ENDPOINT PROTECTOR

BG Klinikum Hamburg

Das BG Klinikum Hamburg schützt Gesundheitsdaten mit Device Control von Endpoint Protector

CASE STUDY | Gesundheitswesen

PROFIL

Branche

Gesundheitswesen

Die Herausforderung

Einfach zu bedienende, funktionale und preisgünstige Lösung für Device Control für 800 Arbeitsplatz-Rechner

Die Lösung

Endpoint Protector Device Control

Warum Endpoint Protector?

- Einfache, intuitive Bedienbarkeit
- Granulare Einstellbarkeit
- Gutes Preis-Leistungs-Verhältnis

www.**endpointprotector**.de

Über das BG Klinikum Hamburg

Das BG Klinikum Hamburg (BGKH) ist eine berufsgenossenschaftliche Unfallklinik. Es sorgt seit 1959 mit neun Fachabteilungen als Traumazentrum für die Versorgung von Schwerverletzten im Akutbereich, in der Rehabilitation und der ambulanten Behandlung. Patienten aller Krankenversicherungen werden hier mit dem Ziel einer Rückkehr in den Lebens- und Berufsalltag betreut.

Die Herausforderung

Medizinische Einrichtungen arbeiten mit Gesundheitsdaten, die unter strengem Schutz stehen. Das BG Klinikum setzt den Schutz bereits seit Jahren mittels Device Control-Funktionalität einer Lösung für Data Loss Prevention um. Als die bestehende Lösung die neue Version des Betriebssystems nicht mehr unterstützte, wurde Ersatz benötigt.

Entscheidend für das BG Klinikum war die granulare Einstellbarkeit von Richtlinien zur Kontrolle von Wechseldatenträgern für das Ein- und Ausschleusen von Daten. Die Lösung sollte über die Außenstellen hinweg zentral administrierbar sein; zugleich sollten lokale Subadministratoren Ausnahmen vor Ort regeln. Für die Einrichtung von Gruppenrechten sollte das Active Directory verwendet werden.

“Mit Device Control von Endpoint Protector sind wir vollauf zufrieden. Wir haben die Kontrolle über alle Geräte und Schnittstellen und können das Ein- und Ausschleusen von Daten minutiös regulieren.”

Axel Schmidt,
IT-Leiter,
BG Klinikum Hamburg gGmbH

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 SYMPLASSON Informationstechnik GmbH, spezialisiert auf die Konzeption und die Betreuung von IT-Systemen mittelständischer Größenordnung und langjähriger IT-Dienstleister des Klinikums, unterstützte das BG Klinikum bei der Suche nach einer neuen Lösung. Endpoint Protector fiel bereits beim ersten Blick durch einfache Administrierbarkeit und intelligente Funktionen auf und wurde für eine Testinstallation ausgewählt. Die Resultate bestätigten den Eindruck; die Entscheidung fiel für Device Control von Endpoint Protector.

In die Überwachung werden 800 Arbeitsplatzrechner einbezogen. Der Roll-Out der Client-Software auf die Endgeräte erfolgte ohne gravierende Störung, denn es war von vorne herein klar, welche Gerätegruppen wie konfiguriert werden müssen, welche Computer mit einem Client beschickt werden sollten und auf welchen auf keinen Fall ein Software-Agent installiert werden darf.

Die Lösung blockiert die Verwendung sämtlicher Geräte an den Arbeitsplatzrechnern, die nicht freigegeben sind. Mitarbeiter, die Vorträge und Präsentationen zum Mitnehmen auf einen USB-Stick kopieren möchten, können USB-Sticks an ihren Desktop-Rechnern verwenden. Die Sticks dafür werden vom Klinikum bereitgestellt, fremde Datenträger können nicht benutzt werden. Die Administratoren können flexibel reagieren, wenn Mitarbeiter von den Einschränkungen ausgenommen werden müssen.

Das BG Klinikum ist mit Endpoint Protector vollauf zufrieden: Die Lösung tut, wofür sie eingerichtet ist, ohne die Administratoren zu belasten. Zu einem späteren Zeitpunkt kann die Funktionalität problemlos um USB-Verschlüsselung und Inhaltskontrolle erweitert werden.

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	