THALES

www.thalesesecurity.com

‹Thales e-Security›

Vormetric Data Security Platform



VORMETRIC DATA SECURITY PLATFORM

Da es nach wie vor mit alarmierender Regelmäßigkeit zu verheerenden Sicherheitsverstößen kommt und die behördlichen Auflagen immer strenger werden, muss Ihr Unternehmen den Schutz von Daten über eine zunehmende Zahl von Umgebungen, Systemen, Anwendungen, Prozessen und Usern erweitern. Die Vormetric Data Security Platform von Thales e-Security macht die organisationsübergreifende Sicherheitsverwaltung für „Data at Rest" äußerst effizient. Sie basiert auf einer erweiterbaren Infrastruktur und besteht aus Produkten einer Plattform, die individuell implementiert werden können. Gleichzeitig bietet die Plattform eine effiziente, zentralisierte Schlüssel- und Richtlinienverwaltung. So können Ihre Sicherheitsteams Ihre Datensicherheitsrichtlinien, die Einhaltung behördlicher Auflagen und Best Practices umsetzen und gleichzeitig den Verwaltungsaufwand und die Gesamtbetriebskosten senken.

Die Plattform bietet Funktionen für den geschützten und kontrollierten Zugriff auf Datenbanken, Dateien und Container und kann Datenbestände in der Cloud, in virtuellen, Big-Data- und physischen Umgebungen sichern. Diese skalierbare, effiziente Datensicherheitsplattform ermöglicht es Ihnen, Ihre dringenden Anforderungen zu erfüllen, und sie versetzt Ihr Unternehmen in die Lage, schnell und flexibel zu reagieren, wenn das nächste Sicherheitsproblem auftaucht oder das nächste Compliance-Gebot eingehalten werden muss.

VERBESSERTE DATENSICHERHEIT UND COMPLIANCE

Wenn Ihre Sicherheitsteams diese flexiblen und skalierbaren Lösungen nutzen, können sie ein breites Spektrum von Anwendungsfällen klären und vertrauliche Daten unternehmensweit schützen. Die Plattform enthält umfassende Funktionen, anhand derer Sie zahlreiche behördliche Auflagen hinsichtlich Datensicherheit und -schutz erfüllen können. Dazu gehören u. a.: Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA) sowie regionale Datenschutzbestimmungen. Die Vormetric Data Security Platform bietet Unternehmen leistungsstarke Tools gegen APTs (Advanced Persistent Threats), zur Absicherung gegen Missbrauch durch Insider und zur Errichtung ständiger Kontrollen, und zwar auch dann, wenn Daten in der Cloud oder auf der Infrastruktur eines externen Anbieters gespeichert werden.

MAXIMALE EFFIZIENZ BEI PERSONAL UND RESSOURCEN

Die Vormetric Data Security Platform macht die Verwaltung einfach und effizient und bietet eine intuitive webbasierte Schnittstelle, eine Befehlszeilenschnittstelle (CLI) sowie Anwendungsprogrammierschnittstellen (APIs). Außerdem unterstützt sie REST, SOAP, Java, Net und C. Mit dieser Lösung können Sie Sicherheitsmaßnahmen für „Data at Rest" konsistent anwenden und so die Effizienz und Produktivität der Mitarbeiter maximieren. Die Plattform unterstützt zudem die Orchestrierung und Automatisierung durch den Vormetric Orchestrator.

FUNKTIONEN

- Transparente Dateiverschlüsselung
- Verschlüsselung auf Anwendungsebene
- Tokenisierung
- Statische Datenmaskierung
- Dynamische Datenmaskierung
- Cloud-Speicherverschlüsselung
- FIPS 140-2, Common-Criteria-zertifizierte Schlüsselverwaltung
- Schlüsselverwaltung als Dienst
- Zugriffskontrolle von privilegierten Nutzern
- Protokollierung der Zugriffsprüfung
- Datenstapelverschlüsselung und Tokenisierung
- Orchestrierungs- und Automatisierungsunterstützung

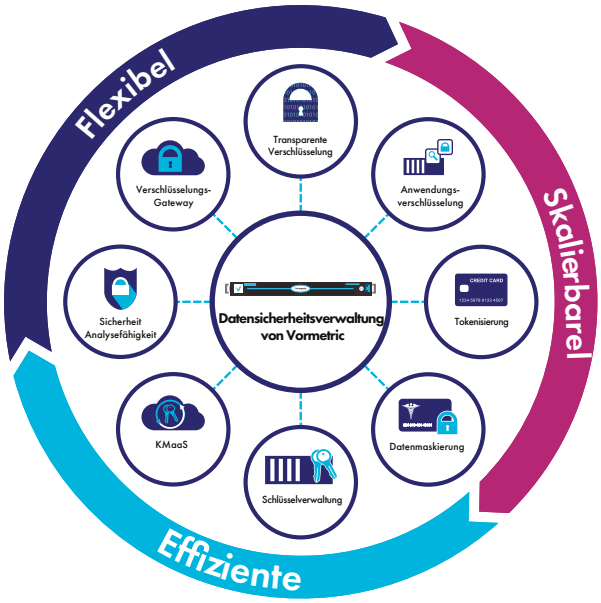
UNERSTÜTZTE UMGEBUNGEN UND TECHNOLOGIEN

- IaaS, PaaS und SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce, Amazon S3 (und kompatible API-Dienste)
- Betriebssysteme: Linux, Windows und Unix
- Big-Data: Hadoop, NoSQL, SAP HANA, Terradata u.a.
- Container: Docker
- Datenbank: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase u. a.
- Beliebige Speicherumgebungen

SC Magazine Awards 2015 Honoree in the U.S.

Computing Security Awards

Frost & Sullivan 2015 Best Practices Award – Global Data Security Platform New Product Innovation Award



VORTEILE DER PLATTFORM

- Zentralisierte Data-at-Rest-Sicherheitsrichtlinien
- Schlüsselverwaltung für die Vormetric Data Security Platform und Verschlüsselungsprodukten von Drittanbietern
- Konsistente Sicherheit und Compliance in physischen, virtuellen, Cloud- und Big-Data-Umgebungen
- Granulare, umsetzbare Dateizugriffsintelligenz dank vordefinierter SIEM-Dashboards
- Schnelle Unterstützung zusätzlicher Anwendungsfälle dank Flexibilität und Erweiterbarkeit

COMPLIANCE

- PCI DSS
- GDPR
- HIPAA/HITECH
- NIST 800-53
- FISMA
- PIPA
- Regionale Vorgaben bezüglich Datenspeicherort und Datenschutz

NIEDRIGERE GESAMTBETRIEBSKOSTEN

Die Vormetric Data Security Platform macht den Schutz von Data-at-Rest einfacher und kostengünstiger. Über die Plattform können Ihre IT- und Sicherheitsorganisationen Daten in Ihrem Unternehmen schnell, einheitlich und wiederholbar schützen. Sie müssen nicht zahllose isolierte und über das ganze Unternehmen verstreute Produkte einsetzen; stattdessen können sie mit der Vormetric Data Security Platform einen konsistenten und zentralisierten Ansatz verfolgen.

PLATTFORMPRODUKTE

Die Vormetric Data Security Platform umfasst folgende Produkte:

- **Vormetric Data Security Manager.** Bietet zentralisierte Kontrollen, die eine konsistente und wiederholbare Verwaltung von Verschlüsselung, Zugriffsrichtlinien und Sicherheitsintelligenz für alle Ihre strukturierten und unstrukturierten Daten ermöglichen. Erhältlich als FIPS-140-2- und Common-Criteria-zertifizierte virtuelle und physische Geräte.
- **Vormetric Transparent Encryption.** Enthält einen Software Agent, der im Dateisystem ausgeführt wird und leistungsstarke Verschlüsselungslösungen und Zugriffskontrollen nach dem Least-Privileged-Prinzip für Dateien, Verzeichnisse und Volumes bietet. Ermöglicht die Verschlüsselung von strukturierten Datenbanken und unstrukturierten Dateien. Verfügt über diese beiden Erweiterungen:
  - **Container Security.** Richtet in Docker™-Containern Kontrollen ein, so dass Sie sicherstellen können, dass andere Container und Prozesse und selbst das Host-Betriebssystem nicht auf vertrauliche Daten zugreifen können. Bietet Funktionen, die Sie für die Verschlüsselung, die Zugriffskontrolle und die Protokollierung von Datenzugriffen auf Pro-Container-Basis benötigen.
  - **Live Data Transformation.** Ermöglicht die Verschlüsselung und periodische Schlüsselrotation von Dateien und Datenbanken – auch während deren Verwendung – ohne Beeinträchtigung der Benutzer, Anwendungen und Business-Workflows.
- **Vormetric Tokenization mit dynamischer Datenmaskierung.** Einfach zu implementierende, formaterhaltende Tokenisierung zum Schutz vertraulicher Felder in Datenbanken sowie richtlinienbasierte dynamische Datenmaskierung für eine sichere Anzeige.
- **Vormetric Application Encryption.** Vereinfacht das Hinzufügen von NIST-Standard-AES-Verschlüsselung und formaterhaltender Verschlüsselung (FPE) zu vorhandenen Anwendungen. Bietet standardbasierte APIs, die für leistungsstarke kryptografische und Schlüsselverwaltungsabläufe verwendet werden können.
- **Vormetric Key Management.** Bietet eine einheitliche Schlüsselverwaltung zur zentralisierten Verwaltung und sicheren Ablage von Schlüsseln für die Produkte von Vormetric Data Security Platform, TDE sowie KMIP-konformen Clients; sorgt zudem für eine sichere Ablage von Zertifikaten.
- **Vormetric Key Management als Dienst & BYOK (Bring Your Own Key).** Ermöglicht eine strenge Überwachung von kryptographischen Schlüsseln und Verschlüsselungsrichtlinien, so dass Sie SaaS-Umgebungen bei gleichzeitiger Minimierung von Komplexität und Risiko umfassend nutzen können.
- **Vormetric Cloud Encryption Gateway.** Ermöglicht Unternehmen den Schutz von Dateien in Cloud-Speicherumgebungen wie Amazon Simple Storage Services (Amazon S3) und anderen S3-kompatiblen Objekt-Speicherdiensten. Bietet Funktionen für Verschlüsselung, Schlüsselverwaltung vor Ort und detaillierte Protokollierung.
- **Vormetric Protection for Teradata Database.** Sorgt für einen schnellen und effizienten Schutz von sensiblen Daten in Ihren Teradata-Umgebungen. Bietet granularen Schutz durch eine mögliche Verschlüsselung bestimmter Felder und Spalten in Teradata-Datenbanken.
- **Vormetric Security Intelligence.** Erzeugt ausführliche Protokolle, die einen detaillierten, prüffähigen Bericht über Dateizugriffsaktivitäten bieten, einschließlich Root-Benutzer-Zugriff. Integrierbar in Sicherheitsinformations- und Ereignis-Managementsysteme (SIEM). Liefert vorgepackte Dashboards und Berichte, die das Compliance-Reporting optimieren und die Bedrohungserkennung beschleunigen.
- **Vormetric Orchestrator.** Automatisiert die Implementierung, Konfiguration, Verwaltung und Überwachung ausgewählter Produkte der Vormetric Data Security Platform. Bietet Funktionen, die durch die Automatisierung von sich ständig wiederholenden Aufgaben Abläufe vereinfachen und dazu beitragen, Fehler zu beseitigen und Implementierungen zu beschleunigen.
- **Vormetric Batch Data Transformation.** Beschleunigt und vereinfacht die Maskierung, Tokenisierung oder Verschlüsselung vertraulicher Spalteninformationen in Datenbanken. Kann vor dem Schutz vorhandener vertraulicher Daten durch Vormetric Tokenization oder Vormetric Application Encryption angewendet werden. Bietet statische Datenmaskierungsservices.

