

## Configuration Protection-Modul

Um Ihre wertvollen Daten vor mutwilligen oder versehentlichen Verlusten zu bewahren, muss Ihre Sicherheitslösung Wechselmedien, physikalische und drahtlose Schnittstellen sowie die Benutzer ins Schutzkonzept miteinbeziehen. SafeGuard Configuration Protection kontrolliert und sichert Ihre Endpoints und Geräte über sämtliche Schnittstellen und garantiert eine flexible und benutzerfreundliche Data Loss Prevention.

### Erhöhte Sicherheit

- Schützt vor Datenlecks und -diebstahl sowie Eindringen und Verbreitung von Malware.
- Granulare Kontrolle: Erkennt und begrenzt Datentransfers nach Gerätetyp, Modell, Seriennummer und Dateityp.
- Datenschutz: Schützt Unternehmensdaten beim Übermitteln an externe Speicher und nimmt bei Offline-Verwendung eine Nachverfolgung vor.
- Blockiert USB- und PS/2-Hardware-Keylogger.
- Beschränkt den Einsatz der U3-Funktion (Autorun) für Wechselmedien.
- Secure Agent: Verhindert eine Umgehung der Sicherheitsrichtlinien durch transparenten Einsatz und Überwachung im Hintergrund.

### Schutzfunktionen: Nutzungskontrolle

- Ports: Erlaubt/blockiert die Nutzung.
- Geräte und Speichermedien: Nimmt Whitelisting nach Typ, Modell und Seriennummer vor.
- Stellt Lesezugriff bzw. Lese-/Schreibzugriff auf portable Speichermedien bereit.
- Blockiert USB- und PS/2-Hardware-Keylogger.
- Dateien: Schränkt Dateiübertragen je nach Dateityp ein.
- Wi-Fi: Stellt Whitelisting mittels SSID bereit.
- Blockiert hybride Netzwerkbrücken.

### Prüfung des Sicherheitsstatus am Endpoint

- Verschafft umfassend Überblick darüber, welcher Benutzer was mit welchem Endpoint verbindet.
- Überwacht sämtliche USB-, PCMCIA-, FireWire- und WiFi-Ports.
- Zeichnet alle aktuellen und beendeten Geräteverbindungen detailliert auf.
- Stellt einfache und aussagekräftige Reports bereit.

## Vorteile

### Erhöhter Systemschutz

- » Überwacht den Datenverkehr in Echtzeit und wendet darauf abgestimmte, detailliert einstellbare Sicherheitsrichtlinien für alle Arten von Schnittstellen und externen Speichergeräten an:
  - » Physikalische Schnittstellen: USB, FireWire, PCMCIA, parallel, seriell usw.
  - » Drahtlose Schnittstellen: WiFi, Bluetooth, Infrarot (IrDA)
  - » Externe Speicher: Wechselmedien, CD/DVD, mobile Festplatten usw.
- » Kontrolliert Lese-/Schreibzugriff auf Basis von Dateityp-Gruppen.

### Maximale Benutzerfreundlichkeit und einfache Verwaltung für Administratoren

- » Sperrt/erlaubt Geräte nach Typ, Modell bzw. Seriennummer.
- » Sperrt Speichermedien auf Wunsch komplett.
- » Visualisiert bestehende Verbindungen zu Unternehmens-Endpoints durch Einsatz von SafeGuard PortAuditor.
- » Setzt Sicherheitsrichtlinien durch, die die Unternehmensanforderungen erfüllen.

### Erhöhte Produktivität und Benutzerfreundlichkeit

- » Fügt sich nahtlos in bestehende Arbeitsabläufe ein.
- » Genießt hohe Akzeptanz auf Benutzerseite, da kein zusätzliches Training erforderlich ist.
- » Erhöht die Systemstabilität durch Sperren unerwünschter Geräte und Laufwerke.

## Leistungsstarke zentrale Administration

- Dank der hohen Richtlinienflexibilität können unterschiedliche Regeln für Domains, Gruppen, Computer oder Benutzer einfach festgelegt werden.
- Integration von Verzeichnisdiensten (z.B. Microsoft Active Directory) ermöglicht schnellen Import von Benutzer- und Computerdaten.
- Unabhängige auf Kernel-Ebene erfolgende Echtzeit-Analysen des systemnahen Port-Traffics optimieren das Richtlinien-Enforcement.
- Geräte im Online-Zustand, die in bestimmten Intervallen nicht mit dem Management Center kommuniziert haben, werden gemäß geltender Richtlinien blockiert und gesperrt.
- Die Kommunikation mit dem SafeGuard Management Center wird über erweiterte XML/SOAP-Protokolle realisiert.
- Alle Client-Aktivitäten/-Status und Sicherheitsereignisse werden protokolliert und zentral gespeichert. Art der Protokolle und Speicherort werden vom Benutzer festgelegt. Administratoren können Protokolldateien und Reports in der Konsole des SafeGuard Management Center\* filtern, ansehen, ausdrucken und exportieren.

## Einfache, zentral verwaltete Installation

- Über MSI-Pakete können die Installationspakete unbeaufsichtigt verteilt und installiert werden.
- Das netzwerkübergreifende Rollout ist einfach und ohne Beteiligung der Benutzer realisierbar.

\* Für zentrale Administration ist das Modul SafeGuard Enterprise Management Center erforderlich. Mehr Infos unter [www.sophos.de](http://www.sophos.de).

## Systemanforderungen

### Betriebssysteme

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

### Produktanforderungen

- » SafeGuard Management Center

### Zertifikate

- » Common Criteria EAL 2

### Sprachen

- » Deutsch, Englisch, Französisch, Italienisch, Japanisch und Spanisch
- » Unicode-basierte Unterstützung weiterer Betriebssystemsprachen

### Port-Kontrolle

#### Physikalische Schnittstellen

- » USB
- » FireWire
- » PCMCIA
- » Secure Digital (SD)
- » Parallel
- » Seriell
- » Modem

#### Drahtlose Schnittstellen

- » Wi-Fi
- » Bluetooth
- » Infrarot (IrDA)

#### Speichermedien

- » Wechselmedien
- » Externe Festplatten
- » CD/DVD-Laufwerke
- » Diskettenlaufwerke
- » Bandlaufwerke