



BEEWATEC

Processes connected with flexibility

Know-how-Schutz für BeeWaTec

PROFIL

Branche

Betriebsausstattungen

Die Herausforderung

Konstruktionszeichnungen, Baupläne und Kundendaten vor Datenverlust und Datendiebstahl schützen

Die Lösung

Endpoint Protector 4

Warum Endpoint Protector?

- Device Control und Content Aware Protection für Fat und Thin Clients
- Zwangsverschlüsselung als Funktion von Device Control
- Granulare Einstellmöglichkeit bis auf User-Ebene
- Benutzeroberfläche intuitiv bedienbar

BeeWaTec schützt Konstruktionen und Pläne für Betriebseinrichtungen und Intra-logistik-Lösungen mit Endpoint Protector



Immer wieder ist zu lesen, dass mittelständische Unternehmen den Wert ihrer Daten unterschätzen und daher den Schutz vor ungewollter Herausgabe vernachlässigen. Nicht so die BeeWaTec GmbH mit Sitz in Pfullingen. Sie ist spezialisiert auf Lösungen für innerbetriebliche Logistik und stellt Montage-Arbeitsplätze, fahrerlose Transportsysteme für die bedarfsgerechte Bereitstellung von Produktionsmaterial und Baukastensysteme für Produktionshilfsmittel wie Regale her. Zudem bietet BeeWaTec mit dem Produktbereich „Basics“ alles, was moderne Firmen für Büro-, Betriebs- und Lagereinrichtungen benötigen. Mit diesen Lösungen sorgt der Anbieter in Werkstätten und den Werkshallen produzierender Unternehmen in ganz Europa für effizientes Arbeiten.

Jede Menge unternehmenskritische Daten

Da das Unternehmen die Systeme selbst entwickelt und optimiert und den Aufbau von Montagelinien und Lagersystemen kundenspezifisch plant, stellen Konstruktionszeichnungen, Baupläne und Kundendaten das entscheidende Know-how und damit das wichtigste Kapital dar. Um diese Daten vor ungewolltem Abfluss zu schützen, werden bereits seit Jahren die USB-Schnittstellen der PCs blockiert. Gleichzeitig wird so verhindert, dass Schadcode über Speichersticks ins Firmennetz gelangt.



**ENDPOINT
PROTECTOR**

„Endpoint Protector gefällt uns sehr, weil die Lösung von der Funktionalität her sehr komplex ist und uns große Flexibilität bei den Einstellmöglichkeiten der Policies gibt. Gleichzeitig ist die Benutzeroberfläche sehr übersichtlich aufgebaut, wir konnten sie vom ersten Moment an intuitiv bedienen und die dahinterliegende Logik leicht nachvollziehen.“

**Jennifer Konrad,
IT-Administratorin
BeeWaTec GmbH**

Immer mehr potenzielle Lecks

„Dann wurden als Reaktion auf die wachsende Gefahr von ungewolltem Datenverlust strengere Sicherheitsrichtlinien eingeführt und weitere Schnittstellen blockiert“, sagt Jennifer Konrad, IT-Administratorin bei BeeWaTec und verantwortlich für Netzwerk, Storage, Backup und Datenbanken an insgesamt sieben Standorten in Deutschland und den Nachbarländern. Schnell zeichnete sich ab, dass die bestehende Lösung den gestiegenen Anforderungen nicht gewachsen war. „Da die Mitarbeiter mit Kunden und Partnern Daten austauschen müssen und dafür z. B. FTP und unterschiedliche Portale nutzen, mussten immer mehr Freigaben eingetragen werden, um die Arbeitsabläufe nicht zu beeinträchtigen“, erläutert sie. „Allerdings konnten die Freigaben nur jeweils für alle Devices oder Schnittstellen erteilt und nicht auf einzelne Abteilungen, Gruppen oder Nutzer heruntergebrochen werden.“ Bald wies der Schutz vor ungewolltem Datenverlust mehr Löcher auf als ein Emmentaler Käse.

Policies bis auf User-Ebene herunterbrechen

Die Lücken wollte BeeWaTec mit einer neuen DLP-Lösung schließen. „Die Hauptanforderungen waren, dass sie jede Art von Schnittstellen, ob physisch oder nicht, an den Endpoints überwachen kann und granulare Einstellmöglichkeiten bis auf User-Ebene bietet“, sagt die Administratorin. „Auch die Thin Clients, die wir neben den PCs im Unternehmensnetz einsetzen, sollte die neue Lösung überwachen.“ Weiterhin war die Anbindung an das Active Directory erforderlich. Für eine möglichst einfache Bedienung sollte die Lösung einer Logik folgen, die sich ohne langwierige Schulung oder Beschäftigung mit dem Handbuch erschließt. Bei einer Internetrecherche stieß sie auf Endpoint Protector von CoSoSys und nahm die Software neben den Produkten anderer Hersteller in die engere Wahl.

