THE DATA PROTECTION COMPANY

SafeNet ProtectFile

LÖSUNGSÜBERSICHT

Vorteile

Transparente, starke und effiziente Verschlüsselung

- Schutz vertraulicher Daten auf Servern im gesamten Unternehmen durch transparente, automatisierte Verschlüsselung auf Dateisystemebene
- Zentrale und sichere Verwaltung von Verschlüsselungs-Keys durch FIPS-zertifizierte Hardware
- Anwendung granularer Richtlinien auf Basis von Benutzern und Gruppen, Dateitypen und Prozessen zur besseren Kontrolle über vertrauliche Daten

Kontrolle privilegierter Benutzer

- Minimierung interner Risiken: Privilegierte Benutzer (z. B. Root- oder Systemadministrator) können zwar autorisierte Aufgaben ausführen, vertrauliche Daten bleiben aber sicher verschlüsselt

Sichere Archivierung von Daten

- Vertrauliche Daten bleiben verschlüsselt und sind für Serveradministratoren auch bei geplanten Sicherungen und Wiederherstellungen unzugänglich.

Sicheres Vernichten von Daten

- Falls erforderlich werden geschützte vertrauliche Daten unlesbar gemacht

Einfache Implementierung und Verwaltung

- Verwendung von Remote-Skripten zur schnellen und einfachen Installation im Hintergrund in großen oder kleinen Umgebungen
- Straffere Administration und geringere Kosten durch zentrale Verwaltung von Richtlinien und Schlüsseln
- Kostengünstigere Skalierung je nach Unternehmensanforderungen

Compliance

- Einhaltung von Compliance-Vorgaben zur Verschlüsselung von Daten und zur Aufgabentrennung

Perimeterbasierte Sicherheitslösungen sorgen heutzutage angesichts der zunehmenden Menge vertraulicher Daten in physischen, virtuellen und cloud-basierten Umgebungen nicht mehr für einen ausreichenden Schutz. Herkömmlicher Perimeterschutz gehört der Vergangenheit an, und folglich haben sich neue Schwachstellen herausgebildet. Damit Unternehmen rundum geschützt sind, muss eine leistungsstarke Datenschutzlösung auf Dateiebene implementiert werden.

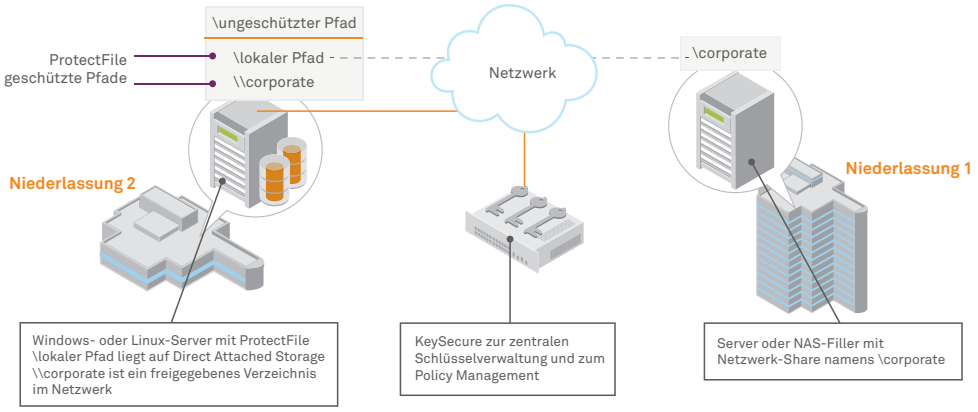
SafeNet ProtectFile schützt vertrauliche Daten auf Servern im gesamten Unternehmen durch einen transparenten, automatisierten Schutz auf Dateisystemebene, granulare Zugangskontrollen, eine zentrale Verwaltung von Schlüsseln und Richtlinien sowie umfassende Audit-Funktionen.

Aufgrund ihrer Menge und ihrer Wichtigkeit sind vertrauliche Daten auf Unternehmensservern für Angreifer beliebte und einfache Ziele. ProtectFile sorgt für eine datenorientierte Sicherheit, indem vertrauliche Informationen im Falle eines Angriffs, Datenmissbrauchs oder Hacks unbrauchbar gemacht werden.

Schutz vertraulicher Serverdaten im gesamten Unternehmen

ProtectFile wird in Kombination mit der SafeNet-Hardware KeySecure für die zentrale Verwaltung von Schlüsseln und Richtlinien eingesetzt, die nach FIPS 140-2 Level 3 zertifiziert ist. So entsteht eine leistungsstarke und skalierbare Sicherheitslösung. ProtectFile verschlüsselt vertrauliche Daten, z. B. Kreditkartennummern, persönliche Daten, Protokolle, Passwörter und Konfigurationsdaten.

Im Anschluss an die Bereitstellung und Inbetriebnahme auf einem Server sorgt ProtectFile für die transparente Ver- und Entschlüsselung in lokalen und Netzwerkordnern auf Dateisystemebene auf Basis von zuvor in KeySecure festgelegten Richtlinien – und zwar ganz ohne Einfluss auf den Geschäftsbetrieb, die Anwendungsperformance oder die Benutzer.



