Beyond basic protection: Advanced protection actions for effective Mobile Threat Defense

How organizations can protect mobile devices from a range of threats, while maintaining employee privacy and productivity
## Table of Contents

**Introduction** ........................................................................................................................................... 3
- Standard protections aren't cutting it any more ................................................................................... 3
- The next level of MTD protection .......................................................................................................... 4
- Spotlight on advanced protection actions ............................................................................................ 5

**Advanced protection actions in MTD** ................................................................................................... 6
- Leveraging VPN technology .................................................................................................................. 6

**Risky apps** ............................................................................................................................................. 9

**Network threats** .................................................................................................................................... 14

**Content threats** ....................................................................................................................................... 17

**Device-based threats** ............................................................................................................................ 21

**Recap** ..................................................................................................................................................... 24

**Conclusion** ............................................................................................................................................... 25
Introduction

Standard protections aren’t cutting it any more

Just a few years ago, enterprises were in the dark about the risk from mobile security threats. Though the growing use of iOS and Android devices for work brought with it many benefits – greater flexibility, productivity, and privacy – it created a security gap: mobile devices were moving in and out of the corporate environment, with security teams often having little visibility, much less control, over the threats these devices were exposed to out in the wild. As mobile has increasingly turned into a preferred work platform, it has become an attractive target for malicious actors. At the same time, attacks have grown more sophisticated. Hackers have exploited vulnerabilities across mobile apps, networks, and operating systems, putting sensitive corporate data at risk, even on devices traditionally thought to be secure.

The introduction of mobile threat defense (MTD) solutions gave enterprises much-needed visibility over their mobile threat landscape. Major improvements have been made to threat detection over the years, with machine learning and threat intelligence enabling MTDs to use smarter and more sophisticated techniques to identify threats. For example, machine learning has enabled pattern recognition and granular inspection of variations in manipulated HTTP content on the web and in apps. And crowd-sourced threat intelligence on IP, URL and domain reputation has been a boon for identifying phishing attacks.

Still, detection is only one part of the mobile security equation. On the protection front – i.e. actions that go beyond visibility to actively prevent attacks and secure corporate resources – the MTD industry has been more constrained. This is in large part due to the way mobile operating systems are built (i.e. application sandboxing), as well as privacy regulations, which have restricted what actions can be taken on mobile devices. Today, many, if not most MTD solutions rely on Enterprise Mobility Management (EMM) systems to take any concrete actions for data protection. Such actions can include remotely wiping or locking a device if it is compromised, disconnecting a device from the corporate network, and removing managed corporate apps from non-compliant devices.

While these actions may be a useful baseline for mobile security, they have a few drawbacks. First, they are insufficient for protecting against the gamut of sophisticated mobile threats that exist today, including malware, data exfiltration, OS vulnerabilities, network attacks, and phishing. Second, EMM protection actions are often delayed and aggressive, resulting in productivity lags. For example, if malware is detected on a device, an EMM platform can remove corporate apps from the device so they are not exposed to the threat. However, restoring the removed apps is often a cumbersome, lengthy process that requires human intervention. By contrast, simply blocking access to the corporate apps upon detection of a threat is more conducive to productivity as access is immediately and seamlessly restored once the threat is remediated.

Moreover, EMM protection actions are not automatically activated in real-time. EMM platforms can be configured to monitor activity on mobile endpoints and send anomalous behavior alerts to admins, who must then act to remediate any threat. However, as Frost and Sullivan state in their “Evolution of Mobile Security” brief, the success of this reactive strategy “depends on exceptionally fast response times from security professionals. There is a significant likelihood that the alert or the response will come too late to prevent substantial damage.” Consider a situation where a device connects to a network with an active threat or goes to a phishing website – within a matter of seconds, the device could be exposed to risk.

Beyond relying on EMM protection actions, many existing MTD solutions may apply more proactive measures to protect devices, such as always-on VPN tunneling or automatic disconnection from Wi-Fi networks. Similar to

EMM protections, in most use cases, these measures are intrusive and suboptimal\(^2\) from a productivity standpoint. An always-on VPN tunnel drains device battery life and Internet speed. Also, employees who use their own devices for work find it unacceptable to have their personal activity constantly tunneled and monitored by their IT department. Likewise, disconnecting devices from a Wi-Fi network can interfere with workflows and productivity. These actions may protect organizations from some mobile threats, but they come at the cost of employee satisfaction and user experience, making them less effective for enterprises.

