

Management Center-Modul

Um Unternehmensdaten wirksam zu schützen und Richtlinien und Vorschriften lückenlos einzuhalten, ist eine zentrale Management-Infrastruktur erforderlich, über die Richtlinien einheitlich konfiguriert und implementiert werden können – besonders in heterogenen IT-Umgebungen. Um ständig ändernden Anforderungen gerecht zu werden, müssen Administratoren Sicherheitsrichtlinien kontinuierlich überarbeiten und gleichzeitig die Transparenz der Sicherheit für den Enduser gewährleisten. SafeGuard Management Center reduziert Trainingskosten und vereinfacht Verwaltungsaufgaben.

SafeGuard Management Center ist ein Modul von SafeGuard Enterprise, der zentralen Lösung zur Verwaltung Ihrer Datensicherheit in heterogenen IT-Umgebungen. Über nur eine einzige Konsole bietet SafeGuard Enterprise vollständige Festplattenverschlüsselung, Verschlüsselung von Wechselmedien, PC-Port-Kontrolle zur Data Loss Prevention (DLP) sowie die Möglichkeit zur Verwaltung weiterer Verschlüsselungsprodukte, damit auf sämtlichen Ebenen für leistungsstarke Sicherheit gesorgt ist.

Zentrale Administration von Datenschutzrichtlinien

- Zentrale, plattformübergreifende Funktionen zur Verwaltung des Schutzes ermöglichen die hierarchische Definition von Sicherheitsrichtlinien – zur Festplattenverschlüsselung, Verschlüsselung von Wechselmedien und DLP-Port-Kontrolle über nur eine einzige Konsole.
- Die Integration in Active Directory greift auf User-, Geräte- und Gruppen-Daten zurück (nicht zwingend erforderlich).
- Ein modularer Mechanismus zur Richtlinienvererbung sorgt für maximale Flexibilität und Effizienz der Verwaltungsabläufe.
- Resulting Set of Policies (RSOP): Die finale vererbte Richtlinie wird für jeden User oder Computer separat ermittelt und kann von Konsolen-Administratoren einfach überprüft werden.
- Sicherheitsrichtlinien werden automatisch und plattformübergreifend verteilt.
- Den einzelnen Organisationseinheiten können Regeln zugeordnet und in Folge für User-/Computergruppen aktiviert werden.
- Geräte, die den Server nicht innerhalb eines gewissen Zeitraums oder einer festgelegten Anzahl von Login-Versuchen kontaktieren, können gesperrt werden.

Hochmoderne Schlüsselverwaltung

- Zentrale Schlüsselverwaltung über nur eine Konsole
- Sichere Speicherung und Wiederherstellung sowie risikofreier Austausch von Schlüsseln in Umgebungen mit unterschiedlichen Geräten und Betriebssystemen
- Automatische Schlüsselzuordnung für Gruppen zum Austausch und zur Verschlüsselung auf Gruppen-Basis
- Sicherer Austausch von Daten zwischen PCs, Wechselmedien und E-Mail-Attachments

Verwaltung von Sicherheitsbeauftragten

- Rollenbasierter Zugang: Vordefinierte und angepasste Rollen für Sicherheitsbeauftragte
- Bei kritischen Aktionen Autorisierung durch zwei Verantwortliche
- Optionale Zweifaktoren-Authentifizierung über Token oder Smartcards
- Auswahl von Sicherheitsbeauftragten über Active Directory
- Zur Richtlinienvererbung hierarchische Gruppenzuordnung von Sicherheitsbeauftragten
- Möglichkeit zur Delegierung von Administratorrechten
- Multisession-fähige Management-Konsole
- Multi-Tenancy-Support: Verwaltung mehrerer separater SafeGuard-Installationen von einer Konsole aus

Vorteile

- » Geringere Administrationskosten durch die zentrale Verwaltung von Richtlinien zur Verschlüsselung mobiler Daten und zur Port-Kontrolle (DLP) von einer einzigen Konsole aus
- » Problemlose Verwaltung von Usern und Geräten in heterogenen IT-Umgebungen bei gleichzeitigem Enforcement von Compliance-Richtlinien
- » Rollenbasiertes User-Management zum granularen Richtlinien-Enforcement für eine gesteigerte IT-Effizienz
- » Zugriff auf detaillierte, druckbare Audit-Protokolle und Reports zur Sicherstellung der Konformität mit Richtlinien und Vorschriften
- » Einfache Wiederherstellung von Kennwörtern und Daten – für ein Höchstmaß an Produktivität bei gleichzeitiger Reduzierung des Helpdesk-Kostenaufwands
- » Umfassende Sicherheit durch Verschlüsselung und Verwaltung von Desktops, Laptops und Wechselmedien

