



## Dialogmarketing-Dienstleister AMEVIDA schützt 3.000 Arbeitsplätze mit Endpoint Protector

CASE STUDY | AMEVIDA

### PROFIL

#### Branche

Dialogmarketing

#### Die Herausforderung

Eine nicht mehr unterstützte Lösung für Gerätekontrolle schnell und mit wenig Arbeitsaufwand ablösen

#### Die Lösung

Endpoint Protector Device Control

#### Warum Endpoint Protector?

- Verwendung wichtiger USB-Geräte trotz USB-Sperre
- Zeitlich begrenzte Freigaben für Sonderfälle

### Über AMEVIDA

Die AMEVIDA SE gehört zu den führenden Anbietern von Customer-Care-Dienstleistungen in Deutschland. Seinen Kunden, insbesondere großen Unternehmen aus Branchen wie Banken und Versicherungen, der Telekommunikation und Informationstechnologie, der Automobilindustrie und Energiewirtschaft sowie Handel und Industrie bietet das Unternehmen ein hochaktuelles Portfolio an Dienstleistungen für Kundenkontaktmanagement für die Bereiche Verkauf, Service und Support. AMEVIDA beschäftigt etwa 2.300 Mitarbeiter am Hauptsitz in Gelsenkirchen und an sechs weiteren Standorten im Ruhrgebiet.

### Die Herausforderung

Dialogmarketing nutzt personenbezogene Daten, die AMEVIDA von den Kunden bereitgestellt werden. Als Auftragsdatenverarbeiter laut DSGVO ist der Dienstleister zum Schutz der anvertrauten Daten verpflichtet und wird im Hinblick darauf von den Auftraggebern auditert. Um die Verwendung von USB-Geräten an den Rechnern einzuschränken, nutzt er deshalb bereits seit Jahren eine Lösung für Gerätekontrolle. Weiterhin muss AMEVIDA Kunden-Vorgaben bei der eingesetzten Hard- und Software einhalten.

Als die neueste Rechner-Generation eingesetzt werden sollte, stellte sich heraus, dass das bisherige Betriebssystem Windows 7 auf den Rechnern nicht mehr installiert werden kann. Die bisher verwendete DLP-Software funktionierte jedoch nicht unter Windows 10, das mit den neuen Rechnern ausgeliefert worden war. Unter großem Zeitdruck musste daher eine neue Lösung gefunden und installiert werden.

“Wir sind sehr zufrieden mit Endpoint Protector. Device Control bietet uns alles, was wir für den Schutz der Auftraggeber-Daten benötigen, und zudem entspanntes Arbeiten dank cleverer Funktionen.”

Florian Liebs,  
Projektmanager,  
AMEVIDA SE

## 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

Eine Internet-Recherche machte AMEVIDA auf Endpoint Protector aufmerksam. Gleich beim ersten Blick auf die Funktionalität des Moduls Device Control zeigte sich, dass sie perfekt zu den Anforderungen passt: Die USB-Ports an den Rechnern können komplett gesperrt werden, zugleich ist per Gruppenrichtlinie die Verwendung bestimmter Geräte mit USB-Anschluss wie der Headsets möglich. Weiterhin können in Ausnahmefällen USB-Ports unkompliziert freigegeben werden. Dass diese Freigaben zeitlich begrenzt erteilt werden können, gefällt der IT-Administration sehr gut, denn die Befristung spart einen Arbeitsschritt. Das gilt auch für die Angaben in den E-Mails, mit denen Mitarbeiter um Freigaben außer der Reihe nachsuchen. Da der Rechnername mit angezeigt wird, weiß der Administrator ohne Nachfrage, für welchen Rechner er die Freischaltung konfigurieren muss.

AMEVIDA entschied sich für Endpoint Protector und erwarb die virtuelle Appliance mit 3.000 Lizenzen für Device Control. Außer den Arbeitsplatzrechnern für die etwa 2.300 Mitarbeiter wurden auch die mobilen Rechner im Unternehmen abgesichert; weitere Lizenzen wurden auf Vorrat beschafft, da das Unternehmen von Mitarbeiterwachstum in der nächsten Zeit ausgeht. Die Installation der neuen Lösung auf dem Server, der Rollout der Client-Software auf die Endgeräte, die Einrichtung der Richtlinien, die Inbetriebnahme – alle Schritte waren selbsterklärend und verliefen störungsfrei.

Die IT-Abteilung von AMEVIDA ist rundum zufrieden mit Endpoint Protector und der neuen Lösung. Der Anbieter hielt das Tempo mit, das die IT vorlegen musste, um das zusätzliche Projekt beim Hardware-Austausch zeitnah umsetzen zu können. Die Software bietet die Funktionalität, die AMEVIDA benötigt. Sie erlaubt intuitives, zügiges Arbeiten und hat sich mit einem Administrationsaufwand von weniger als zehn Minuten täglich als erfreulich wenig zeitintensiv herausgestellt.



**ENDPOINT  
PROTECTOR**

### Endpoint Protector GmbH

E-Mail [info@endpointprotector.de](mailto:info@endpointprotector.de)  
Tel +49 7541 978 26730  
Fax +49 7541 978 26279

### CoSoSys Ltd.

[sales@cososys.com](mailto:sales@cososys.com)  
+40 264 593 110  
+40 264 593 113

### CoSoSys USA

[sales.us@cososys.com](mailto:sales.us@cososys.com)  
+1-888-271-9349