BUYER'S GUIDE

MOBILE PROTECTION

THE 5 PRINCIPLES OF A MOBILE SECURITY SOLUTION THAT IS ROBUST, COMPREHENSIVE, DESIGNED TO KEEP YOUR ORGANIZATION AND SENSITIVE DATA SAFE

Cyber Talk

CONTENTS

INTRODUCTION:
THE MOBILE PROTECTION CHALLENGE

It has never been more challenging for security and risk management leaders to protect the organization's mobile devices and strengthen its mobile security posture.

It's true that protecting corporate mobile devices has never been easy. App stores contain many malicious apps, it is more difficult to spot suspicious email contents and attachments when they come in on mobile, and phishers often exploit vulnerabilities that are specific to mobile apps and for which filters often do not exist.

But, today, the challenge is even more complex – with the attack surface being greater than ever due to the mass mobilization of the global workforce to the home.

> *Mobile security is at the top of every company's worry list these days — and for good reason.*
>
> *(CSO)*

COVID-19 AND THE NEW REMOTE NORMAL

Indeed, in the age of the Covid-19-driven new normal, the remote workforce is increasingly accessing corporate data from mobile devices, often over public WiFi networks that are easy to compromise, sending more emails, messaging more often, and sharing more files than ever.

The result is that exposure and risk is at unprecedented levels. In fact, since March 2020, researchers at Check Point have been observing an enormous rise in the number of attacks and data breaches that are coming in through the mobile endpoint.

These attacks are new and dangerous, and include Coronavirus-related malicious campaigns, sophisticated mobile ransomware attacks, and the weaponization of Mobile Device Management (MDM).

Among the trending threats that have been observed are:

- Fake Covid-19-related apps
- Malware distribution via MDM systems
- Coronavirus contact tracing apps
- Mobile ransomware

And companies of all sizes and across every industry are getting hit. In a survey of nearly 900 security professionals, it was uncovered that 40% had experienced a mobile-related compromise.

Of those who have been compromised:

- **66%** say that the impact was major
- **37%** say that remediation is difficult and expensive
- **45%** confirm that their defenses are lagging the capabilities of the attackers

Research finds that as the pandemic forces companies to accept the idea of permanent massed remote working, CIOs are waking up to the threat of increased cyber attacks.

(ComputerWeekly)

THE IMPACT OF MOBILE ATTACKS

29% HAD TO PAY REGULATORY PENALTIES

59% SUFFERED DOWNTIME

46% HAD OTHER DEVICES COMPROMISED

56% EXPERIENCED DATA LOSS

Source: Verizon 2020 Mobile Security Index Report

THREE KEY HURDLES TO EFFECTIVE MOBILE SECURITY

PROTECTION VS. PRODUCTIVITY?

With the increasing rate of attacks and with the ramifications being so dire, it's almost shocking to know that most organizations prefer to sacrifice mobile security for the sake of business productivity.

Regretfully, the perception that mobile security must be compromised in order to ensure productivity (and that it's ok to do so) is not only erroneous but also leaves organizations greatly exposed to attack.

> *A full 85% of the CISOs surveyed admitted that they sacrificed cybersecurity in the effort to enable employees to work remotely. In the end, some 63% of the respondents say they experienced an increase in the number of cyberattacks.*
>
> *(TechRepublic)*

CAN MDM REALLY PROTECT?

Another misconception is that Mobile Device Management (MDM) solutions can provide robust mobile security. While these solutions do enable administrators to monitor and manage employee mobile devices, they do not provide comprehensive and sufficient protection against cyberthreats.

PROTECTION VS. PRIVACY?

And the third significant hurdle for those charged with protecting the corporate mobile fleet is the privacy imperative.

Namely, organization often struggle to find the right balance between securing employee mobile devices while adhering to the requirements of protecting their personal and payment data, as well as ensuring that the photos, videos, and the web browsing history that reside on their device are not accessed.

Clearly, there is a great need for a solution that can help security professionals overcome the many challenges of mobile protection.

In this paper we set out to help them do just that, by presenting the five principles of the optimal solution for effectively securing the mobile devices that are used by employees, wherever they are.

5 PRINCIPLES FOR SELECTING THE OPTIMAL MOBILE SECURITY SOLUTION

PRINCIPLE #1:
HAVING 360° PROTECTION OF ALL ATTACK VECTORS

Mobile devices have three key vectors of attack – the device's operating system, apps, and the network.

Consequently, the optimal mobile device security solution must demonstrate advanced capabilities for securing each of these three vectors.

> *Mobile users accessing phishing websites are three times more likely to submit their login info than desktop users.*
>
> *(SecurityIntelligence)*

QUESTIONS TO ASK WHEN EVALUATING 360° PROTECTION CAPABILITIES:

- Does the solution perform **real-time risk assessments** across all attack vectors, to detect attacks, vulnerabilities, configuration changes, and advanced rooting and jailbreaking techniques?
- Does the solution conduct **behavioral assessments** of each app that is downloaded to a device for real-time detection and blocking of malicious app downloads?
- Does it leverage **anti-bot capabilities** to block Man-in-the-Middle attacks on the network and prevent data exfiltration to command and control servers?
- Does it **proactively block phishing sites**, even those that have never been seen before, to prevent credentials theft?
- Does it leverage a **global collaborative knowledge base** for gaining access to real-time threat intelligence and sharing knowledge and insights?

