White Paper

Three secrets to becoming a mobile security superhero.

How to Select, Implement and Succeed with Mobile Threat Defense

Symantec | vmware airwatch

Contents

Three secrets to becoming a mobile security superhero

As more workplaces become "everywhere workplaces," cyber threats and attacks increasingly target mobile devices.

Through the eyes of many business leaders, opening a presentation or other document on a mobile device is hardly different from doing the same thing on a laptop. It follows that many business professionals may assume that the same powerful IT security capabilities that work so well to protect computers—cyber-security tools ranging from firewall to IPS, antimalware, antivirus and more—can also protect mobile devices.

In truth, mobile security involves a very different set of challenges than protecting traditional endpoints, i.e., desktops and laptops. Consider that while a laptop computer may connect to just a few different networks throughout a year, mobile devices may connect to tens, if not hundreds, of different cellular and Wi-Fi networks in a day—some of which may be malicious or compromised. Most IT security leaders are well aware of the nuances in protecting mobile devices. According to a recent survey of 800 cybersecurity professionals conducted by the Information Security LinkedIn Group, only 26% of respondents believed that mobile [cyber] attacks are *not* real[1] —meaning that up to 74% of cybersecurity professionals are taking the problem seriously and need to make a plan to convince business leaders that mobile cyber threats are priorities that should be addressed promptly.

In the 2016 Spotlight Report, 74% of respondents reported that either they were not sure or "yes" malware had compromised their organization's mobile devices.

The following sections provide three critical "secrets" that may help in conducting a successful buy-in discussion with business leaders about mobile cybersecurity. Ultimately, the goal is to gain consensus about adopting modern, advanced cybersecurity technologies built from day one to protect mobile devices with the efficacy of cybersecurity for traditional endpoints.

1 BYOD and Mobile Security: 2016 Spotlight Report. Information Security (a LinkedIn Group). 2016.

Secret #1: Don't be careless in the dark

Prove that mobile cyber threats are real

According to the US Department of Health and Human Services[2], there were 260 disclosed, major healthcare breaches in 2015. Of those breaches, nine percent were identified as originating from smart phones, iPads, slates or other mobile devices that may have been exploited by malware or insider data leakage.

Despite mass adoption of BYO mobile devices by users who daily access sensitive information from outside of an organization's secure network, most organizations continue to operate in the dark with no ability to ascertain whether a BYO mobile device was used in a breach. Even company-issued or managed mobile devices leveraging containerization, app wrapping and VPN tunneling are susceptible to malware, viruses, insider data leakage and other threats.

Users also often circumvent restrictive mobile security measures by simply turning to "shadow IT" to illicitly share sensitive information or inadvertently expose it due to malware, malicious profiles, network-based attacks and other next-generation threats that are rapidly becoming less exotic and more mainstream. Even once these gaps in security are acknowledged, there are still barriers in most current environments to addressing them directly.

BARRIER #1: Difficult to measure risk

Due to the lack of visibility over mobile devices—a lack of real-time mobile threat intelligence—it is challenging if not impossible to accurately measure the risk of mobile cyber threats at most organizations. In the 2016 Spotlight Report, 37% of respondents admitted that they did not know whether mobile devices had been involved in security breaches at their organizations, while only 21% could definitively respond "yes." Consequently, the first part of gaining buy-in with business leaders may involve explaining the absence of risk-based mobile authentication and access to metrics for mobile cyber threat risk.

2 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

BARRIER #2: Shortcomings of current enterprise mobile security

Another buy-in theme that may arise with business leaders involves explaining why an organization's current mobile security system is not adequate for today's new cyber-threat landscape. Consider the following arguments that may come from business leaders:

"iOS and Android mobile operating systems already protect devices from harm."

The hacker community constantly looks for vulnerabilities ("chinks in the armor") in mobile operating systems. Patching known vulnerabilities is one of the principal reasons why devices regularly require iOS and Android updates. However, patching is often not an immediate or complete solution: while Apple and Google may patch the OS as soon as they are aware of a vulnerability and engineer a fix, the patch may take a while to trickle down and be implemented by mobile carriers, firmware publishers and device manufacturers. The key to success lies in knowing as soon as a patch is available, assessing risk, and updating all your devices without breaking the existing apps and processes. Meanwhile, hackers can exploit unknown vulnerabilities until security researchers are able to find them, alert the vendors and a patch gets issued. Additionally, the mobile OS cannot protect devices from next-generation cyber-attacks that may involve, for instance, malicious Wi-Fi or cellular networks that redirect traffic to a hacker's server(s).

