Endpoint Protector Basic™

USB-Firewall – Kontrolliert USB Speichermedien

Version (32/64bit): 1.0.3.2

Die Sicherheit Ihrer Daten wird durch die Endpunkte Ihrer PCs oder Notebooks bestimmt. Ohne einen umfassenden Schutz der USB Ports können Daten ungehindert gestohlen, manipuliert oder beschädigt werden. Unbefugtes oder nicht kontrolliertes Verwenden von tragbaren Speichermedien, wie USB Sticks, iPods, MP3 Player, Digitalen Kameras, externen Festplatten, Mobiltelefonen etc., stellt heutzutage eine der größten Bedrohungen für Ihre Datensicherheit dar. Nur die zuverlässige Kontrolle von tragbaren Datenspeichern kann eine vorsätzliche oder zufällige Infektion sowie einen Datendiebstahl verhindern.

Überwachte Gerätetypen:

- *USB Sticks (Normale USB Sticks, U3, etc.)*
- *Speicherkarten (SD, MMC, CF, etc.)*
- *CD/DVD-Spieler/Brenner (intern und extern)*
- *Externe Festplatten*
- *Floppy Laufwerke*
- *Kartenleser (intern und extern)*
- *ZIP Laufwerke*
- *Digitalkameras*
- *Smartphones/BlackBerry/PDAs*
- *iPods / iPhones / iPads*
- *FireWire Geräte*
- *MP3 Player/Media Player Geräte*
- *Biometrische Geräte*
- *Bluetooth Geräte*
- *Drucker*
- *ExpressCard (SSD)*
- *Wireless USB*
- *Etc.*

Die Firewall für Ihre USB Schnittstellen

Endpoint Protector Basic verhält sich wie eine Firewall für die USB Schnittstellen. Der PC-Administrator hat die Kontrolle, welche Geräte als vertrauenswürdig eingestuft werden. Nur diese Geräte funktionieren, alle anderen Geräte können nicht mit dem PC verwendet werden.

Sicherheit für Ihren PC und Ihre Daten

Ihre Arbeitsplatz-PCs oder Notebooks werden vor Risiken und Gefahren wie Datenlecks, Datendiebstahl, Podslurping, etc., ausgehend von modernen tragbaren Datenspeichermedien, geschützt.

Verwaltung von tragbaren Datenspeichern / Geräte Typen

Der PC-Administrator kann mit der Software spezifische Geräte oder Geräte Typen autorisieren. Durch die Autorisierung einzelner Geräte wird den PC- Anwendern das Verwenden eines bestimmten Gerätes erlaubt. Jeder andere tragbare Datenspeicher, der mit dem PC verbunden wird und nicht durch den Administrator autorisiert wurde, ist nicht funktionsfähig. Speichermedien, von denen automatisch Software gestartet wird, wie z.B. U3 smart Sticks (USB Sticks mit einer CD-ROM Autorun Funktionalität), werden nicht automatisch aktiv.

E-Mail Benachrichtigung

Für den Fall, dass ein nicht autorisiertes Gerät mit einem geschützten PC verbunden wird, kann eine E-Mail Benachrichtigung an den PC-Administrator gesendet werden.

Dateiprotokollierung (File Tracing)

Die Dateiprotokollierung zeichnet jeden Datentransfer von und zu mobilen Datenträgern auf. So entsteht ein lückenloser Bericht mit Dateinamen, Zeitstempel und Benutzerdaten.

Geräteprotokoll

Für spätere Audits kann ein Protokoll über alle mit dem PC verbundenen USB Geräte erstellt werden.

"Offline" Fähigkeit

Arbeitsplatz-PCs oder Notebooks, die temporär über keine Internet-verbindung verfügen, bleiben geschützt. E-Mail Benachrichtigungen werden bei der nächsten Internetverbindung versendet.

Administrative Kontrolle / Administratorenpasswort

Das optionale Administratorenpasswort schützt die Konfiguration, falls mehrere Benutzer über die Rechte eines Administrators verfügen.

