White Paper

Predictive Mobile Threat Defense

Next-Generation enterprise mobile security provides proactive threat defense and runs on predictive intelligence, crowd wisdom and non-invasive employee experiences.

Symantec™

Introduction

As the connected world becomes even more connected by the day, cyber threats have been retooled to attack ubiquitous mobile endpoints. While attack vectors still include physical (device) threats, the focus has shifted more toward exploiting vulnerabilities in networks, mobile apps, mobile operating systems and mobile user behavior. It follows that next-generation mobile security must be able to holistically protect sensitive data leveraging a multi-layered security model that can stay ahead of attackers in all of the mobile attack vectors.

Most current mobile security programs were designed to respond reactively to attacks rather than to proactively find intrusions and stop them in their tracks before damage is done. With the evolution of threats to multiple attack vectors, purely reactive security does too little, too late: reactive measures on their own cannot match the viral pace at which attacks can spread. Targeted, well-planned attacks may not need much of a window to acquire huge amounts of sensitive data.

This paper explores next-generation mobile security technologies and threat defense strategies that leverage pervasive analytics to predictively identify threats and, if necessary, proactively stop attacks without disrupting users' mobile productivity.

Why Current Approaches Fail

Traditionally, enterprise mobile security has been based on MDM (mobile device management) and containerization as part of reactive strategies or proactive but intrusive approaches like VPN tunneling to remediate threats and attacks. Organizations have measured success for their reactive measures by calculating time-to-resolution or costs of downtime. However, with so much of business and customer success depending on mobility in the connected world, organizations and mobile users can no longer tolerate downtime. Mobile security "success" must be redefined.

Many IT departments have mirrored their mindsets for protecting desktop/laptop computing over to protecting mobile endpoints. The problem that arises is an "apples and oranges" dilemma. Mobile security requires different approaches for reasons that include:

- *Different Resources:* Mobile devices can "die" on a daily basis due to limited battery power. That is why mobile operating systems try to optimize on processes whereas desktops and laptops can handle multiple security apps to simultaneously run in the background.
- *Different Operating Systems:* Due to the design of modern mobile operating systems (i.e., app sandboxing), apps are limited from monitoring and controlling other apps.
- *Different User Behavior:* The BYOD trend is here to stay. By converging work and personal life into a single companion device, employees can work more collaboratively and efficiently. However, it can be a challenge to enforce security policies on an employee-owned device. Both BYO and company managed devices are vulnerable to a unique user behavior: whether they intend to or not, mobile users connect to multiple networks including public hotspots in potentially high-risk zones such as cafes, airports and hotels.

Instead of measuring success solely by the number of intrusions reactively remediated, mobile security programs can become more adaptive, measuring success additionally by the number of threats (among the multiple attack vectors) identified and remediated prior to a potential attack.

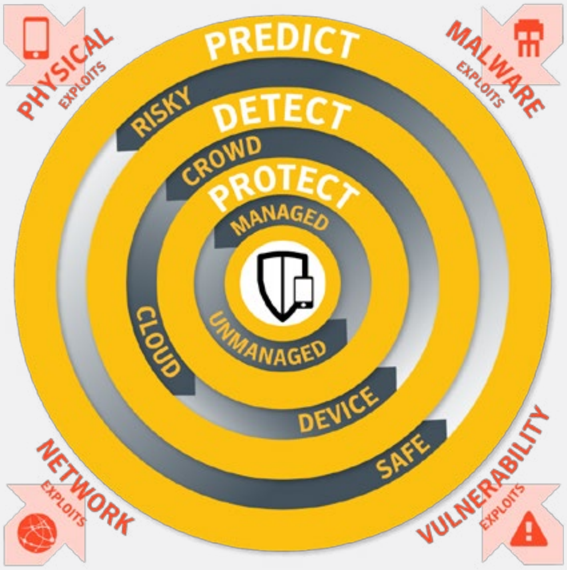
Problems with MDM, Containerization and VPN Tunneling

These three current approaches share in common the problem of either failing IT departments or failing mobile users. The following explains why the approaches cannot function alone or together in any combination to deliver mobile threat defense that satisfies both IT departments and users:

1. **MDM (or EMM):** While MDM can ensure that basic security and compliance policies are set on mobile devices, it lacks active threat detection. It can only passively enforce mobile security best practices without the ability to proactively seek, identify and defend against device, app and network-level attacks, threats, and intrusions.
2. **Secure Containers (Containerization):** Containerization does not provide complete device security. They offer no proactive threat defense to identify attacks and vulnerabilities outside of containers, and containers, themselves, can be hacked.

