IAM-EXPERTENLEITFADEN ZUR ERSTELLUNG EINES BUSINESS-CASE

Teil eins von drei: Modernisierung veralteter Web-Access-Management(WAM)-Lösungen

WHITEPAPER

INHALTSÜBERSICHT

ANALYSTENMEINUNG

Obwohl Web-Access-Management-Technologien sich bereits etabliert haben und auch Identity-Federation seit Jahren von Unternehmen genutzt wird, haben das Interesse für diese Technologien und auch deren Nutzung in letzter Zeit enorm zugenommen. Kunden – insbesondere deren operativen Abteilungen – fordern Lösungen, die eine Antwort auf neue Anforderungen wie das Onboarding von Geschäftspartnern, den Zugriff von Kunden auf Services oder den Zugang zu Cloud-Dienstleistungen bieten. Die IT muss auf diese Situation reagieren und eine Standardinfrastruktur für all die verschiedenen Anforderungen an die Kommunikation und Zusammenarbeit im stark vernetzten Extended Enterprise erstellen. Die Bedeutung von Access-Management und Federation verschiebt sich folglich von einer eher taktischen IT-Herausforderung hin zu einer strategischen Komponente der IT-Infrastruktur, die eine höhere geschäftliche Agilität ermöglicht.

Quelle: 2016 KuppingerCole Access Management and Federation Leadership Compass (KuppingerCole Leadership Compass zu Access-Management und Federation 2016)

EINLEITUNG

Als Identity- und Access-Management(IAM)-Experte wissen Sie, dass sich die Anforderungen Ihres Unternehmens im Bereich der Zugriffssicherheit enorm verändert haben. Verglichen mit den heutigen Herausforderungen war die Zugriffskontrolle auf lokale Anwendungen eher einfach zu lösen.

Heute werden immer mehr Anwendungen in die Cloud verlagert und auch die Anzahl mobiler Apps nimmt zu. Überall gibt es APIs und die Anzahl an Geräten, Identitäten, Domains, Sites, Stacks und IT-Umgebungen explodiert förmlich. Auch die Endpunkte, die ein Unternehmen schützen muss, gehen heute in die Milliarden. Nicht nur Mitarbeiter, auch Auftragnehmer, Lieferanten, Distributoren und Kunden benötigen heute einen eigenen Zugang.

Hinzu kommt: Ältere Web-Access-Management(WAM)-Lösungen – auch wenn sie damals als De-facto-Standard galten – sind heute überfordert. Sie können sich natürlich stur stellen und die Quadratur des Kreises versuchen. Bedenken Sie aber, dass es nicht nur um Mehrkosten geht: Das Risiko, dass Ihr altes System die Benutzererfahrung und die Sicherheit negativ beeinträchtigt, ist enorm hoch.

Im Grunde wissen Sie, dass es Zeit für eine neue Lösung ist.

Bei der Sicherheit geht es nicht mehr nur darum, potenzielle Angreifer draußen zu halten. Genauso wenig geht es um ein einmaliges Event. Moderne Unternehmen brauchen ein Sicherheitskonzept, das sich an die Uhrzeit sowie den Standort, das Verhalten, das Netzwerk und das Gerät eines Benutzers dynamisch anpasst.

Fest steht: Der alte, durch Grenzen definierte Ansatz mit Firewalls und Passwörtern hat heute ausgedient. Die digitale Transformation erfordert einen neuen Ansatz: einen, der auf Identitäten basiert.

Eine moderne Lösung für einen sicheren Zugriff auf Basis von Identitäten bietet Ihnen die nötige Sicherheit und noch viel mehr.

Doch wie können Sie andere davon überzeugen?

Ganz einfach: Durch einen soliden Business-Case. Zeigen Sie Entscheidern, welche Vorteile IAM Ihrer Organisation bietet:

- Schnellere Time to Market für neue Anwendungen und Services
- Höhere Sicherheit für Anwendungen, egal ob lokal oder in der Cloud
- Geringere IT-Kosten und bessere Planbarkeit der Betriebsausgaben

Dies sind nur einige der vielen Vorteile einer modernen Zugangslösung. Und es ist kein Zufall, dass Sie damit die wichtigsten strategischen Zielsetzungen Ihres Unternehmens unterstützen können.

