Seen @ Macworld: Endpoint Protector DLP and MDM solutions

Aaron Kraus

Seen @ Macworld is Appletell's column highlighting great apps, accessories, and developers we met at the recent Macworld / iWorld Expo. It's all the buzz, cool gadgets, and new gear you need to know about from the Expo!

Everyday users are becoming more aware of security (Heartbleed, anyone?). But for corporate IT departments, keeping data secure has been a requirement for quite some time. Endpoint Protector was at this year's Macworld Expo, and we sat down with the team to discuss their Data Loss Prevention (DLP) and Mobile Device Management (MDM) solutions for Macs, iDevices, Android devices, and Windows. The rising usage of Macs in enterprise organizations means a rising need to protect them, and Endpoint Protector's unique features offer corporate IT departments a tool to deal with the Apple flood.

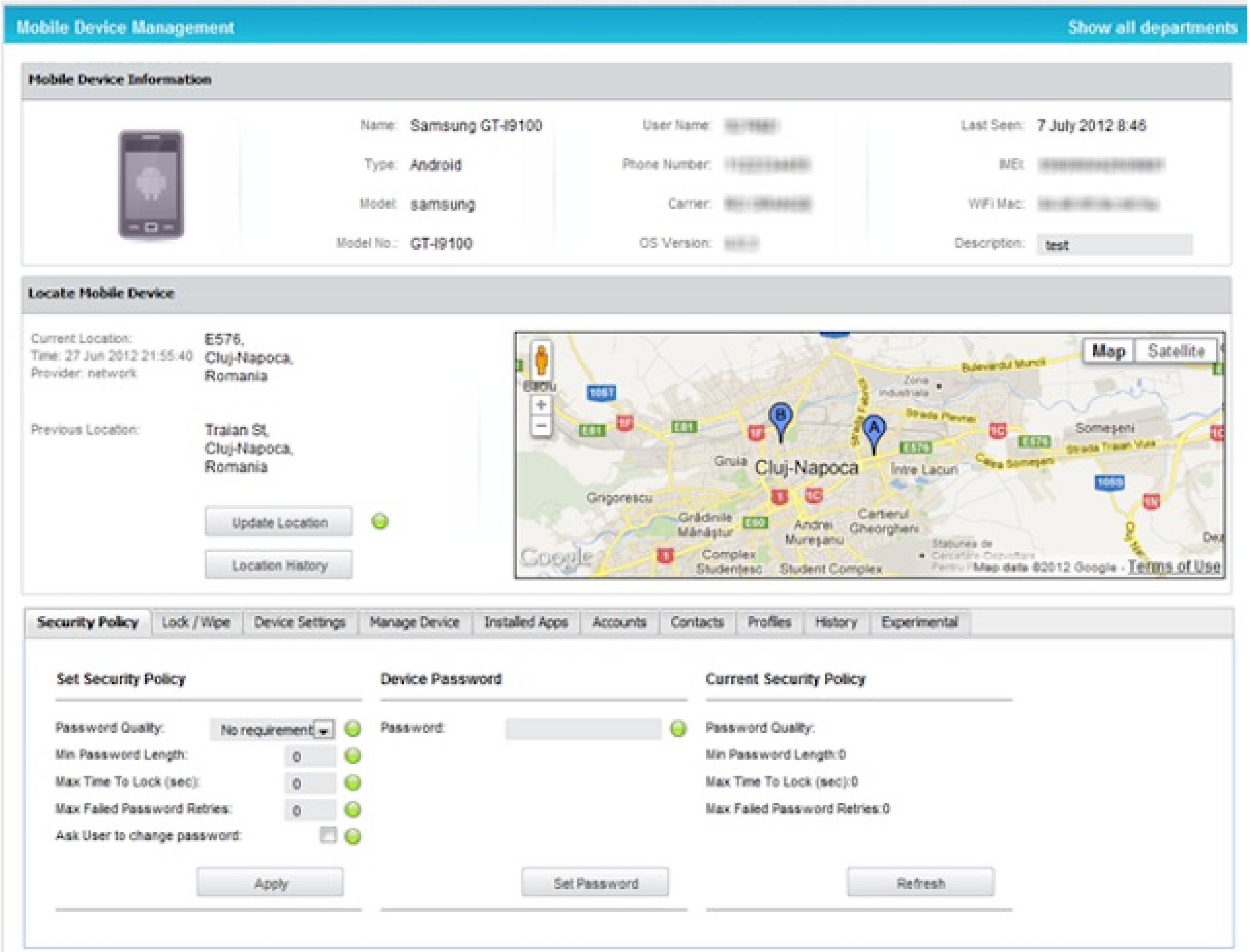
Plug the Holes

Everybody's concerned about security, but the real issue isn't necessarily about making computers secure, it's about keeping your data secure. Viruses can be a headache for companies, but data breaches are far more harmful. DLP is one tool that can help stop both accidental and intentional information leaks—like attaching a spreadsheet that contains credit card info to an email, or stealing a company database to sell to a competitor or identity thieves. The Endpoint Protector agent on Macs keeps track of files, information, and activities on your organization's computers, and reports it all to a centralized server. This offers security or network admins a great tool for keeping an eye on activity happening inside their organization. Plus, it's cross-platform so you can use it as a single DLP solution for your entire network.

Endpoint Protector lets you identify the types of information your company needs to protect, such as account numbers, and then set up rules to govern what employees can do with that information. The Apple-esque web interface offers an intuitively simple but powerfully granular way to do this, so you can apply rules that make sense for your business. Once you've defined your rules, you can select a number of actions to either allow or disallow for that info, including use of various web browsers/email clients, messaging services, and cloud services. In this way, you could restrict employees use of email or instant messaging to exchange files, but allow them to post to the company-provided Microsoft OneDrive for filesharing.

