WHITE PAPER

Symantec
by Broadcom

Beyond Basic Protection: Advanced Mobile Threat Defense

How to Protect Mobile Devices from Multiple Threats while Maintaining Privacy and Productivity

TABLE OF CONTENTS

Introduction

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 including greater flexibility, productivity, and privacy, it created a security gap: mobile devices were moving into and out of the corporate environment, and security teams often had little visibility, and even less control, over the threats these devices were exposed to. As employees increasingly prefer a mobile work platform, it has become an attractive target for malicious actors. At the same time, attacks have grown more sophisticated. Hackers exploit 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 the mobile threat landscape. Major threat detection improvements have been made, 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 the granular inspection of variations in manipulated HTTP content on the web and in apps. 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—actions that go beyond visibility to actively prevent attacks and secure corporate resources—the MTD industry has been more constrained. This is largely due to the way mobile operating systems are built (application sandboxing), as well as privacy regulations, which have restricted which 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 noncompliant 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 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. 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:

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

This white paper examines MTD protection actions that contain all or some of the advanced characteristics presented above. These actions help organizations achieve the highest level of threat defense while preserving business workflows and user experience, two features 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 not one optimal way to use protection actions. While there are best practices, each business will ultimately adapt its protection strategy to its unique needs and risk tolerance.

Spotlight on Advanced Protection Actions

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

On-Device Protection Actions

On-device protection actions ensure that threats are thwarted even when a mobile device is disconnected from the Internet, 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 Protection Actions

Real-time protection actions ensure 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 Protection Actions

Smart protection actions both isolate specific threats and protect corporate resources, 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, communications of that specific app can be blocked, instead of blocking all communications from the device. This means if a device is under a network attack, access to sensitive corporate resources can be blocked and those resources can be protected, 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, where 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.
   - For example, if a mobile user connects to a risky Wi-Fi hot spot, a secure VPN tunnel can be activated to allow the user to continue using their device and access 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 a multi-layered implementation. If one action cannot be activated, another kicks in, such as blocking access to sensitive corporate resources in cases when a secure VPN tunnel cannot be established, or if 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 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, this paper focuses on actions that drive effective and efficient mobile security for enterprises. Organizations should see the following examples 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 and are targeted and activate on demand, and some include all of the characteristics.

COMPLEX EXPLOITS DRIVE THE NEED FOR MORE SOPHISTICATED PROTECTION ACTIONS

Table 1: Mobile Threat Advanced Protection Actions by Threat Category

Threat Category	Protection Action	OS	Characteristic
Risky Apps	Block communication with malicious command-and-control (C&C) servers	✓ iOS ✓ Android	✓ On-device ✓ Real-time ✓ Smart
	Block access to sensitive resources	✓ iOS ✓ Android	✗ On-device ✓ Real-time ✓ Smart
Network	Automatic launch of VPN tunnel when network threat is detected	✓ iOS ✓ Android	✗ On-device ✓ Real-time ✓ Smart
	Block access to sensitive corporate resources	✓ iOS ✓ Android	✓ On-device ✓ Real-time ✓ Smart
	Block access to fake corporate Wi-Fi hot spots	✓ iOS ✓ Android	✓ On-device ✓ Real-time ✓ Smart
Content	Tunnel all traffic through a secure web gateway	✓ iOS ✓ Android	✗ On-device ✓ Real-time ✗ Smart
	Block access to unwanted content	✓ iOS ✓ Android	✓ On-device ✓ Real-time ✗ Smart
	Block SMS phishing messages	✓ iOS ✓ Android	✓ On-device ✓ Real-time ✓ Smart
Device-Based	Automatically disconnect malicious VPNs	✓ iOS ✗ Android	✓ On-device ✓ Real-time ✓ Smart

The Use of 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 can be an always-on implementation or an on-demand implementation, resulting in four 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.

