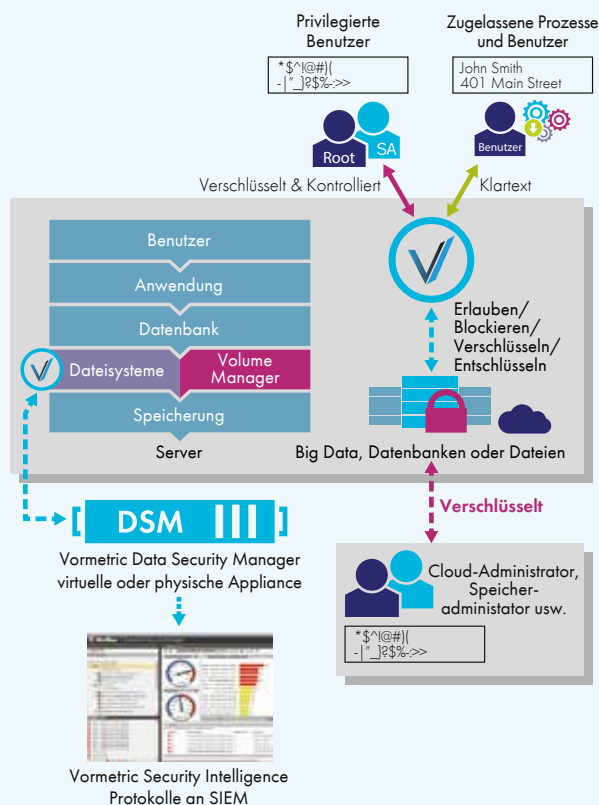


SICHERN SIE SENSIBLE DATA-AT-REST DORT, WO SIE SICH BEFINDEN

- Halten Sie Sicherheitsvorschriften für Data-at-Rest ein, indem Sie Dateien, Laufwerke und mit diesen verbundene Cloud-Speicher durch Verschlüsselung, Zugriffskontrolle und Audit-Protokollierung für Datenzugriff dort sichern, wo sie sich befinden – in mehreren Clouds, vor Ort und in System-, Big-Data- sowie Containerumgebungen
- Vereinfachen Sie die Datensicherheitsadministration durch zentrale Schlüsselverwaltung, Verschlüsselung und Zugriffsrichtlinien für alle Umgebungen in der Cloud und im Rechenzentrum
- Schützen Sie bestehende und neue Datensätze schnell vor Datenschutzverletzungen, ohne dass sich dies auf Anwendungen, Benutzer oder Arbeitsabläufe auswirkt
- Setzen Sie mühelos die Kontrolle von privilegierten Benutzerzugriffen um, die es Administratoren ermöglicht, wie gewohnt zu arbeiten, ohne jemals sensiblen Daten ausgesetzt zu sein
- Minimieren Sie Ausfallzeiten für Bereitstellung und Wartung, indem Sie die Verschlüsselung und Neuausstellung von Schlüsseln durchführen, während Daten verwendet werden

«Thales eSecurity»

VORMETRIC TRANSPARENT ENCRYPTION VON THALES



Vormetric Transparent Encryption verschlüsselt, setzt Zugriffsrichtlinien um und protokolliert alle Zugriffe auf Dateien, Festplatten und verbundene Cloud-Speicher.

HERAUSFORDERUNG: MEHR DATEN IN MEHR UMGEBUNGEN VOR MEHR BEDROHUNGEN SCHÜTZEN

Zur Sicherung sensibler Daten gehört viel mehr, als nur die Datenbanken und Dateien im Rechenzentrum vor Ort zu sichern. Das typische Unternehmen von heute nutzt drei oder mehr IaaS- oder PaaS-Anbieter sowie fünfzig oder mehr SaaS-Anwendungen, Big-Data-Umgebungen und Container-Technologien sowie seine eigenen internen virtuellen Anwendungen und privaten Clouds.

Noch komplizierter wird es durch die Tatsache, dass Cyber-Angriffe immer raffinierter und gefährlicher und Compliance-Anforderungen sowie gesetzliche Vorschriften rund um den Schutz sensibler Daten immer strenger werden.