The next level of MTD protection

Limited MTD protection actions are gradually becoming a thing of the past. The most advanced form of MTD today includes technology and capabilities that actively protect against a wide range of mobile threats without sacrificing employee privacy and productivity. As mobile devices continue to play a critical role in business, organizations are demanding solutions that can balance these requirements. According to Verizon's Mobile Security Index 2019, 85% of interviewed organizations said they need to take mobile security more seriously, but almost half said they sacrificed mobile security for business performance. The perception that implementing a mobile security solution can interfere with productivity and user experience can be improved by adopting what we refer to as “advanced” protection actions. Specifically, these actions are:

- **On-device**: Enable faster reaction times and constant protection, even when devices are disconnected from the Internet.
- **Real-time**: Proactively thwart attacks, immediately and automatically when a threat is detected.
- **Smart**: Target the exact threat without impacting other resources or processes, and kick in on-demand.

This white paper examines MTD protection actions that contain all or some of the advanced characteristics presented above. The actions reviewed can help organizations achieve the highest level of threat defense while preserving business workflows and user experience – what a truly valuable MTD solution ought to provide. This paper is not meant to be an exhaustive list of protection actions. Rather, it explores a set of effective measures for enterprise mobile security, based on existing technology provided by iOS and Android. There is no one optimal way to use protection actions. While there are best practices, each business will ultimately need to adapt its protections strategy to its needs and risk tolerance.

Spotlight on advanced protection actions

The most effective MTD solutions – those that balance between an organization’s security and business needs – will include advanced protection actions with the following characteristics:

**On-device:** This ensures that threats are thwarted even when a mobile device is disconnected from the Internet, or regardless of another service, such as an EMM, running on the device and receiving detection information. On-device actions also enable faster reaction times, protecting corporate assets immediately upon threat detection.

**Real-time:** Devices and corporate resources are protected immediately and automatically when a threat is encountered – not after damage has been done. Real-time actions are necessary to proactively stop threats from turning into major attacks or breaches.

**Smart:** These protection actions isolate specific threats on one hand, and protect corporate resources on the other, so usability and productivity are not compromised. Smart protection actions include two main operational characteristics:

1. They target the exact threat without impacting other resources or processes on the device. For example, if there is a high-risk app on the device, the communications of that specific app can be blocked, instead of blocking all communications from the device; if a device is under a network attack, access to sensitive corporate resources can be blocked (therefore protecting those resources), while access to other apps, such as social media, continues as usual. Compared to more rigid protection actions like disconnecting a device from Wi-Fi, smart protection actions do not interrupt device usage and workflows. They follow a “castle and jail” approach whereby predefined corporate resources and apps are protected (“castle”) from exploitation by malicious actors, and risky apps and communications are isolated (“jail”) so malware doesn’t spread to the corporate network and sensitive business systems.

2. They are activated on-demand, only when the threat is present. If for example a mobile user connects to a risky Wi-Fi hotspot, a secure VPN tunnel can be activated to allow the user to continue using their device and accessing corporate resources seamlessly. Once the user disconnects from the Wi-Fi network, or the threat isn’t present anymore, the VPN tunnel is turned off. Selective versus constant use of a VPN tunnel has less impact on privacy and productivity.

An important advantage of many advanced protection actions is that they allow for multi-layered implementation. If one action cannot be activated, another kicks in, i.e. blocking access to sensitive corporate resources in cases where a secure VPN tunnel cannot be established, or the organization prefers not to use a tunnel. A multi-layered approach enables organizations to effectively adapt protection actions to their security and privacy policies.
Advanced protection actions for effective Mobile Threat Defense

Advanced protection actions in MTD

The mobile threat landscape is evolving and with complex exploits comes the need for more sophisticated protection actions. The actions examined in this paper are divided by threat category: apps, network, content, and device. While each category may contain additional protections, the paper focuses on those that drive effective and efficient mobile security for enterprise. Organizations should see the below as possibilities they can leverage to reach an optimal balance between security, employee privacy, and productivity. In contrast to reactive protection actions, the advanced actions below all operate in real-time. Some take place on-device, some are smart (i.e. they are targeted and kick in on-demand), and some include all three characteristics.

<table>
<thead>
<tr>
<th>Threat category</th>
<th>Protection Action</th>
<th>OS</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risky apps</td>
<td>Blocking communication</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Preventing installation</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Blocking communication with malicious command-and-control (C&amp;C) servers</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Blocking access to sensitive resources</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Automatic launch of VPN tunnel when network threat is detected</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td>Network</td>
<td>Blocking access to sensitive corporate resources</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Blocking access to fake corporate Wi-Fi hotspots</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Tunneling all traffic through a secure web gateway</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Blocking access to unwanted content</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>Blocking SMS phishing messages</td>
<td>📲</td>
<td>✅</td>
</tr>
<tr>
<td>Content</td>
<td>Automatically disconnect malicious VPNs</td>
<td>📲</td>
<td>✅</td>
</tr>
</tbody>
</table>

