

Vormetric Transparent Encryption



Herausforderung: sensible Daten in einer Vielzahl wechselnder Umgebungen vor zunehmenden Bedrohungen schützen

Der Schutz sensibler Daten erfordert 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.

Erschwerend kommt hinzu, dass Cyber-Angriffe immer raffinierter und gefährlicher werden. Es gibt ständig neue Compliance-Vorschriften und regulatorische Bestimmungen zum Schutz sensibler Informationen, und bestehende Verordnungen wurden verschärft.

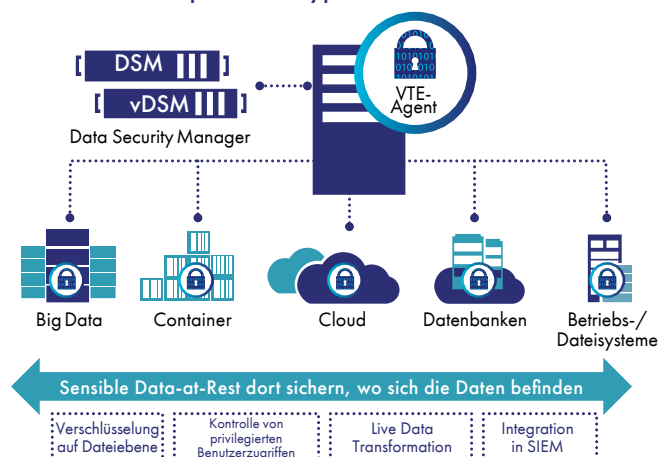
Lösung: Vormetric Transparent Encryption

Vormetric Transparent Encryption (VTE) bietet Data-at-Rest-Verschlüsselung mit zentraler Schlüsselverwaltung, Kontrolle von privilegierten Benutzerzugriffen und detaillierter Audit-Protokollierung für Datenzugriffe, die Unternehmen dabei unterstützen, die Anforderung an Compliance und Best Practices für die Sicherung von Daten, egal an welchem Ort sie sich befinden, zu erfüllen. Der nach FIPS 140-2 Level 1 validierte VTE-Agent befindet sich auf Dateisystem- oder Geräteebene, und die Verschlüsselung und Entschlüsselung ist für alle darüber laufenden Anwendungen transparent. VTE bietet umfangreiche Zugriffskontrollen, mit denen Unternehmen festlegen können, wer wann mit welchen Zugriffsrechten auf die Daten zugreifen darf.

Sichern Sie sensible Data-at-Rest dort, wo sich die Daten befinden

- Erfüllen Sie dank einer Hardware-beschleunigten Verschlüsselungslösung, die Dateien, Laufwerke und verbundene Cloud-Speicher sichert und gleichzeitig Zugriffskontrolle und Audit-Protokollierung für Datenzugriff in physischen, virtuellen und Cloud-Umgebungen ermöglicht, die entsprechenden Anforderungen an Compliance und Best Practices.
- Die skalierbare Lösung lässt sich einfach und schnell bereitstellen und bietet zentrale Schlüsselverwaltung, Verschlüsselungs- und Zugriffsrichtlinien für eine Vielzahl an Clouds, sowohl on-premises als auch in Big-Data- und Container-Umgebungen.
- Dank einfach einzurichtender Kontrollen von privilegierten Benutzerzugriffen können Administratoren wie gewohnt arbeiten, gleichzeitig jedoch Daten vor bestimmten Benutzern und Gruppen schützen, die eine potenzielle Bedrohung darstellen.

Vormetric Transparent Encryption



- Nutzen Sie detaillierte, aussagekräftige Sicherheitsereignisprotokolle, die beispiellosen Einblick in Datenzugriffsaktivitäten bieten, damit Sie Bedrohungen schneller erkennen und verhindern können.
- Umfangreichste Plattformentstützung der Branche. Schützt strukturierte und unstrukturierte Daten, auf die Linux-, UNIX- und Windowssysteme zugreifen, sowie Cloud-Speicherumgebungen wie Amazon S3 und Azure Files.
- Vermeiden Sie mit der Option Live Data Transformation Ausfallzeiten für die anfängliche Verschlüsselung und die Neuinstallation von Schlüsseln. Keine andere Datenverschlüsselungslösung bietet diese einzigartige Funktion.

