Symantec SEP Mobile Deployment

A CustomerONE Story

Introduction

In 2017 Symantec acquired Skycure, a leader in mobile threat defense. Now a part of Symantec's Integrated Cyber Defense Platform, Skycure was rebranded to Symantec Endpoint Protection Mobile (SEP Mobile). SEP Mobile allows us to complete our mobile threat defense solution, giving us the ability to predict and detect the broadest range of existing and unknown threats. SEP Mobile's predictive technology uses a layered approach that leverages massive crowd-sourced threat intelligences, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits, with or without an Internet connection.

SEP Mobile uses multi-layer predictive techniques to deliver a single, unified solution that proactively protects mobile devices across all major mobile operating systems.

Closes the Threat Protection gap in Mobile Device Management (MDM)

Traditional MDM and Enterprise Mobility Management (EMM) solutions do not actively identify threats. Instead, those tools are in place to help users configure and import software on mobile devices.

Detects vulnerabilities affecting mobile operating systems and applications

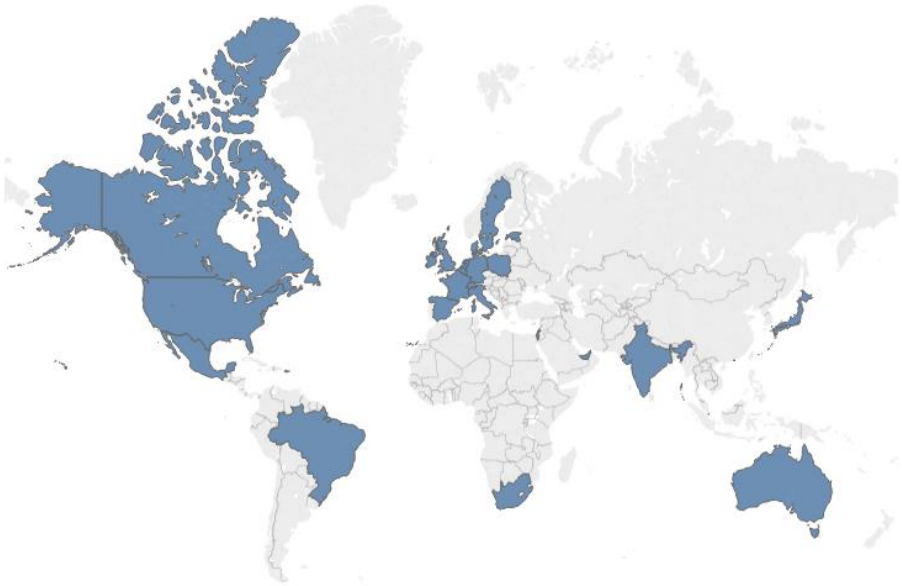
Lack of visibility persists across all IT systems, but threats to mobile devices have grown rapidly in recent years. For instance, Symantec's 2018 Internet Security Threat Report (ISTR) noted that mobile malware variants increased to 27,000 in 2017 compared to 17,000 in 2016, a 54% year-over-year increase.

Manages connections to untrusted Wi-Fi networks

SEP Mobile manages untrusted networks using crowd-sourced threat intelligence networks, to protect an increasing number of mobile devices that are connected to corporate resources. Mobile devices connect to anywhere from 10 to 100 times more networks than traditional IT devices, such as laptops. Many of those networks are beyond the visibility and safeguards provided by enterprise security teams.

Our approach

Global Scope: 7,810 Mobile Lines, 24 Countries, 30 Carriers



To deploy SEP Mobile at Symantec, the project team defined the scope and project timeline to support 7,810 mobile lines, across 24 countries and 30 mobile carriers globally.

An important consideration was to decide if SEP Mobile should be integrated with Symantec's current MDM solution and what would be required to comply with data protection and privacy regulations in each country where the solution would be deployed.

The project plan consisted of a multi-pronged approach including: preparing the IT environment, conducting a pilot, communications, training and support.

Preparing the IT environment

Preparing the IT environment consisted of segmenting all Symantec end users into groups based on several criteria including: size; region; organization, and country privacy controls. This subcategorization helped to mitigate any potential negative impact for special use cases (e.g. European privacy laws and sales engineering).