On-device ✅ Real-time 🔴 Smart ⬅️

Leveraging VPN technology

Most of the protection actions presented above rely on VPN technology. How the VPN is implemented differs based on the architecture and capabilities of each mobile operating system. A VPN can operate in two ways: 1. as an encrypted tunnel through which traffic passes securely between the device and a network; 2. as a selective traffic blocker. In the latter, specific traffic passing through the VPN is dropped and never leaves the device. Each of these implementations can be always-on or on-demand, resulting in 4 variations: always-on tunnel, on-demand tunnel, always-on selective traffic blocker, and on-demand selective traffic blocker. All of the variations protect against threats in real time, but they differ in their other characteristics, as shown below.
Advanced protection actions for effective Mobile Threat Defense

VPN implementations

<table>
<thead>
<tr>
<th></th>
<th>Tunnel</th>
<th>Traffic blocker*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always-on</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>On-demand</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

- On-device
- Real-time
- Smart

*Only specific traffic is blocked. Non-blacklisted traffic does not pass through the blocker, ensuring continued user access.

Let's look at the main advantages and disadvantages of each implementation.

1. **Always-on tunnel**

   **PROS**
   - Enables 24/7 secure web browsing and mobile app usage by tunneling traffic through content inspection and web filtering gateways
   - Best for compliance purposes as it provides full logs of all device traffic

   **CONS**
   - Impact on end-user privacy because traffic is tunneled through a server-side gateway
   - Latency and connectivity issues can interfere with productivity
   - Relies on VPN server to continuously be up and running

2. **Always-on selective traffic blocker**

   **PROS**
   - Enables 24/7 blocking of specific URLs and domains
   - On-device, meaning traffic is not tunneled and monitored externally, so minimal impact on user privacy

   **CONS**
   - Greater impact on device performance and battery life, compared to on-demand selective traffic blocker, and to VPN tunnels, because inspection is done on-device\(^3\) - instead of in the cloud
   - While user traffic is not being monitored externally, there may still be a perceived privacy issue among end-users when traffic-blocking is activated because a VPN icon appears on the device. However, this notion of privacy infringement can be mitigated with clear user communications in the MTD app.

---

\(^3\) *Inspection is done on-device but it's possible to leverage cloud servers to get more accurate URL reputation.*
3. **On-demand tunnel**

**PROS**
- Protects against threats with minimal impact on device usage, battery and productivity, as the VPN tunnel is activated only when the device is under threat
- Less invasion of privacy because traffic is not constantly being tunneled
- Allows end-users to continue using their device seamlessly when connected to a network posing a threat

**CONS**
- Needs an Internet connection to work
- Tunneling can face latency/connection glitches, potentially interfering with productivity

4. **On-demand selective traffic blocker**

**PROS**
- Minimal impact to privacy as VPN traffic-blocking is client-side – data is not shared with a remote server
- Less impact on battery and device performance as activation occurs only when a threat is detected

**CONS**
- If used to protect corporate resources, users won't have access to them upon detection of a threat, therefore productivity is affected
- As with the always-on selective traffic blocker, here too end-users may perceive the activation of the VPN as infringing on their privacy, when in fact traffic does not leave the device. Good communication with employees can help mitigate concerns over privacy.

It should be noted there is no “right or wrong” in terms of which VPN implementation to use. Each of them will be utilized in different circumstances and for protection against different threats. In many cases, organizations will be able to rely on more than one VPN implementation to enable multi-layered protection. For example, when a device is under a network attack, the traffic-blocking VPN can automatically and immediately be activated while the device waits for a VPN tunnel to be established, to allow continuous, secure use of the device. Once the tunnel is activated, the traffic-blocker is disabled. If a VPN tunnel cannot be established, the device will automatically activate the traffic-blocker to prevent access to sensitive resources.

In the following sections of this paper, we discuss how VPN technology can be leveraged to provide value in the context of the different protection actions. Each section begins with an overview of the threat category, followed by a deeper discussion of the specific protection actions, and a look at some relevant statistics.
Risky apps

Enterprises are increasingly being exposed to data leakage and privacy breaches from mobile apps – including widely-used apps that are generally believed to be secure. Like web and desktop apps, many of the mobile apps employees use on a daily basis are vulnerable to risk; but these apps are often installed and managed by mobile users themselves – rather than enterprise IT – so organizations have less visibility and control over what data these apps can access.

Risky apps can manifest in various forms, such as malware coming from sideloaded apps that do not go through official app store vetting or illegitimate apps that manage to sneak through app store detection. But the risks are not always obvious. Even trusted apps can exhibit suspicious or unwanted behaviors, such as data leakage, data mishandling, or code vulnerabilities, making them no less of a risk to organizations. In fact, research from Appthority shows that within enterprise, non-malware app risks are far more prevalent than actual malware threats.
Advanced protection actions for effective Mobile Threat Defense

Protection actions against risky apps

Actions vary by iOS or Android, as each operating system has its own structure and capabilities.

Android

On Android devices, MTD solutions can provide multi-layered protection against risky apps. The actions below are designed to prevent an app from proceeding at different points of its lifecycle.

Preventing installation of risky apps

An MTD solution can prevent the installation of risky apps immediately upon the download of their installation files, or when end users attempt to install the apps.

