ENDPOINT PROTECTOR

AED Engineering

AED Engineering schützt Windows- und Linux-Rechner mit Endpoint Protector

CASE STUDY | AED Engineering

PROFIL

Branche

Soft- und Hardware-Entwicklung

Die Herausforderung

Plattform-übergreifende Data Loss Prevention für Windows- und Linux-Rechner

Die Lösung

Endpoint Protector DC, CAP, eDiscovery, EasyLock

Warum Endpoint Protector?

- Unterstützung für Windows und Linux
- Auswertungen auf Knopfdruck
- Kontrolle über Dateibewegungen

www.**endpointprotector**.de

Über AED Engineering

Die AED Engineering GmbH in München ist spezialisiert auf Ingenieursdienstleistungen für Embedded Elektronik. Mit rund 60 Mitarbeitern entwickelt sie Software beispielsweise für Bordnetzarchitekturen, Fahrerassistenzsysteme oder Wireless Sensoren für Kunden in der Automobilindustrie, Luftfahrt, Medizintechnik und Telekommunikation. Darüber hinaus übernimmt AED die Entwicklung von Embedded Hardware von der Konzeption bis zur Serienfertigung und bestückt Prototypen und Kleinserien auf einer eigenen Elektronikfertigungslinie.

Die Herausforderung

Da AED mit Unternehmen der Automobilindustrie zusammenarbeitet, ist sie gehalten, die dort üblichen Standards umzusetzen. Für die Informationssicherheit ist der Standard TISAX (Trusted Information Security Assessment Exchange) maßgeblich. Im Zuge einer Umstellung der IT-Landschaft und der anstehenden TISAX-Zertifizierung sollte der Sicherheitslevel durch eine DLP-Lösung angehoben und der Schutz sowohl personenbezogener Daten als auch sensibler Informationen und geistigem Eigentum vor unerwünschtem Abfluss verbessert werden. Die einzusetzende Lösung sollte die Benutzerzuordnung aus dem Active Directory erlauben sowie bei der Administration und der Erstellung von Auswertungen möglichst wenig Aufwand verursachen. Da in der Software-Entwicklung Linux-Rechner verwendet werden, war die Hauptanforderung die plattformübergreifende Unterstützung für Windows und Linux.

“Mit Endpoint Protector steht uns DLP wie auf Windows auch für unsere Linux-Rechner zur Verfügung, in Kombination mit komfortablen Tools für die Überwachung von Geräten und Dateitransfers und die Erstellung von Auswertungen. Wir sind sehr zufrieden.”

Steffen Prochnow,
Systemadministrator,
AED Engineering GmbH

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 Geschäftsleitung und die IT der AED diskutierten unterschiedliche Lösungsansätze; die Produkte mehrerer Anbieter wurden evaluiert, darunter Endpoint Protector. Während bei den allgemeineren Anforderungen Unterschiede zwischen den Produkten nicht gravierend erschienen, sah dies bei der Hauptanforderung anders aus: Endpoint Protector überzeugte ganz eindeutig bei der Unterstützung der verschiedenen Betriebssysteme. Die Entscheidung fiel daher zugunsten von Endpoint Protector.

AED beschaffte die Lösung als virtuelle Appliance mit Lizenzen für insgesamt 80 Windows- und Linux-Rechner über sämtliche von Endpoint Protector angebotenen Module – Device Control, Content Aware Protection, eDiscovery und EasyLock – hinweg. Die Installation ging in Minutenschnelle und ohne Probleme vonstatten; nach einer kurzen Einweisung durch Mitarbeiter von Endpoint Protector konnten die ersten Richtlinien eingerichtet werden. Diese hatte die IT zuvor mit der Geschäftsführung festgelegt, sie waren an die Mitarbeiter kommuniziert worden und wurden dann in der neuen Lösung technisch umgesetzt und nach und nach aktiv geschaltet.

Im Vordergrund stehen die Richtlinien für den Umgang mit Speichermedien. Die Mitarbeiter können keine fremden mobilen Geräte mehr an ihren Rechnern verwenden. Nach einer Bestandsaufnahme, bei der die IT-Administration durch das breite Spektrum angeschlossener Geräte überrascht war, wurden sie komplett gesperrt. Die Administration kann alle Datentransfers überwachen und Auswertungen unter unterschiedlichen Gesichtspunkten vornehmen. Mit der Verwaltung der Lösung ist sie nur wenige Minuten im Monat beschäftigt. Lediglich für Ubuntu 18 war Support von Endpoint Protector erforderlich.

Seit der Inbetriebnahme hat Endpoint Protector alle Erwartungen erfüllt; IT-Administration und Geschäftsführung der AED sind mit der Lösung und der Unterstützung durch das Team von Endpoint Protecor sehr zufrieden.

ENDPOINT PROTECTOR

	Endpoint Protector GmbH	CoSoSys Ltd.	CoSoSys USA
E-Mail	info@endpointprotector.de	sales@cososys.com	sales.us@cososys.com
Tel	+49 7541 978 26730	+40 264 593 110	+1-888-271-9349
Fax	+49 7541 978 26279	+40 264 593 113	