VORMETRIC DATA SECURITY MANAGER

Der Vormetric Data Security Manager (DSM) zentralisiert die Verwaltung und die Richtlinien für alle Produkte der Vormetric Data Security Platform. Der DSM versetzt Unternehmen in die Lage, Compliance-Anforderungen, gesetzliche Vorgaben und Branchen-Best-Practices effizient zu erfüllen und umzusetzen, wenn entsprechende Implementierungen und Anforderungen anstehen. Die Lösung lässt sich in LDAP-Verzeichnisdienste integrieren, so dass Sie Kontrollen für Benutzer und Gruppen einrichten und damit sicherstellen können, dass Sicherheitsrichtlinien im gesamten Unternehmen befolgt werden. Die Lösung stellt auch die Protokolle bereit, die benötigt werden, um die strengsten Compliance-Anforderungen zu erfüllen.

SICHERES, ZUVERLÄSSIGES UND FIPS-ZERTIFIZIERTES SYSTEM

Zur Maximierung der Betriebszeit und Sicherheit verfügt der DSM über redundante Komponenten und die Fähigkeit, Geräte-Cluster in Bezug auf Fehlertoleranz und hoher Verfügbarkeit zu bilden. Richtlinien mit strenger Aufgabentrennung können definiert werden, so dass gewährleistet ist, dass kein einzelner Administrator die vollständige Kontrolle über Datensicherheitsaktivitäten, kryptographische Schlüssel oder die Administration erlangt. Außerdem unterstützt der DSM eine Zwei-Faktor-Authentifizierung für den Verwaltungszugriff.

FLEXIBLE IMPLEMENTIERUNG

Der DSM unterstützt zahlreiche einzigartige Umgebungen und erfüllt eine ganze Reihe von Sicherheitsanforderungen; er ist in verschiedenen Formfaktoren erhältlich:

- Virtual Appliance, gemäß FIPS 140-2 Level 1 zertifiziert
- V6000-Hardware, gemäß FIPS 140-2 Level 2 zertifiziert
- V6100-Hardware, die gemäß FIPS 140-2 Level 3 zertifiziert und mit einem Thales nShield Solo Hardwaresicherheitsmodul (HSM) mit nShield Remote Access Support ausgerüstet ist

Die Plattform ist auch auf den Amazon Web Services (AWS) und Microsoft Azure Marktplätzen verfügbar.

KEY FEATURES

- Zentrale Verwaltungskonsole für alle Plattformrichtlinien und Schlüssel
- Multi-Tenancy-Unterstützung
- Bewährte Skalierung bis 10.000+ Agenten
- Clustering für Hochverfügbarkeits-
- Toolkit und programmatische Schnittstelle
- Einfache Integration in vorhandene Authentifizierungsinfrastruktur Support von
- RESTful APIs
- Multi-Faktor-Authentifizierung und nShield Remote Administration
- Orchestrierungs- und Automatisierungssupport

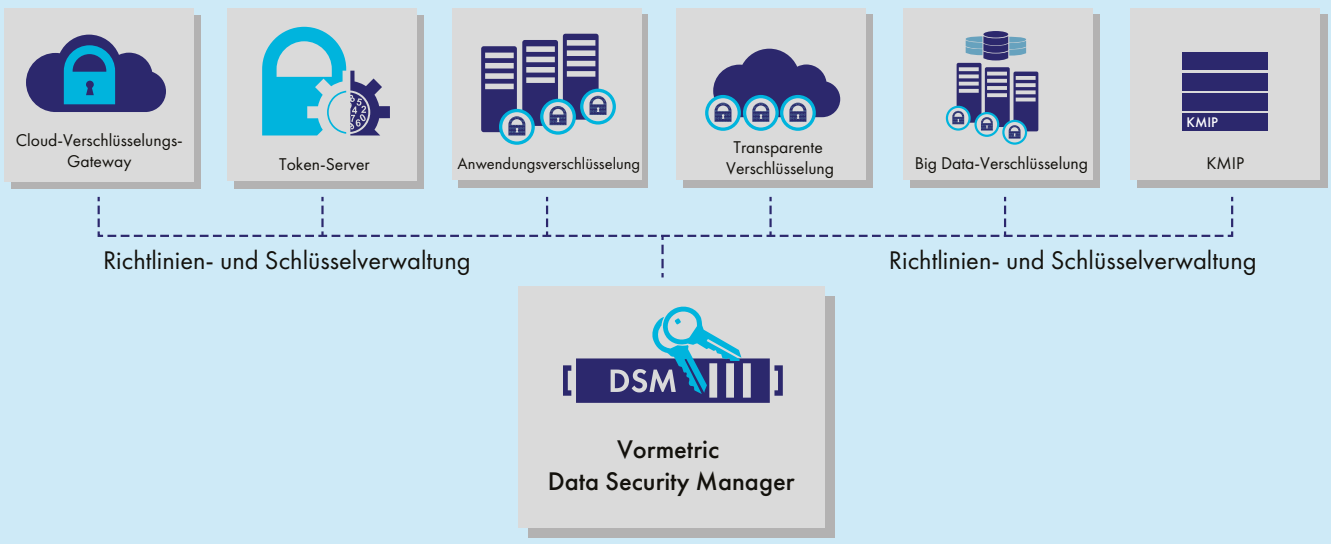
TECHNISCHE DATEN

Plattform-Optionen

- FIPS 140-2 Level 1 Virtual Appliance
- FIPS 140-2 Level 2 Hardware Appliance
- FIPS 140-2 Level 3 Hardware Appliance
- AWS und Azure Marketplaces



Der V6100 DSM bietet nShield HSM Secure Remote Administration mit Multifaktor-Smartcard-Authentifizierung.



EINHEITLICHE VERWALTUNG UND ADMINISTRATION IM GESAMTEN HYBRID-UNTERNEHMEN

Der DSM minimiert Kosten durch die Möglichkeit einer zentralen Verwaltung heterogener kryptographischer Schlüssel. Dazu gehören Schlüssel, die von Produkten der Vormetric Data Security Platform, von IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE und KMIP-konformen Verschlüsselungsprodukten generiert wurden. Der DSM verfügt über eine intuitive webbasierte Konsole und APIs für die Verwaltung kryptographischer Schlüssel, Richtlinien und unternehmensweiter Audits. Das Produkt zentralisiert darüber hinaus die Protokollerfassung.

DSM-SPEZIFIKATIONEN

Hardware-Spezifikationen	
Gehäuse	1U-Rack-montierbar; BxLxH: 43,18 cm x 52,07 cm x 4,5 cm
Gewicht	V6000: 9,8 kg; V6100: 10 kg
Speicher	16 GB
Festplatte	Dual SAS RAID 1 konfiguriert mit FIPS manipulationssicheren Siegeln
Serieller Port	1
Ethernet	2 x 1 GB
IPMI	1 x 10/100 MB
Netzteile	2 abnehmbare, 80+-zertifizierte (100 VAC - 240 VAC/50 - 60 Hz) 400 W
Gehäuse-Eindringungserkennung	Ja. Enthält auch FIPS manipulationssichere Siegel an der obersten Abdeckung.
Max. Wärmeabstrahlung	410 BTU max.
Betriebstemperatur	10 bis 35 °C (50 bis 95 °F)
Lagertemperatur	-40 bis 70 °C (-40 bis 158 °F)
Relative Luftfeuchtigkeit bei Betrieb	8 bis 90 % (nicht kondensierend)
Relative Luftfeuchtigkeit bei Lagerung	5 bis 95 % (nicht kondensierend)
Zulassung durch die zuständigen Sicherheitsbehörden	FCC-, UL-, BIS-Zertifizierungen
FIPS 140-2 Level 3 HSM	V6100-Modell, das mit einem nShield Solo HSM ausgerüstet ist
HSM Remote Administration	nur V6100; erfordert optionales nShield Remote Administration Kit
Software-Spezifikationen	
Administrative Schnittstellen	Secure Web, CLI, SOAP, REST
Anzahl der Managementdomänen	1.000+
API-Unterstützung	PKCS #11, Microsoft Extensible Key Management (EKM), SOAP, REST
Sicherheitsauthentifizierung	Benutzername/Passwort, RSA Multifaktor-Authentifizierung (optional)
Cluster-Unterstützung	Ja
Backup	Manuelle und geplante sichere Backups. M von N Schlüsselwiederherstellung.
Netzwerkmanagement	SNMP, NTP, Syslog-TCP
Syslog-Formate	CEF, LEEF, RFC 5424
Zertifizierungen und Validierungen	FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level 3 Common Criteria (ESM PP PM V2.1)
Virtual-Appliance-Mindestspezifikationen – Empfehlung für Virtual Appliance	
Anzahl CPUs	2
RAM (GB)	4
Festplatte (GB)	100 GB
Unterstützung von Thin Provisioning	Ja

VORMETRIC TRANSPARENT ENCRYPTION

Vormetric Transparent Encryption bietet Funktionen für die Verschlüsselung von „Data at Rest", die Zugriffskontrolle für privilegierte Benutzer und die Erfassung von Sicherheitsintelligenzprotokollen. Mit dieser Lösung können strukturierte Datenbanken und unstrukturierte Dateien geschützt werden. Dazu gehören Dateien in physischen, virtualisierten, Big-Data-, Docker- und Cloud-Umgebungen.

Der transparente Ansatz dieser Lösung versetzt Unternehmen in die Lage, Verschlüsselungen zu implementieren, ohne Änderungen an Anwendungen, Infrastruktur oder Geschäftspraktiken vornehmen zu müssen. Im Gegensatz zu anderen Verschlüsselungslösungen endet der Schutz nicht, nachdem die Verschlüsselung angewendet wurde. Vormetric Transparent Encryption sorgt kontinuierlich für die Protokollierung des Zugriffs und für die Befolgung der Richtlinien, die vor unbefugtem Zugriff durch Benutzer und Prozesse schützen. Mit diesen Funktionen können Sie den Schutz und die Kontrolle Ihrer Daten dauerhaft sicherstellen.

SKALIERBARE VERSCHLÜSSELUNG IN ALLEN IHREN UMGEBUNGEN

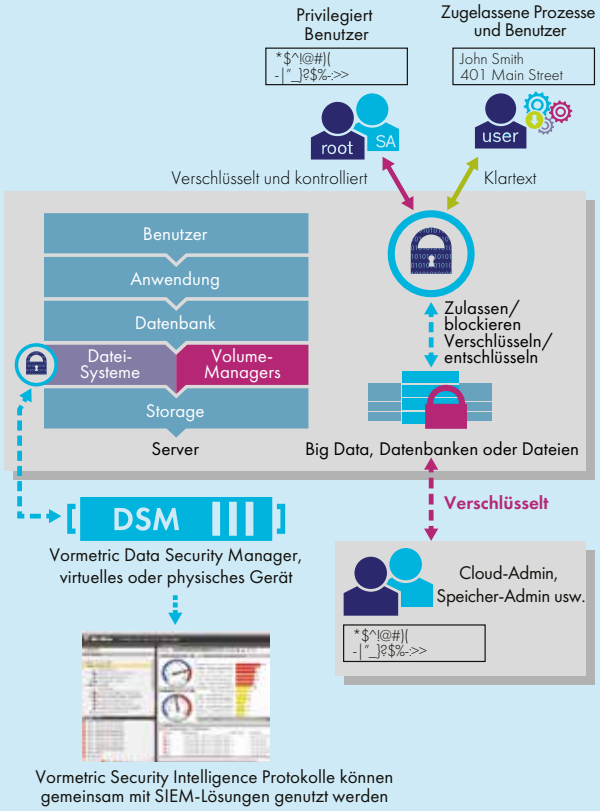
Bei der Vormetric Transparent Encryption handelt es sich um einen Agenten, der auf Dateisystemebene oder Volume-Ebene auf einem Server ausgeführt wird. Der Agent ist für eine umfassende Auswahl an Windows-, Linux- und Unix-Plattformen erhältlich und kann in physischen, virtuellen, Cloud-, Docker- und Big-Data-Umgebungen – unabhängig von der zugrunde liegenden Speichertechnologie – eingesetzt werden. Administratoren führen alle Richtlinien und die Schlüsselverwaltung über den Vormetric Data Security Manager (DSM) durch.