Upon download - Deleting/quarantining app files

An MTD app can automatically be set to analyze app installation files as soon as they are downloaded. If the files are found to be risky, the MTD app can immediately and automatically delete or quarantine the files on the device.

Upon installation – Blocking installation via MTD app installer

The installation of risky apps can also be prevented when the MTD app is set as a device's default installer. An MTD app can generally be configured as the installer on Android, enabling it to analyze apps downloaded from third-party app stores, before the actual app installation takes place. When users try to install a risky app, the MTD installer will prevent them from proceeding.

After installation – Terminating processes of running apps

If a risky app passed the installation stage or was already installed on the device, and is running, the MTD solution can be set to automatically terminate the app's processes. The MTD mobile app can run an analysis of the app's files. If the app is found to be risky, it will be prevented from leaking data and executing any actions on the device.

Repackaged apps mimic the look and functionality of legitimate apps but include malicious code. In 2016, various third-party app distributors released repackaged versions of popular mobile game Pokemon GO, which included malware that allowed hackers to spy on users and steal data from their devices. End-users often download such apps from the app store without knowing they are malicious. Upon download and analysis of a repackaged app, an MTD app can detect its malicious behavior and can be set to block the app's installation on the user's device (see “Upon download” above). If the app passes the installation stage and a user opens it on their device, the MTD agent will detect that the app is running and will automatically terminate its processes (see “After installation” above).
Advanced protection actions for effective Mobile Threat Defense

Tools (39%), Lifestyle (15%), and Entertainment (7%) were the most frequently seen categories of malicious apps.  

After installation – Blocking communication of risky apps

Android exposes an API that allows MTD solutions to block all communications from specific apps. When this protection action is enabled, apps defined as risky by an organization’s mobile security policy will be prevented from creating network traffic and communicating with their command-and-control server (i.e. apps will be jailed). Admins can also configure MTD solutions to automatically block communications of a risky app until the MTD completes analysis of the app and determines that it is safe.

Popular iOS and Android apps often use third-party app analytics tools, including screen recordings, to track user interaction and make sure the app is working properly. The analytics SDKs generally do not require app developers to mask sensitive data captured from screen recordings, allowing anyone who has access to the files to see information such as passwords and credit card numbers. Admins can use their MTD app to quarantine these leaky apps and prevent sensitive data from being exposed.

iOS

Blocking communication with malicious command-and-control (C&C) servers

iOS supports the capability to block an app's communication with malicious C&C servers. MTD solutions can leverage this capability to prevent apps from executing malicious commands on the device or stealing sensitive information. In this case, only communications with the malicious C&C server will be blocked, while other communications from the app will not be affected. As this functionality does not rely on an MDM solution, admins can apply this protection in near-real time, across both managed and unmanaged devices, to immediately and effectively protect against new malware campaigns.

Golduck is a traditionally Android-focused malware campaign targeting Android gaming apps, but it also extends to iOS. Several iOS game apps from the official app store have been found to be covertly communicating with Golduck’s malicious C&C servers, enabling hackers to execute malicious commands on iOS devices, like installing additional files and sending SMS messages without the victim knowing. Admins can immediately protect iOS devices against this threat by blocking the app’s communication with Golduck's C&C server.

50% of enterprises protected by Symantec Endpoint Protection Mobile had mobile devices running malicious iOS apps. ⁵

---

⁵ Calculated based on SEP Mobile customers with 1,000 active devices or more.
Blocking access to sensitive resources

In addition to blocking app communication with malicious C&C servers, admins can take a layered approach and block access to sensitive corporate resources. We can think of the former as a "jail," in which malicious app communications are quarantined, and the latter as a "castle," in which sensitive resources are protected from exposure to threats.

Blocking access to resources is an automatic, on-device protection that can be used to defend against several mobile threat vectors (see also Network-based threats) to ensure sensitive data never leaves the device. In terms of risky apps, when malicious or unwanted behavior in an app is detected, the MTD agent on the device blocks access to specific corporate resources defined by the admins of the environment. End-users can still access non-sensitive resources, allowing them to continue using their device for personal use while corporate resources remain protected. This action can be used across both managed and unmanaged devices.

An organization can rely solely on the sensitive resources protection to defend against risky apps, but this protection does not prevent malware from affecting other resources on a device, such private email or files. On the other end of that, blocking app communication alone does not guarantee protection from a malicious app's other possible actions, i.e. deleting files. Using a multi-layered approach is therefore recommended, so that both actions are activated together for optimal protection.

If an app is found to be communicating with a malicious C&C server as in the previous example, and an organization is using a multi-layered protection approach, then both the app's communication with the specific malicious C&C server will be blocked (jail), and the end-user will be prevented from accessing IT-defined corporate resources on the device (castle). Sensitive traffic will not leave the device, but non-sensitive activities can continue.