Wichtigste Vorteile

Transparenter Datenschutz. Kontinuierliche Verschlüsselung auf Dateiebene schützt gegen nicht autorisierten Zugriff durch Benutzer und Prozesse und erstellt für alle Aktivitäten detaillierte Audit-Protokolle über den Datenzugriff, ohne dass Anwendungen, Infrastruktur, Systeme, Managementaufgaben oder Geschäftspraktiken geändert werden müssen.

Nahtlose und einfache Bereitstellung. Vormetric Transparent Encryption Agenten werden auf Servern auf Dateisystem- oder Laufwerksebene bereitgestellt und unterstützen sowohl lokale Festplatten als auch Cloud-Speicherumgebungen wie Amazon S3 und Azure Files.

Definieren Sie granulare Zugriffskontrollen. 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.

Leistungsstarke Hardware-beschleunigte Verschlüsselung. Vormetric Transparent Encryption nutzt ausschließlich starke, standardbasierte Verschlüsselungsprotokolle wie Advanced Encryption Standard (AES) zur Datenverschlüsselung und elliptische Kurvenkryptographie (ECC) für den Schlüsselaustausch. Durch die Nutzung der AES-Hardware-Verschlüsselungsfunktionen moderner CPUs wird der Verschlüsselungs-Overhead minimiert.

Umfassende Sicherheitsintelligenz. Dank detaillierter Audit-Protokollierungen für Datenzugriffe, die nicht nur die Compliance-Anforderungen erfüllen, sondern auch Datensicherheitsanalysen ermöglichen, können Bedrohungen schneller identifiziert und gestoppt werden. Großen Systemanbietern stehen vorab konfigurierte Integrationen und Dashboards zur Verfügung, mit denen abgelehnte Zugriffsversuche auf geschützte Daten entdeckt werden können.

Umfangreiche System- und Umgebungsunterstützung. 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.

Erweiterte Sicherheit

Datentransformation ohne Ausfallzeiten Die Option Live Data Transformation eliminiert die für die anfängliche Verschlüsselung und geplante Neuinstallation von Schlüsseln erforderlichen Ausfallzeiten. Diese patentierte Technologie ermöglicht es, Datenbanken oder Dateien zu verschlüsseln oder neue kryptographische Schlüssel auszustellen, während die Daten verwendet werden, ohne die Anwendungen offline setzen zu müssen.

Container-Unterstützung. Vormetric Container Security erweitert richtlinienorientierte Verschlüsselung auf Dateiebene, Zugriffskontrolle und Audit-Protokollierung für Datenzugriff auf Container-Umgebungen. Die Lösung ermöglicht die 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 sorgt für die einfache und skalierbare automatische Bereitstellung und Wartung von Vormetric Transparent Encryption.

Erweiterte Zugriffskontrollen für Big Data (Hadoop).

Bei der Implementierung in Hadoop-Umgebungen werden Zugriffskontrollen auf Hadoop-Benutzer und -Gruppen erweitert.

SAP HANA qualifiziert. SAP hat Vormetric Transparent Encryption zur Datenverschlüsselung, Schlüsselverwaltung, Kontrolle von privilegierten Benutzerzugriffen sowie granularer Audit-Protokollierung des Datenzugriffs für HANA v2.0 zugelassen.

Lösungsarchitektur

Bereitstellungen bestehen aus dem Vormetric Transparent Encryption Agenten und Vormetric Data Security Manager (DSM) Geräten. Die Richtlinien- und Schlüsselverwaltung erfolgt zentral im DSM. Der DSM ist als nach FIPS 140-2 Level 1, 2 oder 3 zertifiziertes Gerät erhältlich und verfügt über RESTful-, SOAP- und Command-Line-APIs sowie web-basierte Verwaltungsoberflächen.

Erfüllen Sie alle Ihre Datenschutzerfordernisse

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 der [CipherTrust Cloud Key Manager](#).

Über Thales eSecurity

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor zentralen Entscheidungen. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten auf 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.

> thalesecurity.com <



Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel.: +1 888 744 4976 oder +1 954 888 6200 • Fax: +1 954 888 6211 • E-Mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hongkong • Tel.: +852 2815 8633 • Fax: +852 2815 8141 • E-Mail: asia.sales@thales-eseurity.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-eseurity.com