In diesem Whitepaper erfahren Sie, wie Sie mit IAM einen sicheren Zugriff bereitstellen, die digitale Transformation beschleunigen und Ihr Unternehmen voranbringen.

PAIN-POINTS VERALTETER WEB-ACCESS-MANAGEMENT-LÖSUNGEN

WAM-Lösungen eignen sich ganz gut für Web-Apps in einer einzigen Domäne. Diese Architektur wurde vor längerer Zeit konzipiert, um einfache Webressourcen in Firmenrechenzentren zu schützen, was ihr auch ganz gut gelingt.

WAM-Lösungen stellen eine enge Verbindung zwischen veralteten Agents und Regelservern her und sind dabei auf intensive Kommunikation angewiesen. Doch je mehr Ihr Unternehmen auf mobile Lösungen setzt, Apps in die Cloud migriert und mithilfe von APIs alles verbindet, desto weniger kann diese Architektur mithalten.

Wir nennen Ihnen fünf Gründe, warum Ihre WAM-Lösung den heutigen Anforderungen nicht mehr gewachsen ist:

1. SIE KANN KEINE ANWENDUNGEN IN EINER PRIVATE ODER PUBLIC CLOUD SCHÜTZEN.

- Eine Spiegelung der umfangreichen Datenbankinfrastruktur (*s. Abbildung 1*) für Sitzungsspeicherung, Richtlinien und Chiffrierschlüssel ist sehr kostspielig und aufwendig.
- Bleiben die Regelserver vor Ort, entstehen hohe Latenzzeiten zwischen VPN und Cloud.

2. SIE BIETET KEINEN SICHEREN ZUGRIFF AUF NATIVE MOBILE APPS UND REST-APIS.

- Native mobile Apps und REST-APIs tun sich schwer damit, proprietäre Cookie-Token zu übersetzen, die von veralteten WAM-Lösungen generiert werden.
- Sitzungen innerhalb nativer mobiler Anwendungen und REST-APIs sind zustandslos, während veraltete WAM-Lösungen Stateful-Sessions erfordern.

3. FÜR UPGRADES UND SKALIERUNGEN FALLEN EXTREM HOHE KOSTEN AN.

- Das Upgraden von Agents und die Überarbeitung von Regeln zur Einhaltung neuer Vorgaben binden extrem viele Ressourcen. Zusätzlich fallen alle drei Jahre Kosten für systemweite Upgrades an.
- Für die Zugriffskontrolle auf Anwendungsebene ist eine große Anzahl von Regelservern nötig.

4. ES SIND KONTINUIERLICHE INVESTITIONEN IN PROPRIETÄRE LÖSUNGEN ERFORDERLICH.

- Proprietäre Lösungen erfordern Erfahrung in den Bereichen Personalisierung, Entwicklung und Administration sowie häufig auch professionelle Services eines Drittanbieters.

5. SIE BEFINDET SICH IN DER END-OF-LIFE-PHASE ODER KURZ DAVOR.

- Bei einigen WAM-Produkten gibt es ein offizielles End-of-Life-Datum (z. B. bei RSA Access Manager), während bei anderen einfach keine neuen Funktionen mehr entwickelt werden (z. B. bei CA SiteMinder und Oracle Access Manager).
- Eine abnehmende Update-Häufigkeit, eine schlechter werdende Qualität der Software-Releases und statische Verwaltungsoberflächen können auf eine unangekündigte bzw. eine bevorstehende End-of-Life-Phase hindeuten.

