Sales Playbook
Symantec Endpoint Protection Mobile

Play Overview: Symantec Endpoint Protection Mobile (SEP Mobile) protects businesses from mobile cyberattacks. It compliments the SEP family so that Symantec is the ONLY company on the planet to be able to offer world-class cyber security for all endpoints - traditional or modern. SEP Mobile is a 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.

Situation and Pain Points

Current Situation

- Organizations are relying extensively on mobile for user flexibility/productivity, customer responsiveness and other business initiatives.
- Many devices are not owned or managed by the company
- Mobile devices are on and connected 24/7, most often outside the firewall.
- Mobile devices store and access a lot of sensitive data
- This makes them high-value targets for malicious hackers.

Customer Pain Points

- No visibility or control over mobile threats
- Sensitive data is constantly outside the firewall
- 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 tools (EMM/MDM) do not protect against threats

Symantec Solution and Benefit

SEP Mobile – is a Mobile Threat Defense solution that uses a layered approach to proactively predict, detect and protect mobile devices against all mobile threat vectors, leveraging on-device, cloud and crowd-sourced threat intelligence.

Unsafe networks – Immediately identify unsafe and malicious networks and activate protections, like on-demand VPN and corporate resources protections.

Malicious apps – Use crowd-sourced intelligence, static and dynamic analysis, and machine learning to identify malicious apps, sometimes before they are even installed.

System vulnerabilities – Defend against indicators of compromise and system vulnerabilities; notify users and admins as soon as a more secure OS version is available.

Physical threats – Ensure devices are protected against physical threats, like USB debugging and no passcode lock.

Sanity Check List – SEP Mobile "Recipe"

Prove the reality of mobile threats with a live demo

- Engage with the security team and show a live hacking demo, ideally on one of the prospect's devices, to illustrate the reality and the severity of mobile threats. Set up a half-day on-site to expand the exposure and engage as high as possible, including the CISO if possible, even for part of it. ✓
- Verify with those present that their existing solutions did not alert them about the attack that just took place. ✓

Highlight the importance of proactive protection

- Proactive protection is unique to SEP Mobile and essential to ensuring that sensitive data and communications stay secure. Competitors rely on delayed EMM responses. ✓

Illustrate the value of using a public app

- Unique to SEP Mobile, public app simplifies deployments, improves experience and adoption and assures user privacy. ✓

Win with a competitive bake-off if evaluating others

- SEP Mobile is technically superior and offers better value. ✓

Who to Target – Key Titles to Find

Title	Discovery Questions
CISO	• Do you have visibility into mobile threats and organizational risk? • Can you assure compliance with industry regulations and privacy laws?
VP IT Security / Mobility Operations / Threat Prevention Team	• Do you have visibility into mobile threats and organizational risk? • Are you aware that EMM/MDM solutions don't protect against threats? • Do you want a solution that seamlessly and automatically protects your mobile devices without adding additional burden to your team? • Do you want a solution that your users will thank you for?

Qualifying Questions

- How many times have users connected to risky Wi-Fi in the last 30 days?
- How many instances of malware exist on your mobile devices?
- Do you know which devices have unpatched vulnerabilities that should be updated?
- Do you have unmanaged BYOD devices?
- Are you aware that a momentary and undetected breach on a mobile device may expose corporate credentials that can be used later to infiltrate many other corporate systems?
- Can we set up a live on-site demonstration for your IT Security team?

Account Planning

1 **Qualify:** Get to CISO, IT Security or Threat Prevention team and ask about current visibility into mobile threats and exiting risks. Ask about mobility initiatives, BYOD, contractors/agents with devices that cannot be managed.

