertragung der Administration an die Unternehmensleitung
- Self-Service Password Reset (SSPR)
- Kein VPN zu installieren oder verwalten, keine zusätzlichen Tickets für IT-Mitarbeiter

Volle Visibilität bei externen Fernzugriffen

- Vollständige Transparenz externer Fernzugriffe
- Erstellung von Zugriffsberechtigungen in Echtzeit
- Einheitliches Webportal mit integrierten RDP- and SSH-Webclients
- Kontrolle und Transparenz der Aktivitäten Dritter
- Einhaltung der Normen und Empfehlungen der französischen Nationalen Agentur für Sicherheit und Informationstechnologie (ANSSI) und der Unternehmensstandards, Sicherheitshygiene
- Keine gemeinsamen Passwörter

WALLIX
CYBERSECURITY SIMPLIFIED

Technische Daten

> **Federation Protocol**

• OpenID

> **Multi-Faktor-Authentifizierung (MFA)**

• Authentifizierungs-anwendung OTP (WALLIX Authenticator, Google Authenticator, ...)
• Sicherheitsschlüssel FIDO (Yubikey, ...)

> **Self-Service Benutzerportal**

• Registrierung von MFA-Authentifizierungsmethoden
• Self-Service Password Reset (SSPR)

WIE ES FUNKTIONIERT

Schritt 1: Der Geschäftsleiter, der den WALLIX Bastion-Admin beaufsichtigt, meldet seine Dritt-Anbieter an (Just-In-Time-Provisioning).

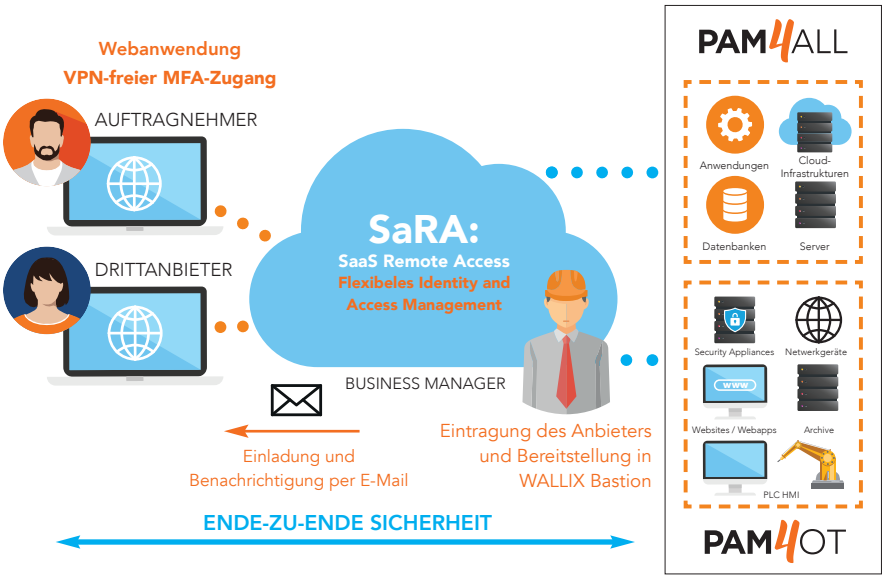
Schritt 2 : Der Auftragnehmer wird per E-Mail eingeladen und über seine Zugangsberechtigung zur internen Unternehmens-Infrastruktur (IT oder OT) informiert.

Schritt 3 : Der Auftragnehmer registriert das Gerät, das er für den zweiten Authentifizierungsfaktor (TOTP, Yubikey) verwenden wird, und gibt dann sein Passwort ein.

Schritt 4 : D er Auftragnehmer authentifiziert sich mit seinem Passwort und seinem zweiten Authentifizierungsfaktor.

Schritt 5: Der Auftragnehmer verbindet sich über ein einheitliches Webportal mit der Unternehmensressource (RDP- und SSH-Sitzungen) und führt die ihm zugewiesenen Aufgaben aus. Je nach Konfiguration kann der Zugriff von einem Genehmigungsantrag abhängig gemacht werden, und der Genehmigende kann die Dauer des Arbeitsauftrags festlegen.

Step 6: Von WALLIX Bastion aus ist es dann möglich, alle Sitzungen der externen Auftragnehmer aufzuzeichnen und zu überprüfen.



Über WALLIX

Als Softwareunternehmen im Bereich Cybersicherheit, ist die WALLIX Group der europäische Spezialist für den Schutz von Zugängen und Identitäten. Die Technologien von WALLIX ermöglichen es Unternehmen, auf die heutigen Herausforderungen des Datenschutzes zu reagieren und garantieren die Erkennung von und die Widerstandsfähigkeit gegen Cyberangriffe. Damit stellen die Lösungen zum einen die Geschäftskontinuität in den Unternehmen sicher, zum anderen gewährleisten sie die Einhaltung gesetzlicher Vorschriften hinsichtlich des Zugriffs auf IT-Infrastrukturen und kritische Daten. Sämtliche Lösungen werden über ein Netzwerk von mehr als 300 Wiederverkäufern und Integratoren weltweit vertrieben. WALLIX ist an der Euronext (ALLIX) gelistet und unterstützt mehr

www.wallix.de

Vorteile

BETRIEBS- EFFIZIENZ

- Optimierung der IT-Resourcen und Ersatz kostspieliger VPN-Lösungen
- Kontrolle über die TCO (Total Cost of Ownership)
- Autonomie der Business-Teams ohne Auswirkungen auf ihre Tätigkeit

SICHERE DIGITALE TRANSFORMATION

- Ferngesteuerter Start von Sitzungen für Drittanbieter
- Nahtlose Benutzererfahrung

TRÄGT ZUR ZERO-TRUST ARCHITEKTUR

- Zero-Trust-konformer Fernzugriff: Schützt Ressourcen, weist granulare Zugriffsrechte zu und erstellt einen Prüfpfad

WALLIX
CYBERSECURITY SIMPLIFIED