



BMTS Technology schützt geistiges Eigentum mit Device Control von Endpoint Protector

Keine Chance für Industriespionage

CASE STUDY | AUTOMOBILZULIEFERER

PROFIL

Branche

Automobilzulieferer

Die Herausforderung

Für den internen Datenaustausch Cloud-Dienste nutzen statt USBSticks und das geistige Eigentum schützen

Die Lösung

Endpoint Protector
Device Control

Warum Endpoint Protector?

- Durchdachte Funktionen
 - Skalierbarkeit
 - Keine gegenseitige Beeinflussung mit anderen Lösungen
-

Über BMTS Technology

BMTS Technology GmbH & Co. KG (www.bmturbosystems.com), entstanden aus einem Joint-Venture der Automobilzulieferer Bosch und Mahle, entwickelt und fertigt innovative Abgasturbolader für Pkw, leichte Nutzfahrzeuge und Off-Highway-Anwendungen. Turbolader spielen eine zentrale Rolle für die Leistung und Effizienz der Motoren; sie verringern die Emissionen und machen die Motoren umweltfreundlicher.

Die Herausforderung

An der Entwicklung und Produktion der Turbolader sind rund 1.300 BMTS-Mitarbeiter an vier Standorten in Deutschland, Österreich und China beteiligt. Das macht den Datenaustausch über Ländergrenzen hinweg notwendig – und den Schutz der Daten vor unkontrolliertem Abfluss.

Bislang nutzten die Mitarbeiter mobile Datenträger vom USB-Speicher bis zum Smartphone. An deren Stelle sollten zentrale Cloud-Dienste treten, damit die Durchgängigkeit der Abläufe verbessert wird und das Unternehmen sein geistiges Eigentum angemessen schützen kann. Für die Kontrolle der mobilen Datenträger suchte BMTS Technology eine skalierbare Lösung für Device Control, die granular einstellbar ist und für Gruppenrechte die Verwendung des Active Directory erlaubt.



„Endpoint Protector bietet einen hervorragenden Funktionsumfang für die Schnittstellenkontrolle, und alles, was wir von der Lösung erwartet haben, hat von Anfang an einwandfrei funktioniert.“

Ata Gülerüç
IT-Leiter, BMTS Technology
GmbH & Co. KG

Über Endpoint Protector

Endpoint Protector schützt Windows-, Mac- und Linux-Rechner vor Datenverlust, Datendiebstahl und Datenlecks, indem alle Datentransfers zu cloudbasierten 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, Speicherkarten an Endpoints mit den Betriebssystemen Windows, macOS und Linux. Starke Sicherheitsrichtlinien verhindern, dass Daten unrechtmäßig oder aus Versehen das Unternehmen verlassen.

Die Lösung

Die Wahl von BMTS Technology fiel auf Device Control von Endpoint Protector. Das Unternehmen betreibt die Lösung als virtuelle Appliance auf zwei Servern in Europa und China mit Lizenzen für die Kontrolle der Arbeitsplatzrechner. Der Rollout der Client-Komponente erfolgte im laufenden Betrieb. Gegenseitige Beeinflussungen mit anderen Lösungen wie dem Virenschutz treten nicht auf.

Ausschlaggebend für die Entscheidung war der über die Anforderungen hinausgehende Funktionsumfang für die Schnittstellenkontrolle. Endpoint Protector überzeugte durch intelligente Funktionen wie die Möglichkeit, dass private iPhones als Modem für eine VPN-Verbindung genutzt werden können, während ihre Verwendung als Datenspeicher am Endpunkt blockiert ist. Auch die Granularität bis auf die Ebene einzelner Geräte lässt keine Wünsche offen.

Das IT-Team von BMTS Technology ist hoch zufrieden mit Endpoint Protector. Die Lösung arbeitet einwandfrei, und der Support, der das Team bei der Installation unterstützt hat, hat ganze Arbeit geleistet.

Endpoint Protector GmbH

E-mail info@endpointprotector.de
Tel +49 7541 978 26730
Fax +49 7541 978 26279

CoSoSys Ltd.

sales@cososys.com
+40 264 593 110
+40 264 593 113

CoSoSys USA

sales.us@cososys.com
+1-888-271-9349