Device Management

Companies working in highly regulated environments such as banks or healthcare providers have even stricter standards for how they must manage information. Endpoint Protector's sophisticated device management features give you precise control over the Macs and iDevices connecting to your network. For Macs, Endpoint Protector offers the ability to manage how users interact with their computers, such as preventing the use of USB ports or CD/DVD drives to write sensitive information. It even allows forced encryption, which means users who do write information to a USB drive must encrypt it, which protects the data if that drive is lost or stolen.



Mobile Device Information

Name: Samsung GT-I9100
Type: Android
Model: samsung
Model No.: GT-I9100
User Name: [redacted]
Phone Number: [redacted]
Carrier: [redacted]
OS Version: [redacted]
Last Seen: 7 July 2012 8:46
IMEI: [redacted]
WiFi Mac: [redacted]
Description: test

Locate Mobile Device

Current Location:
Time: 27 Jun 2012 21:55:40
Provider: network
E576,
Cluj-Napoca,
Romania

Previous Location:
Traian St,
Cluj-Napoca,
Romania

Set Security Policy

Password Quality: No requirement
Min Password Length: 0
Max Time To Lock (sec): 0
Max Failed Password Retries: 0
Ask User to change password: □

Device Password

Password:

Current Security Policy

Password Quality:
Min Password Length:0
Max Time To Lock (sec):0
Max Failed Password Retries:0

On the mobile front, many IT departments are struggling to adapt to a rapidly diversifying environment. Many organizations were built Blackberry-only, but very few are still set up that way. Endpoint Protector's MDM features can centrally manage, track, and control mobile devices running iOS or Android, which provides IT departments the assurance that data isn't leaking out of their control via iPhones. The web interface provides tracking and location services, remote wipe/disable, and forced device encryption to help secure the increasing amount of data that lives on mobile devices.

Endpoint Protector is currently on version 4.0, so there are obviously a ton of features that we couldn’t cover in a brief discussion on the show floor. If you work in corporate IT or your office is struggling to deal with more Macs and iDevices showing up every day, head over to the Endpoint Protector website to check out all the features.

We saw lots of other great products at the show, so be sure to check out our previous coverage of other exhibitors from Macworld / iWorld 2014.