conpal LAN Crypt

Smart
Hochsicher
Persistent

Schutz sensibler Daten für Enterprise-Organisationen

Agile Daten erfordern eine flexible Verschlüsselung

Häufig werden sensible und geschäftskritische Daten wie Geschäftsberichte, Personal- oder Kundendaten weitgehend ungeschützt elektronisch gespeichert. Die Speicherung erfolgt lokal, auf externen Speichermedien, on premise oder in der Cloud – mit signifikant erhöhten Risiken. Die zunehmende „Cloudifizierung" bei der Verwaltung von (sensiblen) Daten sowie dem Management von Anwendungen und Systemumgebungen im Rahmen einer „Mobilisierung" der eingesetzten Endgeräte wie z.B. Notebook, Tablet, Smartphone, lassen das Risiko für Missbrauch, Datendiebstahl und Kontrollverlust exponentiell ansteigen. Hinzu kommt: Die meisten Schutzmaßnahmen sind auf Bedrohungen von außen ausgerichtet, während interne IT-Risiken häufig vernachlässigt werden. Dabei ist der potenzielle Schaden beim Missbrauch von vertraulichen Unternehmensdaten derselbe.

Hier ist eine Sicherheitslösung gefragt, die sich den Anforderungen von Enterprise-Umgebungen anpasst und organisationsweit nur autorisierten Anwendern den Zugriff auf sensible Daten gewährt. Verschlüsselte Inhalte sollten immer persistent verschlüsselt sein, um einen lückenlosen Schutz über verschiedene Plattformen hinweg gewährleisten zu können.

conpal LAN Crypt

conpal LAN Crypt verschlüsselt vertrauliche Dateien persistent. Damit erfolgt die sichere Übertragung (data in transit) sowie die sichere Ablage (data at rest) von vertraulichen Daten in unterschiedlichsten Umgebungen (Cloud Share, File Share, lokale Speichermedien) nachhaltig und revisionssicher.

- Für den Benutzer erfolgt die Verschlüsselung unmerklich im Hintergrund
- Nahtlose Integration in alle Enterprise-Service-Plattformen und 3rd Party Tools durch eine leistungsfähige moderne API-Architektur
- Berechtigung erfolgt durch Zuweisung einer einzigartigen „Schlüsselgruppe" zu einem Benutzerprofil
- Einfache Umsetzung von DSGVO-Anforderungen für interne Belange und für die Verwendung mobiler Medien
- Skalierbare Lösung, bestens geeignet für Projektteams, Abteilungen, Unternehmen oder unternehmensübergreifend

Rollentrennung

conpal LAN Crypt sorgt für eine strikte Rollentrennung zwischen Administrator und Sicherheitsbeauftragen, wodurch sich Datenschutz-Policys konsequent durchsetzen lassen.

- Systemverwaltung nach wie vor durch den Administrator, jedoch ohne Befugnis zur Entschlüsselung von Dateien
- Schlüsselverwaltung und Definition von Zugriffsrichtlinien für Einzelpersonen oder Gruppen durch den Sicherheitsbeauftragten
- Definition der individuellen Zugriffsrechte für Arbeitsgruppen oder einzelne Anwender im Einklang mit den Sicherheitsrichtlinien durch den Sicherheitsbeauftragten

conpal LAN Crypt

Datensicherheit

conpal LAN Crypt ist die nachhaltige Enterprise-Sicherheitslösung, die unbefugte Zugriffe auf sensible Daten konsequent unterbindet.

- Geprüfte und bewährte Sicherheitsalgorithmen
- Benutzerauthentifizierung über X.509-Zertifikate

Sicherheitsadministration

conpal LAN Crypt ermöglicht durch ein ausgefeiltes Administrationskonzept eine schnelle und unkomplizierte Einbindung in Ihre IT-Sicherheitsarchitektur.

- Kosteneffiziente Lösung mit einfachem Installationskonzept ohne zusätzliche Administrations-Infrastruktur
- Integrierte Wiederherstellungsprozesse für den Zugriff auf verschlüsselte Daten in Notfallsituationen

Benutzerkomfort

- Keine Änderungen der Arbeitsumgebung und -gewohnheiten erforderlich
- Optimierte Performance bei Ver- und Entschlüsselung von geschützen Daten auf einem Client

Systemanforderungen

Client 64 Bit

- Windows 10 1803 (RS4), 1809 (RS5), 1903 (19H1), 1909 (19H2), 2004 (20H1), 2009 (20H2) Pro/Enterprise
- Windows Server 2012 R2, 2016, 2019
- Citrix XenApp 7.18 auf Windows Server 2016 und 7.15 LTSR auf Windows Server 2016

Administration 64 Bit

- Windows 10 Build 1803, 1809, 1903, 1909, 2004 Pro/Enterprise
- Windows Server 2012, 2012 R2, 2016, 2019

Unterstützte Datenbanken

- Microsoft SQL Server 2012 SP4, 2016 SP2, 2017, 2019
- Oracle 12
- Oracle 19

Unterstützte Medien und Plattformen

- Medien: Netzlaufwerke, lokale Festplatten, optische Medien, USB, Speichersticks / -karten
- Plattformen: Microsoft Terminal Server, virtuelle Maschinen, OneDrive, Azure SQL, Dropbox, Google Drive, MS Azure (z.B. Clients, Azure DB)

Unterstützte Algorithmen

- Verschlüsselung: AES 128 Bit und 256 Bit, 3DES 168 Bit, DES, IDEA 128 Bit, XOR
- Zertifikate: RSA bis 4096 Bit, eigengeneriert oder durch Einbindung einer PKI, Softzertifikate, Smartcards, Token
- Empfohlene Algorithmen: AES-256
- Empfohlenes Verschlüsselungsformat: XTS-AES
- Hash: SHA256

Haben Sie Fragen? Sprechen Sie uns an!

conpal

Weitere Informationen finden Sie auf unserer Website. Auf Anfrage können wie Ihnen auch die jeweils aktuellen Release Notes bereitstellen.

Dornhofstraße 69 · 63263 Neu-Isenburg · www.conpal.de
SalesSupport@conpal.de
Tel.: +49 (0) 6102 / 751 98 0
Fax: +49 (0) 6102 / 751 98 99