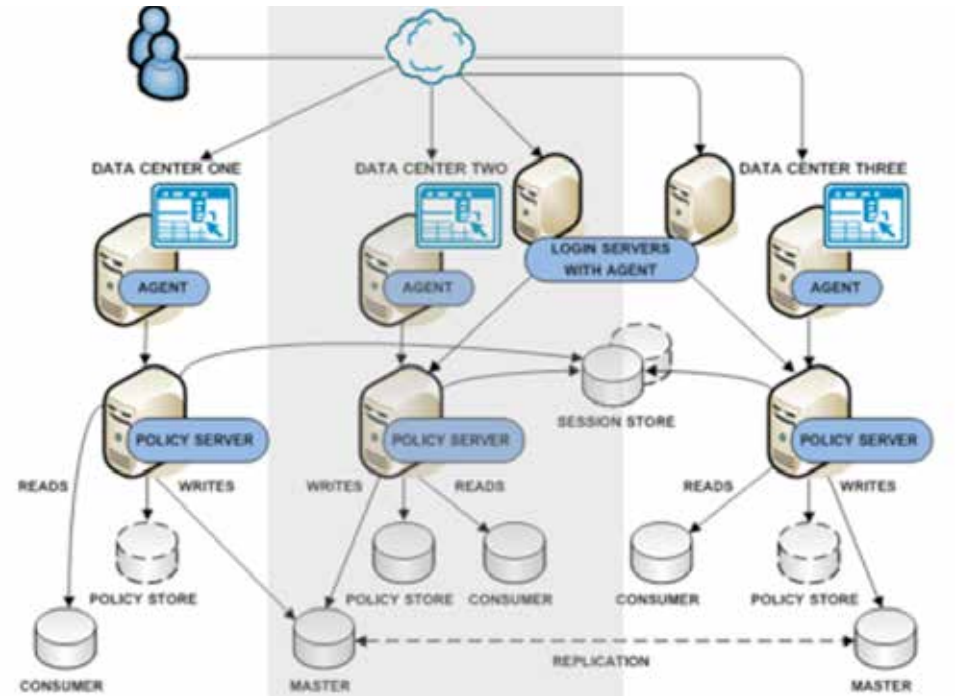

Abbildung 1: Gängige veraltete On-Premises-WAM-Implementierung (CA SiteMinder) mit umfangreicher Infrastruktur, die sich nur schwer in einer Private Cloud replizieren lässt.

ANFORDERUNGEN FÜR EINE MODERNE ZUGRIFFSSICHERHEIT

In einer zunehmend digitalen und mobilen Umgebung muss Ihr Unternehmen alle Benutzer und Geräte kontinuierlich an sämtlichen Zugangspunkten prüfen. Sie müssen einen sicheren Zugriff für alle Nutzer auf alle Anwendungen gewährleisten – unabhängig davon, um welchen Typ von Anwendung es sich handelt oder wo sich diese befinden (Public Cloud, Private Cloud, lokal, Enterprise, Drittanbieter, mobil). Zudem müssen Sie einen Zugriff über mobile Technologien, APIs und die Cloud hinweg ermöglichen.

Doch es reicht nicht nur, dieses hohe Maß an Sicherheit zu garantieren, Sie müssen gleichzeitig auch die nahtlose und positive Erfahrung gewährleisten, die Ihre Benutzer erwarten. Klingt nach Wunschdenken? Vielleicht. Doch genau für diese Anforderungen wurden moderne Zugriffssicherheitslösungen konzipiert.