Protection actions against risky apps prevent threats associated with:

- Credential theft and data leakage (corporate or personal)
- Financial loss and ransomware
- Vulnerable apps (developer code framework vulnerabilities)
- Sideloaded apps (downloaded from untrusted/pirate app distributors)
- Compliance and privacy policy-violating apps
- Risky or unwanted app communication
- Apps that download additional files and exploit OS vulnerabilities

1 in 20 iOS devices (managed or unmanaged) protected by SEP
Mobile has a sideloaded app. ⁶

⁶ Data based on SEP Mobile customers with 1,000 active devices or more.
Advanced protection actions for effective Mobile Threat Defense

Network threats

More so than traditional endpoints, mobile devices are constantly connected, or attempting to connect, to various networks, increasing their exposure to Wi-Fi exploits and interference. Free Wi-Fi may be attractive for users but it can be costly in the end: threat actors can impersonate open hotspots and spy on victims' network activity, redirect traffic to phishing sites, and steal sensitive information – all without victims knowing. Attackers can easily infiltrate vulnerable routers or use cheap tools such as a Wi-Fi pineapple to create fake malicious networks that appear legitimate; users who then connect to these unsecured networks may unwittingly be risking corporate and personal data, and exposing their devices to man-in-the-middle (MITM) and other network-based attacks.

As enterprise workforces are becoming more mobile and employees are increasingly accessing corporate applications on suspicious or unknown networks, the risk from network connection attacks is mounting. A 2018 IDC mobile security decision-maker survey found that, after lost/stolen devices, network-based threats were the top security challenge for IT mobility teams. How can organizations protect themselves from network connection threats and risk of data loss without compromising on employee productivity?

Protection actions against network threats

Automatic launch of VPN tunnel when network threat is detected

MTD solutions can protect against most network connection threats by automatically tunneling traffic through a secure VPN when a threat is identified. This allows end-users to continue using their device seamlessly when risky activity is detected, thus maintaining productivity. Once a device disconnects from a risky network, or there is no longer a threat, the VPN automatically disconnects. Use of a VPN tunnel only when network threats are detected (selective use) has minimal impact on user privacy and on a device's battery life.

Over a period of 3 months: 82% of organizations had mobile users who connected to rogue hotspots; and 1 out of every 100 employees connected to a high-risk network.  

---

8 Data based on SEP Mobile customers with 1,000 active devices or more, over a period of 3 months.
Blocking access to sensitive corporate resources

Admins can also use sensitive resource protection to defend against network attacks. This on-device protection selectively utilizes a traffic-blocking VPN implementation to block access to resources defined as sensitive by the organization; in effect, traffic going to the specific resources is dropped. All other traffic is not affected, allowing end-users to continue accessing non-sensitive corporate resources on their devices.

The resource protection action can be utilized as an additional layer of security on iOS and Android devices when a secure VPN connection cannot be established. This may occur, for example, in SSL-decrypting captive portals or when specific ports are blocked on the network. Upon detection of a network threat, access to sensitive resources is automatically blocked until a VPN tunnel can be established. Recalling the castle and jail approach, here the corporate resources would essentially be isolated from risk (castle), versus quarantining the malicious actors on the device (jail).

In cases where organizations prefer not to use a VPN tunnel at all, corporate resources protection can still be leveraged to ensure protection from network-based threats.

SSL decryption is a potent type of MITM attack that occurs when a malicious actor impersonates a target server, and decrypts the secure communications transmitted between that server and the client. Unaware that their traffic has been intercepted, victims believe their connection is secure. Once communication with the server is approved, attackers can control and monitor the victims’ communications, including their sensitive data. Attackers commonly intercept user communications by establishing fake hotspots with names similar to legitimate networks, for example a hotel guest Wi-Fi network. As such a hotspot can appear legitimate to unsuspecting users, they will connect to the network, sometimes even automatically, essentially giving an attacker control over their communications. An MTD solution can protect against SSL decryption and other network-based threats by automatically tunneling traffic through a secure VPN for the duration of the threat, preventing the traffic from being manipulated. Alternatively, the MTD solution can block access to sensitive resources while users are connected to malicious networks, so that corporate data is not exposed to attackers.
Advanced protection actions for effective Mobile Threat Defense

Blocking access to fake corporate Wi-Fi hotspots

This action allows organizations to prevent their employees from connecting to risky networks under the guise of the corporate brand. Devices that have previously connected to a corporate network will automatically attempt to connect to any hotspot with the same name. Admins can define the official corporate network configuration in the MTD solution; all hotspots that bear the corporate Wi-Fi name but that deviate from the defined properties of the legitimate corporate network will then be blocked on an end-user’s device.