   Many mobile users view containerization as non user friendly, putting severe limitations on their user enablement and mobile productivity. The change in employee behavior, makes the work on the device more cumbersome and forces mobile users to adopt shadow IT, working around containerization, to resume productivity.

   In addition, many of the most important security features of containerization such as password protected access to enterprise apps are now offered natively by the latest versions of mobile operating systems.



Mobile devices are exposed to orders of magnitude more threats than laptops, with attackers actively seeking to breach devices via multiple mobile attack vectors. Staying ahead of the new breed of attacks requires a revolutionary approach to mobile security that goes beyond simply detecting attacks and sending notifications. Only by *predicting* attacks based on multi-layered, crowd-based risk assessment, *detecting* actual attacks, and proactively *protecting* sensitive data on the device and in connected systems can mobile truly be secure.

3. **VPN Tunneling:** While this approach may work well for desktops and laptops, it fails mobile users on multiple levels:
    - *Disrupted User Enablement:* Running VPN tunneling 24/7 results in an unacceptable drain on device battery life. Most BYOD users will not adopt tunneling because they do not wish to have their personal activity tunneled and monitored by their employer or a 3rd-party solution. This can also lead to the problem of Shadow IT defeating the purpose of mobile threat defense.
    - *Lack of Seamless Continuity:* VPN tunneling can cause significant latency problems affecting productivity and workflow. While latency can be mitigated by adding proxy servers, it comes with a hefty price tag. Regardless of the numbers of VPN servers to route traffic, any connectivity issue on a proxy server can kill all data (personal and business) communications on a device.
    - *Incomplete Security:* Communications happening from within an internal network will circumvent the tunneling approach.

Next-generation Mobile Threat Defense

Most users would probably agree that next-generation mobile threat defense should ensure that they remain enabled in the face of almost any cyber threat: downtime for mobile endpoints is not tolerated. Most EMM and MDM professionals would probably agree that next-generation mobile threat defense should also be built from day one for mobility rather than duplicated from legacy efforts to secure desktop and laptop computing. With that frame of reference, the following sheds insights on what is actually possible today with the latest mobile threat defense technologies and strategies:

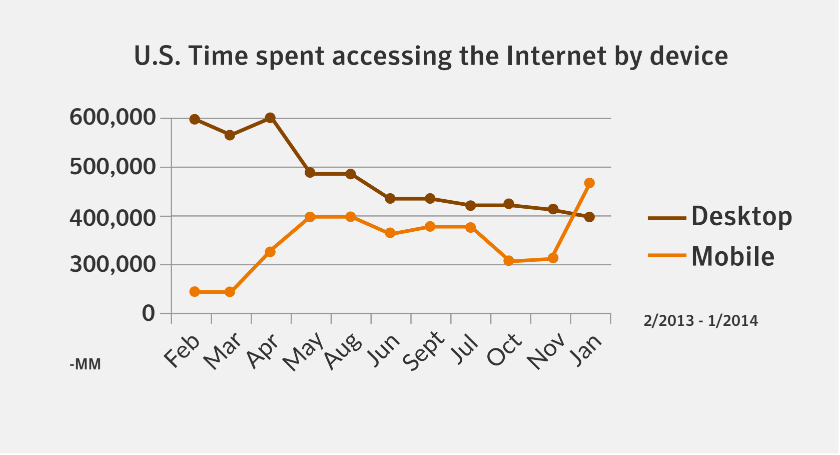
Proactive Mobile Threat Defense: Predictive intelligence and analytics that can instantly extract insights from big data have been pivotal to business success in the connected world. Enterprises can leverage the same powerful capabilities to upgrade their mobile security into a stronger breed of defense. Proactive mobile threat defense maintains intelligent security thresholds 24/7, ensuring business continuity by predicting, detecting and preventing attacks before they can intrude along the full range of mobile attack vectors: physical (device-level), mobile apps, mobile operating system, networks and mobile user behavior.

