ENDPOINT PROTECTOR | by CoSoSys

Landkreis Heidenheim

600 DC- und EasyLock-Lizenzen von Endpoint Protector für das Landratsamt Heidenheim

CASE STUDY | Landratsamt Heidenheim

Profil

Branche

Verwaltung

Die Herausforderung

Compliance mit BSI-Standards für IT-Sicherheit und Schutz personenbezogener Daten für 600 Rechner

Die Lösung

Endpoint Protector

Warum Endpoint Protector?

Ausschlaggebend für die Entscheidung des Landratsamtes Heidenheim für Endpoint Protector war die Möglichkeit, Richtlinien für die Verwendung von mobilen Devices, insbesondere USB-Sticks, hochgradig granular an 600 Rechnern umzusetzen.

Über das Landratsamt Heidenheim

Der baden-württembergische Landkreis Heidenheim mit reizvollen Naturlandschaften, Fundstätten aus der Eiszeit, jahrhundertelanger Tradition als Wirtschaftsregion und modernen Industriestandorten liegt auf der östlichen Schwäbischen Alb im Dreieck Stuttgart – Nürnberg – München. Für die elf Städte und Gemeinden mit 133.000 Einwohnern hat das Landratsamt Heidenheim die Doppelfunktion als untere staatliche Verwaltungs- und kommunale Selbstverwaltungsbehörde inne. Etwa 600 Mitarbeiter sind zuständig für eine Vielzahl von Aufgaben von Arbeitsschutz bis Veterinärwesen, einschließlich Gesundheit, Landwirtschaft und Waffenrecht.

Die Herausforderung

Als EU-Zahlstelle für die Auszahlung von EU-Mitteln für die Landwirtschaft muss das Landratsamt Heidenheim für ein angemessenes Niveau bei der IT-Sicherheit die BSI-Standards gemäß IT-Grundschutz umsetzen und wird regelmäßig auditiert. Da im Landratsamt bis zur Implementierung einer verschlüsselten Cloud zahlreiche Arbeitsprozesse auf die Verwendung von USB-Sticks angewiesen sind, ist strikte Gerätekontrolle an den 600 PC-Arbeitsplätzen ein wichtiger Baustein der IT-Sicherheit, um den Eintrag von Schadcode zu verhindern.

Endpoint Protector deckt unsere Anforderungen sehr gut ab. Neben den Standard-Funktionen bietet Device Control clevere Features für zügige und sichere Arbeitsprozesse ohne Mehraufwand für den Administrator.

Petra Plichta,
Organisation und Informationstechnik,
Landratsamt Heidenheim

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

Gerätekontrolle und Verschlüsselung wurden mittels einer Lösung für Data Loss Prevention umgesetzt. Das Landratsamt entschied sich im Jahr 2017 für Endpoint Protector mit den Modulen Device Control und EasyLock Enforced Encryption und lizenzierte im Jahr 2020 eine Drei-Jahres-Verlängerung für 600 Windows-Rechner. Einige der Angestellten haben zusätzlich zum Arbeitsplatzrechner Zugriff auf behördeneigene Laptops für das Arbeiten im Home Office, an denen auch außerhalb des Netzwerks die Einhaltung der Richtlinien gewährleistet sein muss.

Mit Endpoint Protector lassen sich die 600 Devices im Amt arbeitssparend über eine Konsole erfassen und administrieren. Weiterhin bietet Endpoint Protector granulare Einstellmöglichkeiten. Die Richtlinien für die Gerätekontrolle können nicht nur für Abteilungen oder Gruppen eingerichtet werden, sondern auch für einzelne Personen. Für Petra Plichta, verantwortlich für Organisation und Informationstechnik beim Landratsamt Heidenheim, haben sich Device Control und EasyLock bewährt. Einmal eingerichtet, arbeiten die beiden Module tadellos und sind für die Benutzer gut verständlich. Neben der granularen Einstellbarkeit der Richtlinien schätzt Plichta einige Features im Zusammenhang mit der Verwendung von USB-Sticks ganz besonders. Das ist beispielsweise die Möglichkeit festzulegen, welche Dateitypen auf den USB-Sticks gespeichert werden dürfen. Oder das „Offline Temporary Password“ für die mobilen und Homeworker. Sie können ein zeitlich begrenztes Passwort anfordern, damit sie in einer unerwarteten Situation ein eigentlich blockiertes Gerät am Laptop verwenden können. Die E-Mail an den Administrator, die sich aus der Lösung generieren lässt, enthält alle Informationen, die er für die Freigabe braucht.

	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	