In April 2018, Dutch intelligence caught four Russian agents attempting to intercept Wi-Fi traffic at the headquarters of the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague. The agents reportedly parked a car in front of the OPCW building and began operating technical equipment out of it. The equipment included devices that would allow the agents to spoof the organization’s official Wi-Fi network so that they could intercept employee login credentials. In such scenarios, an MTD solution can block device connection to fake corporate networks, protecting user credentials and corporate data.

Protection actions against network threats prevent risks associated with:

<table>
<thead>
<tr>
<th>Risky networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evil twin networks (fake hotspots, fake corporate hotspots)</td>
</tr>
<tr>
<td>Suspicious hotspots</td>
</tr>
<tr>
<td>Suspicious network hardware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Man-in-the-middle attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL stripping</td>
</tr>
<tr>
<td>DNS hijacking</td>
</tr>
<tr>
<td>Secure traffic decryption</td>
</tr>
<tr>
<td>TLS protocol downgrade</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotspots that manipulate the content in communications between devices and servers</td>
</tr>
</tbody>
</table>

The number of risky Wi-Fi networks in major US tech centers increased by 56% in 2017. ⁹

⁹ Based on major US tech centers, where businesses rely heavily on user mobility.
A risky Wi-Fi is any Wi-Fi that does not provide complete end-to-end secure and private communications.
From Symantec Mobile Threat Intelligence Report 2017: The Year in Review
Content threats

Employees behave less securely on mobile devices: they connect freely to more networks, download risky apps, and access content that may be inappropriate or dangerous for organizations. The latter has become a growing concern in enterprise, as mobile users are more exposed to phishing scams and are more likely to access malicious URLs on their devices. Employees often check their emails on their mobile devices first, and rely more heavily on mobile to communicate with their peers. Mobile phishing can manifest through different channels – SMS, instant messaging apps, gaming apps, social media – that are not protected by standard organizational security measures (i.e. email gateways). In fact, email phishing scams constitute a small percentage of mobile phishing attacks; users are more likely to receive a scam via popular messaging or social media apps. Additionally, smaller screens and mobile interfaces have made it more difficult for users to recognize malicious URLs.\(^1\)

If a victim is successfully duped into clicking a malicious link and entering their corporate credentials – something that happens three times as much to mobile vs. desktop users – attackers can get access to the victim’s device and corporate applications, and then act with free reign within the corporate infrastructure. They can also simply access corporate data that resides on the device or in the cloud. In addition to phishing, risky content can come in the form of: malicious apps and files, communication with malicious command and control servers, websites that violate an organization’s security policy (gambling, adult content, etc) and spam. The protection actions discussed in this section can be used to protect against many of these threats.

Protection actions against content threats

MTD solutions can utilize web filtering capabilities to block malicious or unwanted content on mobile devices. Additionally, they can provide visibility and context on the origin of the content, protecting from malicious links even before a mobile user taps on them.

---

\(^{10}\) Gartner Market Guide for Mobile Threat Defense, Dionisio Zumerle and John Girard, October 30, 2018, pg. 8.
Blocking SMS phishing messages

MTD solutions can analyze incoming SMS messages and determine if they contain malicious links by using various tools, such as real-time URL reputation engines and machine learning. If a message is identified as phishing, it can be blocked (i.e. jailed) on the device without users ever being exposed to it. On iOS, incoming phishing messages can automatically be moved to the “junk” tab. On Android, they can automatically be deleted. Android also provides the ability to alert users to a risky message, enabling them to delete it themselves from their device. The blocking of SMS phishing messages works without requiring that end users click on any incoming links.

In May 2018, customers of an Ohio-based bank reported they were receiving SMS messages on their phones claiming to be from the bank and notifying them that their accounts had been locked. The messages prompted recipients to click on a link to unlock their accounts, leading customers to a phishing website that looked like the real bank site. The fake site asked users to enter their account credentials into a web form to unlock their accounts. In the end, attackers managed to steal credentials from several victims and used the data to successfully withdraw money from ATMs.

A similar scenario could put enterprises at risk. If the victims from the example above used the same credentials to access other resources (such as corporate apps or email) as is often the case, the attackers who stole these credentials could have also gained access to sensitive corporate data. Alternatively, an SMS phishing attack may target employees of an organization directly. Attackers may try to trick employees into providing credentials via SMS phishing and then use the information to access corporate apps. If blocking of SMS phishing messages is enabled on employee devices, the MTD app will analyze the incoming message, detect the malicious URL, and protect users from being exposed to it.

Over a period of 3 months, 1 out of every 10 SEP Mobile customers was exposed to SMS phishing. ¹¹

¹¹ Calculated based on SEP Mobile customers with 1,000 active devices or more.
Blocking access to unwanted content

At a time when data privacy is a key concern for mobile users and privacy regulations are becoming more stringent, end-to-end encryption has been widely used to protect users' data. To accommodate this security standard while still enabling protection against content threats, security teams can use MTD solutions to block malicious or unwanted content directly on a mobile device by using an on-device (client-side) network content blocker. The content blocker leverages a URL reputation engine that inspects URLs, domains, and IPs end users are attempting to access on the device. Admins can define in their MTD solution what type(s) of content violate their company policy, and the MTD app will block this content if end users attempt to access it.