Geht doch: technisch komplex, einfach zu bedienen

In einer Testumgebung konnten die Favoriten zeigen, welches Funktionsspektrum tatsächlich in ihnen steckt und wie sie sich handhaben lassen. „Endpoint Protector gefiel uns sehr, weil die Lösung von der Funktionalität her sehr komplex ist und uns dadurch große Flexibilität bei den Einstellmöglichkeiten der Policies gibt“, beschreibt Konrad ihre Eindrücke aus der Vorab-Installation. „Gleichzeitig erschien uns die Benutzeroberfläche sehr übersichtlich aufgebaut, wir konnten sie vom ersten Moment an intuitiv bedienen und die dahinterliegende Logik leicht nachvollziehen.“ Weitere Pluspunkte sammelte Endpoint Protector mit der zentralen webbasierten Oberfläche für Administration und Reporting und dem im Vergleich zu anderen Lösungen sehr guten Preis-/Leistungs-Verhältnis. >>



**ENDPOINT
PROTECTOR**

Über Endpoint Protector 4

Endpoint Protector 4 schützt Windows-, Mac- und Linux-Rechner vor Datenverlust, Datendiebstahl und Datenlecks, indem alle Datentransfers zu cloud-basierten Diensten und Anwendungen wie Webbrowser, E-Mail, Skype überwacht und gegebenenfalls blockiert werden. Die Lösung überwacht auch den Einsatz tragbarer Speichermedien wie USB-Sticks, CDs / DVDs, HDDs oder Speicherkarten an Endpoints mit den Betriebssystemen Windows, Mac und Linux. Starke Sicherheitsrichtlinien verhindern, dass Daten unrechtmäßig oder aus Versehen das Unternehmen verlassen.

Zusatzschutz durch Zwangsverschlüsselung

BeeWaTec entschied sich daher für Endpoint Protector und erwarb 170 Lizenzen für die PCs und Thin Clients. Eingesetzt werden die Module Device Control und Content Aware Protection sowie die Verschlüsselungslösung EasyLock. „Wir hatten ursprünglich nicht damit gerechnet, dass Zwangsverschlüsselung als eine Funktion von Gerätekontrolle verfügbar ist und über dieselbe Oberfläche wie die anderen Module bedient werden kann“, sagt Konrad. Sie begründet den Erwerb der Zusatzfunktion mit der höheren Sicherheit, den EasyLock für die Daten bietet, die die Mitarbeiter auf USB-Sticks zu den Kunden mitnehmen. Bei Bedarf könnte die IT-Administration mittels eines Unternehmenszertifikates sogar unterbinden, dass die Mitarbeiter Firmendaten auf ihren privaten Rechnern zur Weiterbearbeitung speichern, wo sie sich außerhalb der Kontrolle des Unternehmens befinden und für Wirtschaftsspione leichtere Beute sein können als im Unternehmen.

Mehr Sicherheit mit wenigen Mausklicks

Mit dem Handling von Endpoint Protector und den bisher installierten Funktionen ist sie sehr zufrieden. Auch die Zusammenarbeit mit Endpoint Protector ließ nichts zu wünschen übrig. Auf Fragen und Unklarheiten, die sich bei der Einrichtung ergaben, habe der Support unmittelbar reagiert und Hinweise und Tipps für schnelle Lösungen gegeben.

Als erster Schritt wurden die Policies umgesetzt, die schnell zu mehr Sicherheit führen, die Überwachung der USB-Ports. Nicht jeder Mitarbeiter muss Daten auf Sticks ziehen, die Nutzung der Speichermedien wird an allen Rechnern blockiert. Ausnahmen gibt es für diejenigen, die Unterlagen beim Kunden präsentieren. An diesen Endpoints lassen sich nur genehmigte Devices anschließen; die Mitarbeiter können keine Sticks benutzen, die sie von zuhause mitbringen. So werden Malwarebefall und Spionageangriffe per BadUSB verhindert. Die Verschlüsselungskomponente sorgt dafür, dass die Daten durch Unbefugte nicht einsehbar sind.

Die weiteren Policies kommen an die Reihe, sobald Konrad Zeit dafür findet. „Einmal eingerichtet, benötigt die Lösung keine Betreuung und stellt keine zusätzliche zeitliche Belastung dar“, freut sie sich. „Nur wenn Geräte neu hinzukommen, muss ich handeln, aber das ist im Handumdrehen erledigt.“

Endpoint Protector GmbH

E-Mail: info@endpointprotector.de

Tel: +49-7541-97826-730

Fax: +49-7541-97826-279

CoSoSys Ltd.

sales@cososys.com

+40-264-593110

+40-264-593113

CoSoSys USA

sales.us@cososys.com

+1-888-271-9349



**ENDPOINT
PROTECTOR**

© Copyright 2004-2016 CoSoSys Ltd. All rights reserved. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin, EasyLock, Endpoint Protector Basic, My Endpoint Protector and Endpoint Protector are trademarks of CoSoSys Ltd. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).