THERE ARE FOUR VPN IMPLEMENTATION OPTIONS:

1. ALWAYS-ON TUNNEL

2. ON-DEMAND TUNNEL

3. ALWAYS-ON SELECTIVE TRAFFIC BLOCKER

4. ON-DEMAND SELECTIVE TRAFFIC BLOCKER

Table 2: Four Variations of VPN Implementation

Implementation	Tunnel	Selective Traffic Blocker[a]
Always-on	**Real-time protection** 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.	**Real-time, on-device protection** PROS • Enables 24/7 blocking of specific URLs and domains. • On-device protection means traffic is not tunneled and monitored externally, so there are minimal impacts on user privacy. CONS • Greater impact on device performance and battery life compared to an on-demand selective traffic blocker, and also to VPN tunnels, because inspection is done on the device[b] instead of in the cloud. • While user traffic is not 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.
On-demand	**Real-time, smart protection** 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 tunneled. • Allows end users to continue using their devices seamlessly, even when connected to a network that poses a threat. CONS • Needs an Internet connection to work. • Tunneling can face latency and connection glitches, potentially interfering with productivity.	**Real-time, on-device, smart protection** PROS • Minimal impact to privacy as VPN traffic blocking is done on the client side, so 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 the resources upon detection of a threat, which can affect productivity. • As with the always-on selective traffic blocker, end users may perceive the activation of the VPN as infringing on their privacy, even though traffic does not leave the device. Good communication with employees can mitigate privacy concerns.

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

[b] Inspection is done on the device, but it is possible to leverage cloud servers to get more accurate URL reputation.

IN MANY CASES, ORGANIZATIONS WILL BE ABLE TO RELY ON MORE THAN ONE VPN IMPLEMENTATION TO ENABLE MULTI-LAYERED PROTECTION

It should be noted there is no right or wrong choice 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 the 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. Protection actions against risky apps vary, as each operating system has its own structure and capabilities.

iOS

Block 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.

Block 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, including 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 nonsensitive 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.

Protection in Action

- If an app is found to be communicating with a malicious C&C server, 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-predefined corporate resources on the device (castle). Sensitive traffic will not leave the device, but nonsensitive activities can continue.

50% OF ENTERPRISES PROTECTED BY SES MOBILE HAD MOBILE DEVICES RUNNING MALICIOUS iOS APPS.
25% ORGANIZATIONS HAD DEVICES WITH AN UNTRUSTED iOS PROFILE ON THEM.[1]

[1] Data based on SES Mobile customers with 1000 active devices or more.

Leverage Protection Actions against Risky Apps to Prevent Threats:

- Corporate or personal credential theft and data leakage
- 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

Network Threats

More frequently 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 hot spots 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 become more mobile and employees increasingly access corporate applications on suspicious or unknown networks, the risk from network connection attacks is mounting. How can organizations protect themselves from network connection threats and risk of data loss without compromising employee productivity?

Protection Actions against Network Threats

Automatically Launch a VPN Tunnel When a 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, maintaining productivity. Once a device disconnects from a risky network or there is no longer a threat, the VPN automatically disconnects. The selective use of a VPN tunnel only when network threats are detected has minimal impact on user privacy and on a device's battery life.

Block Access to Sensitive Corporate Resources

Admins can 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 access nonsensitive corporate resources.

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.

Block Access to Fake Corporate Wi-Fi Hot Spots

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 hot spot with the same name. Admins can define the official corporate network configuration in the MTD solution; all hot spots 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.

Protection Actions against Network Threats

Protection in Action

- 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 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 sensitive data. Attackers commonly intercept user communications by establishing fake hot spots with names similar to legitimate networks, for example a hotel guest Wi-Fi network. Unsuspecting users connect to these seemingly legitimate networks, sometimes even automatically, which gives attackers 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 traffic from being manipulated. Alternatively, the MTD solution can block access to sensitive resources while users are connected to malicious networks, so corporate data is not exposed to attackers.
- Recently, 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.