"We have already implemented well-known enterprise mobility management (EMM) and mobile device management (MDM) tools—we're already safe."

While EMM and MDM are necessary tools for enterprise mobility, their security measures are reactive and lack the real-time mobile threat intelligence to take preventive steps to stop threats from evolving into attacks. Also, void of real-time intelligence, EMM and MDM cannot detect active attacks and automatically mitigate them on mobile devices. Continuing to prolong time-to-enforcement could result in a very costly yet very avoidable data breach. Another problem with a reactive approach to mobile security may be a legal one: most organizations operating in the U.S. (or dealing with private information from U.S. residents), by law, must proactively notify the right U.S. State and Federal officials, as well as any channel partners and end-customers whose private data may have been compromised. Recent laws such as the "2016 California Information Security Law" are doubling down on holding organizations accountable for data breaches when many organizations, despite being well aware of new technologies for proactive notification and IT security measures, continued to rely on outmoded reactive approaches to safeguard private information.

Mobile security cannot disrupt our user experience and privacy.

This argument is actually quite valid, and points to another shortcoming of current mobile security. Containerization, mobile gateways, VPN tunneling and most other current on-device ONLY mobile security solutions leveraging private APIs take up a large footprint on devices, stripping them of battery power and bandwidth while infringing on user privacy by rerouting both work-related and personal traffic to third-party servers for inspection. Consequently, many workers refuse to adopt traditional mobile security tools, undermining organizational efforts to benefit from BYOD and the everywhere workplace. Significant advances in proactive mobile security technology have enabled a greatly reduced security footprint on devices while also maintaining user privacy. With today's mobile security options, BYOD users are far more prone to embrace an organization's mobile security policy.

BARRIER #3: It's not real until it happens to you

Once business leaders come to realize that mobile cyber threats are real, the buy-in discussion should raise the stakes by shifting to an enterprise mobile risk assessment. For the first time, cybersecurity leaders can have full visibility and real-time reporting about mobile threat risks to their organization. Typically offered at no cost, mobile risk assessments conducted by mobile threat defense providers, including Skycure, should let business leaders examine a real-time mobile threat map across devices in their own organization — a living picture of active cyber-threats and attacks on their mobile devices, including BYOD. Reactions from business leaders can be startled and horrified upon realizing how risky it actually has been to access, share and use sensitive data on mobile devices.

Another proof-of-concept may come from a "live attack" demo during which a mobile threat defense professional may (with permission, of course) hack into a business leader's device right in front of his or her face—revealing that the organization really has no way of detecting whether a device has been hacked. You may request such "live attack" demo here.

What to report to your CEO and board re: Mobile Threat Defense (MTD)

Upon completing an enterprise mobile risk assessment, cybersecurity professionals can move their buy-in discussion to a final phase in which they report on seven critical outcomes regarding their organization:

1. **Identify**: High-profile public breach and explain why it will not happen here
2. **Report:** Statistical impact of breaches in your industry and potential impact on your company
3. **Report:** Current Enterprise Mobile Risk Score and how the Score compares across your industry
4. **Report:** Number of mobile incidents identified/prevented in the last month
5. **Report:** Which people/devices/department were attacked the most
6. **Report:** Which dataset was targeted the most
7. **Report:** Overall ROI of your investment in Mobile Threat Defense (MTD)

An organization's CEO and/or board want to make decisions based on quantitative results. The real-time threat intelligence gained via mobile threat defense is the only way to "turn the lights on" on mobile threats, allowing business leaders to make data-driven decisions about modernizing their organization's mobile security with mobile threat defense.

Secret #2: Turn the Lights On

Buy the right mobile threat defense solution and do more to prevent data breaches

After garnering buy-in with business leaders, cybersecurity professionals now wonder how to turn the lights on the mobile threat landscape. The following sections detail the top things to consider when buying a mobile threat defense solution, concluding with a proof-of-concept involving the U.S.'s second largest beverage distributor, a private enterprise with annual revenues over $5.4 billion.