Dank der agentenbasierten Architektur der Lösung kann die Verschlüsselung auf Servern durchgeführt werden. Folglich beseitigt die Lösung die Engpässe, unter denen alte, proxy-basierte Lösungen leiden, die alle Daten über feste Knoten auf den Netzwerken routen. Die Leistung und Skalierbarkeit verbessert sich noch weiter durch den Einsatz kryptographischer Hardware-Module, die in modernen CPUs wie Intel AES-NI, IBM Power8 in-core und Oracle SPARC verbaut sind.

LEISTUNGSSTARKE UND GRANULARE BENUTZERZUGRIFFSKONTROLLEN

Der Agent setzt granulare Benutzer-Zugriffsrichtlinien nach dem Least-Privileged-Prinzip durch, die Daten vor APTs (Advanced Persistent Threats) und Missbrauch durch Administratoren schützen.

Die Richtlinien können nach Benutzer, Prozess, Dateityp, Uhrzeit und anderen Parametern angewendet werden. Die Durchsetzungsoptionen sind sehr fein abgestimmt; sie können nicht nur kontrollieren, ob ein Benutzer auf Daten in Klartext zugreift, sondern auch, welche Dateisystembefehle verfügbar sind.



HAUPTVORTEILE

- Verschlüsselung plattform- und umgebungsübergreifend skalierbar
- Einfache Implementierung: keine Anwendungsanpassung erforderlich
- Einrichtung strenger Sicherheitsmaßnahmen gegen Missbrauch durch privilegierte Insider

HAUPTMERKMALE

- Umfassendste Plattform-Unterstützung der Branche: Windows-, Linux- und Unix-Betriebssysteme
- Leistungsstarke Verschlüsselung
- Leistungsfähiger Verschlüsselungs- und Suite-B-Protokoll-Support
- Protokollierung aller zugelassenen, verweigerten und eingeschränkten Zugriffsversuche durch Benutzer, Anwendungen und Prozesse
- Rollenbasierte Zugriffsrichtlinienkontrolle in Bezug darauf, wer wo wann und wie auf welche Daten zugreifen kann
- Möglichkeit, dass privilegierte Benutzer ihre Arbeit ohne Zugriff auf Klartext-Daten ausführen können
- Erweiterungen bieten zusätzliche Funktionen, einschließlich einer granularen Docker-Container-Unterstützung sowie Datentransformationsmöglichkeiten ohne Ausfallzeiten

TECHNISCHE DATEN

Erweiterungslizenzen
- Container-Sicherheit
- Live Data Transformation

Plattform-Unterstützung
- Microsoft: Windows Server 2008 und 2012
  Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu
- UNIX: IBM AIX, HP-UX*, Solaris*

Datenbankunterstützung
- IBM DB2, Microsoft SQL Server, MySQL, NoSQL, Oracle, Sybase u. a.

Anwendungsunterstützung
- Transparent für alle Anwendungen, einschließlich Documentum, SAP, SharePoint, kundenspezifische Anwendungen usw.

Big-Data-Unterstützung
- Hadoop: Cloudera, Hortonworks, IBM
- NoSQL: Couchbase, DataStax,
- MongoDB SAP HANA
- Teradata

Verschlüsselungshardware-Beschleunigung
- AMD und Intel AES-NI
- IBM P8 kryptographischer Koprozessor
- SPARC-Verschlüsselung

Agentenzertifizierung
- FIPS 140-2 Level 1

Container-Unterstützung
- Docker

*HP-UX und Solaris werden nur von Vormetric Transparent Encryption Version 5.x Agents



CONTAINER-SICHERHEIT

Container bieten den Unternehmen zwar ungeahnte Vorteile, diese Technologie birgt jedoch auch neue Risiken. Die Container-Sicherheit von Vormetric bietet kritische Fähigkeiten für die Verschlüsselung, Zugriffskontrolle und den Datenzugriff, so dass die Unternehmen strenge Sicherheitsmaßnahmen für Daten in dynamischen Container-Umgebungen einrichten können.

Bei dieser Lösung handelt es sich um eine Software-Lizenz für Vormetric Transparent Encryption, mithilfe derer Sicherheitsteams Kontrollmöglichkeiten innerhalb von Containern einrichten können. Mit dieser Erweiterung lassen sich Verschlüsselungen, Zugriffskontrollen und Datenzugriffs-Prüfprotokolle auf Pro-Container-Basis anwenden, und zwar sowohl auf Daten in Containern als auch auf externe Speicher, auf die über Container zugegriffen werden kann.

ERFÜLLUNG VON COMPLIANCE-ANFORDERUNGEN

Heutzutage haben viele Sicherheitsteams nur beschränkte Kontrollmöglichkeiten für die Verwaltung und Protokollierung der Zugriffe auf Daten, die sich in Containern und Images befinden. Aus diesem Grund ist es für diese Teams häufig schwierig, alle relevanten internen Sicherheitsrichtlinien und gesetzlichen Vorgaben einzuhalten. Diese Erweiterung der Vormetric Transparent Encryption bietet die Möglichkeiten zur Verschlüsselung, Datenzugriffskontrolle und Prüfung, die Sie für die Befolgung von Compliance-Anforderungen und gesetzlichen Vorgaben benötigen. Sie können die Lösung verwenden, um vertrauliche Daten zu schützen, egal ob Sie Zahlungskarten, Gesundheitsakten oder andere sensible Daten verwalten.

UMFASSENDE, GRANULARE SICHERHEIT IN DOCKER-UMGEBUNGEN

Die Container-Sicherheit von Vormetric nutzt offene Docker-APIs und -Schnittstellen zur Umsetzung von richtlinienbasierten Verschlüsselungen, Zugriffskontrollen und Datenzugriffsprüfprotokollen für Daten, die in Containern gespeichert sind oder auf die über Container zugegriffen werden kann. Mit dieser Lösung erhalten Sie grundsolide Abläufe, eine unkomplizierte Implementierung und den zuverlässigen Schutz, den Sie zur sicheren Implementierung von Produktionsanwendungen benötigen, welche möglicherweise hoch sensible Daten verwenden.

WIRKSAME SCHUTZMASSNAHMEN MIT OPTIMALER EFFIZIENZ

Container-Sicherheit von Vormetric bietet Folgende Vorteile:

- **Umfassende Sicherheitsmaßnahmen.** Sichern Sie Container-Volumes und schützen Sie Daten vor unbefugtem Zugriff oder Export.
- **Granulare Kontrolle und Transparenz.** Einrichtung detaillierter Zugriffsrichtlinien, basierend auf bestimmten Benutzern, Prozessen und Ressourcensets. Isolationsmöglichkeit zwischen Containern, so dass nur autorisierte Container auf vertrauliche Daten zugreifen können.
- **Flexible, effiziente Implementierung.** Implementieren Sie Kontrollen in Container-Umgebungen, ohne dass Sie Änderungen an Anwendungen, Containern oder Infrastrukturen vornehmen müssen.

HAUPTVORTEILE

- Schutz vor Root-/privilegiertem/unbefugtem Benutzerzugriff innerhalb von Containern
- Schutz von Daten gegen Privilege-Escalation-Angriffen aus anderen Containernc
- Einfache Isolierung des Datenzugriffs zwischen Containern
- Einhaltung gesetzlicher Auflagen hinsichtlich Datenzugriffskontrollen und Audits auf Container-Level

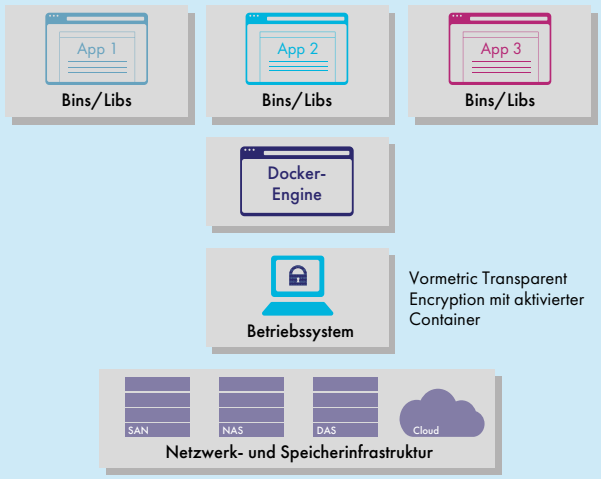
HAUPTMERKMALE

- Verschlüsselung, Zugriffskontrollen und Datenzugriffsprüfprotokolle, sowohl für Docker-Hosts als auch für Images
- Kontrollfunktionen für in Containern gespeicherte Daten sowie für Daten, auf die von Containern aus zugegriffen werden kann
- Granulare Kontrollmechanismen für bestimmte Benutzer, Prozesse und Ressourcensets
- Keine Änderungen an Anwendungen, Containern oder Infrastruktur erforderlich
- Verwendet dieselben Agenten und dasselbe Infrastrukturset wie die transparente Verschlüsselung von Vormetric

TECHNISCHE DATEN

Unterstützte Plattformen/Umgebungen

- Docker
- Red Hat Enterprise Linux, 7.x
- Kann auf physischen Systemen, VMs und AWS EC2-Instanzen ausgeführt werden



LIVE DATA TRANSFORMATION

Bei der Implementierung und Verwaltung der Verschlüsselung von „Data at Rest" werden Sicherheitsteams häufig mit Herausforderungen konfrontiert, wenn sie Klartextdaten verschlüsseln oder neue Schlüssel für bereits verschlüsselte Daten einführen („Rekeying"). Bisher erforderten diese Vorgänge entweder geplante Ausfallzeiten oder arbeitsintensive Datenklon- und Synchronisierungsarbeiten. Die Vormetric Transparent Encryption Live Data Transformation Extension schafft hier Abhilfe, indem sie Verschlüsselungs- und Rekeying-Vorgänge mit beispielloser Verfügbarkeit und administrativer Effizienz ermöglicht.