This protection action utilizes an always-on traffic-blocking VPN that drops any policy-violating content on the device. For example, content defined by the organization as malicious, phishing, scam, illegal or belonging to any other unapproved categories will be blocked. Compared to tunneling all traffic externally (see below) and having it decrypted, blocking access to unwanted content has less impact on privacy as URL inspection is done on-device.

Malvertising is the use of legitimate online ad networks to spread malware. It involves inserting malicious ads into websites and apps, with ads appearing to be completely normal to end-users. On the small screens of mobile devices, users may unintentionally tap on ads when trying to get to a specific area or content on a website. Mobile users who tap, intentionally or unintentionally, on a malicious ad may be redirected to a phishing site or could trigger the downloading of malware onto their device. In one malvertising attack targeting iOS devices in 2018, attackers managed to hijack 300 million browser sessions in 48 hours, redirecting users to malicious scams. Organizations can protect against malvertising attacks by blocking device traffic to websites containing malicious ads (i.e. websites containing malware).

The detection of phishing URLs on endpoints increased by 38.1% from 2017 to 2018.  

12 Symantec Internet Security Threat Report, February 2019
Advanced protection actions for effective Mobile Threat Defense

Tunneling all traffic through a secure web gateway

MTD solutions can leverage a cloud-based secure web gateway (SWG) service that analyzes malicious links as soon as end-users tap on them. An always-on VPN tunnels all device traffic through the SWG which filters URLs, detects malicious code, and governs web access according to the organization’s security policy.

Admins can define granular policies for all devices, both traditional and modern, such as web access per device, URL classifications, what actions users can take in apps, and what resources they can access. The SWG inspects all network traffic according to the corporate policy. Access to specific content is then granted or denied based on the policy.

When mobile traffic is tunneled through a VPN, some MTD vendors leverage additional security modules, such as cloud access security brokers (CASBs) and data loss prevention (DLP) solutions, for protection including basing authorization decisions on the mobile security risk posture. These modules allow organizations to secure cloud apps and services from data leakage.

Websites and apps accessed by employees don’t necessarily need to be malicious for them to pose a risk to an organization. For example, employees may access gambling sites on their corporate-owned devices, making the organization legally liable in addition to the employee. When traffic tunneling through a web gateway service is in place, and the organization has defined gambling websites as unwanted in their security policy, access to these websites will be blocked, both on traditional and modern endpoints across the organization. End-users who try to access policy-violating websites will see details on why the content was blocked.

Protection actions against content threats prevent risks associated with:

- Phishing (SMS, email, apps)
- Malicious apps and files
- Websites violating organizational policy
- Third-party app stores

Scam phone calls, SMS phishing and pharming scams were the third most common Internet crime reported by victims in 2017, resulting in a loss of ~$30 million. ¹³

Device-based threats

Like traditional operating systems, mobile OSs have their own security vulnerabilities. These include: known OS vulnerabilities (disclosed by the mobile OS vendors and published in the Common Vulnerabilities and Exposure database), configuration vulnerabilities such as the absence of a lock screen or the existence of untrusted root certificates on the device, and indicators of compromise such as high privilege shells or risky hosts files, often acting as precursors to device rooting.

Work remains to be done in the MTD industry to provide effective protection against all device-based threats. Organizations can choose to remotely wipe mobile devices when an OS has been exploited, or they can use policy enforcement to prevent non-compliant devices from accessing specific corporate resources. Remote wiping or resource access blocking however, can interfere with mobile device usage and productivity, making them less optimal in an enterprise environment. The challenge remains how to protect mobile endpoints against device-based threats while ensuring business continues as usual.

Malicious iOS profiles

One OS-level threat that MTD solutions can provide direct protection against is iOS “malicious profile” attacks. This threat is not new, and in recent years Apple has made it harder to pull off such attacks. Still, hackers are finding creative ways to bypass Apple's security mechanisms, generally using sophisticated social engineering exploits to trick victims into installing malicious configuration profiles on their devices. iOS configuration profiles include settings for managing the device’s proxy, VPN and certificates. When attackers convince mobile users to install their malicious profile, they can essentially gain control of the device, capture credentials for sensitive data access, and download additional malicious files. Aside from redirecting traffic to malicious sites, attackers can use the profiles - which can also be hidden so victims don’t even know they are there - to install root certificates and configure a malicious VPN on the device, allowing them to intercept and decrypt secure connections.

