SafeGuard® Enterprise versione 5.50

SOPHOS

Modulo Management Center

Un'efficace conformità con la protezione dei dati e le normative di sicurezza richiede una gestione centralizzata per configurare e implementare i criteri in modo omogeneo, specialmente in ambienti IT misti. Gli amministratori devono modificare continuamente i criteri per soddisfare i requisiti in continua evoluzione, garantendo al tempo stesso la trasparenza della protezione. SafeGuard Management Center riduce i costi di formazione e agevola i compiti amministrativi.

SafeGuard Management Center è un modulo di SafeGuard Enterprise, una soluzione centralizzata per la gestione della protezione dei dati in ambienti IT misti. SafeGuard Enterprise offre la crittografia completa del disco e dei supporti rimovibili, oltre al controllo della porta del PC per la prevenzione dalla perdita di dati (DLP) e la gestione di altri prodotti di crittografia, tutto da una console singola, per una protezione multilivello

Gestione centralizzata dei criteri di sicurezza dei dati

- Una gestione di sicurezza centralizzata e multipiattaforma offre la definizione gerarchica dei criteri di sicurezza per una completa crittografia del disco, crittografia dei supporti rimovibili e DLP di controllo della porta, tutto da una console singola.
- L'integrazione con Active Directory sfrutta le informazioni di utente, dispositivo e gruppo, in base alle esigenze.
- Meccanismi di eredità dei criteri modulari consentono la massima flessibilità ed efficienza di gestione.
- Resulting Set of Policies (RSOP): viene calcolato il criterio ereditato finale per ciascun utente o computer, facilmente verificabile dagli amministratori di console.
- I criteri di sicurezza vengono distribuiti automaticamente tra varie piattaforme.
- Vengono assegnate regole a unità organizzative, attivandole per gruppi di utenti/computer, come nel caso di Active Directory; semplice da comprendere per gli amministratori e molto flessibile da abbinare anche nei casi di utilizzi speciali.
- È possibile bloccare dispositivi che non riescono a contattare il server in un intervallo di tempo predefinito o entro un numero definito di tentativi di accesso; lo sblocco è possibile attraverso il sistema di attesa/risposta.
- Gestione flessibile delle chiavi
- La gestione delle chiavi è centralizzata da una console singola.
- Le chiavi vengono archiviate, scambiate e recuperate in modo sicuro in ambienti di sistemi operativi e dispositivi misti.
- Le assegnazioni automatiche delle chiavi per gruppi abilitano la crittografia e la condivisione basate su gruppi.
- Condivisione sicura dei dati tra PC, dispositivi rimovibili e allegati e-mail.

Gestione dei responsabili della sicurezza

- Accesso basato sui ruoli: sono disponibili ruoli dei responsabili della sicurezza predefiniti e personalizzati.
- È disponibile la funzione di doppia autorizzazione da due responsabili per le azioni critiche.
- L'autenticazione a due fattori via token o smartcard è opzionale.
- I responsabili della sicurezza sono selezionabili da Active Directory.
- I responsabili della sicurezza possono essere raggruppati gerarchicamente, consentendo eredità e assegnazioni di criteri basati su gruppi.
- Anche i diritti amministrativi possono essere delegati.
- La console di gestione consente sessioni multiple.
- Supporto multi-tenancy: gestione di installazioni SafeGuard separate multiple da una singola console.

Vantaggi principali

- Minori costi amministrativi attraverso la gestione centralizzata dei criteri di crittografia dei dati mobili e del controllo della porta (DLP) da una console singola.
- Amministrazione omogenea di utenti e dispositivi in ambienti IT misti applicando nel contempo criteri di conformità.
- La gestione utente basata su ruoli abilita l'applicazione di criteri granulari, migliorando l'efficienza IT.
- Possibilità di accedere a log e report di controllo dettagliati e stampabili per la conformità con le normative.
- Recupero semplice di password e dati per una produttività sicura, diminuendo i costi del servizio clienti.
- Sicurezza completa tramite crittografia e gestione di computer desktop, computer portatili e supporti rimovibili.

SafeGuard® Enterprise Management Center versione 5.50

Architettura di sicurezza modulare e flessibile

- Moduli SafeGuard Enterprise aggiuntivi consentono la crescita della soluzione in base alle esigenze.
- Sono disponibili API di gestione con molte funzionalità per applicazioni personalizzate.
- La soluzione si integra con Microsoft Active Directory via LDAP e supporta ambienti Novell.
- Compatibilità con smartcard e token di terze parti.
- Viene garantita la comunicazione client-server protetta basata su XML/SOAP; nessuna riconfigurazione di firewall, supporta il bilanciamento del carico del traffico.