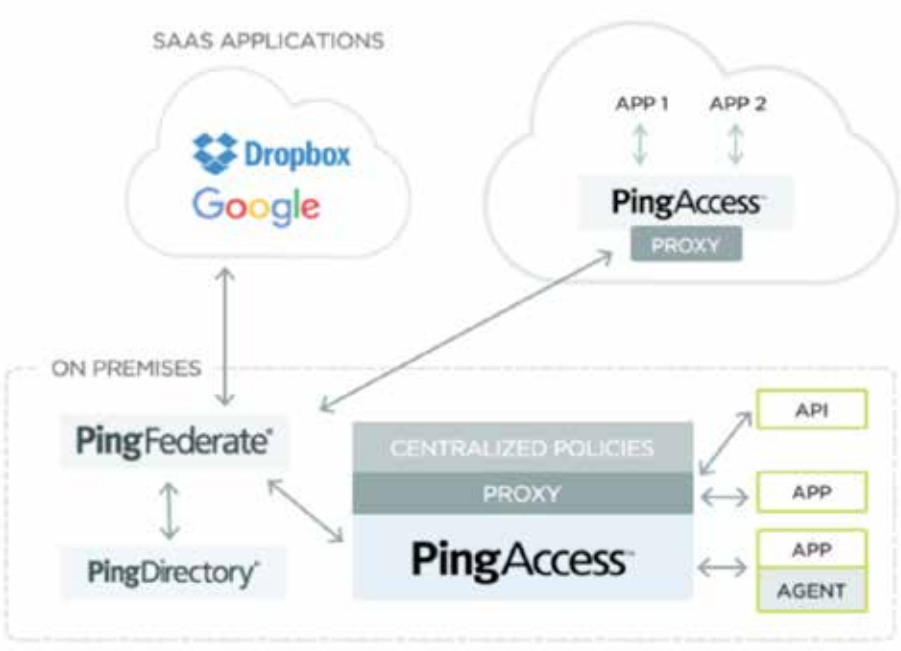

Abbildung 2: Schlanke und Cloud-fähige moderne Access-Security-Implementierung mit optionalem SSO und Verzeichniskomponenten.

Um die Anforderungen einer modernen Zugriffssicherheit zu erfüllen, muss eine erstklassige Identity- und Access-Management-Lösung diese acht Merkmale bzw. Funktionen bieten:

1. SCHLANK UND CLOUD-FÄHIG

- Domänenübergreifende Zugriffssicherheit mit einem Proxy (Access-Gateway), wie in *Abbildung 2* dargestellt, oder agentbasierter Ansatz ohne DNS- oder Netzwerkänderungen
- Out-of-the-Box-Unterstützung für Microsoft IIS-, Apache- und NGINX-Server sowie SDK für benutzerdefinierte Plug-ins

2. ZENTRALISIERTE ZUGRIFFSSICHERHEIT FÜR MOBILE TECHNOLOGIEN, WEB UND APIS

- Geringere Kosten für die Abstimmung zwischen Administratoren und Entwicklern, wobei die Erstellung und Bereitstellung von Regeln für Anwendungen und APIs über eine einzige Konsole erfolgt
- Flexible Skalierung, egal ob Ressourcen lokal oder in der Cloud vorliegen

3. FLEXIBLE AUTORISIERUNGSREGELN ZUR UNTERSTÜTZUNG NEUER GESCHÄFTSBEZIEHUNGEN

- Integrierte Federated-Single-Sign-On(SSO)-Funktionen, damit Partner und Kunden eine schnelle und nahtlose Verbindung mit beliebigen Anwendungen oder Services herstellen können
- Personalisierbare Zugriffsregeln basierend auf Benutzergruppen, Standort, Tageszeit oder Gerät

4. STANDARDBASIERT

- Native Unterstützung für SAML, OAuth 2.0, OpenID Connect (OIDC) und JSON Web Tokens (JWT), was eine standardmäßige Kommunikation für alle Apps und APIs sowie eine größere Interoperabilität sicherstellt
- Geringere Komplexität; Entwickler müssen nicht mehr stundenlang benutzerdefinierten Code schreiben oder Experten für proprietäre Authentifizierungs- und Autorisierungsprotokolle sein.

5. ANPASSUNG AN UNTERNEHMENSANFORDERUNGEN, EINSCHLIESSLICH INTEGRATION MIT NICHT STANDARDMÄSSIGEN ANWENDUNGEN

- Sprachbasierte Kits für .NET, Apache, PHP und Java
- Anwendungsbasierte Kits für Citrix, SAP, Oracle, RSA, IBM und Microsoft
- Unterstützung einer agentlosen Integration für die Weitergabe von Attributen über direkte HTTP-Aufrufe

6. SUBSKRIPTIONSBASIERT INKLUSIVE ENTERPRISE-SUPPORT

- Vorhersehbarer Betrieb und planbare Ausgaben; keine variablen Kosten für Upgrades, Wartung und Support
- Hochwertige neue Releases, bei denen Kundenanforderungen berücksichtigt werden

