

Transparente Multi-User-Verschlüsselungssysteme

Einzigartiger Schutz von vertraulichen Dateien vor unberechtigtem internen und externen Zugriff

Die meisten Schutzmaßnahmen sind auf Bedrohungen von außen ausgerichtet, während die häufigsten internen IT-Risiken vernachlässigt werden. Dabei ist der mögliche Schaden beim Missbrauch von vertraulichen Unternehmensdaten derselbe. In fast jedem Unternehmen werden wertvolle Informationen wie Berichte, Personalunterlagen, Kundendaten oder Forschungsergebnisse ungeschützt elektronisch gespeichert. Als Folge der heutigen zentralen Datenspeicherung auf Servern, der standortübergreifenden Vernetzung von Arbeitsplätzen und der Nutzung mobiler Datenträger werden die Sicherheitsrisiken stetig größer. Immer mehr Unternehmen nutzen zudem IT-Outsourcing zur Kostensenkung, äußern aber gleichzeitig Bedenken bezüglich der Datenvertraulichkeit.

Gefragt ist eine Sicherheitslösung, die unternehmensweit nur autorisierten User-Gruppen Zugriff auf sensible Daten gewährt. Mit entsprechenden Sicherheitsrichtlinien haben unternehmensinterne Server-Administratoren oder das Personal des Outsourcers keine Möglichkeit, vertrauliche Daten einzusehen.

SafeGuard LAN Crypt schützt Ihre vertraulichen Dateien durch Einsatz einer vollständig automatisierten und äußerst effektiven Dateiverschlüsselung, die keine Änderungen des User-Verhaltens erfordert: Die Verschlüsselung läuft transparent und somit unsichtbar im Hintergrund. Jeder Anwender erhält aufgrund seines Profils ein einzigartiges „Schlüsselbund“, mit dem er – wie gewohnt – die freigegebenen Dateien im Klartext lesen kann. Unberechtigte Personen sehen stattdessen nur einen chiffrierten, unleserlichen Zeichensatz.

SafeGuard LAN Crypt trennt die Aufgabenbereiche von Server-Administratoren und Sicherheitsadministratoren und vereinfacht hierdurch die Verwaltung der Datensicherheit erheblich. Während Server-Administratoren auch ohne Besitz der Dokumentenschlüssel die Systemverwaltung wie gewohnt durchführen können, implementieren Sicherheitsadministratoren über eine skalierbare Schlüsselverwaltung individuelle Zugriffsrechte für Arbeitsgruppen und individuelle User in Einklang mit unternehmensinternen Sicherheitsrichtlinien. Somit wird eine strikte Gewaltenteilung der Administration realisiert.

SafeGuard LAN Crypt schützt Unternehmensdaten lückenlos. Die Lösung ist skalierbar und kann sowohl in kleinen temporären Teams, in Abteilungen und in Projekt-Gruppen oder aber unternehmensübergreifend eingesetzt werden.

SafeGuard LAN Crypt – Intelligente Dateiverschlüsselung.

Vorteile**Erhöhte Sicherheit**

- » Transparente Datensicherheit für User-Gruppen und einzelne User
- » Verschlüsselung auf allen Standardmedien und in heterogenen Umgebungen
- » Gewaltenteilung zwischen Server- und Sicherheitsadministrator
- » Einfache Implementierung unternehmensweiter Sicherheitsrichtlinien
- » Flexible Definition von Verschlüsselungsregeln für User-Gruppen
- » Einfache PKI-Integration und Unterstützung von Zertifikaten, Smartcards und USB-Token

Einfache Installation

- » Nahtlose Integration in heterogene IT-Infrastrukturen
- » Einfache und zentrale Administration dank Verwendung bestehender Verzeichnisse und Domains
- » Keine zusätzlichen Upgrades der bestehenden IT-Infrastruktur erforderlich
- » Skalierbar von individuellen User-Gruppen bis hin zu unternehmensweiten Rollouts

Einfache Handhabung

- » Dank Integration in vertraute Arbeitsumgebungen einfach zu handhaben
- » Höhere Akzeptanz vonseiten der User dank maximaler Transparenz und selbsterklärenden Funktionen