To successfully compromise device settings via a malicious profile, attackers count on users who don’t pay attention to iOS configuration dialogs. Mobile users tend to quickly install and approve these configurations when promised free Internet, discounts or services. Attackers can use a Proxy server, change an APN setting, or employ MITM techniques to tamper with certificates and profiles, thereby tricking the victim's device into trusting them. What begins with an oversight on the part of the end-user can result in potentially devastating access to a device and the personal/corporate data it accesses.
Automatically disconnect malicious VPNs

Once a malicious profile is on a device, it can install both a malicious VPN and CA certificate. These two configurations allow attackers to tunnel all device traffic through a malicious server which generally decrypts SSL traffic and exposes all communications, including sensitive data. To protect against these risks, admins can automatically disable malicious VPNs on iOS devices by enabling a secure VPN provided by the MTD solution. As only one VPN can be activated on an iOS device at a time, the MTD solution continues to activate the secure VPN so that the malicious VPN connection cannot be established. Additionally, encrypted traffic tunneled through the secure VPN stays protected, even if a CA is on the device and the attacker has control of the Wi-Fi network.

Mobile users will often follow instructions such as installing files when trying to connect to a free Wi-Fi network, for example at the airport. If users attempt to connect to a fake hotspot that seems legitimate, they may be prompted to download a file before they are granted connectivity. Approving the file download begins the process of installing a malicious configuration profile on the device, adding it to the list of trusted root certificate authorities. When enabled, the attacker can use the profile for malicious actions, for example decrypting SSL communications and accessing personal data. See a demo of a malicious iOS profile attack.

Over a period of 3 months 1 out of every 4 organizations had devices with an untrusted iOS profile on them. ¹⁴

¹⁴ Calculated based on SEP Mobile customers with 1,000 active devices or more.
Advanced protection actions for effective Mobile Threat Defense

Untrusted iOS profile incidents by OS version

- iOS 10: 5%
- iOS 11: 29%
- iOS 12: 66%

Based on SEP Mobile customers with more than 1K active devices.
Recap

The above discussion on “automatically disconnecting malicious VPNs” wraps up our review of advanced protection actions in Mobile Threat Defense. We began this paper with a look at the limitations of EMM protection actions, as well as other actions commonly used by MTD solutions today that are often intrusive and aggressive in their approach to securing corporate data. We then discussed how developments in mobile operating system technology have enabled advanced MTD protection actions – on-device, real-time and smart – to address current protection shortcomings. Advanced protection actions can provide organizations optimal mobile security without compromising on end-user productivity and privacy.

The subsequent sections of the paper explored advanced protection actions in each of the major mobile threat categories: risky apps, network, content and device-based. In risky apps, we looked at MTD actions that can prevent a malicious app from proceeding on a device at different stages of its lifecycle (download, installation, and execution). In network threats, we discussed how VPN tunneling and blocking access to resources can be used as an effective protection combination against network connection threats – one of the biggest security challenges for IT mobility teams. The content threats section discussed the growing risk to enterprise from mobile phishing, and actions that can be taken to protect from malicious content and links, even before mobile users are directly exposed to them. Lastly, the device-level section examined what recourse organizations can take against malicious iOS profiles, a threat that can put corporate data at risk.

Each threat section looked at how VPN technology is leveraged by protection actions to achieve more effective threat defense across different use cases. The VPN implementations and protection actions rely on a “castle and jail” approach in which threats are jailed on a device, and corporate resources are castled to protect them from risk. As there is no one ideal protection model, we discussed how layering protection actions allows organizations to adapt their protection strategy to their security and privacy policies. Each section in the paper also provided mobile threat statistics, many of which are based on data from actual enterprises protected by Symantec Endpoint Protection Mobile.

Innovation in MTD protection actions is a continuous journey that involves mobile OS vendors, MTD vendors, customers, end users, and even hackers – as threats become more sophisticated, so too will the techniques used to protect against them.
Advanced protection actions for effective Mobile Threat Defense

Conclusion

Embracing the next level of protection actions

Enterprises are increasingly recognizing the need for MTD solutions to address security challenges arising from today’s growing mobile workforce. Progress has been made in mobile threat detection, but work remains to be done on the protection end. Rudimentary protection actions that generally react to threats in delay or interfere with employee privacy and productivity are failing to meet enterprise mobile security needs. In fact, there is no reason to rely solely on these actions anymore.

Technological developments in mobile security are enabling advanced protection actions that can proactively and instantly protect organizations from threats across all attack vectors – from malicious apps and mobile phishing to risky networks and MITM attacks – without being invasive for employees. On-device protection actions ensure a faster response to threats and work even when there is no Internet connection. Real-time actions protect devices immediately and automatically upon threat detection. Smart actions protect sensitive resources while isolating threats (castle and jail approach), and are only activated when a threat is present, thus having a minimal impact on end users. With one in every three organizations suffering a mobile breach last year\(^\text{15}\), now, more than ever, organizations need such advanced protection actions to effectively keep their data secure.

\(^\text{15}\) [Verizon Mobile Security Index 2019](https://www.verizonwireless.com/about/corporate-social-responsibility/verizon-mobile-security-index)