KEINE AUSFALLZEITEN VERSCHLÜSSELUNG UND SCHLÜSSELROTATION

Live Data Transformation bietet folgende Hauptfunktionen:

- **Verschlüsselungsimplementierung ohne Ausfallzeiten.** Die Lösung ermöglicht es Administratoren, Daten zu verschlüsseln, ohne Ausfallzeiten zu verursachen oder Benutzer, Anwendungen und Geschäftsprozesse zu beeinträchtigen. Während des Verschlüsselungsprozesses können Benutzer und Prozesse mit der Nutzung von Datenbanken oder Dateisystemen wie gewohnt fortfahren.
- **Nahtlose unterbrechungsfreie Schlüsselrotation.** Sowohl Best Practices für Datensicherheit als auch viele gesetzliche Vorschriften erfordern eine regelmäßige Schlüsselrotation. Mithilfe von Live Data Transformation können Sie diese Anforderungen schnell und effizient erfüllen. Mit dieser Lösung können Sie die Schlüsselrotation durchführen, ohne Daten duplizieren oder die betroffenen Anwendungen offline nehmen zu müssen.
- **Intelligentes Ressourcenmanagement.** Für das Verschlüsseln von umfangreichen Datensätzen müssen möglicherweise CPU-Ressourcen in erheblichem Maße und über einen längeren Zeitraum hinweg in Anspruch genommen werden. Live Data Transformation bietet intelligente Funktionen für die CPU-Verwaltung, so dass Administratoren zwischen dem Ressourcenbedarf für die Verschlüsselung und anderen Geschäftsprozessen einen Ausgleich herstellen können. Beispielsweise kann ein Administrator eine Ressourcenmanagementregel definieren, die vorsieht, dass die Verschlüsselung während der Geschäftszeiten nur 10 %, jedoch nachts und an Wochenenden 70 % der CPU-Ressourcen in Anspruch nehmen darf.
- **Versionierte Sicherungskopien und Archive.** Mit der Versionierungsverwaltung von Schlüsseln bietet Live Data Transformation eine effiziente Datensicherung und Archiv-Wiederherstellung, die einen schnelleren Zugriff erlaubt. Bei einem Datenwiederherstellungsprozess werden archivierte kryptographische Schlüssel, die durch den Vormetric Data Security Manager wiederhergestellt wurden,

HAUPTVORTEILE

- Erweiterung der Verschlüsselungsimplementierung bei gleichzeitiger Minimierung von Ausfallzeiten und Speicheranforderungen
- Niedrigere Kosten für Verschlüsselungsimplementierung und Wartung
- Minimale Beeinträchtigung der Benutzer durch die Verschlüsselung
- Unterbrechungsfreie Schlüsselrotation sorgt für höhere Sicherheit und eine bessere Erfüllung gesetzlicher Auflagen
- Raschere Wiederherstellung von Daten, die mit älteren Schlüsseln verschlüsselt wurden

TECHNISCHE DATEN

Unterstützte Betriebssysteme

- Microsoft: Windows Server 2008 und 2012
- Linux: Red Hat Enterprise Linux (RHEL) 6 und 7, SuSE Linux Enterprise Server 11 und12

Cluster-Unterstützung

- Veritas Cluster Server Active/Passive
- Microsoft Cluster: File Cluster, SQL Server Cluster

Datenbankunterstützung

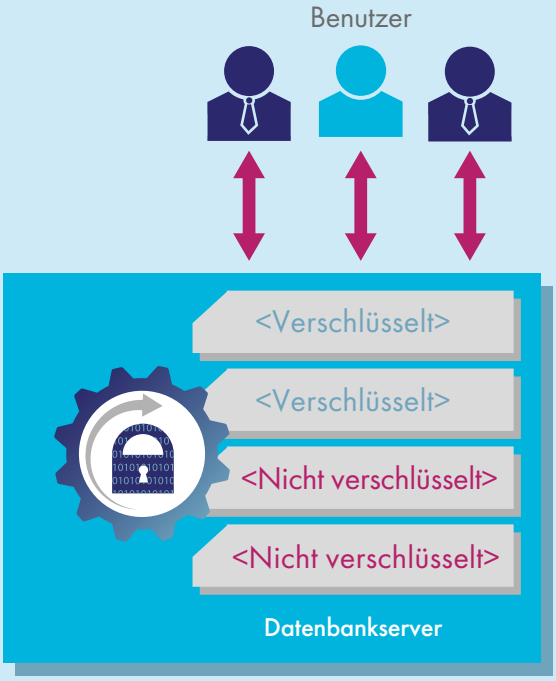
- IBM DB2, IBM Informix, Microsoft SQL Server, Oracle, Sybase usw.

Big-Data-Unterstützung

- Cassandra, CouchBase, Hadoop, MongoDB,SAP HANA

Datensicherungs-/Wiederherstellungsunterstützung

- DB2-Sicherung, NetBackup, NetWorker, NTBackup, Oracle Recovery Manager (RMAN), Windows Server Volume Shadow Copy Service (VSS)



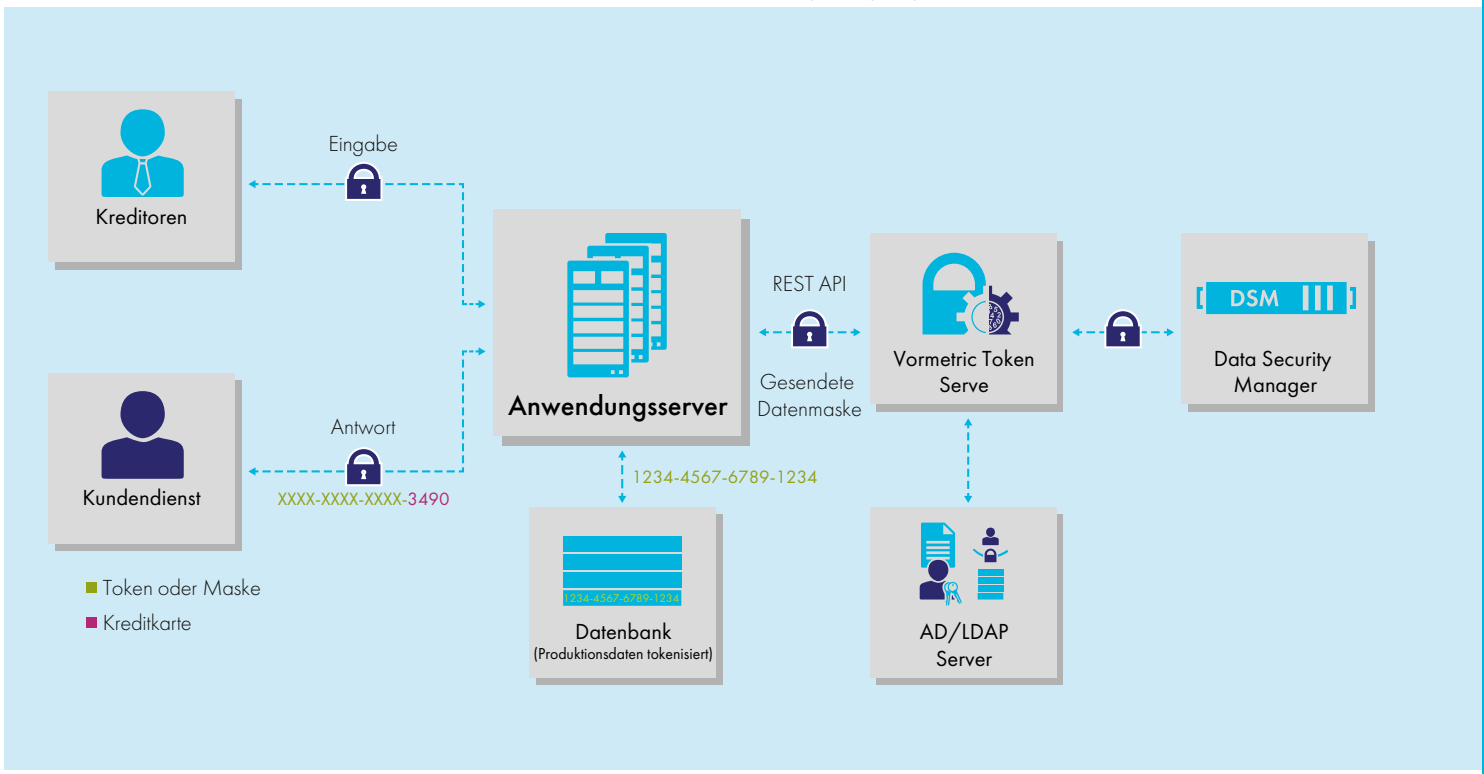
VORMETRIC TOKENIZATION MIT DYNAMISCHER DATENMASKIERUNG

Vormetric Tokenization mit dynamischer Datenmaskierung reduziert den Aufwand und die Kosten, die für die Einhaltung von Sicherheitsrichtlinien und gesetzlichen Auflagen wie PCI DSS (Payment Card Industry Data Security Standard) erforderlich sind, ganz erheblich. Die Lösung bietet eine Datenbank-Tokenisierung und eine dynamische Display-Sicherheit. Jetzt kann Ihr Unternehmen seine Ziele in puncto Sicherung und Anonymisierung vertraulicher Daten effizient erreichen, und zwar unabhängig davon, ob sich diese im Rechenzentrum, in Big-Data-Umgebungen oder in der Cloud befinden.

OPTIMIERTE TOKENISIERUNG UND DYNAMISCHE DATENMASKIERUNG

Die Tokenisierung von Vormetric erleichtert die formaterhaltende Tokenisierung zum Schutz sensibler Felder in Datenbanken und zum Hinzufügen richtlinienbasierter dynamischer Datenmaskierung für Anwendungen. Die Lösung bietet die folgenden Vorteile:

- **Dynamische Datenmaskierung.** Administratoren können Richtlinien erstellen und ein vollständiges Feld tokenisiert zurückgeben oder Teile eines Felds dynamisch maskieren. So könnte ein Sicherheitsteam beispielsweise Richtlinien festlegen, dass einem Mitarbeiter aus dem Kunden-Support lediglich die letzten vier Ziffern von Kreditkartennummern angezeigt werden, während sein Vorgesetzter die vollständigen Nummern im Klartextformat sehen kann.
- **Implementierung ohne Störung des laufenden Betriebs.** Mit den formaterhaltenden Tokenisierungsfunktionen der Lösung können Sie den Zugriff auf sensible Daten einschränken, ohne das bestehende Datenbankschema zu ändern. Dank der REST-API-Implementierung sind Anwendungsentwickler in der Lage, komplexe Tokenisierungsfunktionen schnell, einfach und effizient einzurichten.
- **Batch Data Transformation.** Mit diesem optionalen Dienstprogramm können für hohe Volumen vertraulicher Datensätze ohne langwierige Wartungsfenster und Ausfallzeiten Token generiert werden. Sie können sensible Spalten in Produktionsdatenbanken und in Datenbankkopien maskieren, bevor diese an Drittanbieter-Entwickler und Big-Data-Umgebungen gesendet werden.



HAUPTVORTEILE

- Entfernen von Karteninhaberdaten aus dem PCI DSS-Bereich mit minimalen Kosten und minimalem Aufwand
- Umfassendere Nutzung von Cloud-, Big-Data- und outgesourcten Modellen – ohne größeres Risiko
- Einrichtung strenger Sicherungsmaßnahmen, die sensible Daten vor Cyber-Angriffen und Insider-Missbrauch schützen

HAUPTMERKMALE

- Virtual Cluster Nodes ermöglichen schnelle Steigerung und Senkung von Kapazitäten
- Implementierbar in AWS, virtualisierten und physischen Umgebungen
- Optionales Dienstprogramm für Batchdatentransformation optimiert umfassende Tokenisierung
- Granulare, richtlinienbasierte dynamische Datenmaskierung

TECHNISCHE DATEN

Tokenisierungsfunktionen:

- Formaterhaltend
- Kryptographische Token (alphanumerisch)
- Random Token (nur Ziffern)
- Single und Multi Use Token
- Datumstokenisierung

Dynamische Datenmaskierungsfunktionen:

- Richtlinienbasiert
- Alphanumerische Unterstützung
- Anpassung von Maskenzeichen

Validierungssupport:

- Luhn-Check

Virtual Appliance:

- Open Virtualization Format (.ovf)
- ISO (International Organization for Standardization) (.iso)
- Amazon Machine Image (.ami)

Systemanforderungen:

- Mindestanforderungen an Hardware: 4 CPU Kerne, 16 - 24 GB RAM
- Mindestspeicherkapazität Festplatte: 80 GB

Anwendungsintegration:

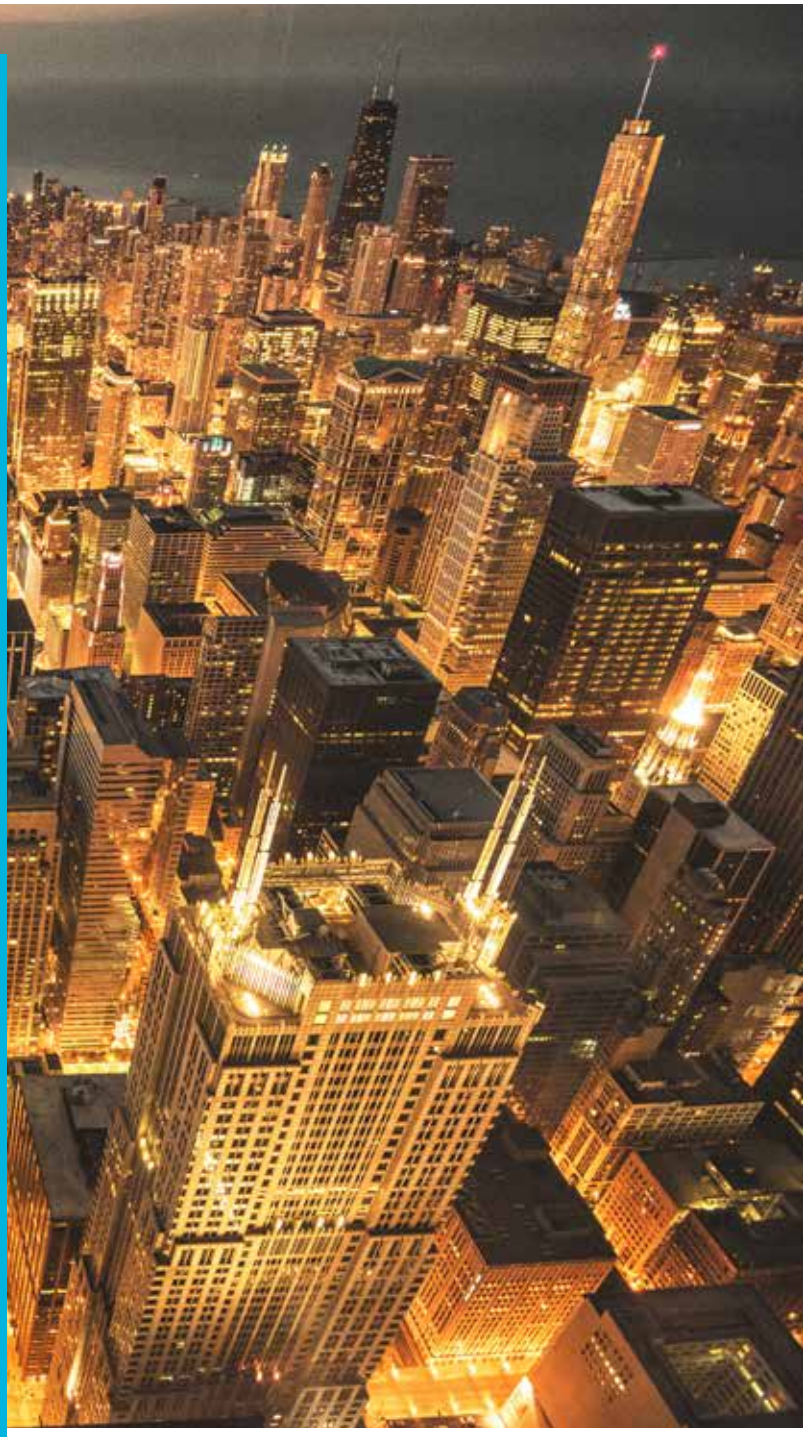
- REST-APIs

Authentifizierungsintegration:

- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD)

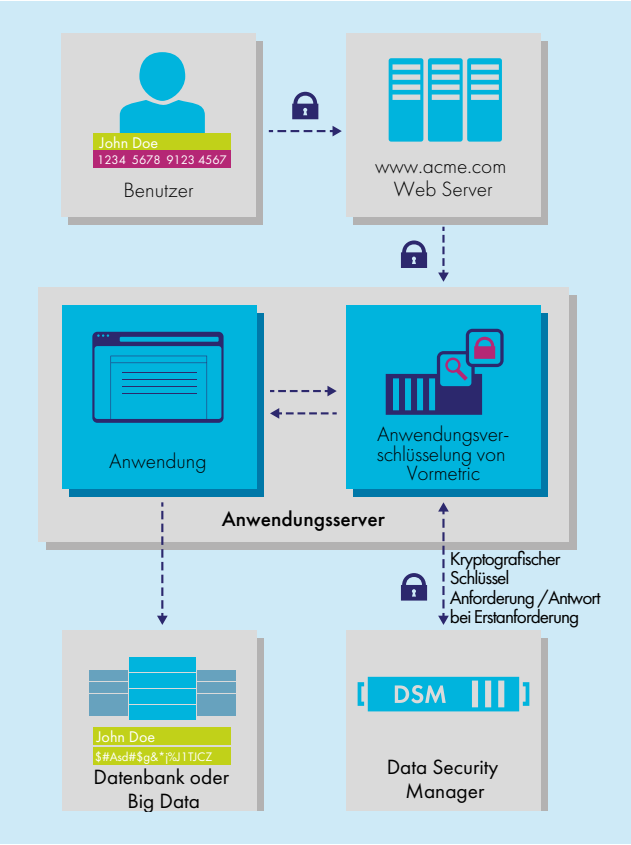
Leistung:

- Mehr als 1 Million Tokenisierungstransaktionen in Kreditkartengröße pro Sekunde, pro Token-Server (mit mehreren Threads und Batch- (oder Vektor-) Modus auf einem 32-Core-Server (Dual Socket Xeon E5-2630v3) mit 16 GB RAM



VORMETRIC APPLICATION ENCRYPTION

Mit Vormetric Application Encryption können Sie bestimmte Dateien oder Spalten in Datenbanken, Big-Data-Knoten und PaaS-Umgebungen verschlüsseln. Vormetric Application Encryption ist eine Bibliothek, die die Integration von Verschlüsselungsfunktionen auf Anwendungsebene in bestehende Unternehmensapplikationen vereinfacht. Sie stellt eine Reihe dokumentierter, standardbasierter APIs für Kryptografie- und Schlüsselverwaltungsvorgänge bereit. Vormetric Application Encryption beseitigt den Zeitaufwand, die Komplexität und die Risiken, die mit der Entwicklung und Implementierung einer unternehmenseigenen Verschlüsselungs- und Schlüsselverwaltungslösung einhergehen.



GERINGERE KOMPLEXITÄT UND KOSTEN BEI VERSCHLÜSSELUNG AUF ANWENDUNGSEBENE

Vormetric Application Encryption vereinfacht das Hinzufügen von Verschlüsselungsfunktionen zu bestehenden Anwendungen. Entwickler können Bibliotheken für Java, NET und C verwenden, um die Kommunikation zwischen Anwendungen und dem Vormetric Application Encryption Agent zu erleichtern. Dieser Agent verschlüsselt Daten und gibt den resultierenden verschlüsselten Text an die Anwendung zurück. Dabei wird entweder der NIST-Standard AES-CBC oder die formaterhaltende Verschlüsselung (FPE) verwendet. Die gesamte Richtlinien- und Schlüsselverwaltung erfolgt über den Vormetric Data Security Manager, wodurch die Sicherheitsabläufe vereinfacht werden.

EINHALTUNG BEHÖRDLICHER AUFLAGEN IN DER CLOUD UND IN BIG-DATA-UMGEBUNGEN

Mit dieser Lösung können Sie die Richtlinien und behördlichen Auflagen erfüllen, die eine Verschlüsselung bestimmter Felder auf Anwendungsebene erfordern. Die Lösung kann vertrauliche Daten verschlüsseln, bevor diese in Datenbanken, Big-Data-Repositorys oder PaaS-Umgebungen gespeichert werden.

VORMETRIC BATCH DATA TRANSFORMATION DIENSTPROGRAMM

Mithilfe der Batchdatentransformation von Vormetric Batch Data Transformation kann Ihr Unternehmen umfangreiche Datensätze ohne langwierige Wartungsfenster und Ausfallzeiten verschlüsseln – und ohne Anwendungen, Netzwerkkonfigurationen oder Speicherarchitekturen ändern zu müssen.

HAUPTVORTEILE

- Eliminiert den Zeitaufwand, die Komplexität und das Risiko beim Aufbau einer unternehmensinternen Verschlüsselungslösung
- Zentralisierte Kontrolle von Anwendungsebenen- und Dateisystem-Verschlüsselung
- Schutz sensibler Daten über ein breites Spektrum an Plattformen und unternehmenseigenen und PaaS-Umgebungen hinweg
- Kein Zugriff durch böswillige DBAs, Cloud-Administratoren, Hacker und Vollzugsbehörden auf wertvolle Daten
- Optimierung von umfangreichen Verschlüsselungsmigrationen anhand der Vormetric Batch Data Transformation Utility

TECHNISCHE DATEN

Unterstützte Umgebungen:
- Microsoft .NET 2.0 und höher
- Java 7 und 8
- C

Integrationsstandard:
- OASIS PKCS#11 APIs

Verschlüsselung:
- AES
- Formaterhaltende Verschlüsselung FF3

Betriebssysteme:
- Linux
- Windows 2008 und 2012

Performance:
- 400.000 Verschlüsselungstransaktionen in Kreditkartengröße pro Sekunde (z. B. Single Thread, 32 Core, 16 GB, C)

Richtlinien- und Schlüsselverwaltung:
- Vormetric Data Security Manager

Zeichenunterstützung:
- ASCII
- Unicode

Zertifizierung:
- FIPS 140-2 Level 1 – in Bearbeitung

VORMETRIC KEY MANAGEMENT

Mit Hilfe der Vormetric Schlüsselverwaltung können Sie Schlüssel aus allen Produkten der Vormetric Data Security Platform zentral verwalten sowie Schlüssel und Zertifikate für Drittanbietergeräte sicher speichern und inventarisieren. Dazu gehören auch Verschlüsselungsprodukte von IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE und KMIP-konforme Verschlüsselungsprodukte. Durch die Konsolidierung der Schlüsselverwaltung im Unternehmen können Richtlinien systemübergreifend konsistent implementiert und Schulungs- und Wartungskosten gesenkt werden.

VEREINFACHTE SCHLÜSSELVERWALTUNG UND ZERTIFIKATSSPEICHERUNG

Als in der Vergangenheit die Anwendungen und Geräte, für die eine Verschlüsselung genutzt wurde, sprunghaft anstiegen, nahm auch die Anzahl der verwendeten Schlüsselverwaltungsgeräte entsprechend zu. Dieser Zuwachs bei den Schlüsselverwaltungssystemen machte hochverfügbare verschlüsselte Umgebungen komplexer und teurer. Außerdem ließen diese unterschiedlichen Schlüsselverwaltungsgeräte häufig wertvolle Zertifikate ungeschützt, wodurch diese zu einer leichten Beute für Hacker wurden. Diese nicht verwalteten Zertifikate konnten außerdem unerwartet ihre Gültigkeit verlieren, was zu ungeplanten Ausfallzeiten wichtiger Dienste führen konnte.

Vormetric Key Management ermöglicht es Ihnen, Ihre Möglichkeiten zu erweitern, so dass Sie nicht nur Schlüssel für die Lösungen von Vormetric Key Management effektiver verwalten können, sondern auch Schlüssel und Zertifikate von Drittanbieterprodukten. Darüber hinaus können Sie mit Vormetric Key Management als Dienst für die Cloud die BYOK-Dienste von Cloud-Anbietern nutzen und zugleich die volle Kontrolle über Schlüssel über deren gesamten Lebenszyklus einrichten.