Die wichtigsten Funktionen

Datensicherheit

- Umfassende Sicherheitslösung zur Unterbindung unbefugter Zugriffe auf Daten
- Schutz wertvoller Unternehmensdaten und vertraulicher personenbezogener Daten
- Strikte Gewaltenteilung der Verantwortlichkeiten von Server- und Sicherheitsadministrator
- Optimaler Schutz beim IT-Outsourcing, da Mitarbeiter eines externen Dienstleisters die Dateien verwalten, aber nicht im Klartext lesen können
- Einsatz bewährter und vielfach getesteter Sicherheitsalgorithmen
- User-Authentisierung mittels X.509-Zertifikaten
- Unterstützung von Smartcards und USB-Token

Sicherheitsadministration

- Einfache, zentrale Installation, Konfiguration und Administration in bestehende IT-Umgebungen unter Verwendung bestehender Verzeichnisdienste und Domains
- Problemlose Integration in bestehende PKI-Systeme
- Kosteneffiziente und schnell zu implementierende Lösung, die ohne zusätzliche Infrastruktur auskommt
- Durchdachte Recovery-Strategie, um auf verschlüsselte Daten auch im Notfall zugreifen zu können
- Flexible und leistungsstarke Administration API, welche die Integration von SafeGuard LAN Crypt in beliebige Provisioning-Systeme ermöglicht und den Unternehmens-Workflow unterstützt

Benutzerkomfort

- Berechtigte User können ihre gemeinsam genutzten Informationen geschützt ablegen – ohne Gefahr des unberechtigten Zugriffs Dritter
- Persistente Verschlüsselung
- Keine Änderung der gewohnten Arbeitsumgebung und Arbeitsweise nötig
- Hohe Akzeptanz auf Userseite, da kein zusätzliches Training erforderlich ist
- Keine Einbußen bei der Fileserver-Performance – ein Endpoint Client Agent nimmt Ver- und Entschlüsselung vor

Dritthersteller

- Kompatibel mit SafeGuard Data Exchange 5.40 und höher
- Sicherer Zugriff auf verschlüsselte Dateien von zugelassenen Anti-Malware-Produkten (z.B. Sophos)
- Unterstützt Microsoft SQL Server- und Oracle-Datenbanken
- Unterstützt Microsoft Active Directory und Novell eDirectory
- Administration API ermöglicht Integration in beliebige Provisioning-Systeme
- Integration von Microsoft Crypto API: Durch Cryptographic Service Provider (CSP) können beliebige RSA-fähige Komponenten von Drittherstellern für die User-Authentisierung eingesetzt werden (z.B. Smartcards oder USB-Token)
- Aladdin eToken-zertifiziert

Weitere Informationen

Mehr Informationen zu Sophos und sämtlichen SafeGuard-Lösungen finden Sie hier:
www.sophos.de

Systemanforderungen

Hardware

- » PC mit Intel Pentium- oder kompatibelem Prozessor

Betriebssystem (32 Bit)

- » Windows XP Professional SP2, SP3
- » Windows Vista (Ultimate/Enterprise/Business) SP1, SP2
- » Windows 7 (Ultimate/Enterprise/Professional)
- » Windows Server 2003 R2 SP2 mit Terminal Server Services
- » Windows Server 2003 R2 SP2 mit Citrix Presentation Server 4.5

Betriebssystem (64 Bit)

- » Windows 7 (Ultimate/Enterprise/Professional)

Unterstützte Fileserver-Betriebssysteme

- » Microsoft Windows (Versionen 2003 und 2008)
- » Novell Netware

Unterstützte Medien

- » Netzwerklaufwerke, lokale Festplatten, CD, DVD, USB-Speichermedien und Speicherkarten

Standards/Protokolle

- » Authentisierung: Benutzer-Authentisierung über X.509v3-Zertifikate
- » PKCS#12
- » LDAP zum Zugriff auf Microsoft Active Directory und Novell eDirectory
- » Verschlüsselung: 3DES 168 Bit, IDEA 128 Bit, AES 128 Bit und 256 Bit
- » Hash: MD5, SHA-256
- » Token: Smartcards und USB-Token via Crypto API

Sprachen

- » Deutsch, Englisch, Französisch