



# Die Märkte Stuttgart schützen personenbezogene Daten mit Endpoint Protector Device Control

## CASE STUDY | Märkte Stuttgart

### PROFIL

#### Branche

Marktwesen

#### Die Herausforderung

Die Benutzung von USB-Speichermedien verhindern, ohne die Arbeit zu beeinträchtigen

#### Die Lösung

Endpoint Protector Device Control

#### Warum Endpoint Protector?

- Einfache Bedienung
- Richtlinien für einzelne Benutzer und Geräte
- USB-Verschlüsselung kann ergänzt werden

## Über die Märkte Stuttgart

Das Marktwesen in Stuttgart ist eng mit der Entwicklung der Stadt verbunden. Bereits im dreizehnten Jahrhundert gab es in der Stadt regelmäßig Wochen- und Jahrmärkte. Heute betreibt die Märkte Stuttgart GmbH die schönste Markthalle Deutschlands, ein historisches Jugendstilgebäude, und den Großmarkt. Zudem organisiert sie weitere Märkte wie Wochen-, Floh- und Krämermärkte. In ihrer Hand liegt die Bereitstellung und Instandhaltung der gesamten Infrastruktur, die für die Märkte benötigt wird, von der Vergabe der Standplätze über die Energieversorgung bis zur Abfallbeseitigung.

## Die Herausforderung

Im Zusammenhang mit dem Betrieb und der Organisation der Märkte verarbeiten die Märkte Stuttgart in erheblichem Umfang personenbezogene Daten wie Adress-, Kontakt- und Kontodaten. Neben den PCs in der Geschäftsstelle sind zahlreiche externe Erfassungssysteme im Einsatz, die ebenfalls eine USB-Schnittstelle aufweisen: Wiegeterminals auf dem Großmarkt, Messgeräte für den Stromverbrauch, Fahrerkarten für die LKW-Fahrer. Die Daten werden auf mobilen Erfassungssystemen oder USB-Speichern transportiert und in der Geschäftsstelle ausgelesen. Daraus ergab sich im Hinblick auf die Umsetzung der DSGVO Handlungsbedarf, um die sensiblen Daten vor unbefugtem Zugriff, Verlust und Datendiebstahl zu schützen.

„Mit Endpoint Protector haben wir die volle Kontrolle darüber, wer wann über welche Schnittstelle Daten ein- oder ausschleust, und können bei der Verwendung von USB-Sticks DSGVO-konform arbeiten.“

Klaus Broghammer  
IT-Leiter, Märkte Stuttgart 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.



## ENDPOINT PROTECTOR

## Die Lösung

Eine Lösung für Gerätekontrolle sollte die mit USB verbundenen Risiken verringern. Die Märkte Stuttgart beauftragten ihren IT-Dienstleister, die H+S Systemhaus GmbH, mit der Suche nach einem einfach zu bedienenden, granular einstellbaren Produkt. Dieser schlug nach einer Testinstallation Endpoint Protector vor, da die Lösung nicht nur die Basisanforderungen im Zusammenhang mit Device Control erfüllte, sondern darüber hinaus weitere Optionen wie USB-Verschlüsselung und das gesamte Funktionsspektrum für Data Loss Prevention mit Inhaltskontrolle bietet.

Die Märkte Stuttgart nutzen das Modul Device Control für 30 Endgeräte, in erster Linie PCs und Wiegeterminals. Zunächst wurden sämtliche Schnittstellen einschließlich der USB-Ports auf allen Endgeräten blockiert. Für Peripheriegeräte wie Maus und Tastatur wurden Richtlinien eingestellt, die das Anschließen anderer Geräte unterbinden. Da nur wenige Mitarbeiter mobile Festplatten, USB-Sticks oder Kartenleser an ihrem Rechner verwenden müssen, wurden für sie die Schnittstellen freigeschaltet, die sie für ihre tägliche Arbeit benötigen.

Alle anderen, die Geschäftsleitung eingeschlossen, müssen bei Bedarf eine zeitlich befristete Freigabe für die gewünschte Schnittstelle einrichten lassen. Da sich die Richtlinien bis auf die Ebene einzelner Benutzer, Rechner und mobiler Datenträger definieren lassen, lässt sich ein USB-Port einfach und schnell freischalten, wenn sich beispielsweise durch Abwesenheit eines Kollegen die Notwendigkeit ergibt, dass ein anderer Kollege einspringt, der normalerweise keine Berechtigung hat.

Mit Device Control können die Märkte Stuttgart kontrollieren, wer wann über welche Schnittstelle Daten ein- oder ausschleust, und die USB-Geräte im Unternehmen im Hinblick auf die DSGVO sicher verwenden.

### 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