7. KOMPATIBILITÄT MIT BESTEHENDER ARCHITEKTUR

- Lösung sollte mit veralteten Systemen harmonieren, sodass Sie neue Features ohne Einfluss auf das Geschäft ausprobieren können.
- Kompatibilität mit gängigen älteren Systemen wie CA SiteMinder (SSO), Oracle A.M., RSA A.M., IBM Tivoli A.M. und Central Authentication Service (CAS)

8. MIGRATION OHNE AUSFALLZEITEN

- Vollständige Implementierung in einer Unternehmensumgebung innerhalb weniger Wochen
- Agentbasierte und proxybasierte Implementierungen oder eine Kombination davon unterstützen die Zugriffssicherheit sowohl für veraltete als auch neue Anwendungen.
- Durch Tokenvermittlung wird eine nahtlose Endbenutzererfahrung für schwer zu migrierende Anwendungen sichergestellt.

SO PROFITIERT IHRE GESAMTE ORGANISATION VON EINER MODERNISIERUNG

Wenn es darum geht, Entscheider von einer modernen Zugriffssicherheitslösung zu überzeugen, sollten Sie auch Vorteile aufzeigen, die weit über Ihren direkten Bereich hinausgehen. Schließlich kommt eine gut durchdachte Lösung Ihrer gesamten Organisation zugute.

Sicherheit und Compliance

- Reduziert das Risiko von Sicherheitslücken und einer Nichteinhaltung geltender Vorschriften dank zentralisierter, regelbasierter Zugriffskontrolle
- Mehr Sicherheit ohne Beeinträchtigung der Produktivität, kontextbezogene Zugriffssicherheit

IT-Verantwortliche

- Zentrale Zugriffskontrolle für praktisch sämtliche Ressourcen, egal wo
- Zukunftssichere Lösungen auf Basis offener Standards, sodass die Gefahr eines Vendor-Lock-in verringert wird
- Höhere IT-Kapazitäten mit einfach zu wiederholenden, sicheren Rollouts neuer Apps
- Vernetzung von Anwendungen mit Drittanbieter-APIs ermöglicht neue Partnerbeziehungen

IT-Budgetverantwortliche

- Geringere Anforderungen an die lokale Hardware
- Geringerer Bedarf an Professionell Services dank einem vorhersehbaren Subskriptionsmodell
- Geringere Anzahl von IT-Mitarbeitern für die Verwaltung mehrerer komplexer Altlösungen nötig

Anwendungsentwickler

- Geringere Abstimmungskosten dank optimierter und zentralisierter Autorisierungsprozesse
- Schnellere Time to Market für neue Anwendungen und Services

Personal

- Geringerer Bedarf an hoch qualifizierten und auf bestimmte Lösungen spezialisierten Mitarbeitern

HOHE EINSPARPOTENZIALE

Natürlich ist Ihr Business-Case nicht vollständig, wenn Sie nicht sagen können, wie sich eine IAM-Lösung unterm Strich finanziell auswirkt. Viele denken, dass die Implementierung neuer Lösungen mit einem hohen Preis verbunden ist. Doch wenn es um die Modernisierung der Zugriffssicherheit geht, stehen tatsächlich die hohen Einsparungen im Vordergrund.

Einsparungen bei der Infrastruktur

Die Migration auf eine moderne Zugriffssicherheitslösung eröffnet allein schon durch die Reduzierung der Server – sowie der entsprechenden Arbeitskräfte, Utilitys und Wartungs- bzw. Supportleistungen für Server-Hardware – in der Regel erhebliche Einsparpotenziale. Veraltete WAM-Lösungen erfordern typischerweise lokale Infrastruktur zur Speicherung von Sitzungen, Richtlinien und Chiffrierschlüsseln. Moderne Lösungen wie PingAccess bauen dagegen auf dem Headless- und Stateless-Konzept auf und ermöglichen so eine schlanke Implementierung auf Cloud-Plattformen zu deutlich geringeren Kosten.

