USB-Schnittstellen an Macs überwachen

PROFIL

Branche

Medienwirtschaft

Die Herausforderung

Urheberrechtlich geschützte Texte und Bilder vor Datenverlust und Datendiebstahl schützen

Die Lösung

Endpoint Protector 4

Warum Endpoint Protector?

- Technisch führend bei der Überwachung von Macs
- Virtuelle Appliance für minutenschnelle Installation
- Benutzeroberfläche intuitiv bedienbar
- Temporäre Offline-Freigaben für USB-Geräte und Computer

ENDPOINT PROTECTOR

Das Medienunternehmen Stünings Medien verhindert mit Endpoint Protector 4 Datenverlust und Malwarebefall

In Medienunternehmen werden für die Produktion statt PCs häufig Mac-Rechner eingesetzt. Das war, als die Informationstechnologie Einzug in den Büros hielt, eine Frage der Zuverlässigkeit der Rechner und des Bedienkomforts, und außerdem sahen sie einfach gut aus. Dabei ist es dann meist geblieben, Mac-Nutzer schulen nicht wirklich gern auf PC um. So verhält es sich auch bei der Stünings Medien GmbH, die mit rund 110 Mitarbeitern für ihre Kunden Komplettlösungen in den Geschäftsfeldern Druckerei, Verlag, Internet und Werbung umsetzt: Für die Bearbeitung der Projekte sind 75 Apple-Rechner im Einsatz.

Arbeiten mit geschützten Inhalten

Stünings Medien ist die größte Druckerei in Krefeld und gibt zudem Fachzeitschriften, Reiseführer und Nachschlagewerke heraus, erstellt Prospekte, Kataloge und Kunden-magazine und entwickelt Internet-Auftritte und Apps für Smartphones und Tablets. Die Herausforderung dabei: Die Mitarbeiter arbeiten mit urheberrechtlich geschütztem Material, das das Unternehmen von Kunden oder Dienstleistern wie externen Autoren oder Fotografen bezieht. Die nicht autorisierte Veröffentlichung würde auf Stünings Medien zurückfallen und neben einem gewaltigen Image-Schaden erhebliche finanzielle Folgen herbeiführen. >>

„Mit Endpoint Protector haben wir den Überblick über die Aktivitäten der Mitarbeiter und können sie unter unterschiedlichen Gesichtspunkten auswerten, beispielsweise welche Geräte angeschlossen und welche Daten kopiert oder verschoben werden."

Ory Janßen,
IT-Leiter
Stünings Medien GmbH

USB-Geräte als Malware-Schleudern

Seit kurzem ist zudem Malware ein Problem für Macs. Zwar ist die Anzahl im Vergleich mit dem Aufkommen an Windows-Schädlingen verschwindend gering, aber dass überhaupt Schadcode in Umlauf ist, der die Sicherheitsfunktionen der als gut geschützt geltenden Plattform unterlaufen kann, lässt aufmerken und darauf schließen, dass die zunehmende Verbreitung von OS X den Aufwand für die Entwicklung lohnt. Da USB-Devices ein bewährtes Instrument für die Verbreitung von Schadcode sind, zog Stünings Medien den Einsatz einer Lösung für Data Leak Prevention in Betracht, genauer gesagt des Teilbereiches Gerätekontrolle. „Mit der Überwachung der Schnittstellen wollen wir verhindern, dass Mitarbeiter Speichergeräte wie Smartphones oder USB-Sticks unklarer Herkunft am Arbeitsplatz anschließen und möglicherweise Malware einbringen oder aber Unterlagen auf die Devices kopieren", sagt Ory Janßen, IT-Leiter bei der Stünings Medien GmbH.