Modulare und flexible Sicherheitsarchitektur

- Wächst durch zusätzliche SafeGuard Enterprise-Module mit Ihren Anforderungen
- Management-API mit zahlreichen Funktionen für kundenspezifische Anwendungen
- Integration in Microsoft Active Directory über LDAP sowie Unterstützung von Novell-Umgebungen
- Kompatibilität mit Smartcards und Token von Drittanbietern
- Sichere, XML/SOAP-basierte Client-Server-Kommunikation: Keine Neukonfiguration der Firewall, Unterstützung der Lastverteilung des Datenverkehrs

Verwaltung von BitLocker Laufwerkverschlüsselung auf Windows 7 und Vista

- Einheitliche Sicherheitsrichtlinien können in Umgebungen mit unterschiedlichen Betriebssystemen und Geräten durchgesetzt werden
- Zentralisierte Schlüsselverwaltung für Backup und Recovery
- Optional wählbar: BitLocker™ Laufwerkverschlüsselung
- SafeGuard Enterprise meldet den BitLocker-Gerätestatus

Unterstützung von Verzeichnisdiensten

- Bestehende Infrastrukturdaten z.B. zu Usern, Computern, Gruppen und X.509-Zertifikaten können aus Microsoft Active Directory-fähigen Verzeichnissen importiert werden
- Spezielle SafeGuard Enterprise User-Accounts sind unnötig
- SafeGuard Enterprise-Sicherheitsbeauftragte können aus der Gruppe der Active Directory-User gewählt werden
- Novell-Umgebungen werden unterstützt

Administratorseitiges Lizenz-Management

- Aktivierung neuer SafeGuard-Module mittels einfachem Lizenz-Update
- Tracking des Einsatzes von SafeGuard Enterprise-Modulen zur Aufrechterhaltung der Lizenz-Compliance

Automatisierte Installation

- Kompatibel mit typischen Software-Verteilungsmechanismen über MSI-Pakete. Kann auch über bestehende Software-Managementsysteme wie Altiris, Microsoft SCCM oder NetInstall automatisch verteilt und installiert werden
- Die Konfigurations-Standardinstellungen ermöglichen eine schnelle Implementierung in Testumgebungen

- Ein Server-Installationsassistent vereinfacht den Installationsvorgang auf allen SafeGuard- und Microsoft-Serverkomponenten

Kenntwort-Wiederherstellung und Helpdesk-Optionen

- Ein integrierter Challenge/Response-Wiederherstellungsassistent bietet Hilfestellung bei vergessenen User-Kennwörtern
- Ein webbasiertes Helpdesk für outgesourcete Umgebungen ist in der Lizenz des Management Center enthalten
- Zur Integration spezifischer Helpdesks steht eine API zur Verfügung
- Eine lokale Selbsthilfe-Option zur Wiederherstellung vergessener Kennwörter ohne Hilfestellung durch das Helpdesk: Optionen zur lokalen Selbsthilfe sowie Challenge-Fragen und -Antworten können über das Management Center konfiguriert werden

SafeGuard Management API unterstützt:

- Verzeichnisdienst-Operationen, automatische Synchronisierung
- Zuordnung von Usern zu Geräten
- Schlüsselzuordnung an Geräte/User
- Verarbeitung von Inventar- und Protokollberichten
- Verwaltung von Zertifizierungen und Token
- Challenge-Response für kundenspezifische Helpdesk-Anwendungen

Echtzeit-Status, Protokolle und Reports zur Sicherheit

- Alle Client-Aktivitäten/-Status, Administratoraktionen und Sicherheitsereignisse werden protokolliert und zentral gespeichert
- Art der Protokolle und Speicherort werden vom User festgelegt
- Administratoren können Protokoll-Reports filtern, einsehen und ausdrucken
- Das optionale Standalone-Tool SGNState berichtet den Verschlüsselungsstatus an externe Konsolen (z.B. LANDesk oder Network Access Control-Lösungen [NAC])

Systemanforderungen

Betriebssysteme

- » Microsoft Windows 7 (32 und 64 Bit)
- » Microsoft Windows Vista (32 und 64 Bit; SP 1, SP 2)
- » Microsoft Windows XP (32 Bit; SP 2, SP 3)
- » Microsoft Windows Server 2008 und 2008 R2 (32 und 64 Bit)
- » Microsoft Windows Server 2003 (32 Bit)

Zertifizierungen

- » FIPS 140-2 zertifizierte SafeGuard Cryptographic Engine
- » Aladdin eToken-tauglich

Standards und Protokolle

- » Symmetrische Verschlüsselung: AES 128/256 Bit
- » Asymmetrische Verschlüsselung: RSA
- » Hash-Funktionen: SHA-256, SHA-512
- » Kennwort-Hashing: PKCS #5v2
- » Smartcard/Token: PKCS #11, PKCS #15, Microsoft CSP, PC/SC, Kerberos
- » PKI: PKCS #7, PKCS #12, X.509-Zertifikate
- » Datentransfer: SOAP, XML, SSL, LDAP

Sprachen

- » Deutsch, Englisch, Französisch, Japanisch

Unterstützte Datenbanken

- » Microsoft SQL Server 2005, 2008, Express
- » Verschlüsselte Kommunikation zwischen Datenbank und Management-Centern