Einsparungen bei Lizenzierung und Support

Durch die Aufschlüsselung der Lizenzierungskosten älterer Stack-Produkte können Sie sich einen genauen Überblick über Ihre Ausgaben verschaffen, doch das kann sehr aufwendig sein. Als Faustregel können Sie für die jährlichen Wartungs- und Supportausgaben 20 bis 25 Prozent der jährlichen Lizenzierungsgebühren ansetzen. Doch viele Kunden mit veralteten Lösungen stellen fest, dass sich die Nutzung ihrer älteren WAM-Systeme im Laufe der Zeit verändert. Bei abnehmender Nutzung sind die Wartungs- und Supportkosten proportional höher, als sie eigentlich sein sollten. Ein Subskriptionsmodell bietet einen umfassenden Überblick und ermöglicht eine genauere Planung Ihrer laufenden Kosten.

Personaleinsparungen

Je nach Größe und Komplexität der Umgebung benötigt man für veraltete WAM-Lösungen mehrere Vollzeit-Administratoren, um die Anwendungen zu schützen und eine Beeinträchtigung der Geschäftsprozesse durch die Zugriffssicherheit auszuschließen. Die Ressourcen für Betrieb und Wartung dieser Systeme, die oft Tausende Agents auf Hunderten von Servern umfassen, treiben die Kosten in die Höhe. Upgrade-Zyklen, die alle drei Jahre anstehen und mehrere Hundert Stunden professioneller Services erfordern, erhöhen die Kosten noch mal. Weil veraltete Lösungen nicht in der Lage sind, Richtlinien für API- und Webanwendungssicherheit gleichermaßen zu nutzen, wird der Verwaltungsaufwand sogar verdoppelt. Im Gegensatz dazu erfordern moderne Lösungen für den sicheren Zugriff auf Basis einer Gateway-Architektur wesentlich weniger Wartung. Außerdem können Sie Richtlinien für Webanwendungen und APIs in jeder beliebigen Domäne gleichermaßen benutzen.

FAZIT

Moderne Access-Management-Lösungen bieten die nötige Skalierbarkeit und Flexibilität, um Ihre strategischen Unternehmensziele zu erreichen. Angefangen beim sicheren Rollout neuer Cloud- und mobiler Anwendungen bis hin zum Aufbau neuer Geschäftsbeziehungen – von den Vorteilen einer modernen Zugriffsverwaltung profitiert Ihre gesamte Organisation.

Hier noch mal die wichtigsten Vorteile einer modernen identitätsbasierten Lösung, die Ihre Unternehmensinitiativen und Ihre Geschäftsziele unterstützt.

Schnellere Time to Market für neue Anwendungen und Services

- Geringere Kosten für die Abstimmung zwischen der zentralen IT und Anwendungsentwicklern
- Kürzere Time to Value dank gemeinsam nutzbarer Richtlinien für mobile, Web- und Cloud-Apps
- Kürzere Integrationszeiten mit Out-of-the-Box-Unterstützung für praktisch alle Plattformen
- Verbesserung bestehender Beziehungen und Aufbau neuer Beziehungen dank einem sicheren Zugriff für Partner

Höhere Sicherheit für Anwendungen, egal ob lokal oder in der Cloud

- Zentralisierte Zugriffssicherheit für alle mobilen, Web- und Cloud-Apps, egal ob kommerziell oder selbstständig entwickelt
- Schutz von Ressourcen je nach Benutzer-, Anwendungs- oder Zugriffsszenario
- Geringeres Risiko von Sicherheitslücken, da Identitätsbetrug durch unabhängige Anwendungen vermieden wird
- Bessere IT-Compliance mit zentralisierter Regelverwaltung für den Zugriff auf alle Ressourcen

Geringere IT-Kosten und bessere Planbarkeit der Betriebsausgaben

- Weniger veraltete isolierte Implementierungen dank zentralisierter Zugriffssicherheit
- Bessere Skalierung der Lösung und geringerer Hardware-Einsatz
- Stabilisierung von Kosten und IT-Workloads mit vorhersehbaren Subskriptionsmodellen und Updates
- Nutzung offener Standards, um die Gefahr eines Vendor-Lock-ins zu vermeiden und den Bedarf an spezialisierten Fachkräften zu minimieren

#3237 | 06.17 | v004