IT collaborated with Symantec's Global Security Office (GSO) to integrate SEP Mobile and AirWatch, with GSO providing security and privacy guidance. The IT team used AirWatch to manage technological aspects of the deployment, including the number of application pushes per day, and the end user devices included in each wave. The integration entailed several steps:

Import deployment security groups into AirWatch

This was a straightforward process, although it required a phased approach due to European privacy regulations, which was achieved via size and geographic group segmentation in AD.

Import exclusion security group into AirWatch

AirWatch was setup to only push application and configuration to AD groups. However, Symantec required that the application be pushed to AirWatch Smart Group to satisfy our exception requirement for some members of Sales and Sales Enablement. The technical lead for the project worked with the AirWatch vendor to implement a new logic that allowed IT to push to Smart Group, introduced in AirWatch version 9.2.

SEP Mobile compliance notification

We customized the compliance notification, so it looked like other notifications users received, and branded it from IT and our Global Security Office. We recommend this co-branding to other companies.

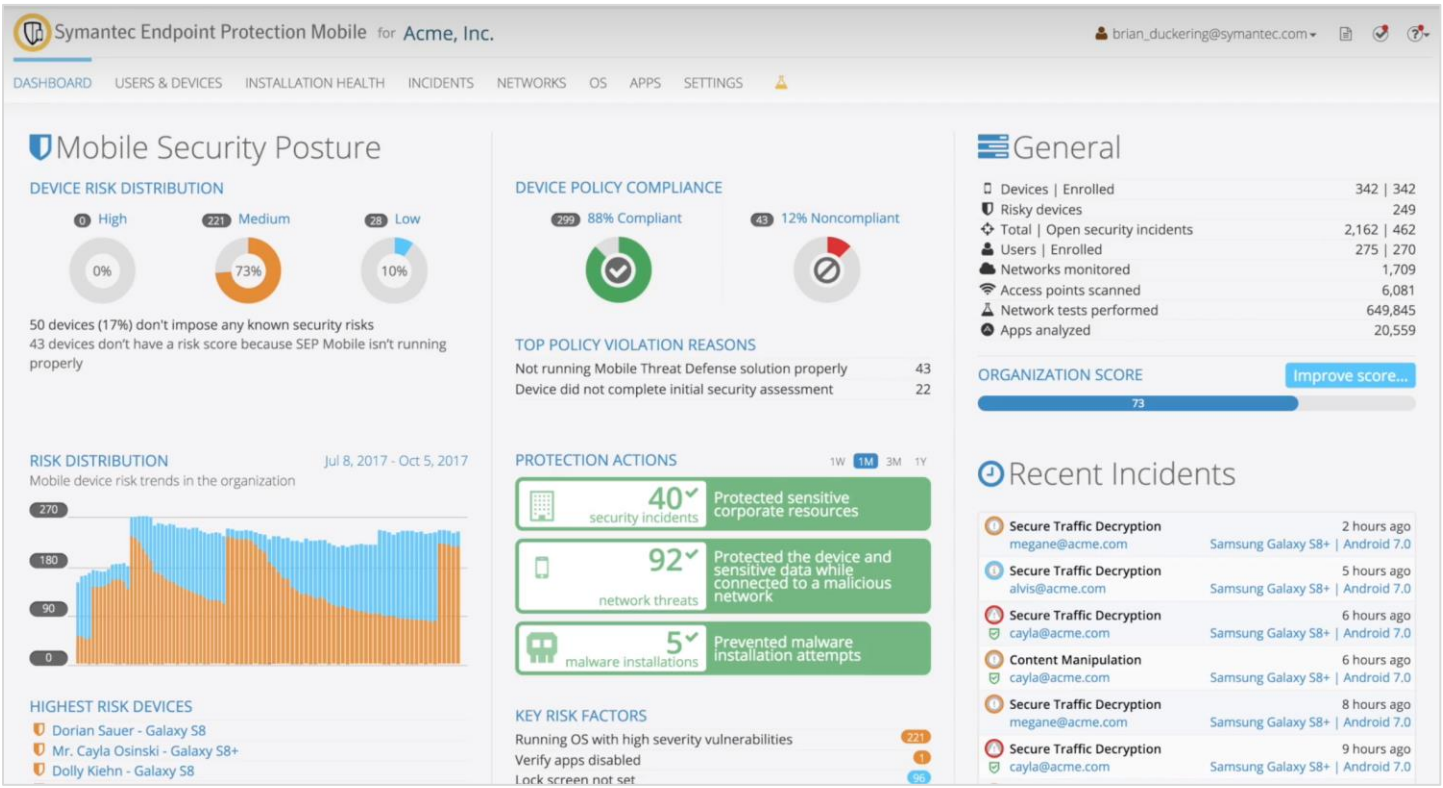
The notification is also very detailed, letting the user know the exact device and what specifically is non-compliant. This level of data also enables our IT support teams to quickly serve our users.