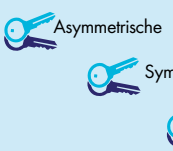
Integrierte Schlüssel und Richtlinien von Vormetric



TDE-Schlüssel



Sichere Depot-Schlüssel und Zertifikate



- Manueller Schlüsselimport
- Schlüsseldepot
- Berichterstellung
- Skripterstellungs-schnittstelle
- Protokollierung
- Aufnahme
- Abruf
- Entfernung

KMIP-Schlüssel



Selbstverschlüsselnde Laufwerke, Bandbibliotheken usw.

STARKE, PRÜFFÄHIGE KONTROLLEN

Vormetric Key Management bietet die Zuverlässigkeit und hohe Verfügbarkeit des Vormetric Data Security Managers (DSM). Der DSM wird als Virtual Appliance und über zwei Hardware-Geräte angeboten: V6000 und V6100. Bei V6100 handelt es sich um ein gemäß FIPS 140-2 Level 3 zertifiziertes Gerät, das mit einem Thales nShield Solo-Hardwaresicherheitsmodul (HSM) ausgerüstet ist. Die Plattform ist auch auf den Amazon Web Services und Microsoft Azure Marktplätzen verfügbar.

HAUPTVORTEILE

- Betriebliche Effizienz
- Ständig verfügbare, sichere Speicherung und Inventarisierung von Zertifikaten und kryptographischen Schlüsseln
- Proaktive Warnhinweise auf den Ablauf von Zertifikaten und Schlüsseln
- Berichte mit Status- und charakteristischen Informationen, Audit-Support

TECHNISCHE DATEN

Verwaltung von Sicherheitsobjekten
- x.509-Zertifikate
- Symmetrische und asymmetrische kryptografische Schlüssel

Verwaltung
- Secure-Web, CLI, API
- Massenimport digitaler Zertifikate und kryptographischer Schlüssel
- Bewertungen zum Import
- Extrahiert Basis-Attribute von hochgeladenen Zertifikaten und Schlüsseln für die Berichterstellung
- von Befehlszeilenskripts
- Abruf und Entfernung

Schlüssel- und Zertifikatsformate für Suche, Warnmeldungen und Berichte
- Symmetrische Algorithmen für kryptografische Schlüssel: 3DES, AES128, AES256, ARIA128, ARIA256
- Asymmetrisch Algorithmen für kryptografische Schlüssel: RSA1024, RSA2048, RSA4096
- Digitale Zertifikate (X.509): DER, PEM, PKCS#7, PKCS#8, PKCS#12

Drittanbieter-Verschlüsselung
- Microsoft SQL TDE, Oracle TDE, IBM Security Guardium Data Encryption, KMIP-Clients
- Beispiele für Partner: Nutanix, Linoma, NetApp, Cisco, MongoDB, DataStax, Huawei

API-Unterstützung
- PKCS#11, Microsoft Extensible Key Management OASIS KMIP

Schlüsselverfügbarkeit und Redundanz
- Sichere Replizierung von Schlüsseln über mehrere Geräte mit automatisierten Sicherungskopien

VORMETRIC KEY MANAGEMENT ALS DIENST FÜR DIE CLOUD

Für die meisten Unternehmen sind heute Cloud-Bereitstellungsmodelle zum Standard für eine breite Palette an Anwendungen geworden. Für zahlreiche Unternehmen, insbesondere diejenigen in hoch regulierten Branchen, wird der Einsatz von Verschlüsselung und Schlüsselverwaltung in zunehmendem Maße alltäglich. Mit der kontinuierlichen Zunahme der Verschlüsselung steigt auch die Anzahl der Schlüssel – und damit wächst auch das potenzielle Risiko, falls nicht ständig eine effektive Schlüsselüberwachung eingesetzt wird. Vormetric Key Management als Dienst (KMaaS) für die Cloud verleiht Ihrem Unternehmen die strikte Kontrolle über kryptographische Schlüssel und Richtlinien, so dass Sie Cloud-Dienste bei einem gleichzeitigen Mindestmaß an Komplexität und Risiko umfassend nutzen können.

OPTIMIERTE SCHLÜSSELVERWALTUNG FÜR CLOUD-DIENSTE

Für eine zuverlässige Einhaltung der relevanten behördlichen Auflagen und Sicherheitsrichtlinien müssen die Unternehmen über eine strenge, unabhängige Überwachung Ihrer kryptographische Schlüssel verfügen. Viele Cloud-Anbieter erleichtern diesen Ansatz durch das Angebot von BYOK-Diensten. Mithilfe dieses Ansatzes können die Unternehmen Cloud-Dienste nutzen und zugleich zur Erfüllung der Unternehmens- und Prüfanforderungen für eine Trennung von Aufgaben, Compliance-Reporting und Lebenszyklusverwaltung sorgen.

Vormetric KMaaS bietet robuste, konforme Lösungen für die Schlüsselüberwachung, die sich in die BYOK-Dienste von Cloud-Anbietern integrieren lassen. KMaaS kann zur Unterstützung Ihrer geschäftlichen Anforderungen in der Cloud oder an Ihren Standorten eingerichtet werden. Bei beiden Implementierungen bietet diese Lösung eine intuitive, benutzerfreundliche Schnittstelle mit einfacher Implementierung und sofortiger Skalierbarkeit. Vormetric KMaaS nutzt die von Cloud-Anbietern bereitgestellten BYOK-APIs und erlaubt damit die volle Kontrolle über den Schlüsselverwaltungslebenszyklus, einschließlich Schlüsselerzeugung, Hochladen, Aktualisieren, Speichern, Aufheben und Berichterstellung.

AM STANDORT ODER IN DER CLOUD: ES IST IHRE ENTSCHEIDUNG

Flexible Implementierungsmodelle versetzen die Unternehmen in die Lage, ihre eigenen speziellen Anforderungen zu erfüllen. Vormetric KMaaS bietet folgende Optionen:

- **Cloud-Dienst.** Mit dieser Option profitieren Sie von den Vorteilen einer auf FIPS 140-2 Level 1 basierenden Lösung in der Cloud und erhalten gleichzeitig eine optimale Kontrollmöglichkeit. Diese Bereitstellung „als Dienst" bedeutet, dass es nicht erforderlich ist, eine hoch verfügbare Schlüsselverwaltungslösung für den Standort zu konzipieren, zu implementieren und zu warten.
- **On-Premise-Dienst.** Wenn Ihr Unternehmen eine regulierte Kontrolle ihrer Schlüssel am Standort benötigt, so ist dies die optimale Lösung. Mit diesem Dienst können Sie Schlüssel in FIPS 140-2 Level 3 zertifizierten Hardwaregeräten an Ihren Standorten speichern und gleichzeitig ein abonnementbasiertes, nutzungsorientiertes Preisgestaltungsmodell nutzen.

HAUPTVORTEILE

- Robuste, konsistente Kontrolle und Transparenz zur Überwachung von Daten in Cloud-Umgebungen
- Effiziente Erfüllung von Compliance-Anforderungen von Prüfern und Regulierungsbehörden
- Erhebliche Reduzierung von Kosten und Aufwand bei der Implementierung und Ausführung einer Schlüsselverwaltung

HAUPTMERKMALE

- Schlüsselspeicher und Datenbestände getrennt
- Umfassende, granulare Prüfprotokolle für kryptografische Schlüssel und Zertifikatsverwaltungsaktivitäten
- Erzeugung und Modifizierung von Schlüsseln und Richtlinien auf Knopfdruck
- Benutzerfreundliches Portal für die Lebenszyklusverwaltung von Schlüsseln

TECHNISCHE DATEN

- Unterstützte SaaS-Anbieter: Salesforce
- Anforderung: Salesforce-Plattformverschlüsselung
- FIPS 140-2 Level 3 Vorort-Service
- FIPS 140-2 Level 1 SaaS
- OAuth Federation Salesforce-Integration



VORMETRIC CLOUD ENCRYPTION GATEWAY

Mit dem Vormetric Cloud Encryption Gateway können Sie Dateien in Cloud-Speicherumgebungen wie Amazon Simple Storage Service (Amazon S3) und anderen mit S3 kompatiblen Objektspeicherdiensten schützen. Mit dem Cloud Encryption Gateway lassen sich sensible Daten verschlüsseln, bevor sie in der Cloud-Umgebung gespeichert werden, so dass Sicherheitsteams die Kontrolle über die kryptographischen Schlüssel haben. Die Lösung bietet die Transparenz und Kontrolle, die Sie für den Schutz sensibler Daten vor zahlreichen Bedrohungen benötigen. Das Cloud Encryption Gateway nutzt den Vormetric Data Security Manager zur Schlüssel- und Richtlinienverwaltung.

STARKE KONTROLLFUNKTIONEN FÜR IN DER CLOUD GESPEICHERTE DATEN

Das Vormetric Cloud Encryption Gateway wird als virtuelle Appliance bereitgestellt, die in der Cloud oder in Ihrem Rechenzentrum implementiert werden kann. Bei beiden Lösungen hat Ihr Sicherheitsteam stets die volle Kontrolle über die kryptographischen Schlüssel. Das Cloud Encryption Gateway bietet die folgenden Vorteile:

- **Transparente, unkomplizierte Implementierung.** Bietet transparente Verschlüsselung und Entschlüsselung von Dateien durch das Abfangen von Datenverkehr zwischen Benutzern und der Cloud.
- **Starke Schlüsselverwaltung.** Ermöglicht Ihnen zu jedem Zeitpunkt eine granulare, prüfbare Kontrolle von Richtlinien und Schlüsseln.
- **Detaillierte Übersicht und Prüffähigkeit.** Generiert Prüfprotokolle, die einen detaillierten Einblick in Datenzugriffsaktivitäten erlauben und somit eine wertvolle Unterstützung für das Compliance-Reporting und forensische Maßnahmen bieten.
- **Intelligente Risikoerkennung.** Überwacht Amazon S3 und andere Cloud-Speicherumgebungen, die mit S3-APIs kompatibel sind. Erkennt unverschlüsselte Dateien, die gegen Sicherheitsrichtlinien verstoßen, und verschlüsselt sie automatisch.

