

Symantec Endpoint Protection Mobile

How to Sell At-A-Glance

Product Overview

Symantec Endpoint Protection Mobile (SEP Mobile) offers comprehensive mobile threat defense solution for both managed and unmanaged devices, delivering superior depth of threat intelligence to help predict, detect and prevent an extensive range of known and unknown threats. SEP Mobile's advanced technology uses a layered approach that leverages massive crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively help protect enterprise mobile devices against malware, network threats, and vulnerability exploits.

Target Market and Buyers

1. **Primary Audience: Enterprise-size Organizations (Global 2000) and regulated verticals** – Large organizations that rely on mobility for user flexibility/productivity, customer responsiveness and other business initiatives.
2. **Secondary Audience:** Medium-size (500+ users) – Data rich orgs that understand there are big consequences of a data loss.
3. **Target Buyer: CISO** – Needs visibility into organizational threats and risks; wants compliance, user privacy and a proven solution.
4. **Target Buyer: VP IT Security/Mobility Operations** – Needs a single, comprehensive mobile security solution with automated protections that don't require manual intervention or third-party remediation; needs simple deployment, high adoption rates and out-of-the-box integrations with EMM and SIEM solutions.

Customer Challenges

- Need visibility and control over mobile threats – zero visibility today
- Sensitive data is constantly outside the firewall on mobile devices
- Mobile devices don't have protections against malware
- Users are connecting to suspicious Wi-Fi networks
- No way to evaluate and manage the ever-changing organizational risk introduced by each mobile device
- Existing mobility management tools (EMM/MDM) do not protect against mobile threats

Why We Win

- **Holistic, Layered Mobile Security** – Comprehensive mobile threat defense solution for both managed and unmanaged devices, delivering superior depth of threat intelligence to help predict, detect and prevent threats from all mobile attack vectors.
- **Proactive Protections, Not Just Detections** – Only SEP Mobile has automated, on-device protections that do not depend on manual or third-party remediations to keep sensitive data secure.
- **Public App** – The fully functional enterprise app is available from the public app stores. Competitors rely on private APIs, so the apps have to be signed, repackaged and redeployed with every update, they can't assure privacy and key functionality may be deprecated at any time.
- **Enterprise Readiness** – Customers always compliment our mature console, flexible admin and user notification options, built-in integrations, scalability, reports and prioritized recommendations for reducing risk.

Use Cases

- **Enterprise Mobility** – Organizations that rely extensively on mobile for user flexibility/productivity, customer responsiveness and other business initiatives can protect mobile devices, data and communications against malicious attacks.
- **Securing Managed AND Unmanaged Devices** – IT admins can easily protect their sensitive data on devices they don't/can't manage without privacy concerns – BYOD, contractors, doctors, independent agents, etc.
- **Compliment EMM** – Many organizations adopted EMM/MDM solutions to address enterprise mobility, but while these solutions address device management, security and threat defense are not addressed.

Discovery Questions

1. **Do you have visibility into mobile threats?** How many instances of malware are on your mobile devices? How many risky networks have your users connected to in the last 30 days? Which devices should update to a more secure OS version?
2. **Are you aware that EMM/MDM solutions don't protect against mobile threats?** The major EMM solution providers all partner with us to provide mobile security to their customers.
3. **Do you want a solution that seamlessly and automatically protects your mobile devices and mobile data without adding additional burden to your IT team?**
4. **Do you want a mobile security solution that your users will thank you for?**
5. **Are you putting as much effort into securing your mobile devices as you are your traditional endpoints?**
6. **Can you respond to questions from your Board/CISO about how much risk your mobile infrastructure introduces?**
7. **Can your mobile solution assure compliance with industry regulations and privacy laws?**

Overcoming Objections

1. **Objection:** I already have an EMM/MDM solution.
Response: EMM is designed for device management, and sometimes app and content management, but only addresses physical security, like wiping a lost phone. The major EMM vendors partner with us to offer mobile security to their customers, and we integrate with them to support your existing policies.
2. **Objection:** We only use mobile devices for email.
Response: For most companies, email contains a tremendous amount of sensitive data that should be protected. Would you be willing to copy your competitors on every email you send? Also exposing email credentials will allow an attacker to easily breach your systems from another computer at a later date.
3. **Objection:** We only allow iOS/Apple devices and those are secure.
Response: Did you know that there were more iOS vulnerabilities discovered and patched in the first quarter of 2017 than in all of 2016? Every company with at least 200 iOS devices has malware, and all mobile devices are susceptible to network attacks. We can also demonstrate how easy it is to hack an iPhone in 30 seconds.
4. **Objection:** All mobile devices are BYOD, so we can't secure them.
Response: That is a valid concern for managing mobile devices with an EMM/MDM solution. However, SEP Mobile uses a public app that is no different from any other app on the public stores, so can't see other apps or monitor your communications. We use patented technology to deliver comprehensive mobile security without violating privacy or impacting the mobile experience or battery life.

Competition

Competitor	What the Competition Says	How to Block the Competition
Zimperium	Device-only solution is the best and can protect even if network connection is lost.	Trying to do everything on the device is very limiting and drains scarce mobile resources, like battery. They just offer a small subset of what SEP Mobile can do.
Lookout Mobile Security	With 100M devices worldwide, Lookout has unparalleled global insight into the full spectrum of mobile risks, threats, and vulnerabilities.	Lookout was designed as a consumer product and bundled widely, but who knows how many are actually used. The quality of the data and insight is far more important, as we have proven by identifying more threats and zero days than Lookout in every comparison.
Check Point SandBlast Mobile	The industry's only unified, cross-platform solution to protect enterprises from mobile breaches.	The SEP family is more complete and comprehensive. Check Point purchased Lacon over 2 years ago and haven't made significant improvements since; the console is still primitive and hard to use. Test the products side-by-side to see who identifies more threats and offers better visibility and control.

Licensing Information

Symantec Endpoint Protection Mobile	
Device Protection	iOS and Android Devices
License Meter	Per Device
Max # Devices	1

Additional Resources

- Datasheet
- First Meeting Deck

For more information, visit www.symantec.com/products/endpoint-protection-mobile

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on [Facebook](#), [Twitter](#), and [LinkedIn](#).



350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com