LÖSUNG: VORMETRIC TRANSPARENT ENCRYPTION

Vormetric Transparent Encryption bietet Data-at-Rest-Verschlüsselung mit zentraler Schlüsselverwaltung, Kontrolle von privilegierten Benutzerzugriffen und detaillierter Audit-Protokollierung für Datenzugriff, die Unternehmen dabei unterstützen, die Anforderung an Compliance-Berichterstattung und Best Practices für die Sicherung von Daten an dem Ort, an dem sie sich befinden, zu erfüllen. Vormetric Transparent Encryption schützt strukturierte Datenbanken, unstrukturierte Dateien und damit verbundene Cloud-Speicher, auf die von Systemen vor Ort, über mehrere Cloud-Umgebungen und sogar innerhalb von Big-Data- und Container-Implementierungen zugegriffen wird. Die Lösung erfüllt bei minimalem Aufwand und zu minimalen Kosten Datensicherheitsanforderungen. Dabei kommt es zu so gut wie keinen Unterbrechungen und die Implementierung erfolgt nahtlos – sowohl Geschäfts- als auch Betriebsprozesse können während der Bereitstellung und Einführung unverändert weiterlaufen.

VORMETRIC TRANSPARENT ENCRYPTION VON THALES

WICHTIGSTE VORTEILE

- **Kontinuierlicher Schutz.** Richtlinien, die vor nicht autorisiertem Zugriff durch Benutzer und Prozesse schützen, werden fortlaufend umgesetzt und für alle Aktivitäten werden detaillierte Audit-Protokollierungen für Datenzugriff erstellt.
- **Granulare Kontrollen.** Wenden Sie granulare Benutzerzugriffsberechtigungen mit geringsten Privilegien an, die Daten vor externen Angriffen und Missbrauch durch privilegierte Benutzer schützen. Benutzer und Gruppen können bestimmte Richtlinien von Systemen, LDAP/Active Directory, Hadoop und Containern anwenden. Zu den Kontrollen gehören auch Zugriff nach Prozess, Dateityp, Tageszeit und sonstigen Kennzahlen.
- **Sicherheitsintelligenz.** Dank detaillierter Audit-Protokollierungen für Datenzugriff, die nicht nur die Anforderungen an Compliance- und forensische Berichterstattung erfüllen, sondern auch Datensicherheitsanalysen durch gängige Systeme zur Verwaltung von Sicherheitsdaten und Ereignissen (Security Information and Event Management – SIEM) ermöglichen, können Bedrohungen schneller identifiziert und gestoppt werden.
- **Nicht eingreifend und einfach bereitzustellen.** Die Verschlüsselungsagenten für Vormetric Transparent Encryption werden auf Servern auf Dateisystem- oder Laufwerksebene bereitgestellt und unterstützen sowohl lokale Festplatten als auch Cloud-Speicherumgebungen wie Amazon S3 und Azure Files. So ist Verschlüsselung und Zugriffskontrolle möglich, ohne dass Anwendungen, Infrastruktur, Systemmanagementaufgaben oder Unternehmenspraktiken geändert werden müssen.
- **Leistungsstarke Verschlüsselung.** Vormetric Transparent Encryption nutzt ausschließlich starke, standardbasierte Verschlüsselungsprotokolle wie Advanced Encryption Standard (AES) zur Datenverschlüsselung und elliptische Kurvenkryptographie (ECC) für den Schlüsselwechsel. Der Agent ist gemäß FIPS 140-2 Level 1 validiert.
- **Umfassende Speicherungsunterstützung.** Unterstützt lokale und Netzwerk-Dateisysteme unter Windows, Linux und UNIX sowie Speicheroptionen von Amazon S3 und Azure Files vor Ort oder in Cloud-Umgebungen.
- **Systemunterstützung.** Der Agent ist für eine breite Auswahl an Windows-, Linux- und UNIX-Plattformen erhältlich und kann in physischen, virtuellen sowie Cloud-, Container- und Big-Data-Umgebungen genutzt werden – unabhängig von der zugrunde liegenden Speichertechnologie. Agenten können sowohl lokal vor Ort als auch in mehreren Cloud-Umgebungen bereitgestellt werden. Dieses Agent-basierte Bereitstellungsmodell beseitigt die Engpässe und Latenzen, die ältere Proxy-basierte Verschlüsselungslösungen plagen.
- **Hardware-beschleunigte Verschlüsselung.** Durch Verwendung der AES-Hardware-Verschlüsselungsfunktionen moderner CPUs (Intel AES-NI, AMD AES-NI, IBM-Power8-Verschlüsselung und Oracle-SPARC-Verschlüsselung) wird der Mehraufwand für die Verschlüsselung minimiert und eine Verschlüsselung mit optimaler Leistung auch in virtuellen und Cloud-Umgebungen ermöglicht.