Funktionsreichtum mit einfacher Bedienung

Die Suche nach einem Produkt, das sich gut für die Überwachung von Macs eignet, förderte eine überschaubare Anzahl von Herstellern und Produkten zutage. Zwei davon, darunter Endpoint Protector 4 des Herstellers CoSoSys, nahmen die IT-Verantwortlichen genauer unter die Lupe. Auf den ersten Blick fiel Janßen an Endpoint Protector die übersichtliche und funktional gegliederte Benutzerkonsole auf, die eine geradezu intuitive Bedienung der Lösung versprach. Entscheidend war dann der Umfang an technischer Funktionalität für die Überwachung der Macs, mit dem Endpoint Protector überzeugte. Als besonders gut gelöst sind ihm die Reporting-Funktionen und die Möglichkeit aufgefallen, zeitbegrenzt Passwörter für die Benutzung von Devices zu vergeben. Stünings Medien entschied sich für die virtuelle Appliance von Endpoint Protector 4 und setzt das Modul Device Control für Mac OS X ein.

Die Appliance war schnell aufgesetzt; über die browserbasierte Konsole wurde die Client-Software an die Endpoints verteilt. Nach einigen Tagen im Monitoring-Modus und der Auswertung sämtlicher Aktionen mit USB-Geräten im Zeitraum wurden die Berechtigungen entsprechend der Unternehmensrichtlinien eingestellt. Inzwischen ist die Lösung seit einigen Monaten in Betrieb und überwacht die USB-Schnittstellen. Janßen ist ausgesprochen zufrieden mit der Lösung; sein Feedback sieht der Hersteller als Anreiz für Funktionserweiterungen in künftigen Releases.

>>

ENDPOINT PROTECTOR

Über Endpoint Protector 4

Endpoint Protector 4 schützt Windows- und Mac-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, Mac und Linux. Starke Sicherheitsrichtlinien verhindern, dass Daten unrechtmäßig oder aus Versehen das Unternehmen verlassen.

Geräte-Freigaben unterwegs

Die Möglichkeit, Schnittstellen offline freizugeben, kommt den Arbeitsprozessen bei Stünings Medien entgegen. „Einige Mitarbeiter sind häufig bei den Kunden vor Ort, um Konzepte und Entwürfe zu präsentieren", erläutert er. „Sie müssen unterwegs auch mit USB-Geräten arbeiten und Daten transferieren können, während ihr MacBook nicht mit dem Unternehmensnetz verbunden ist." In diesem Zustand kann Endpoint Protector nicht prüfen, ob das Device am Rechner benutzt werden darf, und blockiert den Zugriff. In solchen Situationen kann mit einem temporären Passwort eine „Sondererlaubnis" erteilt werden. Je nach Situation kann die Offline-Freigabe zwischen einer halben Stunde und 30 Tagen gültig sein.

Reports auf Knopfdruck

Zudem ist für ihn das intuitive und detaillierte Reporting eine große Hilfe. „Wir haben den Überblick über die Aktivitäten der Mitarbeiter und können sie unter unterschiedlichen Gesichtspunkten auswerten, beispielsweise welche Geräte angeschlossen werden, wofür die Mitarbeiter sie verwenden, welche Daten kopiert oder verschoben werden", betont er. Die Unternehmensrichtlinien können technisch unterstützt durchgesetzt werden, indem bei entsprechenden Aktionen auf die Policies hingewiesen beziehungsweise die Verwendung von Geräten sehr granular blockiert werden kann.

Und falls es doch zu einem Datenleck kommen sollte, was bei keiner Sicherheitslösung restlos ausgeschlossen werden kann, lässt sich der Vorfall aufklären. Die IT-Administration kann nachvollziehen, wer welche Daten auf welches Gerät transferiert hat, und einen etwaigen Datenverlust anhand der Log-Dateien nachweisen.

	Endpoint Protector GmbH	**CoSoSys Ltd.**	**CoSoSys USA**
E-Mail:	info@endpointprotector.de	sales@cososys.com	sales.us@cososys.com
Tel:	+49-7541-97826-730	+40-264-593110	+1-888-271-9349
Fax:	+49-7541-97826-279	+40-264-593113	

ENDPOINT PROTECTOR