> “
>
> 58% of information workers surveyed work from another public location while traveling or from a client location.
>
> ”
>
> — *Forrester, 2014*

Future-Proofing for the Third Platform: In January 2014, total API (mobile app) traffic for the first time surpassed total desktop access to the Internet according to comScore. The signs are clear to hackers: resources should target mobile platforms. Mobile Security teams that continue to use legacy IT investments originally designed for desktop-based assets would be the easiest targets and low-hanging fruits for hackers.

Crowd Wisdom and Social Proofing: Security and risk leaders would like to enforce security policy across the multiple attack vectors of mobility, however, users will not adopt security measures that disrupt their productivity.

Prioritizing mobile productivity above all else, mobile workers may join public locations (hotspots, public Wi-Fi networks) when cell-tower bandwidth is limited. Next-generation mobile threat defense should be able to recognize which public locations are suspicious, i.e. by correlating millions of data points gathered from public networks via crowd wisdom and by performing anomaly detection. Though more complicated and costly, attackers can launch attacks via cellular interfaces even when users turn off their devices' Wi-Fi. Crowd wisdom and instant socializing of detected threats from other mobile devices can infuse next-generation mobile threat defense with the real-time "social proofing" to accurately and efficiently flag suspicious public hotspots. A similar "social proofing" threat detection can be applied to mobile app downloads.



Gaining User Trust and Adoption: What happens if mobile security does all of the above but the user does not take the appropriate action in the name of preserving productivity? Mobile Threat Defense must ensure that users are more likely than not to take appropriate actions and not leave themselves more vulnerable to attacks, whether on BYO or company-owned devices. Ideally, next-generation mobile threat defense should continuously educate and garner the trust of end users by showing relevant, timely and actionable alerts.

Several important ways of gaining employee trust and rapid adoption include providing:

- *Non-Invasive Experiences:* Most employees, contractors and partners prefer mobile security to work in the background without infringing on their privacy.
- *Minimal Footprint:* In order to maintain mobile security thresholds 24/7, the mobile threat defense solution should constantly run in the background, which is only possible by minimizing the solution's footprint regarding battery and bandwidth utilization.

- *Ease-of-use:* If a mobile security solution disrupts the familiar mobile experiences of employees, it may cause adoption churn.
- *Accurate Alerts:* Non-adoption of mobile security can also result from alert fatigue caused by too many false-positives notifying end-users about vulnerabilities and threats. Eventually, end users will start ignoring alerts.

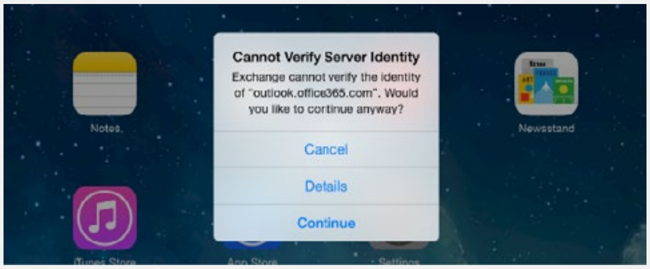
Symantec Endpoint Protection Mobile

Symantec provides next-generation mobile threat defense with Symantec Endpoint Protection Mobile (SEP Mobile), offering proactive capabilities and predictive intelligence to help ensure user enablement and seamless business continuity. SEP Mobile's multi-layered predictive technology is based on years of research and leverages massive crowd-sourced intelligence to identify threats across all attack vectors:

- Physical Defense
- Network Defense
- Malware Defense
- Vulnerability Defense

Symantec believes that with the astounding growth of cyber threats, next-generation mobile threat defense should deliver hands-off management and many automated features that can rapidly evolve: it is the only way to constantly stay ahead of attackers anywhere in the world. Symantec also believes that mobile security programs should be future-proofed for next-generation attacks and offer the following foundation to measure true mobile security success:

What is the appropriate next action?