ERWEITERTE SICHERHEIT

- **Datentransformation ohne Ausfallzeiten** Fügen Sie die Option Live Data Transformation hinzu, um die für die anfängliche Verschlüsselung und geplante Neuinstallation von Schlüsseln erforderlichen Ausfallzeiten zu verkürzen. Mithilfe dieser Option arbeiten Anwendungen und Dienste nach der Installation von Vormetric Transparent Encryption auf dem Server während der Verschlüsselung von Daten und der entsprechenden Neuinstallation von Schlüsseln normal weiter.
- **Container-Unterstützung.** Vormetric Container Security erweitert richtlinienorientierte Verschlüsselung auf Dateiebene, Zugriffskontrolle und Audit-Protokollierung für Datenzugriff von Vormetric Transparent Encryption auf Container-Umgebungen. Die Lösung ermöglicht Verschlüsselung auf Dateiebene und Zugriffskontrollen für Container-Benutzerrollen und Daten, die in Container-Images gespeichert werden oder auf die über Container-Images zugegriffen wird.
- **Automatische Bereitstellung und Wartung.** Vormetric Orchestrator automatisiert die Bereitstellung, Konfiguration, das Management und die Überwachung von Vormetric-Transparent-Encryption-Bereitstellungen und unterstützt dabei Operationen zu vereinfachen, Fehler zu beseitigen und Bereitstellungen zu beschleunigen.
- **Erweiterte Zugriffskontrollen für Big Data (Hadoop).** Bei der Implementierung in Hadoop-Umgebungen werden Zugriffskontrollen auf Hadoop-Benutzer und -Gruppen erweitert.
- **SAP-HANA-geprüft und zugelassen.** SAP hat Vormetric Transparent Encryption geprüft und als für die Nutzung in SAP-Umgebungen geeignet zugelassen.

LÖSUNGSARCHITEKTUR

Bereitstellungen bestehen aus dem Vormetric Transparent Encryption Agenten und Vormetric Data Security Manager (DSM) Geräten. Agenten werden auf Servern in Rechenzentren sowie Cloud-, Container- oder Big Data-Umgebungen bereitgestellt. Die Richtlinien- und Schlüsselverwaltung erfolgt zentral im DSM. Das DSM ist als nach FIPS 140-2 Level, 2 oder 3 zertifiziertes Gerät erhältlich und verfügt über RESTful-, SOAP- und Command-Line-APIs sowie web-basierte Verwaltungsoberflächen.

ERFÜLLEN SIE ALLE DATENSCHUTZANFORDERUNGEN

Thales eSecurity vereinfacht das Sichern von Data-at-Rest durch umfangreiche, auf der Vormetric Data Security Plattform erhältliche Datensicherheitslösungen. Dazu gehören **Vormetric Tokenisierung mit dynamischer Datenmaskierung**, **Vormetric Application Encryption** und **CipherTrust Cloud Key Manager**.

WEITERE INFORMATIONEN

Besuchen Sie uns unter www.thalesecurity.com und erfahren Sie, wie unsere erweiterten Datensicherheitslösungen überall dort Vertrauen schaffen, wo Informationen erstellt, geteilt oder gespeichert werden.