COSOSYS

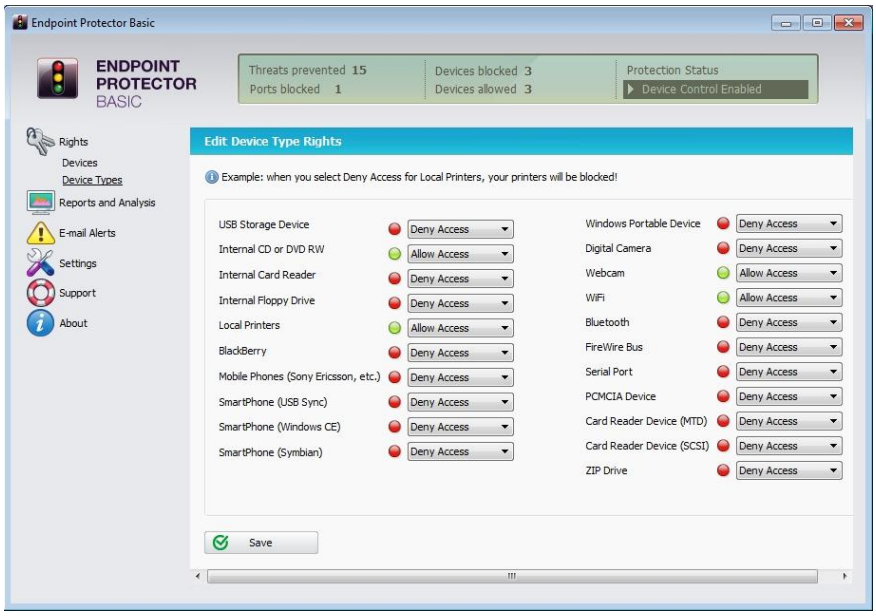
Erfahren Sie, wie Daten auf Ihren PC gelangen und durch wen Daten von Ihrem PC kopiert werden. Das Durchsetzen Ihrer Sicherheits-richtlinien und der Schutz Ihrer USB Ports ist einfacher als je zuvor.

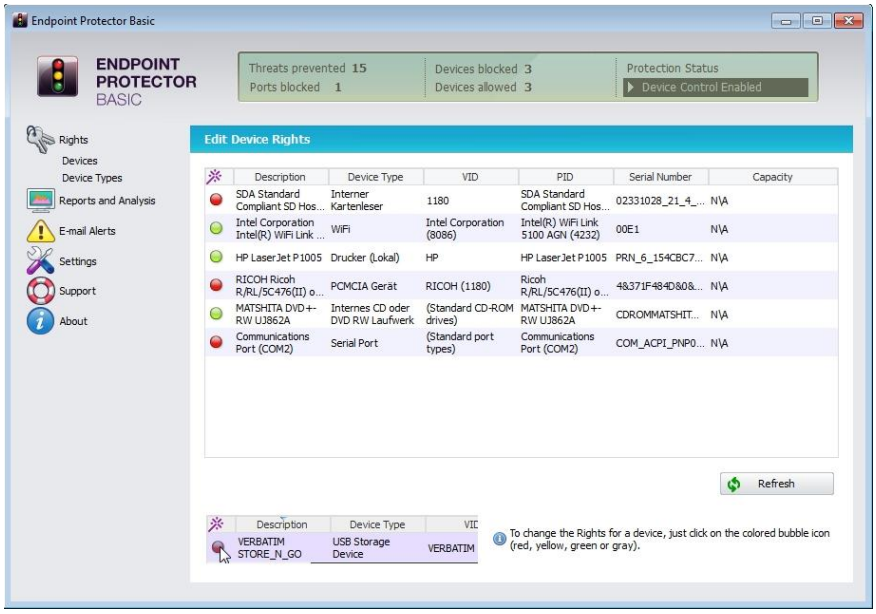
Systemanforderungen

- *Windows 7 (32/64bit)*
- *Windows Vista (32/64bit)*
- *Windows XP (SP2) (32/64 bit)*
- *Windows 2003*
- *Administratorenrechte*
- *32 MB Festplattenspeicher*

Die intuitive Bedienoberfläche erlaubt es Ihnen in wenigen Augenblicken, Ihre USB und anderen Schnittstellen erfolgreich zu schützen.

Endpoint Protector Basic ist besonders für den Einsatz in kleinen und mittelständischen Unternehmen geeignet.





Endpoint Protector Basic bietet PC Besitzern einen sicheren und komfortablen Schutz ihres Arbeitsumfelds beim Umgang mit tragbaren Datenspeichern. Der Produktivitätsvorteil durch portable Medien wird in keiner Weise eingeschränkt, da durch die Klassifizierung von vertrauenswürdigen Geräten der Einsatz dieser Geräte jederzeit ermöglicht oder eingeschränkt werden kann.

Die Benutzeroberfläche von Endpoint Protector Basic ist in mehreren Sprachen verfügbar: Deutsch, Englisch und Französisch.

Besuchen sie **www.EndpointProtector.de** für eine kostenlose Testversion und weitere Informationen.

CoSoSys Ltd.
E-Mail: sales@cososys.com
Telefon: +40-264-593110
Fax: +40-264-593113

CoSoSys North America
sales.us@cososys.com
+1-208-850 7563

CoSoSys Deutschland
sales.de@cososys.com
+49-7541-978-2627-0
+49-7541-978-2627-9

Created on 18 December 2010