Cannot Verify Server Identity

Exchange cannot verify the identity of "outlook.office365.com". Would you like to continue anyway?

More than 90% of users click on Continue, compromising their Exchange identity (username and password)

- *Holistic Mobile Threat Defense:* Extend visibility and mobile security beyond the device and monitor multiple attack vectors across network, malware and vulnerability exploits.
- *Predictive Intelligence:* Symantec is a pioneer and leading provider of Mobile Threat Intelligence. SEP Mobile leverages devices as sensors along with crowd wisdom to ensure that intrusion and threat analysis is focused on the correct data among an endless ocean of threats and vulnerabilities.
- *Non-Disruptive User Enablement:* SEP Mobile helps to build trust with employees, contractors and partners by providing them with non-invasive experiences that do not disrupt their privacy, productivity and user experience.

Use Cases - Enterprise Integrations

Adding Active Security Insights into MDM and EMM Solutions

SEP Mobile can easily integrate with an organization's MDM/EMM (such as AirWatch or MobileIron) to add active threat identification at the device, app and network-levels. All Symantec MDM/EMM integrations enhance seamless policy enforcement of existing security policies across all company-owned and BYO devices without disturbing user enablement. SEP Mobile can be deployed automatically, seamlessly leveraging existing MDM accounts and single sign-on capabilities. Additionally, for organizations with no MDM solution deployed, SEP Mobile offers basic MDM capabilities such as setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

1. **Protecting Corporate Assets via VPN Integration** SEP Mobile can leverage third-party VPN integrations to disallow non-compliant devices from connecting to corporate networks while under attack or while the mobile user has entered into a high-risk zone identified by SEP Mobile. For companies without a mobile VPN solution, SEP Mobile can automatically route sensitive traffic via SEP Mobile VPN to secure communication for as long as a device is in a high risk zone.
2. **Enriching a Security Operation Center (SOC) with Mobile Threat Data** Complete visibility is a critical part of proactive mobile threat defense and ensuring efficient and rapid remediation. SEP Mobile, via its REST-based API, can integrate with any SIEM solution such as ArcSight (HP), IBM, McAfee or Splunk to provide complete visibility into all mobile threats, attacks and application vulnerabilities on both company-owned and BYO devices. The logs can be imported via both Syslog and proprietary log formats such as Common Event Format (CEF).

> “
>
> IDC defines the third platform as innovation and growth that is “built on the technology pillars of mobile computing, cloud services, big data and analytics, and social networking.
>
> ”

3. **Auto Deployment and Quarantining High Risk Devices via Exchange Integration** Moving all mobile users, including BYOD users, onto a mobile security program can be a challenge. SEP Mobile mitigates adoption problems by
a) ensuring non-disruptive user enablement
b) providing non-invasive user experiences
c) mandating that users must download SEP Mobile and keep it running in the background in order to send/receive emails and calendar invites through Exchange servers. In this way, SEP Mobile keeps IT informed of anyone who attempts to uninstall or delete SEP Mobile. This integration can also be used to quarantine high-risk devices from accessing sensitive information over email.

SEP Mobile's threat intelligence identifies millions of threats around the world that were identified by socializing via crowd wisdom. The free SEP Mobile app is available for download in both the Apple and Google app stores. With SEP Mobile, devices become sensors and feed non-private information to the SEP Mobile threat analysis engine to constantly improve overall security for everyone.

Conclusion

Next-generation mobile threat defense is now within reach for any organization. Smarter and more purpose-built for mobility and portability, next-generation mobile security leverages the same third-platform advantages that many organizations are using to accelerate innovation and growth. Ultimately, the mobile threat defense and intelligence provided by SEP Mobile enables trusted user enablement, seamless business continuity and proactive, hands-off protection driven by predictive intelligence that stays ahead of attackers anywhere in the world.

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.

Symantec™