SANS Enterprise Mobile Security Checklist

The SANS Institute, a large provider of information security training, certification and research, has issued a checklist to help cybersecurity leaders make the right decision about end-to-end mobile security. Atop of their recommendations is the need for "simple, holistic management and monitoring of a mobile device fleet" by way of integrating mobile threat defense into an organization's EMM (Enterprise Mobility Management).[3] "Holistic management and monitoring" refers to the importance of preventing, detecting and remediating mobile cyber threats and attacks along multiple attack vectors: it is no longer feasible to continually layer an IT security stack with dedicated mobile cybersecurity products that simply cannot adapt quickly enough to the new threat landscape, which is constantly in flux.

Figure 1: Four mobile cyber-attack surfaces that require a "holistic" approach to mobile cybersecurity.

3 Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices (White Paper). The SANS Institute. 2015.

The SANS checklist is segmented into five focus areas of mobile threat defense (MTD) with requirements listed for each area as follows:

SANS Mobile Security Selection Criteria

	Requirements	Priority	Additional Info
Deployment process	Support app download from public stores	High	Official app should be available on Apple's App Store and Google Play
	Overall ease of deployment	High	Considering required actions by the end user and the admin
End user experience	Low impact on device battery usage	High	Usage should be under 3%
	Low data usage	Medium	Both on cellular network and Wi-Fi
	App maintains end user's privacy	High	Not exposing sensitive user information
	Clear display of detected threats and mitigation options	High	Provide a clear and simple display of detected threats with an advisory for mitigating them
	Provide automatic mitigation options for most threats	High	For minimizing actions required from the end user
Threat detection	**Network Threats**		
	Secure communication downgrading (SSL stripping) attack detection	High	Man-in-the-middle attack in which the device communication is downgraded from SSL to plain text
	Secure traffic decryption (SSL decryption) attack detection	High	Man-in-the-middle attack in which traffic from the end user's device is decrypted by the attacker
	Content manipulation attack detection	Medium	Attack in which the content of a web page is altered in order to manipulate the end user
	Rogue networks detection	High	Identify anomalies in public hotspots to identify rogue networks
	Ability to perform automatic mitigation on detected network threats	High	Mitigate network threats without end user intervention, keeping traffic secure without losing connectivity
	Malware		
	Detection of malicious apps based on different app properties	High	For instance, app source, requested permissions, certificate, etc.
	Detection of repackaged/fake apps	High	Detection of malicious apps that impersonate legitimate apps
	Detection of malicious apps based on signatures/known exploits	Medium	Using standard antivirus capabilities
	Ability to block malicious app installation	High	Intervene in real time to stop installation in case the app is risky
	Detection of iOS malware	Medium	Ability to detect new and existing iOS malware such as XcodeGhost and YiSpecter
	Detection of malicious profiles on iOS devices	High	Malicious profiles can be used for monitoring/controlling activity on an iOS device
	Device vulnerabilities		
	Ability to identify jailbroken or rooted devices	Medium	Detection and policy enforcement on these non-compliant devices
	Ability to identify device OS vulnerabilities	High	Present vulnerability details and risk clearly for each device
	Ability to prompt end users to upgrade their device OS version	Medium	Ability to do this as soon as the update is available (sometimes even before the formal vendor announcement arrives)
Management and administration	Provide visibility on detected threats and vulnerabilities	High	Present a clear, detailed description of each threat (including network and malware) and vulnerability (OS/ device configuration)
	Provide an overall risk estimate per device	High	Risk calculation should take into account current threat, device history, vulnerabilities, etc.
	Provide forensic capabilities on identified threats	Medium	Present details about the impact of each detected threat
	Provide the option to define an organization-level compliance policy	High	Devices that do not comply with the organizational policy can be blocked from using organizational resources
	Reporting	High	Provide reporting capabilities, including scheduled email reports, support for different data formats (tables, graphs) and document formats (PDF, CSV)
Other	EMM integration	High	Work with or without an existing EMM solution such as AirWatch, MobileIron and XenMobile
	SIEM integration	High	Support integration with different SIEM systems (ArcSight, McAfee ESM, Splunk, etc.) for exporting detected threats
	Provide a third-party API	Low	Provide a third-party API for retrieving device security information

Figure 2: The SANS checklist provides key guidelines for the RFP processes. While most Mobile Threat Defense (MTD) (and Mobile Threat Protection) solutions are piecemealed together, only a handful of MTD solutions were built from the ground up, dedicated to next-generation mobile cybersecurity.