HAUPTMERKMALE

- Transparente Implementierung
- Robuste Schlüsselverwaltung und Verschlüsselung
- Erweiterbare Architektur ermöglicht horizontale, kosteneffiziente Skalierbarkeit
- Wirksame Cloud-Speichersicherheit und Compliance-Kontrollen

TECHNISCHE DATEN

Virtual Appliance

- Open Virtualization Format (.ovf)
- Verteilung Hardware-Mindestanforderungen: 4 CPU-Cores, 4 G RAM
- Festplatten-Mindestanforderungen: 100 GB

Unterstützte Dienste

- Amazon S3
- Caringo Object Storage
- KMaaS for Salesforce

Authentifizierungsintegration

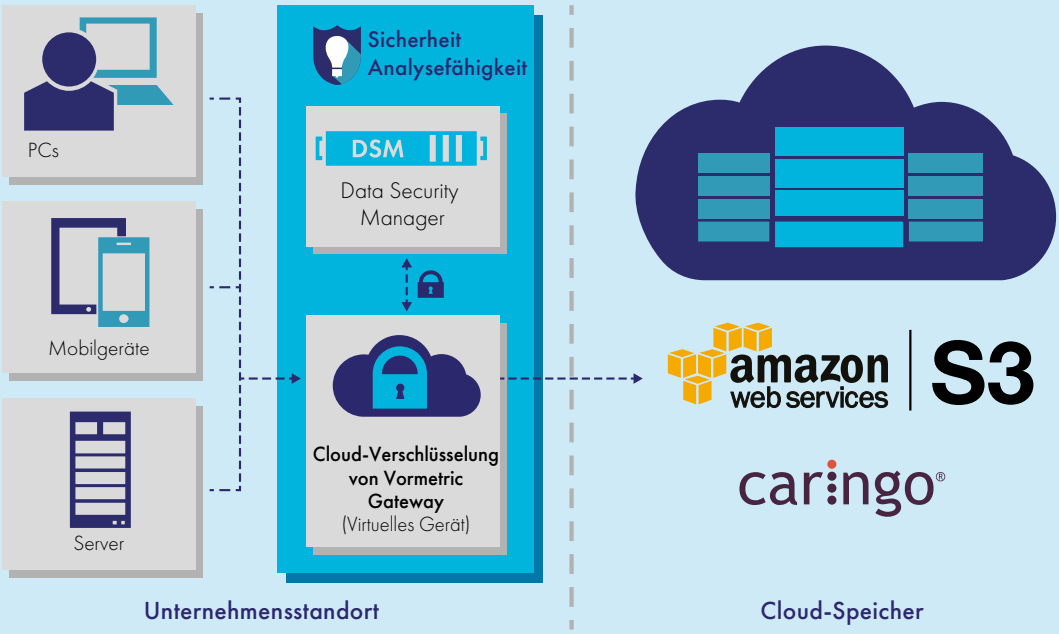
- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD) – nur Amazon S3

Richtlinien

- Verschlüsselung nach Dateityp
- Automatische Schlüsselrotation

MongoDB-Version

- 2.6.9 oder höher



SCHUTZ VON VORMETRIC FÜR TERADATA-DATENBANKEN

Durch das Sammeln umfangreicher Volumen an Unternehmensdaten in Teradata-Umgebungen sind Unternehmen in der Lage, Erkenntnisse und strategische Werte in bisher beispielloser Weise abzuschöpfen. Diese Datenaggregierung kann jedoch auch nie zuvor dagewesene Risiken in sich bergen. Ohne ordnungsgemäße Schutzfunktionen können die in diesen Umgebungen angehäuften sensiblen Daten unabsichtlich durch privilegierte Administratoren enthüllt oder von böswilligen Insidern und externen Angreifer gestohlen werden. Dank Vormetric kann sich Ihr Unternehmen nun vor diesen Risiken schützen. Vormetric Protection for Teradata Database ermöglicht eine schnelle und effiziente Implementierung robuster Sicherheitsfunktionen für „Data at Rest" in Ihren Teradata-Umgebungen.

HÖHERE SICHERHEIT BEI WENIGER UNTERBRECHUNGEN UND NIEDRIGEREN KOSTEN

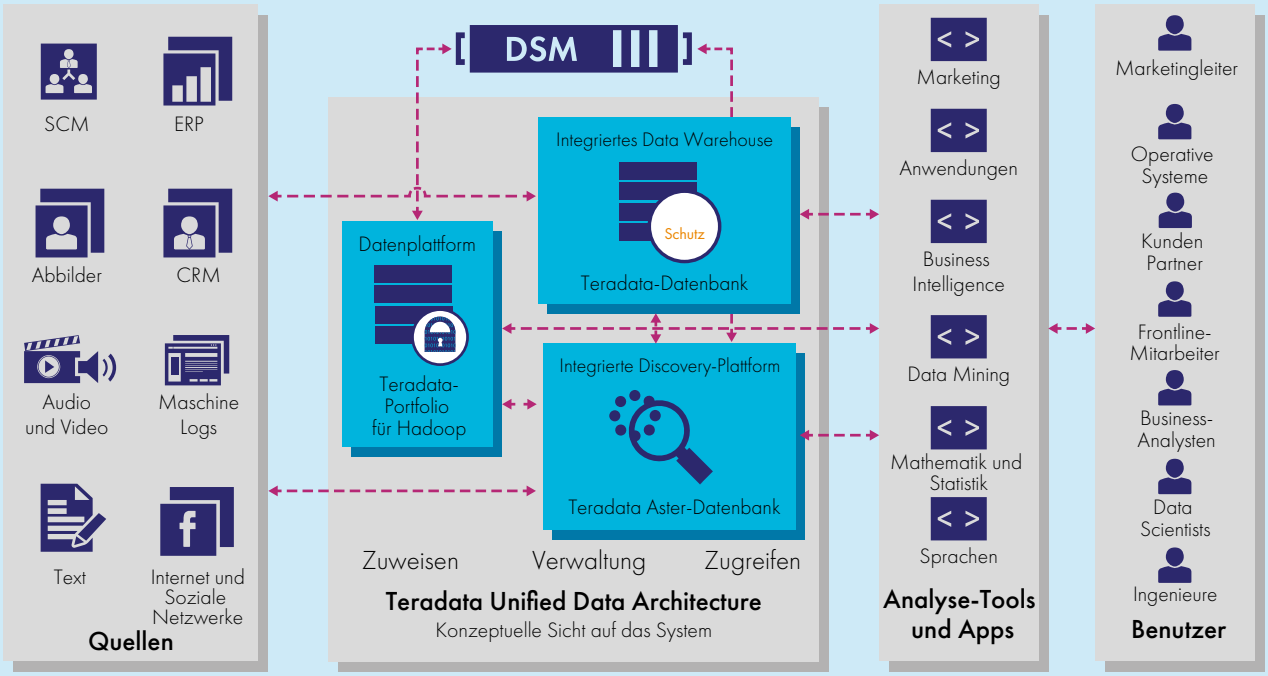
Die Vormetric Protection for Teradata Datenbank vereinfacht den Schutz vertraulicher Datensätze und ermöglicht die Verschlüsselung bestimmter Felder und Spalten in Teradata-Datenbanken. Die Lösung bietet außerdem NIST-zugelassene, formaterhaltende Verschlüsselungsfunktionen (FPE) zur Verschlüsselung sensibler Datensätze, ohne dass deren Format oder Feldschemata geändert werden müssen. Sie minimiert nicht nur die möglichen Auswirkungen der Verschlüsselung auf zugehörige Anwendungen und Workflows, sondern trägt auch dazu bei, die wachsenden Speicheranforderungen im Zusammenhang mit herkömmlichen Verschlüsselungskonzepten zu vermeiden.

HAUPTVORTEILE

- Zentralisierte und optimierte „Data-at-Rest"-Verschlüsselung und Schlüsselverwaltung
- Erhöhte Sicherheit ohne Beeinträchtigung des Werts von Big-Data-Analysen
- Schutz gegen Cyber-Angriffe und Missbrauch durch privilegierte Benutzer
- Schnelle Implementierung

HAUPTMERKMALE

- Einsatz granularer Kontrollen, die dem Administrator die Durchführung operativer Tätigkeiten ohne Zugriff auf vertrauliche Klartextdaten erlauben
- Hohe Leistungsfähigkeit, Skalierung mit der Anzahl der Teradata-Knoten
- Nutzung von FPE minimiert wachsenden Speicherbedarf und Beeinträchtigung durch die Verschlüsselung
- Mühelose Integration von benutzerdefinierten Funktionen (UDFs) für die Verschlüsselung/ Entschlüsselung in bestehenden SQL-Code
- Verwendungsmöglichkeit verschiedener Schlüssel für verschiedene Spalten durch Kunden
- Unterstützung von ASCII-Text und Unicode, dadurch flexible Sprach- und Technologieunterstützung Zertifizierte Teradata-Verschlüsselungslösung
- Certified Teradata encryption solution



OPTIMIERTE VERSCHLÜSSELUNGSIMPLEMENTIERUNG UND -VERWENDUNG

Die Lösung reduziert die Komplexität für Entwickler, indem sie dokumentierte, standardbasierte Anwendungsprogrammierschnittstellen (APIs) und benutzerdefinierte Funktionen (UDFs) bereitstellt, die für kryptographische und Schlüsselverwaltungsabläufe eingesetzt werden können. Mit der Lösung können Teradata-Benutzer ganz leicht ihre eigenen Profile (einschließlich Auswahl aus Standard-AEs-Verschlüsselung und FPE) zum Senden von Verschlüsselungs- und Entschlüsselungsanforderungen konfigurieren.

ZENTRALISIERTE SCHLÜSSEL- UND RICHTLINIENVERWALTUNG

Vormetric Protection for Teradata Database arbeitet nahtlos mit dem Vormetric Data Security Manager (DSM) zusammen, einer gemäß FIPS zertifizierten Appliance zur Schlüsselverwaltung und -speicherung. Der DSM erlaubt Ihnen eine zentrale Schlüsselverwaltung und den Zugriff auf Richtlinien für Vormetric Protection for Teradata Database, auf andere Lösungen der Vormetric Data Security Platform sowie auf Verschlüsselungsprodukte von Drittanbietern. Mit dem DSM können Sie Schlüssel und Richtlinien für Vormetric Transparent Encryption verwalten. Dieses Produkt kann dafür verwendet werden, Ihr Teradata-Gerät für Hadoop zu schützen..

TECHNISCHE DATEN

Unterstützte Plattformen:

- Teradata-Datenbankversionen 14.0, 14.10, 15.0 und 15.10

Betriebssysteme:

- SUSE Linux Enterprise Server (SLES), Versionen 10 oder 11

Maximale Spaltenbreiten:

- ASCII: 16 KB
- Unicode UDFs: 8KB



VORMETRIC SECURITY INTELLIGENCE

Vormetric Security Intelligence generiert detaillierte, ausführbare Sicherheitsereignis-Protokolle, die einen einzigartigen Einblick in die Dateizugriffsaktivitäten liefern. Mit dieser Lösung kann Ihr Unternehmen unverzüglich Warnmeldungen nutzen, welche eine automatisierte Eskalation und Reaktion auslösen. Diese Protokolle lassen sich auf unkomplizierte Weise in SIEM-Systeme integrieren, und Sie können verdächtige Aktivitäten effizient nachverfolgen und untersuchen und Compliance- und Sicherheitsberichte erstellen.

GRANULARE, UMSETZBARE SICHERHEITSINTELLIGENZ

Früher basierten SIEMs auf Protokollen von Firewalls, IPS und NetFlow-Geräten. Da diese Erkenntnisse auf Netzwerkebene erfasst werden, können solche Systeme enorme Datenvolumen generieren, was die Ermittlung der wirklich wichtigen Ereignisse für Administratoren zu einer echten Herausforderung macht. Darüber hinaus weisen diese Systeme einen Schwachpunkt auf, der häufig ausgenutzt wird: Sie bieten keinerlei Einblick in Datenzugriffsversuche und Ereignisse, die auf Servern auftreten. Vormetric Security Intelligence beseitigt diesen Schwachpunkt und liefert zielgerichtete, kritische Erkenntnisse hinsichtlich Dateizugriffsaktivitäten. Als Folge trägt die Lösung dazu bei, die Bedrohung zu eliminieren, dass ein nicht autorisiertes oder kompromittiertes Benutzerkonto heimlich Zugriff auf vertrauliche Daten erlangt.