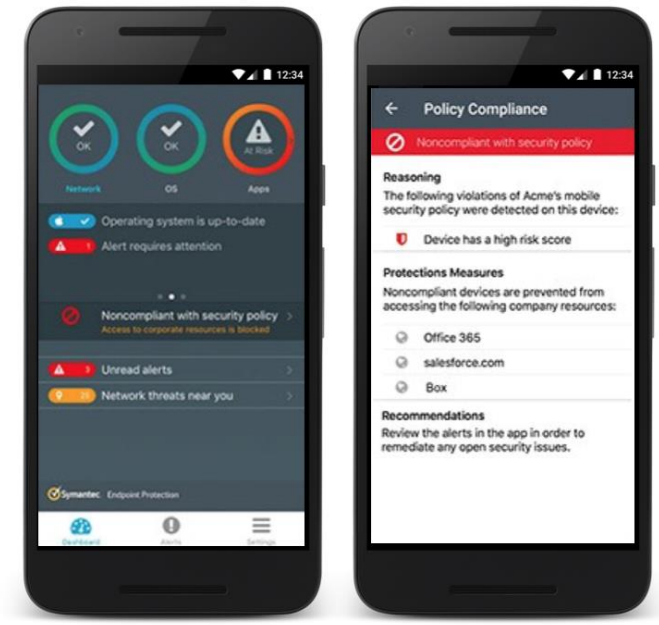
Turn off compliance enforcement in SEP Mobile console

Turning off compliance enforcement during deployment is important because it takes approximately 15 to 20 minutes for the SEP Mobile app to fully scan a new device the first time to avoid false positives. Once the first complete device scan was finished, the team turned on security compliance once again without issues.

Pilot

User acceptance testing was completed with a subset of the IT and GSO organizations, and then to the entire organization to ensure smooth installations and user adoption. This sampling allowed us to see how our compliance was enforced and how it impacted a small group of users. It also allowed us to obtain a benchmark and adjust our overall deployment strategy. The SEP Mobile management dashboard, as demonstrated below, enabled us to track the security posture in the environment.





HOW SEP Mobile Reports Suspicious Activity

The graphic shows what users will see if their mobile devices become noncompliant with Symantec's security policy using SEP Mobile.

SEP Mobile Deployment and Steady State

With all preparations completed, the team began a phased rollout of the app, starting with seven U.S. groups. The team could automatically push the SEP Mobile app to Symantec's U.S. workforce, but employees in other countries had to manually install the app to comply with regional privacy restrictions.

Each of the seven U.S. workforce groups consisted of 575 end users. Following a smooth rollout for the first group, the team increased the daily volume by 25% to over 1,000 pushes per day and maintained this volume from the second through the final group. Once deployment to all seven U.S. groups was completed the app was made available to the global workforce.

Throughout the entire deployment, the team encountered only one major incident, which involved the SEP Mobile app exceeding the number of daily "calls" allowed to the AirWatch application programming interface (API). AirWatch has since raised the number of daily calls permitted from apps to its API.