The six requirements called out in Figure 2 are uniquely challenging or impossible to completely fulfill by most MTD solutions. Only a truly holistic MTD with multilayered reach across all of the SANS Institute's four mobile cyber-attack surfaces can meet the requirements. Next, details about the highlighted requirements reveal why it is critical to build MTD natively from day one: piecemeal strategies cannot handle the holistic load of the SANS checklist.

Requirement 1: Support app download from public stores

Holistic mobile threat defense consists of just a few parts, one of which is a public app that workforces can download onto both their company-issued and BYO devices. MTD apps should be published on the Apple App Store and Google Play stores for a few reasons:

1. BYOD users realize that public iOS and Android apps will not infringe on their privacy and hence easy to adopt
2. Public apps are simple to deploy and maintain, unlike private apps, which require enterprise signing and preparation, and must be deployed by EMM solutions, repeated every time there is an update
3. Public apps are required to use only public APIs, which deliver persistent value and are less prone to deprecation, as with private APIs

Requirement 2: Low impact on device battery usage

Traditional mobile security apps have disrupted user experience by taking up a big footprint on devices — consuming lots of battery power and bandwidth. Next-generation mobile threat defense solves the problem by using a layered approach which leverages not just the device, but also cloud servers for incremental analysis, significantly reducing its device footprint, yet able to proactively identify and protect from real-time threats, even if network connections are blocked or compromised.

Requirement 3: App maintains end-user privacy

Mobile end-users, and most enterprises, insist on a solution that will not compromise the privacy of personal content and communications as a condition of adoption. Today's MTD apps can carry out all critical tasks on the customer's device without requiring access to content or redirecting mobile traffic to third-party servers for inspection. Further, public MTD apps must comply with iOS and Android end-user privacy restrictions.

Requirement 4: Rogue network detection

Beyond the reach of EMM and MDM solutions, mobile threat defense should be able to analyze the tens or hundreds of cellular and Wi-Fi networks that mobile devices encounter — and find suspicious anomalies by way of a) crowd-sourced intelligence, b) reputation services, c) Active Honeypot (a patented approach of luring hackers into accessing fake data).

Requirement 5: Detection of repackaged/fake apps

Traditional anti-malware and antivirus solutions built for desktop and laptop computers were not designed to detect mobile apps that appear in almost every way to be legitimate (including occasional successful postings on the App Store and Google Play). Only after being successfully installed and running on a mobile device will a repackaged/fake app perform its exploit. Mobile threat defense can employ a variety of innovative tools including crowd-sourced intelligence, incremental analysis and behavioral analysis to determine in real time whether the app is safe or not.

Requirement 6: Detection of malicious profiles on iOS devices

Mobile threat defense must also be able to adapt for sophisticated, next-generation cyber-threats, including iOS malicious profiles that leverage vulnerabilities inherent to the design of the iOS platform. Hackers can trick victims into installing their profile that will provide the visibility and control over the device to spy on communications, steal data and credentials, or use the device as a launch pad for broader hacking, even into the organization's private network.

What does the "ideal MTD" look like?

The renowned SANS checklist does a great job of helping cybersecurity leaders select the right MTD. This section describes real-world considerations (important MTD features) to take into account when actually implementing the right MTD.

Ideal 1: Seamless EMM integration

Mobile threat defense should not change the configuration of an organization's existing EMM, meaning that the MTD integration via REST API should satisfy at least two conditions: 1) no scripting necessary 2) the integration process should maintain a simple UX from start to finish for both IT and end-users.

Ideal 2: Unified event management via SIEM

In addition to seamless EMM integration, MTD should provide real-time mobile threat intelligence and other data feeds to an organization's SIEM, thereby condensing real-time visibility and control over all endpoints behind and beyond the firewall under one umbrella of reporting and rules compliance.

Ideal 3: Active protection with or without Internet

As highlighted in the SANS checklist, the new threat landscape targets multiple mobile attack vectors. As a result, MTD must be able to actively (in real-time) detect threats and attacks across all mobile attack vectors without taking up a large device footprint. The right MTD architects a balance of cloud and on-device activities to help ensure mobile cyber threats and attacks do not succeed—even during failover or when a device is disconnected from a cellular or Wi-Fi network.