2 **Convince:** Set up a half-day on-site demonstration of threats and risks – invite CISO. Explain the value of a solution that not only detects threats, but actually protects without relying on third parties or manual intervention. Discuss user privacy and how competitors cannot offer this because they use sideloaded apps

3 **Propose:** If competition is present, encourage a side-by-side comparison. Be sure to highlight the value of active protections, public app, crowd-sourced intelligence, end-user privacy, maturity of the console, built-in integrations with EMM/MDM and SIEM, flexibility of

Sales Playbook
Symantec Endpoint Protection Mobile

Key Symantec Differentiators

Product Level: Protection, not just Detection

- Only SEP Mobile has automated, on-device, stand-alone protections that do not depend on manual or third-party remediations to keep sensitive data secure.
- Unique mNAC (Mobile Network Access Control) features monitor and protect communications to secure data.
- SRP (Selective Resource Protection) protects specified systems and services any time a device cannot be trusted

Product Level: Superior User Experience and Assured Privacy

- Public app is as easy to install as a game and updates automatically
- Privacy by Design ensures user privacy across all mobile activities
- Protects both business and personal activities
- Uses less than 3% of device battery and resources
- When compromised, blocks corporate connections, but not private
- Automatically returns to full access when threat is removed
- Lowest false positive rates and available non-interactive mode
- Users trust apps that come from the public app stores

Product Level: Advanced Intelligence

- Massive crowd-sourced intelligence rapidly identifies both good and bad networks and apps, and uniquely can identify when devices (including Android) have an available security update and protect from zero days
- Advanced Indicators of Compromise detect what others can't

Company Level: Most Mature and Enterprise-ready

- Most advanced, enterprise-ready console and architecture
- Deploy to thousands in minutes – and zero-touch app updates
- Out-of-the-box integrations with all major EMMs and SIEMs
- Flexible notification controls for admins and users
- Detailed and summary risk reports for board-level presentation

Competitive Kill Points

Silver Bullets to Compete against:

Zimperium, Lookout Mobile Security, Check Point SandBlast Mobile

All competitors	• Can detect threats, but must rely on manual or third-party remediation • Require an EMM solution for protections or policy enforcements • Rely on private apps that uses private APIs and must be sideloaded • Makes deployment and updates very painful and lower adoption rates • Can't assure privacy, so not ideal for BYOD or contractor/agent use • Private APIs may be deprecated, eliminating product functionality • Not designed for BYOD – invasive EMM requirements and privacy concerns
Zimperium	• Claims "device-only" solution is better, but is only a subset of SEP Mobile • Trying to do everything on the device limits functionality and kills the battery • Consumes battery and other mobile resources (up to 40% or more) • Customers claim high false positives and primitive management console
Lookout	• Consumer focus – only recently targeting enterprise with few successes • Primary focus on Android malware and weak on network protections
Check Point	• Originally Lacoon – acquired, but not improved or integrated • Immature console – menu of manual options that require time and expertise

Handling Objections

Objection	Response
SEP Mobile is a network solution	***Objection is not accurate:*** • The solution has proven over and over in side-by-side comparisons that it detects and protects against more threats across ALL vectors, network, malware, vulnerabilities & physical
If SEP Mobile loses network connection, it can't function	***Objection is not accurate:*** • SEP Mobile has all of its primary protections function on-device and independent of network connection. • Connection to the cloud can be used for secondary malware analysis. • Zimperium never has the option of leveraging server processing
Lookout has a much larger pool of "agents" for crowd intelligence	***Objection is only partially true:*** • Lookout *does* has more agents (mobile apps) out there, many due to consumer bundling that have never been used, but… • Lookout's agents do not collect the breadth or depth of actionable intelligence from the devices, apps and networks as SEP Mobile

Customer Success Sound Bites

> *"Having SEP Mobile is like having a secret informant on hackers. SEP Mobile actually predicts attacks and can help you prevent them. When you have more than 35,000 mobile devices to secure like we do, that's crucial."*
> *Richard Moore, Head of IS, New York Life*

> *"Our SEP Mobile defense is constantly active, using predictive intelligence to know when to take necessary automated steps such as VPN tunneling. Everyone is using SEP Mobile and I am not getting 3 a.m. calls and amber alerts about mobile security."*
> *Amir Kadar, Director of IT Infrastructure, Ceragon*

Solution Options

SEP Mobile

– Stand-alone enterprise mobile security

– With EMM integration (automatic enrollment + ability to report health status, compliance status and/or Compromised Device for corporate policy enforcement)