Gestione di BitLocker Drive Encryption in Windows 7 e Vista

- Sono attuabili criteri di sicurezza coerenti in ambienti di sistemi operativi e dispositivi misti.
- Le chiavi possono essere gestite centralmente con backup e recupero protetti.
- BitLocker Drive Encryption è opzionale.
- SafeGuard Enterprise offre report sullo stato del dispositivo BitLocker.

Supporto per i servizi directory

- È possibile importare dati di infrastruttura (utenti, computer, gruppi, certificati X.509 ecc.) da directory supportate di Microsoft Active Directory in base alle esigenze.
- Non sono richiesti account utente specifici di SafeGuard Enterprise.
- I responsabili della sicurezza di SafeGuard Enterprise sono selezionabili tra gli utenti di Active Directory.
- Sono supportati ambienti Novell.

Gestione delle licenze da parte degli amministratori

- È possibile attivare nuovi moduli SafeGuard semplicemente aggiornando la licenza.
- È anche possibile tenere traccia dei moduli SafeGuard Enterprise per conformità con la licenza.

Installazione automatica

- Sono supportati meccanismi di distribuzione software standard tramite pacchetti MSI, con distribuzione e installazione automatica utilizzando i sistemi di gestione del software esistenti (es. Altiris, Microsoft SCCM, NetInstall).
- Impostazioni di configurazione predefiniti consentono una rapida implementazione in ambienti di prova.
- Un programma di installazione guidata semplifica l'installazione di componenti server SafeGuard e Microsoft.

Opzioni di recupero della password e servizio clienti

- Un programma integrato di recupero guidato di tipo attesa/risposta offre assistenza con le password utente dimenticate.
- Un servizio clienti basato sul Web per ambienti in outsourcing è incluso con la licenza Management Center.
- È disponibile un'API per l'integrazione personalizzata con il servizio clienti.

- Un'opzione di autosupporto locale per il recupero di password dimenticate elimina la necessità di contattare il servizio clienti. Opzioni di autosupporto locale e domande/risposte di verifica sono configurabili attraverso il Management Center.

L'API di SafeGuard Management supporta:

- Operazioni di directory e sincronizzazione automatica
- Assegnazione da utente a dispositivo
- Assegnazione di chiavi a dispositivi/utenti
- Elaborazione di registro, inventario e report
- Gestione di certificati e token
- Domanda/risposta per applicazioni di autosupporto personalizzate

Stato, registri e report di sicurezza in tempo reale

- Tutte le attività/gli stati dei client, le azioni degli amministratori e gli eventi di sicurezza vengono registrati e archiviati centralmente per offrire assistenza nei controlli di conformità.
- I tipi di registri e i percorsi di archiviazione sono definiti dall'utente.
- Gli amministratori possono filtrare, visualizzare e stampare i rapporti di registro.
- Uno strumento SGNState autonomo opzionale offre a console esterne un report sullo stato della crittografia (es. soluzioni LANDesk o per il controllo degli accessi di rete [NAC]).

Requisiti di sistema

Sistemi operativi

- Microsoft Windows 7 (32 e 64 bit)
- Microsoft Windows Vista (32 e 64 bit; SP 1/2)
- Microsoft Windows XP (32 bit; SP 2, SP 3)
- Microsoft Windows Server 2008 e 2008 R2 (32 e 64 bit)
- Microsoft Windows Server 2003 (32 bit)

Certificazioni

- Utilizza un motore crittografico SafeGuard con certificazione FIPS 140-2
- Compatibilità con Aladdin eToken

Standard e protocolli

- Cifratura simmetrica: AES 128/256 bit
- Cifratura asimmetrica: RSA
- Funzioni hash: SHA-256, SHA-512
- Hash delle password: PKCS #5v2
- Smartcard/token: PKCS #11, PKCS #15, Microsoft CSP, PC/SC, Kerberos
- PKI: certificati PKCS #7, PKCS #12, LDAP, X.509
- Trasferimento dati: SOAP, XML, SSL

Versioni in altre lingue

- Inglese, francese, tedesco, giapponese

Database supportati

- Microsoft SQL Server 2005, 2008, Express
- Comunicazione crittografata tra database e centri di gestione

Boston, USA | Oxford, Regno Unito

SOPHOS
WWW.SOPHOS.COM