

SPHiNX Data Encryption Suite

Highlights

- Schützt Daten vor unautorisiertem Zugriff
- Erfüllt Compliance-Anforderung für virtuelle und physikalische Tapes
- Einsatz auf bestehenden SPHiNX-Plattformen ohne störenden Einfluss auf Host-Server-Umgebungen
- Leistungsstarke 256-Bit AES-Verschlüsselung (Advanced Encryption Standard)
- Komplettes Key-Lifecycle-Management
- Nahtlose Integration der von der SPHiNX unterstützten physikalischen Tape Drives und Libraries
- Kein separater Key-Server erforderlich

Bei der optionalen Data Encryption Suite handelt es sich um ein lizenziertes Software-Feature der Corporate Edition von SPHiNX™. Dieses Feature ermöglicht es, Compliance-Anforderungen und strenge Datensicherheitsstandards der auf Disk oder Tape gespeicherten Daten einzuhalten. Data Encryption Suite verwendet den Verschlüsselungsalgorithmus nach AES (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit. Komprimierung und Verschlüsselung erfolgen inline beim Schreiben der Daten auf die SPHiNX. Bei einer planmäßigen Migration der Daten auf physikalische Tapemedien bleiben die Daten verschlüsselt, wodurch ein gesicherter Transport der Tapes in eine andere Lokation sichergestellt werden kann.

Integriertes Key-Management

Das Key-Management ist die entscheidende Komponente für eine sichere Handhabung der Encryption-Keys. Die Data Encryption Suite verfügt über einen integrierten Key-Server, der den gesamten Key-Lifecycle – von Random-Key-Generierung und Key-Verteilung, über die Key-Wiederherstellung bis hin zum Löschen der Encryption-Keys – unterstützt. Der Key-Server generiert für jede zu verschlüsselnde Datei einen symmetrischen Schlüssel nach dem Zufallsprinzip (Random) und schließt gleichzeitig eine erneute Key-Verwendung aus.

Die verschlüsselten Daten werden immer separat von den in der Key-Datenbank gespeicherten Verschlüsselungs-Keys gehalten. Bevor ein Zugriff auf Keys gestattet wird, muss eine Authentifizierung erfolgen. Die Keys sind automatisch vor Verlust geschützt, indem noch vor Verwen-

dung der Keys die Key-Datenbank auf ein SPHiNX oder in ein NAS-System gesichert wird. Keys können außerdem von verschiedenen SPHiNX-Systemen genutzt werden. Dies stellt einen Datenzugriff auf in replizierten Umgebungen gespeicherten Daten sicher.

Leichte Handhabung

Encryption Policies können über einen Standard-Webbrowser mit einem intuitiven Interface konfiguriert werden. Per Mausklick können Konfigurationseinstellungen vorgenommen werden. Zudem ist es möglich, zu definieren, welche kritischen Daten bei der Erstellung von virtuellen Pools oder Cartridges verschlüsselt werden sollen. Ein Administrator konfiguriert die Encryption-Funktionen und verhindert dadurch, dass unautorisierte Personen absichtlich oder unabsichtlich die Konfigurationseinstellungen modifizieren können.

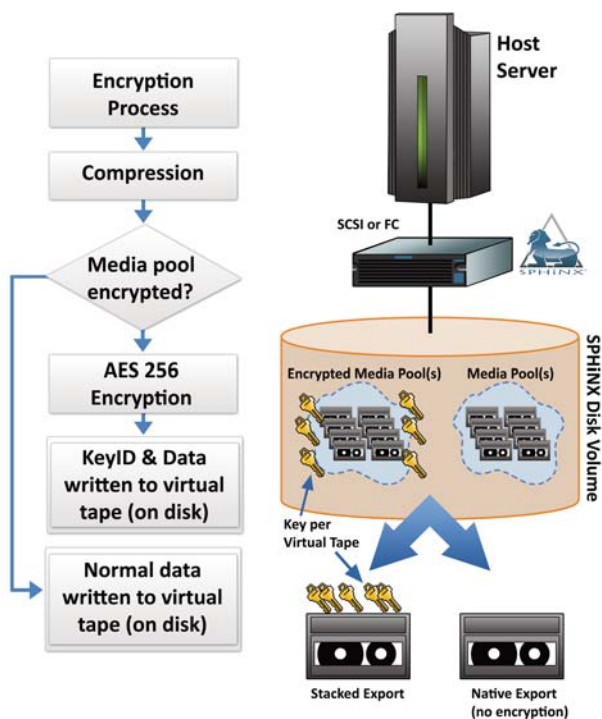
Flexibilität

Die Verschlüsselung erfolgt inline entweder automatisch oder manuell. Dies stellt sicher, dass kritische Unternehmensdaten dann geschützt sind, wenn es notwendig ist.

Interoperabilität

Die Data Encryption Suite erfordert keine Änderungen der Host-Server-Umgebungen oder der Backup-Strategien. Encryption und Key-Management sind transparent, alle anderen SPHiNX-Funktionen laufen weiterhin normal ab. Die Data Encryption Suite kann mit jedem Host-System interagieren, das von der SPHiNX unterstützt wird. Eine sichere Migration der verschlüsselten Daten zu einem angeschlossenen Tape-Drive oder einer Library kann ebenfalls veranlasst werden.

Data Encryption Architektur



Data Encryption Spezifikationen

Unterstützte Systeme

Crossroads SPHiNX Corporate Edition (SPHiNX-CX)

Verschlüsselungsverfahren

Softwarebasierte Verschlüsselung, optional: hardwarebasierte Verschlüsselung

Key-Verschlüsselungsverfahren

Symmetrische Key-Verschlüsselung

Unterstützter Verschlüsselungsalgorithmus

256-Bit Advanced Encryption Standard (AES-256-CBC)

Key-Management-Verfahren

Innerhalb SPHiNX vollintegrierte Key-Server und Key-Datenbank

Random-Key-Generierung für jedes verschlüsselte Virtual Tape Cartridge

Vollständiges Key-Lifecycle-Management (Generierung, Verteilung Speicherung und Schutz)

Sicherheit und Zugriffssteuerung

Anwender muss über SPHiNX-Administratorrechte verfügen

Konfiguration und Management

Einfache Administration über SPHiNX-Anwenderschnittstelle

Verschlüsselung des gesamten Medien-Pools oder von einzelnen Virtual Cartridges

Manuelles bzw. konfigurierbares automatisches Management

Auditlogging

Alle relevanten Verschlüsselungsfunktionen werden zum Zwecke der Nachverfolgung aufgezeichnet

Über die CROSSROADS Europe GmbH

Crossroads ist führender Anbieter von Lösungen für die Bereiche Datensicherung und Datensicherheit. Crossroads Systems, Inc. hat seinen Hauptsitz in Texas/Austin, die europäische Zentrale liegt mit der Crossroads Europe GmbH in der Nähe von Stuttgart. Crossroads Systems, Inc. wird an den Pink Sheets gehandelt (Zeichen: CRDS). Finanzberichte, Pressemeldungen und Dokumentationen werden über den OTCIQ Web-Service auf der Pink Sheet Website veröffentlicht. Weiterführende Informationen unter www.crossroads.com.