17.03.09
Von: pat

Endpoint Protector 2009: Verbesserter Schutz für Unternehmensdaten

CoSoSys bringt eine neue überarbeitete Version ihrer erfolgreichen Endpunkt Sicherheitslösung heraus. Mit Endpoint Protector 2009 wird die Kontrolle tragbarer Datenspeicher, der Schutz vor Datenverlusten und die Sicherheit im Unternehmen perfektioniert.
Die neue Version 2009 beinhaltet eine verbesserte Bedienung, optimierte Schutzmechanismen für die Schnittstellen USB, Firewire, Bluetooth etc. sowie neue Funktionen, um die Produktivität jeder Organisation zu erhöhen.

CoSoSys, Hersteller für Software zur Überwachung, Sicherung und Kontrolle tragbarer Speichermedien veröffentlicht die Version 2009 von Endpoint Protector zum Schutz vor Informationsmissbrauch, Datenverlusten und Datendiebstahl. Die aktuelle wirtschaftliche Gesamtsituation verstärkt die Risiken und den Druck für Unternehmen jeder Größe. Mitarbeiter, die um ihre Zukunft bangen, sind besonders anfällig für die Preisgabe von Firmendaten bis hin zum vorsätzlichen Kopieren von vertraulichen Kundendatenbanken.

Endpoint Protector 2009 ist die derzeit modernste Lösung, um Datenverluste über die am PC befindlichen Schnittstellen (wie USB, Firewire, Bluetooth etc.) zu verhindern. Die Interna einer Organisation sind vor „Abfluss“ geschützt (Data Loss Prevention).

In der neuesten Version bietet Endpoint Protector 2009 zum bereits bestehenden Geräte-Whitelistverfahren das neue Datei-Whitelist-verfahren. Diese bislang einmalige Funktion ermöglicht es Organisationen, genau festzulegen, welche Daten auf tragbare Datenspeicher kopiert werden dürfen. Selbstverständlich kann Endpoint Protector 2009 wie bisher auch alle Kopiervorgänge protokollieren.

Eine weitere neue Funktion ist der globale „Lockdown“. Die gesamten Endpunkte des Netzwerks werden gleichzeitig gesperrt. Tragbare Geräte sind blockiert und begonnene Datentransfers unterbrochen.

Das neue WEB Cockpit von Endpoint Protector 2009 bedeutet eine enorme Zeitersparnis für Administratoren. Die von Grund auf erneuerte WEB-basierte Benutzeroberfläche des Administratorenbereichs ist mehrsprachig (Deutsch, Englisch, Französisch, Ungarisch und Rumänisch), intuitiv bedienbar und anwenderfreundlich gestaltet. Die hinzugefügten

Assistenten vereinfachen, erleichtern und beschleunigen viele Arbeiten. Durch die neue System-Snapshot Funktion wird ein schnelles Wiederherstellen früherer Einstellungen und Policies möglich.

Endpoint Protector 2009 bietet eine große Anzahl an überwachten Gerätetypen, von iPods, Digitalkameras und USB Sticks bis hin zu SSD ExpressCards und Druckern. Zudem wurde die Synchronisation mit dem Active Directory verbessert.

Für Firmennetzwerke, in denen Benutzer über Administratorenrechte verfügen, wurde ein zusätzlicher Schutz eingerichtet, der es Benutzern unmöglich macht, die Software zu stoppen oder zu deinstallieren.

„Unser Ziel ist es, Unternehmen jeder Größe aus allen Branchen die Freiheit zu geben, in einem sicheren Umfeld mit tragbaren Datenspeichern zu arbeiten“, sagt Roman Foeckl, CoSoSys CEO. „Durch die aktive Kontrolle der zugelassenen mobilen Geräte können Missbrauch und Datenverluste verhindert werden. Unternehmen erreichen somit eine Steigerung der Produktivität beim Einsatz mobiler Datenspeicher, die risikoarm, kontrolliert und überwacht zum Einsatz kommen“.

Endpoint Protector 2009 wurde entwickelt, um Gefahren, die von innen ausgehen, zu minimieren, die Risiken von Datendiebstahl und Datenverlusten zu reduzieren und jede Nutzung tragbarer Datenspeicher zu überwachen. Die Software gibt der IT-Abteilung die Werkzeuge, die benötigt werden, um präventiv die Verwendung tragbarer Datenspeicher zu reglementieren und alle Datentransfers von und zu den Geräten zu protokollieren. Zudem kann eine Verschlüsselung aller Daten auf tragbaren Datenspeichern erzwungen werden, damit auch im Falle eines Verlustes die Informationen geschützt sind. Die neue Endpoint Protector 2009 Version ist als **kostenlose 30 Tage Version** zum Download oder online als Demo unter http://www.EndpointProtector.com verfügbar.

- Verwandte Themen
- Trend Micro: Eine DLP-Lösung verhindert zum Beispiel, dass bis zu einen gewissen Datum außerhalb der Buchhaltung Jahresbilanzen eingesehen werden können
- Lumension Security: Data Loss Prevention reicht von der Sicherung sensibler Daten auf Desktop-Rechnern und Notebooks bis zu mobilen Geräten und austauschbaren Datenträgern
- T-Systems: Ein umfassendes Information Lifecyle Management im Unternehmen ist die wichtigste Grundlage für DLP