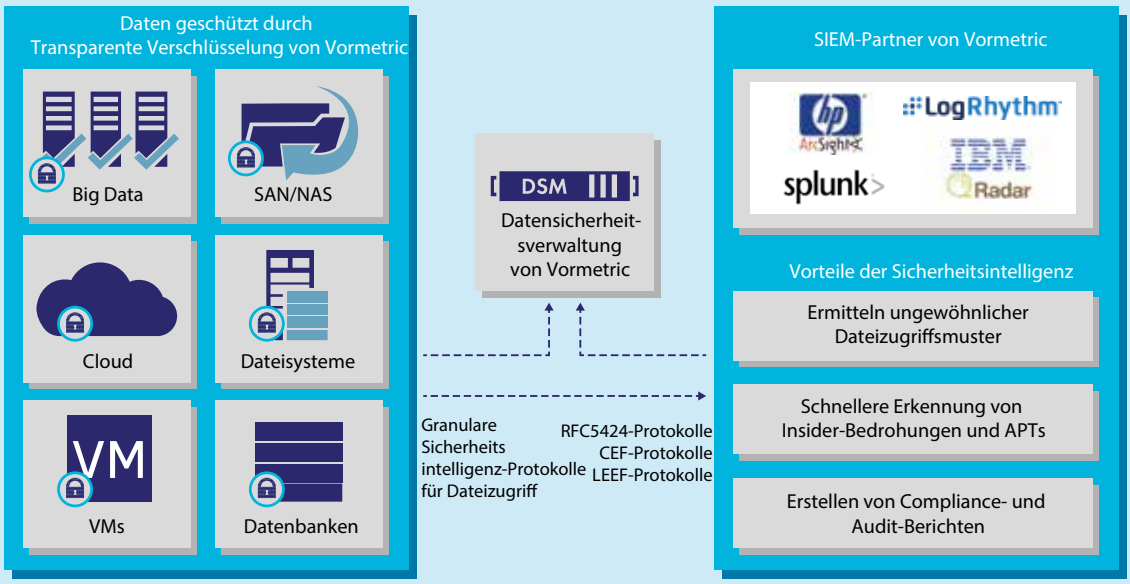
Die Vormetric Security Intelligence Protokolle bilden einen Audit-Trail gewährter und verweigerter Zugriffsversuche durch Benutzer und Prozesse. Die detaillierten Protokolle der Lösung können dahingehend überprüft werden, wann Benutzer und Prozesse auf Daten gemäß welchen Richtlinien zugegriffen haben und ob Zugriffsanforderungen zugelassen oder abgelehnt wurden. Diese Protokolle können effizient mit Ihrer SIEM-Plattform ausgetauscht werden, wodurch irreguläre Prozesse und Benutzerzugriffsmuster, die weitere Untersuchungen erfordern, aufgedeckt werden können. Beispiel: Ein Administrator oder ein Prozess greift plötzlich auf viel größere Datenvolumen als normalerweise zu oder versucht, einen nicht autorisierten Download von Dateien durchzuführen. Ein solches inkonsistentes Nutzungsmuster könnte ein Hinweis auf einen APT-Angriff oder auf böswillige Insider-Aktivitäten sein.

UMSETZBARE PROTOKOLLE, DIE EINE SCHNELLE REAKTION AUSLÖSEN

Die Vormetric Security Intelligence Protokolle liefern sofortige Erkenntnisse, die sich in das Zentrum für Sicherheitsabläufe Ihres Unternehmens – einschließlich möglicherweise vorhandener Workflows und automatisierter Skripts – einspeisen lassen. So können Sie dank Vormetric Security Intelligence sicherstellen, dass Risiken erkannt, kommuniziert und auf schnellste und effizienteste Weise beseitigt werden.

OPTIMIERUNG VON AUDITING UND COMPLIANCE

Um die zahlreichen behördlichen Auflagen und Vorschriften einhalten zu können, müssen Organisationen den Nachweis erbringen, dass ein Datenschutz implementiert und einsatzbereit ist. Vormetric Security Intelligence dient u. a. dazu, einem Prüfer die Wirksamkeit der Verschlüsselung, Schlüsselverwaltung und Zugriffsrichtlinien nachzuweisen. Der detaillierte Einblick und die Integrationsfunktionen von Vormetric Security Intelligence tragen dazu bei, die Maßnahmen für Audits und kontinuierliches Compliance-Reporting zu optimieren.



HAUPTMERKMALE

- Detaillierterer Einblick in Zugriffe auf vertrauliche
- Daten Sofortige Warnmeldungen können eine schnelle automatisierte
- automatisierte Reaktion auslösen Schnellere Erkennung von APT- und Insider-Bedrohungen
- Export von Protokollen in die gängigsten Protokollformate: Syslog RFC5424, CEF und LEEF
- Schnelle Integration mit Vormetric SIEM Partnern
- Konsolidierte und konsistente Compliance- und Audit-Berichterstellung

TECHNISCHE DATEN

SIEM Partner Integration

- FireEye Threat Prevention Platform
- HP ArcSight
- IBM Security QRadar SIEM
- Informatica Secure@Source
- McAfee ESM
- LogRhythm Security Intelligence Platform
- SolarWinds
- Splunk



VORMETRIC ORCHESTRATOR

Der Vormetric Orchestrator automatisiert die Implementierung, Konfiguration, Verwaltung und Überwachung von Produkten der Vormetric Data Security Platform. Mithilfe dieser Funktionen können Organisationen ihre Implementierungen in Unternehmensrechenzentren und hybriden Cloud-Umgebungen skalieren und gleichzeitig den Verwaltungsaufwand und die Gesamtbetriebskosten drastisch reduzieren.

AUTOMATISIERUNG FÖRDERT SKALIERBARE, EFFIZIENTE ABLÄUFE

Für große Unternehmen und Cloud-Service Provider stellt der Wandel die einzige Konstante dar: Änderungen bei Betriebssystemen, Workloads, Datenbanken und Netzwerkkonfigurationen. Der Vormetric Orchestrator bietet die Automatisierung, die Sie benötigen, um mit diesen Änderungen Schritt zu halten. Durch die Automatisierung von sich wiederholenden Aufgaben vereinfacht der Vormetric Orchestrator Abläufe, hilft bei der Beseitigung von Fehlern und beschleunigt Implementierungen. Die Lösung reduziert den Bedarf an Personalressourcen für die Wartung und Erweiterung von Verschlüsselungsimplementierungen, so dass sich Ihre Teams auf dringendere Aufgaben und strategische Prioritäten konzentrieren können. Der Vormetric Orchestrator bietet folgende Vorteile:

- **Höhere betriebliche Effizienz dank Automatisierung.** Die Lösung ermöglicht eine automatische Implementierung und Wartung von Produkten der Vormetric Data Security Platform. So vereinfacht sie beispielsweise bei einem geschäftskritischen Betriebssystem-Patch das Einrichten der Aufgabe, die den Orchestrator anweist, automatisch Hunderte von Servern mit einer neuen Version des Vormetric Transparent Encryption Agent zu aktualisieren.
- **Effiziente Integration in Ihre Umgebung.** Die Lösung zeichnet sich durch eine Plug-In-Architektur aus, welche die schnelle Integration in zahlreiche Konfigurationsmanagement-Lösungen ermöglicht, einschließlich eigener Tools und gängiger Lösungen wie Chef. Der Vormetric Orchestrator bietet einen Zugriff sowohl auf RESTful API als auch auf CLI und lässt sich problemlos in Ihre bestehenden IT-Automatisierungssysteme oder in Ihre interne Skripterstellung integrieren.
- **Flexible Implementierungsoptionen.** Flexible Implementierungsoptionen. Der Vormetric Orchestrator ist als virtuelle Appliance für Mainstream-Virtualisierung und öffentliche Cloud-Plattformen erhältlich. Nach der Installation in Ihrem Rechenzentrum kann die Lösung Produkte der Vormetric Data Security Platform in Remote-Rechenzentren, privaten Cloud-Umgebungen und öffentlichen Clouds verwalten.

HAUPTVORTEILE

- Automatisierung beschleunigt Implementierungen und steigert die betriebliche Effizienz
- Skalierbare Verschlüsselung bei gleichzeitiger Senkung der Gesamtbetriebskosten
- Erweiterte Verschlüsselungsmöglichkeiten dank breiter Umgebungsunterstützung

TECHNISCHE DATEN

Virtual Appliance

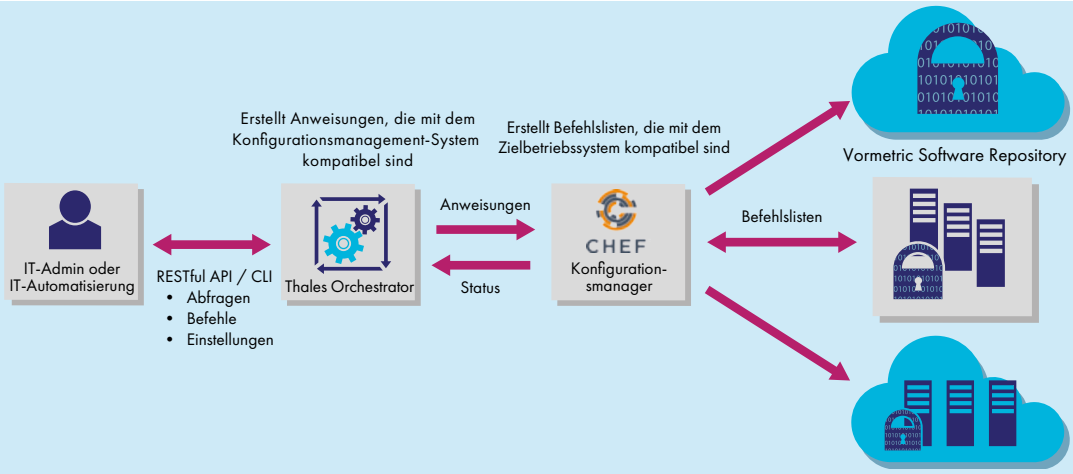
- Open Virtualization Format (.OVF) Verteilung Speicher-
  - Mindestanforderungen: 4 GB
  - CPU-Anforderungen: 4 virtuelle CPUs
- Amazon Web Services Amazon Machine Image (AMI)

Unterstützung Konfigurations-Manager

- Chef (mehrere Chef-Server zugelassen)

Automatisierungsunterstützung

- Vormetric Transparent Encryption Agenten
  - Agenten-Installation
  - Agenten-Registrierungsmechanismen
    - Shared Secret
    - Aktualisierungen
  - Fingerabdruck-Agent
- Vormetric Data Security Manager Konfiguration



THALES

www.thalesesecurity.com

Informationen zu Thales e-Security

Thales e-Security ist führender Anbieter von fortschrittlichen Datensicherheitslösungen und -services, die überall dort Vertrauen schaffen, wo Daten erstellt, geteilt oder gespeichert werden. Wir stellen sicher, dass die Daten, die Unternehmen und Regierungsbehörden gehören, sowohl gesichert als auch vertraulich behandelt werden, und zwar im Unternehmen selbst, in der Cloud, in Rechenzentren oder Big-Data-Umgebungen, ohne dabei die Unternehmensprozesse einzuschränken. Sicherheit reduziert nicht nur Risiken, sie ist ein Wegbereiter für digitale Initiativen, die mittlerweile unser tägliches Leben durchdringen, wie bei digitalem Geld, bei elektronischen Identitäten, beim Gesundheitswesen, bei vernetzten Fahrzeugen und mit dem Internet der Dinge (IoT) sogar bei Haushaltsgeräten. Thales bietet alles, was eine Organisation benötigt, um Daten, Identitäten und geistiges Eigentum zu schützen und zu verwalten, sowie regulatorische Konformität herzustellen. Unsere Instrumente hierfür sind Verschlüsselung, erweiterte Schlüsselverwaltung, Tokenisierung, Kontrolle privilegierter Benutzer und Hochsicherheitslösungen. Sicherheitsexperten auf der ganzen Welt verlassen sich auf Thales, wenn es darum geht, die digitale Transformation ihrer Organisation zu beschleunigen. Thales e-Security ist Teil der Thales Group.

Folgen Sie uns auf:

Amerika – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 oder +1 954 888 6200 • Fax: +1 954 888 6211 • E-Mail: sales@thalesesec.com
Asien-Pazifik-Raum – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-Mail: asia.sales@thales-esecurity.com
Europa, Naher Osten, Afrika – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-Mail: emea.sales@thales-esecurity.com

© Thales - April 2017 • PLB62722