conpal LAN Crypt

Smart
Sicher
Persistent

Schutz sensibler Daten für Unternehmen und Organisationen

Agile Daten erfordern die flexible Verschlüsselung

Häufig werden sensible und geschäftskritische Daten wie Geschäftsberichte, Personal- oder Kundendaten nicht adäquat geschützt elektronisch gespeichert. Die Speicherung erfolgt lokal, auf externen Speichermedien, on-premises oder in der Cloud – mit signifikant erhöhten Risiken. Die zunehmende „Cloudifizierung“ bei der Verwendung 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 durch Unachtsamkeit, Datendiebstahl und Kontrollverlust signifikant ansteigen. Hinzu kommt: Die meisten Schutzmaßnahmen sind auf Bedrohungen von außen ausgerichtet, während interne IT-Risiken häufig vernachlässigt werden. Dabei ist der potenzielle Schaden bei Datenverlust 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 und Gerätegrenzen hinweg gewährleisten zu können. Auch beim Austausch mit Externen ist Verschlüsselung ratsam.

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 Speicher- und auch Wechselmedien) 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 eines einzigartigen „Schlüsselbundes“ zu einem Benutzerprofil
- Einfache Umsetzung von DSGVO-Anforderungen für interne Belange auch bei der 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 IT-Administrator, jedoch ohne Befugnis zur Entschlüsselung von Dateien
- Schlüsselverwaltung und Definition von Zugriffsrichtlinien für Einzelpersonen oder Gruppen durch den Sicherheitsbeauftragten
- Sicherheitsadministration durch individuelle Zugriffsrechte für Arbeitsgruppen oder einzelne Anwender im Einklang mit den Sicherheitsrichtlinien

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
- Option zur passwortbasierten Ver- und Entschlüsselung von Dateien dank „Portable“ Funktion **inklusive portabler Clients für alle Plattformen**

Sicherheitsadministration

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

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

Benutzerkomfort

- Keine Änderungen der Arbeitsumgebung und -Gewohnheiten erforderlich
- Optimierte Performance bei Ver- und Entschlüsselung von geschützten Daten auf einem Client
- Erstellung und Verwendung Passwort-basierter Schlüssel durch den Nutzer für den gesicherten Austausch mit Externen

Unterstützte Medien und Plattformen

- Medien: Netzlaufwerke, lokale Festplatten, optische Medien, Speichersticks / -karten, Cloud Speicher
- Plattformen: Microsoft Terminal Server, virtuelle Maschinen, Microsoft Office365

Systemanforderungen

Administration 64 Bit

- Windows 11, Windows 10 Pro/Enterprise 19H2 oder höher
- Windows Server 2022, 2019, 2016

Clients:

- 64-Bit Windows-Rechner: Windows 11, Windows 10 Pro/Enterprise 19H2 oder höher
- Mac-Rechner: macOS 11 (M1 & Intel), 10.15, 10.14
- iPhone/iPad: iOS 15 & 14, iPadOS 15 & 14
- Android: 12, 11, 10 und 9
- Windows Server 2022, 2019, 2016
- Citrix XenApp 7.18 auf Windows Server 2016 und 7.15 LTSR auf Windows Server 2016

Unterstützte Datenbanken

- Microsoft SQL Server 2019, 2017
- Oracle 19

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 wir 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