OVER A PERIOD OF THREE MONTHS, 82% OF ORGANIZATIONS HAD MOBILE USERS WHO CONNECTED TO ROGUE HOT SPOTS; 1 OUT OF EVERY 100 EMPLOYEES CONNECTED TO A HIGH-RISK NETWORK[2].

Leverage Protection Actions against Network Threats to Prevent Risks:

- Risky networks
  - Evil twin networks including fake hot spots and fake corporate hot spots
  - Suspicious hot spots
  - Suspicious network hardware
- Man-in-the-middle attacks
  - SSL stripping
  - DNS hijacking
  - Secure traffic decryption
  - TLS protocol downgrade
- Content manipulation
  - Hot spots that manipulate the content in communications between devices and servers

[2] Data based on SES Mobile customers with 1000 active devices or more.

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. This has become a growing concern in enterprises, as mobile users are more exposed to phishing scams and are more likely to access malicious URLs on their devices. Mobile phishing can manifest through different channels—SMS, instant messaging apps, gaming apps, social media—that are not protected by standard organizational security measures. In fact, email phishing scams constitute a small percentage of mobile phishing attacks; users are more likely to receive a scam via messaging or social media apps. Additionally, smaller screens and mobile interfaces make it more difficult for users to recognize malicious URLs.

If a victim is successfully duped into clicking a malicious link and entering their corporate credentials, which happens more frequently to mobile users, attackers can get access to the victim's device and corporate applications, and then have free reign within the corporate infrastructure. They can also 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 C&C servers, websites that violate an organization's security policy (gambling, adult content, etc), and spam.

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.

Block 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 (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, so they can delete it from the device. Blocking SMS phishing messages works without requiring end users to click on any incoming links.

Block 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 user 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 network content blocker. The content blocker leverages a URL reputation engine that inspects the URLs, domains, and IPs end users are attempting to access on the device. Admins can define in their MTD solution what types 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; 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 and having it decrypted, blocking access to unwanted content has less impact on privacy, as URL inspection is done on the device.

Tunnel 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, actions users can take in apps, and what resources they can access. The SWG inspects all network traffic according to the policy. Access to specific content is 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.

Protection Actions against Content Threats

Protection in Action

- 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 the 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.
- 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.
- 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.

OVER A PERIOD OF THREE MONTHS, 1 OUT OF EVERY 10 SES MOBILE CUSTOMERS WAS EXPOSED TO SMS PHISHING[3].

Leverage Protection Actions against Content Threats to Prevent Risks:

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

[3] Data based on SES Mobile customers with 1000 active devices or more.

Device-Based Threats

Like traditional operating systems, mobile OS 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 host 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 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.

Protection Actions against Device-Based Threats

Malicious iOS Profiles

MTD solutions can provide direct protection against 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 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 and 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 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.

Protection in Action

- 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 hot spot 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.

Conclusion

Developments in mobile operating system technology have enabled advanced on-device, real-time, and smart MTD protection actions to address current mobile protection shortcomings. Advanced protection actions can provide organizations optimal mobile security without compromising end user productivity and privacy. Advanced protection actions in each of the four major mobile threat categories (risky apps, network, content, and device-based) help organizations strengthen their mobile security posture.

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, layering protection actions allows organizations to adapt their protection strategy to their security and privacy policies.

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.

ENTERPRISES INCREASINGLY RECOGNIZE THE NEED FOR MTD SOLUTIONS TO ADDRESS SECURITY CHALLENGES ARISING FROM TODAY'S GROWING MOBILE WORKFORCE

Embrace the Next Level of Protection Actions

Enterprises increasingly recognize 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 can delay or interfere with employee privacy and productivity, and 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 enable 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. Now, more than ever, organizations need such advanced protection actions to effectively secure their data.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SYM-AMTD-WP100 January 16, 2024