

## Configuration Protection-Modul

Um Ihre wertvollen Daten vor mutwilligen oder versehentlichen Verlusten zu bewahren, muss Ihre Sicherheitslösung Wechselmedien, physikalische und drahtlose Schnittstellen sowie die User 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**

- Schutz vor Datenlecks und -diebstahl sowie Eindringen und Verbreitung von Malware
- Granulare Kontrolle: Erkennen und Begrenzen des Datentransfers nach Gerätetyp, Modell, Seriennummer und Dateityp
- Datenschutz: Schutz der Unternehmensdaten beim Übermitteln an externe Speicher und Nachverfolgen bei einer Offline-Verwendung
- Blockieren von USB- und PS/2-Hardware-Keyloggern
- Beschränkter Einsatz der U3-Funktion (Autorun) für Wechselmedien
- Secure Agent: Verhindert eine Umgehung der Sicherheitsrichtlinien durch transparenten Einsatz und Überwachung im Hintergrund

**Schutzfunktionen: Nutzungskontrolle**

- Ports: Erlauben/Blockieren der Nutzung
- Geräte und Speichermedien: Whitelisting nach Typ, Modell und Seriennummer
- Nur Lesezugriff bzw. Lese-/Schreibzugriff auf portable Speichermedien
- Blockieren von USB- und PS/2-Hardware-Keyloggern
- Dateien: Eingeschränkte Dateiübertragen je nach Dateityp
- Wi-Fi: Whitelisting mittels SSID
- Blockieren hybrider Netzwerkbrücken

**Prüfung des Sicherheitsstatus am Endpoint**

- Umfassender Überblick darüber, welcher User was mit welchem Endpoint verbindet
- Überblick über alle USB-, PCMCIA-, FireWire- und WiFi-Ports
- Detaillierte Aufzeichnung aller aktuellen und beendeten Geräteverbindungen
- Einfaches und aussagekräftiges Reporting

**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.
- » Kontrolle des Lese-/Schreibzugriffs auf Basis von Dateityp-Gruppen

**Mit folgenden Funktionen profitieren Administratoren von maximaler Benutzerfreundlichkeit und einfachster Verwaltung:**

- » Einfaches Zulassen/Sperren je nach Gerätetyp, -modell bzw. Seriennummer
- » Komplette Sperrung sämtlicher Speichermedien
- » Visualisierung von bestehenden Verbindungen zu Unternehmens-Endpoints durch Einsatz von SafeGuard PortAuditor
- » Enforcement von Sicherheitsrichtlinien, die die Unternehmensanforderungen erfüllen

**Erhöhte Produktivität und Benutzerfreundlichkeit**

- » Enduser müssen ihre gewohnten Arbeitsabläufe nicht ändern
- » Hohe Akzeptanz auf Userseite, da kein zusätzliches Training erforderlich ist
- » Erhöhte Systemstabilität durch Sperren unerwünschter Geräte und Laufwerke

<sup>1</sup> Mit SafeGuard PrivateCrypto (unterstützt auch 64 Bit)

## Leistungsstarke zentrale Administration

- Mittels hoher Richtlinienflexibilität einfaches Festlegen unterschiedlicher Regeln für Domains, Gruppen, Computer oder User
- Import von User- und Computerdaten mittels Integration von Verzeichnisdiensten (z.B. Microsoft Active Directory)
- Verbessertes Richtlinien-Enforcement über unabhängige auf Kernel-Ebene erfolgende Echtzeit-Analysen des systemnahen Port-Traffics
- Geräte, die nicht in bestimmten Intervallen mit dem SafeGuard Management Center kommuniziert haben, können per Richtlinie blockiert oder gesperrt werden, wenn sie online sind.
- Kommunikation mit dem SafeGuard Management Center über erweiterte XML/SOAP-Protokolle
- Alle Client-Aktivitäten/-Status und Sicherheitsereignisse werden protokolliert und zentral gespeichert. Art der Protokolle und Speicherort werden vom User festgelegt. Administratoren können Protokolldateien und Reports in der Konsole des SafeGuard Management Center\* filtern, ansehen, ausdrucken und exportieren.

## Einfache, zentral verwaltete Erstinstallation

- Die Installationspakete können zentral und unbeaufsichtigt über MSI-Pakete verteilt und installiert werden.
- Einfaches Rollout über das Netzwerk – ohne Beteiligung der Enduser

\* 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 Vista (32 Bit<sup>1</sup>, 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

<sup>1</sup>Windows 7 (32, 64 Bit) wird ab der nächsten Veröffentlichung unterstützt