



Haßberg Kliniken

CASE STUDY | Gesundheitswesen

PROFIL

Branche

Gesundheitswesen

Die Herausforderung

Die Haßberg Kliniken waren auf der Suche nach einer DLP-Lösung, Mitarbeiteraktivitäten im Zusammenhang mit Datentransfers sensibler Inhalte zu kontrollieren und gleichzeitig Compliance-Vorschriften einzuhalten. Um die Maßnahmen im Rahmen der IT-Sicherheit nochmals zu stärken, sollte eine zusätzliche Schutzebene eingezogen werden, um Datenlecks, -verluste und -diebstähle zu verhindern.

Die Lösung

Endpoint Protector by CoSoSys

Warum Endpoint Protector?

Ausschlaggebend war das Preis-Leistungs-Verhältnis von Endpoint Protector sowie die Möglichkeit, das Produkt als Stand-alone-Lösung einzusetzen. Ihr damaliges Antivirensystem war dazu nicht in der Lage.

Über die Haßberg Kliniken

Die Haßberg-Kliniken sind ein Verbund von Allgemeinkrankenhäusern im Landkreis Haßberge an den Standorten Haßfurt und Ebern. Sie sichern die Grund- und Regelversorgung der Landkreis Bevölkerung und genießen einen sehr guten Ruf für spezialisierte medizinische Leistungen über die Landkreisgrenzen hinaus. Durch eine intensive Vernetzung zwischen den Experten in den Krankenhäusern und den medizinischen Zentren auf dem Klinikgelände wird eine hohe Qualität der medizinischen Leistungen angeboten. Insgesamt werden jährlich rund 10.300 stationäre und fast 17.200 ambulante Fälle von einem hochqualifizierten Ärzte- und Pflegeteam betreut.

Die Herausforderung

Digitale Patientenakten sind anfälliger für Diebstahl und Verlust als physische Akten und werden daher durch verschiedene Datenschutzgesetze geschützt.

Als Netzwerk von Gesundheitseinrichtungen müssen die Haßberg Kliniken eine Vielzahl vertraulicher Daten schützen, wie z.B. Patientendaten, persönliche Gesundheitsinformationen (PHI), persönlich identifizierbare Informationen (PII) usw.

Aufgrund der mangelnden Kenntnisse des medizinischen Personals im Bereich IT und Datensicherheit benötigen die Haßberg Kliniken eine zuverlässige DLP-Lösung, die ihnen hilft, die Aktivitäten der Mitarbeiter im Zusammenhang mit der Datenübertragung nachverfolgen zu können und alle Geräte zu kontrollieren und zu überwachen.



“Wir haben uns für Endpoint Protector vor allem wegen der verschiedenen Einstellungsmöglichkeiten für Geräte und der zentralen Steuerung der Rechte für alle Clients entschieden. Auch die übersichtliche und einfache Update-Verteilung hat uns gefallen.”

Jörg Behm,
IT Leiter

Über Endpoint Protector

Endpoint Protector ist eine branchenführende, plattformübergreifende DLP-Software für Windows, macOS, Linux-Computer, Thin Clients und Desktop-as-a-Service (DaaS) Lösungen. Sie ist die ideale Wahl für Unternehmen, die mit Multi-OS-Netzwerken arbeiten. Das modulare Format der Lösung ermöglicht es ihnen, die richtigen Tools für ihre spezifischen Anforderungen zu mischen und anzupassen. Die Lösung setzt Datenverlusten, Datendiebstahl und Datenlecks ein Ende, indem sie alle Datenübertragungen an Cloud-basierte Dienste und Anwendungen wie Webbrowser, E-Mail oder Skype überwacht und blockiert. Sie überwacht auch die Verwendung von tragbaren Speichermedien wie USB-Sticks und Speicherkarten. Robuste Sicherheitsrichtlinien verhindern, dass Daten das Unternehmen unrechtmäßig oder versehentlich verlassen.

Die Lösung

Das Modul Device Control von Endpoint Protector erfüllt die Anforderungen des Unternehmens perfekt. Es kann Mitarbeiter oder Außenstehende daran hindern, sensible Dateien auf tragbare Speichermedien wie USB-Sticks zu kopieren und so sicherstellen, dass vertrauliche Daten nicht außerhalb des Krankenhausnetzwerks übertragen werden.

Das Modul erlaubt den Anschluss und die Übertragung von Dateien nur auf vertrauenswürdige Geräte, wie z.B. solche, die von der Einrichtung an ihre Mitarbeiter ausgegeben wurden oder die die darauf kopierten Daten automatisch verschlüsseln.

“Wir haben uns für Endpoint Protector aufgrund der verschiedenen Einstellungsmöglichkeiten (Berechtigungen) für Geräte (CD-Laufwerke, USB-Sticks, etc.) sowie der zentralen Steuerung der Rechte für alle Endpunkte und der mandantenspezifischen Einstellungsmöglichkeiten entschieden”, sagt Jörg Behm, IT Leiter.

Die Haßberg-Kliniken bewerteten Endpoint Protector auf einer Skala von 1 bis 5 (eins ist "mangelhaft", zwei ist "mittelmäßig", drei ist "gut", vier ist "sehr gut" und fünf ist "ausgezeichnet"). Die Durchschnittsnote liegt bei 4,6, wobei die höchste Punktzahl für die Produktfunktionalität, die einfache Installation, den Support und die Updates sowie die Reaktionszeit bei Support und Fragen vergeben wurde.

Uns gefiel, dass die Update-Verteilung des Produkts klar und einfach ist“, sagte Jörg Behm, IT Leiter.

Sie vergaben 4 Punkte für Granularität und Benutzerfreundlichkeit.

Das Support-Team reagiert sehr schnell und gibt schnelles Feedback und Hilfe bei Problemen,“ fügte Herr Behm hinzu.

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