PRINCIPLE #2:

FULL VISIBILITY INTO THE RISK LEVEL OF THE MOBILE WORKFORCE

> *With remote work here to stay, security professionals need ways to maintain visibility, monitoring and threat detection when the network perimeter, which has been disintegrating for years, has become almost non-existent.*
>
> *(SecurityIntelligence)*

Having a complete picture of the organization's mobile security posture is critical to effectively mitigating risk and accelerating response when needed.

The implications of a visibility gap include greater exposure to attack and a compromised ability to resolve and remediate if an attack does hit.

The most effective tool for bridging the gap and for managing mobile threats is an advanced and intuitive visual dashboard that provides real-time threat intelligence with visibility into the threats that are impacting the mobile fleet.

QUESTIONS TO ASK WHEN EVALUATING CAPABILITIES FOR PROVIDING FULL VISIBILITY:

- Does the solution have a **cloud-based** and **easy-to-manage** dashboard?
- Does the dashboard provide **full visibility into incoming threats** as well as into the security posture of mobile devices?
- Does the dashboard enable **granular policy configuration**?
- Does it ensure **adherence to corporate policies** when users attempt to access corporate data with their mobile device?
- Does it provides an **application vetting service** to further expand mobile application deployment security?

PRINCIPLE #3:

SCALABILITY, FOR SECURING THOUSANDS OF DEVICES IN NO TIME

> *Enterprises, particularly those who enforce a bring your own device (BYOD) policy, are inundated with the growing number of devices and operating systems.*
>
> *(EnterpriseMobilityExchange)*

The different types of devices and operating systems that comprise an organization's fleet of mobile devices are many, including iOS and Android, 'bring your own devices' (BYOD), and corporate-owned units.

And that's just the tip of the iceberg.

What this means is that the optimal mobile security solution must be able to support every device type, operating system, and device-ownership model.

And, as the organization grows, it should also be able to scale without adding complexity to the security operation.

QUESTIONS TO ASK WHEN EVALUATING FLEXIBILITY:

- Can the solution protect both **corporate- and personally owned** devices?
- Does the solution **seamlessly integrate** with all the market-leading mobile device management and unified endpoint management solutions?
- Does it **easily integrate with other security tools**, such as SIEM or threat intelligence?
- Does it enable **zero-touch enrollment** for mass deployment of mobile devices, without the intervention of end-users?

PRINCIPLE #4:
MAXIMIZING THE USER EXPERIENCE

"The main challenge is how to implement an app vetting process that does not overwhelm the administrator and does not frustrate the users."

(Gartner)

There is no doubt that the mobile device is a strategic enabler of productivity. Introducing any interruption to the employee's mobile user experience due to background activity of the mobile security solution will hinder performance. And this is clearly unacceptable.

Accordingly, the optimal mobile protection solution must avoid impact on device usability, the browsing experience, data consumption, and battery life.

QUESTIONS TO ASK WHEN EVALUATING THE SOLUTION'S POTENTIAL IMPACT ON THE USER EXPERIENCE:

- Can the solution detect threats **without impacting device performance**?
- Can it ensure safe and **disruption-free web-browsing** and **file sharing?**
- Does the solution provider take a preventative approach by offering easy-to-access and clear **knowledge about the risks** that a device may be exposed to?

PRINCIPLE #5:
ENSURING PRIVACY BY DESIGN

> *While no one would deny the need to ensure enterprise security in the BYOD era, it must not come at the expense of employee privacy.*
>
> *(Wired)*

Ensuring employee privacy is an additional critical mandate.

Though ensuring data privacy can be very challenging when operating in a BYOD model, and particularly at a time when the lines between using mobile devices for work versus personal needs have become blurred following the coronavirus outbreak and global work from home directives.

Nevertheless, going soft on privacy is not an option.

As such, the optimal mobile security solution must also be designed for uncompromising privacy protection.

QUESTIONS TO ASK WHEN EVALUATING THE SOLUTION'S PRIVACY PROTECTION CAPABILITIES:

- Does the solution **collect device metadata only**?
- Does it ensure that **IT admins never see which apps** the user has downloaded onto their device?
- Does it ensure that admins **never see which websites employees are browsing** on their device?
- Does the solution **anonymize the data** it uses for analysis?

IN SUMMARY

Ours is a mobile world. And threat actors have taken notice, continually seeking new mobile infection vectors and improving their techniques to bypass security protections.

For organization to make sure that the corporate data that is contained on their employees' mobile devices is secured, they need advanced protection against multiple threats including malware, phishing, Man-in-the-Middle attacks, OS exploits, and more.

They also need access to real-time risk assessments and visibility into threats impacting the mobile fleet. Moreover, they must ensure that disruption to employee productivity is prevented, as is access to their private data.

As such, the optimal mobile device security solution must be driven by the five principles we have discussed, namely:

- A 360° view of security across device, apps, and the network
- Full flexibility and scalability
- Full visibility into the risk level of the mobile workforce
- Privacy protection by design
- An optimal user experience

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally.
Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks.
Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

To learn more about us, visit: www.checkpoint.com

Cyber Talk