thalescpl.com

THALES

Sicherer Zugriff auf virtuelle Umgebungenund private Clouds

Der Wechsel zu virtualisierten Infrastrukturen und privaten Clouds

Unternehmen setzen auf virtualisierte Desktop-Infrastrukturen (VDI) und private Clouds, um mehr Sicherheit, geschäftliche Agilität und Kosteneffizienz zu erreichen.

Um jedoch die Integrität und Vertraulichkeit der Daten in ihrer virtualisierten Umgebung unabhängig davon zu schützen, ob sie aus dem Rechenzentrum gestreamt werden oder der Zugriff über ein privates Cloud-Gateway erfolgt, müssen Unternehmen immer noch sicherstellen, dass die Benutzer die sind, die sie vorgeben zu sein, wenn sie auf diese Lösungen und Infrastruktur zugreifen.

Hindernisse bei der Sicherung virtueller Umgebungen

Unternehmen, die den Zugriff auf ihre virtualisierten Umgebungen sichern wollen, sehen sich mit mehreren zentralen Herausforderungen konfrontiert:

- **Vielfalt der Endpunkte:** Thin Clients, Zero Clients, Server und mobile BYOD-Geräte, die sowohl privat als auch im Unternehmen genutzt werden, erfordern alle eine geräteunabhängige Authentifizierungsstrategie.
- **Sicherheitslücken bei Passwörtern:** Unternehmen, die ihre virtualisierten Umgebungen ausschließlich mit einem Passwort schützen, gefährden ihre Informationsressourcen und setzen sie Bedrohungsvektoren wie Phishing, Social Engineering, Brute-Force-Angriffen, generischer Malware, dem Erraten von Passwörtern und dem Diebstahl von Zugangsdaten aus.
- **Ortsunabhängiger Zugriff:** Während einige Unternehmen ihre virtualisierte Infrastruktur innerhalb der Firewall des Unternehmens bereitstellen, ermöglichen andere auch Beratern oder Partnern den Zugriff, die sich außerhalb der Firewall des Unternehmens (in der DMZ) befinden. Daher ist eine starke Authentifizierung ebenso entscheidend wie die Möglichkeit, einen sicheren Zugriff aus der Ferne zu ermöglichen.
- **Compliance:** Um Sicherheitsprüfungen zu bestehen und regionale, branchenspezifische und Corporate-Governance-Vorschriften einzuhalten, müssen Unternehmen nachweisen, dass sie wissen, wer wann worauf zugreift.
- **Budgetzwänge:** Um in Bezug sowohl auf Direkt- als auch Gemeinkosten im Rahmen ihrer aktuellen Budgets zu bleiben, verzichten Unternehmen möglicherweise auf stärkere Zugriffskontrollen für ihre wertvollsten Informationsbestände und Ressourcen.

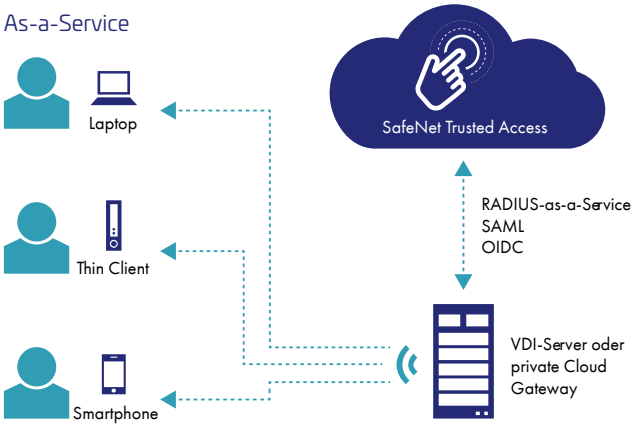
Wesentliche Vorteile

- Erhöhte Sicherheit
- Reibungslose Authentifizierung
- Reduzierter Verwaltungsaufwand
- Vereinfachte Compliance

Einfache und starke SafeNet-Zugriffsverwaltung und -Authentifizierung

SafeNet-Lösungen für Zugriffsverwaltung und Authentifizierung bieten einen sicheren Zugriff auf die virtualisierte Infrastruktur:

- **Von jedem Gerät aus**, einschließlich Thin Clients, Zero Clients und BYOD-Mobilgeräten
- **Auf jede VDI-Anwendung** dank der vorkonfigurierten Integrationen mit Citrix, VMware und AWS für eine schnelle und einfache Bereitstellung
- **Auf jeder Sicherheitsebene** über verschiedenste Authentifizierungsmethoden



Reibungslose Verwaltungsstrategie

SafeNet-Lösungen für Zugriffsverwaltung und Authentifizierung reduzieren den IT-Verwaltungsaufwand und vereinfachen die Einhaltung von Richtlinien:

- Zero-Touch-Verwaltung der Lebenszyklen von Benutzerkonten und Token einschließlich automatischer Bereitstellung, Aktualisierung und dem Entzug von Berechtigungen und Token
- Ein zentraler Verwaltungspunkt für die einmalige Definition von Zugriffsrichtlinien und deren Durchsetzung in Ihrem gesamten IT-Ökosystem
- Management by Exception durch schwellenwert- und ereignisbasierte Warnmeldungen in Echtzeit
- Ein einheitlicher Prüfpfad für alle Zugriffsaktivitäten auf lokale, virtuelle und Cloud-basierte Ressourcen

Unterstützte Authentifizierungsmethoden

SafeNet Trusted Access unterstützt eine umfassende Palette von Multi-Faktor-Authentifizierungsmethoden wie z. B:

- OTP-Push
- OTP-App
- OTP-Hardware
- Musterbasierte Authentifizierung
- Out-of-band über E-Mail und SMS-Textnachrichten
- Passwort
- Kerberos
- PKI-Anmeldedaten
- Google Authenticator
- Authentifizierung ohne Passwort
- Biometrisch
- Stimmenbasiert
- Drittanbieter

Vorteile einer Lösung mit SafeNet Trusted Access

- Effektives Risikomanagement
- Balance zwischen Komfort und Sicherheit
- Universelle Authentifizierung

Verwaltungsplattform

- SafeNet Trusted Access

Über die SafeNet-Lösungen für Zugriffsverwaltung und Authentifizierung

Mit den branchenführenden Lösungen für Zugriffsverwaltung und Authentifizierung von Thales können Unternehmen den Zugriff auf IT-, Web- und Cloud-basierte Anwendungen des Unternehmens zentral verwalten und sichern. Durch den Einsatz von richtlinienbasiertem SSO und universellen Authentifizierungsmethoden können Unternehmen effektiv Sicherheitsverletzungen verhindern, sicher in die Cloud migrieren und die Einhaltung gesetzlicher Vorschriften vereinfachen.

Um mehr über die Lösungen für die Zugriffsverwaltung von Thales zu erfahren, besuchen Sie https://cpl.thalesgroup.com/de/access-management oder nehmen Sie auf https://www.brighttalk.com/webcast/2037/334449 an einem Livedemo-Webinar teil.

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

ISO 27001:2013 CERTIFIED

GDPR Ready

> cpl.thalesgroup.com/de <

Kontaktieren Sie uns – alle Geschäftsstellen und Kontaktangaben finden Sie auf cpl.thalesgroup.com/de/contact-us