Technische Daten

Verschlüsselung auf Dateisystemebene

- Server: Dateiserver, Webserver, Anwendungsserver, Datenbankserver und andere Geräte mit kompatibler Software
- Netzwerk-Shares: SMB/CIFS, NFS
- Remote-Installation im Hintergrund zur einfachen Bereitstellung in beliebig großen Umgebungen

Verschlüsselungsalgorithmen

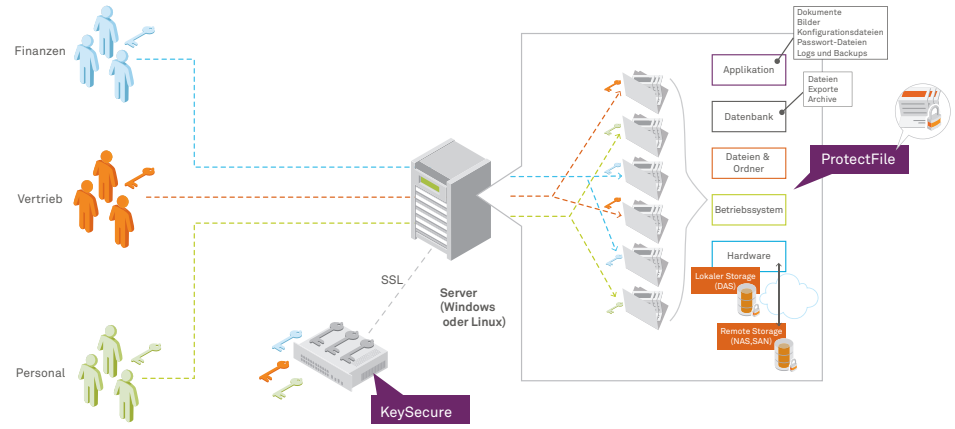
- AES

Unterstützte Plattformen

- Big Data: Apache Hadoop
- Cloud: AWS EC2 und S3
- Linux
  - Oracle: Unbreakable Enterprise Kernel
  - Red Hat Enterprise
  - Suse
- Microsoft Windows

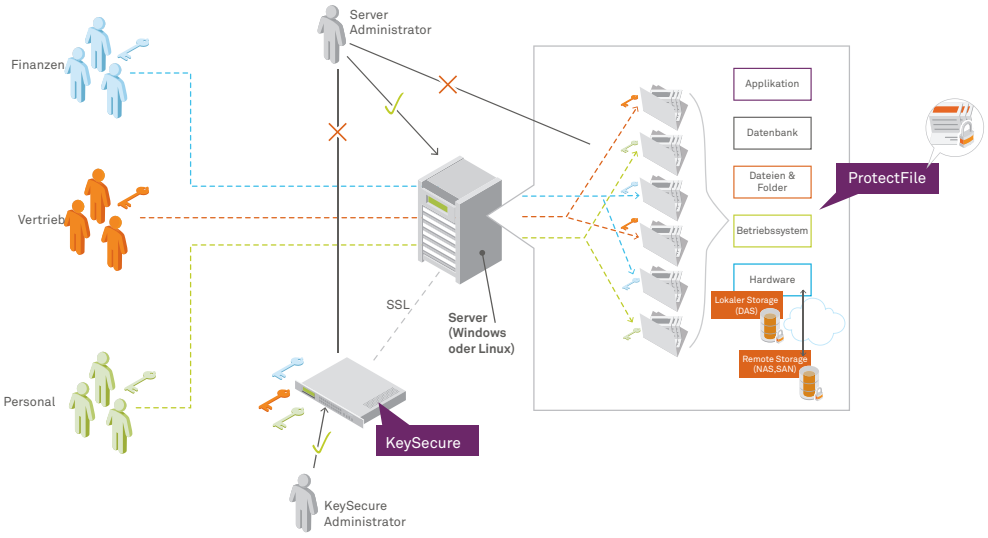
Zugriffsbeschränkung für vertrauliche Daten auf gemeinsam genutzten Servern

In gemeinsam genutzten Serverumgebungen speichern verschiedene Abteilungen und Arbeitsgruppen vertrauliche Daten auf demselben Server. Mit ProtectFile und KeySecure können Administratoren Serverdaten ganz einfach nach Abteilung trennen und entsprechende Richtlinien festlegen, die Benutzern den Zugriff auf diese Daten nur mit dem geeigneten Verschlüsselungs-Key erlaubt.



Starke Aufgabentrennung

Zur Umsetzung von Security-Best-Practices ist eine Aufgabentrennung enorm wichtig und sorgt für die Einhaltung aufsichtsbehördlicher Vorgaben und den Schutz vertraulicher Daten vor internen Bedrohungen. ProtectFile und KeySecure ermöglichen die Implementierung granularer Zugriffskontrollen, die administrative Aufgaben vom Zugriff auf Daten und Verschlüsselungs-Keys trennen. Serveradministratoren können z. B. auf verschlüsselte Dateien und Ordner mit vertraulichen Daten zugreifen, um die physische Infrastruktur zu verwalten (Sicherung und Archivierung von Daten), können diese Daten allerdings nicht im Klartext einsehen.



Verbesserte Compliance

ProtectFile unterstützt die Einhaltung verschiedenster Richtlinien, die eine Datenverschlüsselung vorschreiben, u.a. die sichere Speicherung von Kreditkartennummern zur Einhaltung des Payment Card Industry Data Security Standard (PCI DSS), oder personenbezogener Informationen zur Einhaltung verschiedener landesweiter Datenschutzvorschriften und elektronischer Patientendaten zur Einhaltung des HIPAA-Standards im Gesundheitswesen.

Kontakt: Eine Übersicht unserer Niederlassungen und die entsprechenden Kontaktdaten finden Sie unter **www.safenet-inc.com**.
Folgen Sie uns: www.safenet-inc.com/news-media