Ideal 4: Automated protection

Zero days and other mobile breaches can happen in an instant and compromise not only the device, but everything it has access to. The old "time-to-enforcement" metric is based on the outmoded premise that security is a reactive measure, and that is clearly insufficient in today's world of advanced mobile threats. In addition to user and admin notifications that threats exist, MTD solutions must be able to proactively prevent exploits from gaining hold in the first place and not rely solely on other systems, such as EMMs to enforce policies after a time delay. Features like Selective Resource Protection (SRP) should automatically protect sensitive corporate systems from being accessed from a device that connects to a suspicious network, and Secured Connection Protection (SCP) would attempt to activate a VPN to secure communications from prying eyes.

Ideal 5: Predictive threat mitigation

Three vital tools in a mobile threat defense solution include: machine learning, crowd-sourced intelligence and a predictive mobile threat intelligence engine. All of these MTD tools help to continually improve the MTD's intelligence in automatically managing cybersecurity thresholds for constantly changing "zero days." If chatter arises regarding threats in one part of the world, business leaders want to be reassured that MTD users in that geography have had their mobile cybersecurity thresholds automatically raised. Also, by analyzing mobile threat intelligence from millions of monthly tests, MTD can pull big data cyber-threat insights that can further improve risk-based mobile security.

Secret #3: Drive ongoing mobile cybersecurity success

Continually improve mobile threat defense efficacy

Proof-of-Concept: RNDC (Republic National Distributing Company)

John Dickson, Director of IT Infrastructure and Cybersecurity at Republic National Distributing Company (RNDC), participated in a joint webinar with EMM provider, VMware AirWatch® and MTD leader, Symantec. Dickson explained in the webinar that RNDC is no different from the majority of enterprises taking advantage of BYOD and the everywhere workplace — but they are especially challenged to protect their workforce's mobile devices. As a highly lucrative private U.S. enterprise with a substantial transportation, logistics and distribution workforce along with large mobile sales and customer service teams, RNDC cannot accept downtime due to a major data breach. The following sections examine RNDC's transformative journey from traditional IT security to next-generation IT security with mobile threat defense.

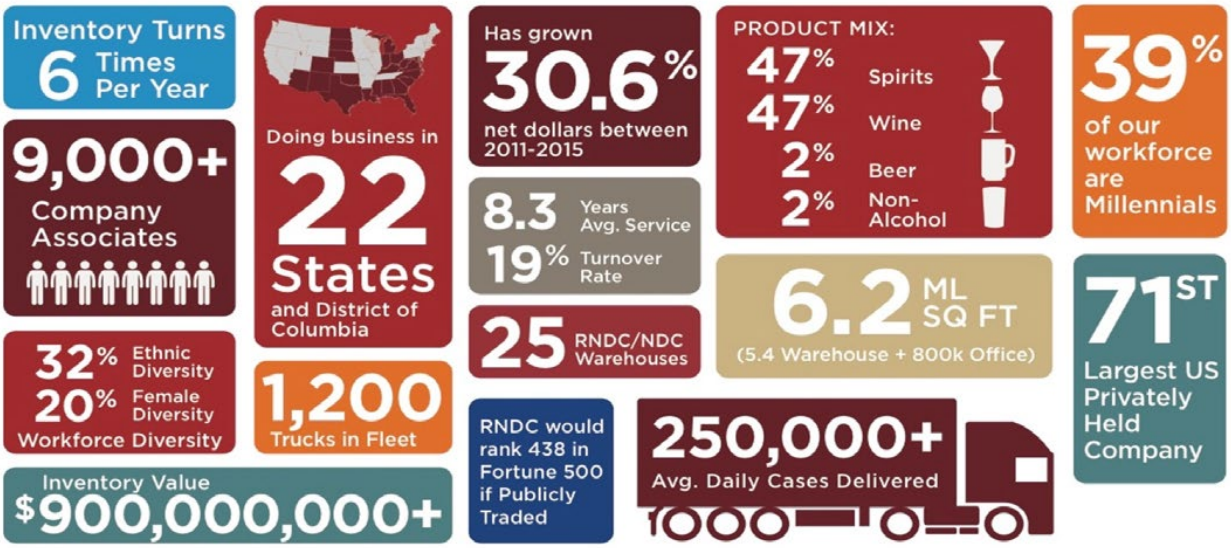

Figure 3: RNDC at-a-glance

Act 1: Management buy-in

John Dickson noted in the webinar that RNDC's rationale to consider mobile threat defense stemmed from the realization:

> *"Mobile is where PC was 20 years ago. But mobile is actually more valuable and more vulnerable than other corporate devices. You don't just need to manage these devices; you need to secure them, too."*

Dickson's buy-in dialogue with RNDC business leaders began with a couple of startling demos as follows:

- **Demo #1:** Via an iOS malicious profile exploit, John used SEP Mobile demo tools to take over the CFO's iPhone in less than 60 seconds.
- **Demo #2:** Next, the SEP Mobile POC on 250 devices showed that 30% of their devices had known vulnerabilities and a whopping ten devices had malware including keystroke loggers. Note: RNDC business leaders had, as requested, downloaded SEP Mobile's free iOS or Android public MTD app prior to the demos.

The demos effectively motivated RNDC's business leaders to see how their IT teams and workforce would react to mobile threat defense.

Act 2: User and IT buy-in

One of the key evolutions in mobile cybersecurity involves a much deeper focus on good user experience (UX). When presented with poor UX, end-users will adopt "shadow IT" and work-around an organization's IT security measures or refuse to adopt mobile security policies on their BYO devices.

At RNDC, Dickson was glad to see how receptive users were to running the public SEP Mobile app on their devices—no noticeable device footprint, no draining of battery life and no infringement of privacy by redirecting work and personal traffic from mobile devices to third-party servers for inspection.

The high user adoption of SEP Mobile also reassured IT that the solution was providing the most accurate "living picture" of mobile cyber threats and attacks. Any BYO device not running SEP Mobile would not allow its owner to access RNDC's corporate email or other sensitive information. In the end, both IT and end-users were very receptive to how SEP Mobile protected devices from exploits and proactively alerted them with specific, clear instructions about how to change user behavior if inadvertently putting their device (and RNDC's data) at higher risk.

Act 3: Outcomes and ROI realization

During the webinar, Dickson acknowledged that SEP Mobile "integrated like glue with AirWatch." The integration was painless, and once a device has been deemed risky by SEP Mobile, that device can automatically be excluded from access to sensitive information or from the corporate network entirely until the risk is removed. While Dickson had narrowed his mobile threat defense search to solutions built from the ground-up for mobile cybersecurity, he found that other MTD solutions did not fulfill all of the requirements from the SANS Institute. Strong misgivings included:

- Complex UX (not good for end-users or IT staff)
- Scripting requirements (requires more IT resources and scripting skills)
- Private APIs used in apps that risk being removed in the next OS version
- Lack of network protection (truly holistic MTD must protect all mobile attack vectors)
- Lack of intelligence (MTD must intelligently adjust thresholds based on changing situations)

After rolling out SEP Mobile, Dickson and his team at RNDC gained a new ability to visualize up-to-the-minute risk status of the organization's entire mobile device fleet. Dickson was able to report on trends about risk distribution, and SEP Mobile provides prioritized recommendations about where and how to reduce and remediate the highest risk devices and situations, including policy updates, cyber-education, patching and other safeguards to protect RNDC's data beyond the firewall on mobile devices.

Dickson needed only one dashboard, to manage risk across all endpoints—and he was able to see real-time stats about a) network threats b) vulnerabilities c) malware. Dickson and RNDC were no longer in the dark about mobile cybersecurity.

Watch a short video of John Dickson explaining why he went with SEP Mobile and VMware AirWatch to secure all his mobile devices.

Summary

It's not hard to become a mobile security superhero

Who wouldn't want to be the superhero of their organization – successfully tackling the critical and complex task of defending mobile devices from the myriad threats to both the devices and the corporate data they access?

Surprisingly, the first and biggest challenge can be convincing others that the threats are real and serious, and action must be taken. Once that is accomplished, there are great resources and a lot of help available to evaluate your own situation and what features to prioritize in order to solve the problem for your organization. Lastly, follow those who have successfully gone before you to chart your own path out of the darkness and into the light of Mobile Threat Defense visibility.

Securing mobile devices is a whole new challenge compared to the security methods for traditional computing devices, but you are not alone and the path is well lit.

Would like to see how Symantec works with AirWatch?

SEP Mobile for AirWatch is an advanced integration that fully allows you to deploy a risk-based mobile security strategy. Upon flagging a device as high risk, SEP Mobile for AirWatch can block access to sensitive information and enforce other policies, which can easily be authored via a simple central management portal.

Request Demo

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

Symantec.com

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.