The team saw less than 5% of rollouts involve incidents, most of which were user-related issues, including:

- 75% of tickets were users who did not open the SEP Mobile app to finish device configuration
- 20% of the tickets were for devices that were replaced but no longer in AirWatch
- 5% of the tickets were for users who were in the free environment and needed to be removed

SEP Mobile users now receive an automated email whenever their devices become noncompliant. The automated email continues every week until the user complies with corporate security requirements. The automated email frees IT from having to manually contact users who are noncompliant.

Since deploying SEP Mobile our concerns have shifted from deployment to usage. Today, user questions revolve around interpreting alerts from SEP Mobile. The alerts, while very detailed, sometimes require a little insight to understand. In Symantec, IT support staff can resolve these cases with a combination of user education around how the specific mobile exploit works and additional details about the incident (available from the SEP Mobile console). The result is a user that is more informed about their mobile device's security, and a clearer understanding of how SEP Mobile protects them from exploits.

This health alert is quite comprehensive and, in most cases, quite helpful with one exception. A SEP Mobile health alert will trigger whenever a device has been offline for three days. Companies deploying SEP Mobile should consider what the right balance is for compliance user alerts.

SEP Mobile development has added the ability to exclude specific devices at our request, so there is a solution available for one-off cases; however, there is not currently a general way to relax this particular alert across the enterprise.

Communications

A thorough end user communications plan is crucial to success. It was important that users understood when SEP Mobile would be delivered to their device, how it added additional protection, the easy one-time set up process, that it consumes very little battery space, and that it does not track their usage. "Many end users had questions about privacy, so it was important that we were transparent and addressed the concerns through a series of FAQs," said Phu Nguyen, Symantec Mobility Service Owner. The communications plan consisted of:

- A Microsoft PowerPoint slide deck for use in presentations to key stakeholders
- Branding guidelines for the new SEP Mobile app
- A general awareness article in the company-wide IT newsletter
- Both end user and IT support knowledge articles
- On-device notifications and end-user prompts for installation

Training and support

The project team invested significant time in training and support to ensure project success. These activities included cross-training Symantec's IT Service Desk and deskside support teams by SEP Mobile and AirWatch subject matter experts (SMEs), including former Skycure Senior Director of Customer Success and Support Alberto Rodrigues, and the Skycure Customer Success Team (CST).

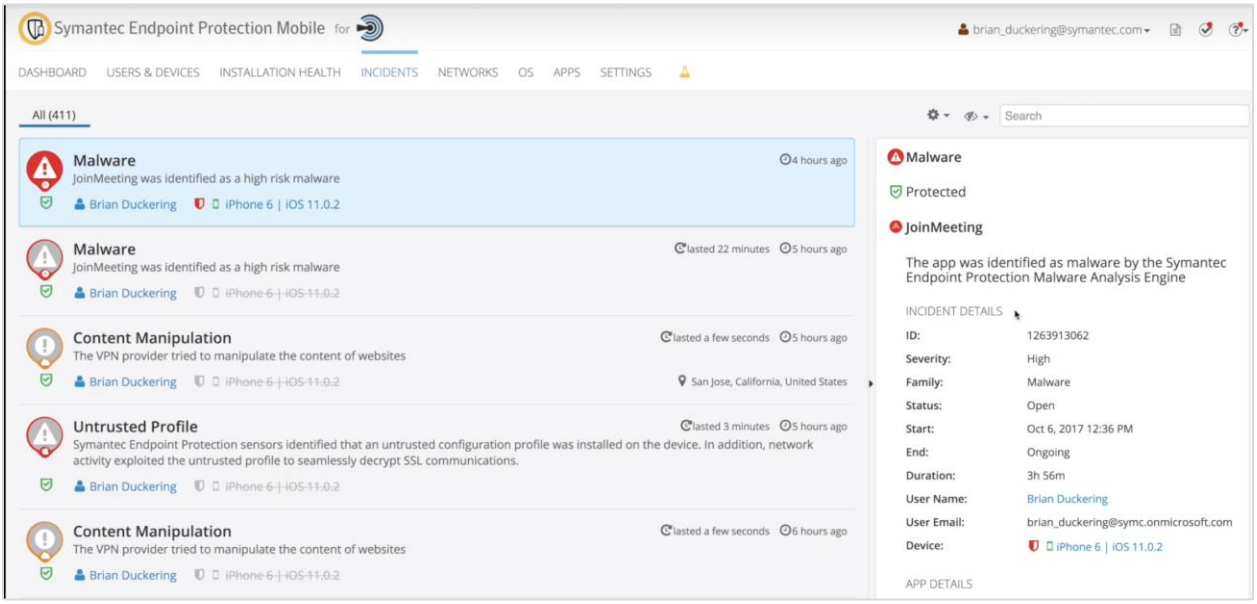
An end user support workflow; which provided the categorization, prioritization, and routing to manage incident resolution was created based on the support workflow of IT Infrastructure Library (ITIL) best practices and included Level 1, Level 2, and Level 3 support. We also developed user documentation including self-help, installation guides, configuration cheat sheets, frequently asked questions (FAQs), and troubleshooting logs.

"As mobility usage increases in the enterprise, SEP Mobile provides modern security in the ever-changing landscape of the digital workplace," said Sheila Jordan, Senior Vice President and Chief Information Officer.

Critical Success Factors

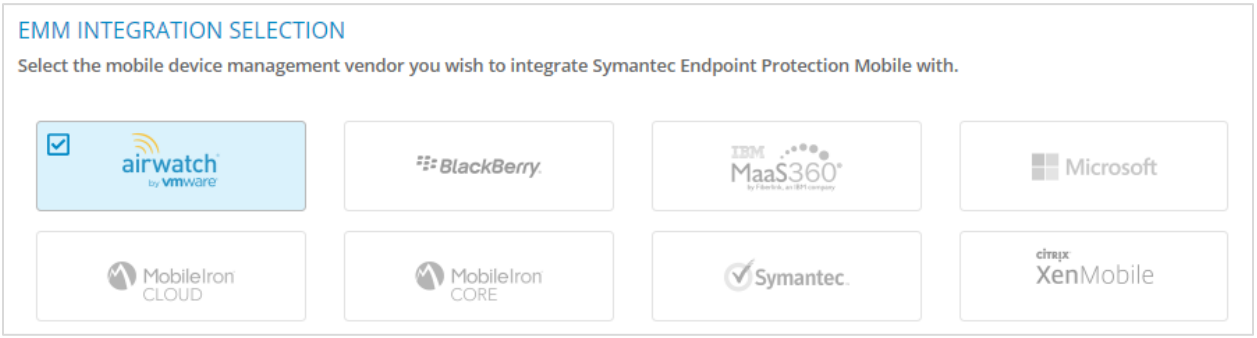
Pre-deployment critical success factors included:

- Conducting a pilot to ensure smooth installations and user adoption
- Establishing a working communications team for the project's duration
- Holding training events with the internal IT Service Desk and other user support functions
- Involving an SEP Mobile SME during training sessions
- Scheduling changes with corporate IT's change advisory board (CAB)
- Accounting for the deployment size and amount of required resources is key
- Automating deployment by leveraging SEP Mobile integration functionality with AirWatch and other MDM solutions
- Capitalizing on SEP Mobile's ability to integrate with existing security tools, such as the enterprise SIEM Splunk for security logs, so that alerts can be monitored from a security operations centers perspective



SEP Mobile Incident Dashboard

A final point to consider is if your MDM is on the cloud environment. The integration between MDM and SEP Mobile will require constant communication using API. It is important to make sure that there no restrictions on API calls with your MDM vendor. SEP Mobile is certified with the following Enterprise Mobility Management (EMM) vendors:



To learn more

This brief was intended to give you a broad look at how Symantec IT deployed SEP Mobile internally. Your Symantec representative can show you how to adapt our blueprint to make your own SEP Mobile journey even smoother.

If you would like an even more in-depth experience, visit our Executive Briefing Centers at our U.S. headquarters in Mountain View, California, or in Reading, U.K. Executive briefings provide you an exclusive opportunity to learn how Symantec solutions can protect your business and network environments. We'll customize the briefing to meet your specific goals, and we'll also give you a sneak peek at new technologies and challenges on the horizon.

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