**MOBILE SECURITY**

What is Mobile Security?

Mobile security, which refers to the protection of mobile devices against cybersecurity threats, is a top-of-mind concern for today’s companies due to the growing use of mobile devices for business purposes. As remote workers access corporate data and applications using untrusted mobile devices, companies require an easy-to-use solution that protects their data without negatively impacting employee productivity

.

## Components of a Mobile Security Solution

Mobile security is complex because of the large number of potential attack vectors – devices can be targeted at multiple levels:

* **Applications:** Malware can be developed and deployed as malicious apps that users unwittingly install on their devices. Mobile security solutions should be able to detect and block downloads of these malicious apps.
* **Network:** Mobile devices and the legitimate apps that run on them can be targeted at the network level. Man-in-the-Middle, [phishing](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/), and other attacks take advantage of network connectivity to steal data or deliver malicious content. Mobile security involves blocking these network-level attacks.
* **OS:** Both iOS and Android operating systems can contain exploitable vulnerabilities, which are used for jailbreaking/rooting devices either by users or by malware. This provides an attacker with advanced permissions on the device, breaking its security model. Mobile security incorporates real-time risk assessments, configuration monitoring, and other tools to detect exploitation of device vulnerabilities.

## Top Threats to Mobile Security

Mobile devices suffer from a number of potential cyber threats. Some of the most common and impactful include:

* **Malicious Apps and Websites:** Mobile devices can have [mobile malware](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/mobile-malware/)  installed on them and access malicious online content.
* **Mobile Ransomware:** Mobile ransomware is one type of malicious app that is becoming more common and impactful as more valuable and sensitive data is stored on mobile devices.
* **Phishing:** Mobile devices have access to a number of different communications media – email, SMS, social media, etc. – making them an ideal platform for performing phishing attacks that steal data or carry malicious content.
* **Man-in-the-Middle Attacks:** Mobile communications do not always use secure technologies, making them vulnerable to interception for eavesdropping or modification of data.
* **Advanced Jailbreaking and Rooting Techniques:** Jailbreaking and rooting provide elevated permissions on a mobile device, enabling an attacker to take a greater range of malicious actions.
* **OS Exploits:** Like any other software, mobile operating systems can contain exploitable vulnerabilities that place them and their users at risk.

## Top Hurdles to Effective Mobile Security

Mobile security should be a priority for organizations; however, some common misconceptions about it – as outlined in Check Point’s [mobile security buyer’s guide](https://www.checkpoint.com/downloads/resources/mobile-security-buyers-guide.pdf) – can cause organizations to compromise the protection of their mobile devices:

* **Protection vs. Productivity?** The belief that business productivity and security are at odds is a common misconception. As a result, some organizations may choose not to implement strong mobile security in an attempt to protect business productivity.
* **Protection vs. Privacy?** Strong cybersecurity requires visibility into potential threats, but mobile devices can also carry personal data, such as photos, videos, and more. The need to balance privacy and security can make finding a mobile security solution difficult.
* **Can MDM Really Protect?** [Mobile device management (MDM)](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mdm/) solutions are a tool designed to enable remote monitoring and management of mobile devices. However, they do not offer robust cybersecurity protections. The common misconception that MDM is sufficient for security decreases mobile protection and can block deployment of strong mobile security solutions.

## Effectively Protecting Mobile Devices

[Secure mobile access](https://www.checkpoint.com/solutions/mobile-security/) is an important component of an enterprise cybersecurity strategy. As mobile devices become a more widely-used option for remote work, the data, applications, and systems that they access are at increased risk of compromise by infected devices.

At the same time, mobile security needs to prioritize the needs of the device users, including privacy and usability. Achieving this while providing effective [mobile threat defense](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-threat-defense-mtd/) requires a mobile security solution that implements these core principles of optimal mobile threat defense:

* **Covering All Attack Vectors:** Mobile devices can be attacked via multiple vectors, including at the application, network, and operating system levels. A mobile security solution should provide protection at all of these levels.
* **Full Risk Visibility into Mobile Risk:** Risk visibility is an essential component of enterprise risk management strategies. Mobile security solutions must be capable of providing security teams with an accurate accounting of the risk level of the remote workforce.
* **Enterprise-Level Scalability:** Enterprises may have thousands of devices to manage and secure. Mobile security solutions should be capable of supporting a large and diverse (including both Android and iOS devices) set of devices used for business.
* **Optimized User Experience:** Mobile devices are popular because they increase employee productivity. Mobile security solutions must be designed to have minimal impact on the user experience.
* **Privacy by Design:** Mobile devices used for work may be BYOD and dual-use devices. These devices must be secured in a way that does not compromise the privacy of the devices’ users.

Check Point Harmony Mobile is the market-leading Mobile Threat Defense solution. It keeps corporate data safe by securing employees’ mobile devices across all attack vectors: apps, network and OS. Designed to reduce admins’ overhead and increase user adoption, it perfectly fits into the existing mobile environment, deploys and scales quickly, and protects devices without impacting user experience or privacy. To learn more about Harmony Mobile’s capabilities, [request a personalized demo](https://pages.checkpoint.com/mobile-threat-defense-demo.html). You’re also welcome to try out Harmony Mobile in your own environment with a [free trial](https://pages.checkpoint.com/sandblast-mobile-trial-request.html).

### Why is mobile security important?

Securing mobile devices has become increasingly important as the number of devices and the ways those devices are used have expanded dramatically. In the enterprise, this is particularly problematic when employee-owned devices connect to the corporate network.

Increased corporate data on devices increases the draw of [cybercriminals](https://www.techtarget.com/searchsecurity/definition/cybercrime) who can target both the device and the back-end systems they tap into with mobile [malware](https://www.techtarget.com/searchsecurity/definition/malware). IT departments work to ensure that employees know what the acceptable use policies are, and administrators enforce those guidelines.

Without mobile device security measures, organizations can be vulnerable to malicious software, data leakage and other mobile threats. Security breaches can cause widespread disruptions in the business, including complicating IT operations and affecting user productivity if systems must shut down.

**THIS ARTICLE IS PART OF**

### [The ultimate guide to mobile device security in the workplace](https://www.techtarget.com/searchmobilecomputing/The-ultimate-guide-to-mobile-device-security-in-the-workplace)

* Which also includes:
* [**mobile security (wireless security)**](https://www.techtarget.com/whatis/definition/mobile-security)
* [**4 types of mobile security models and how they work**](https://www.techtarget.com/searchmobilecomputing/tip/4-types-of-mobile-security-models-and-how-they-work)
* [**7 mobile device security best practices for businesses**](https://www.techtarget.com/searchmobilecomputing/feature/7-mobile-device-security-best-practices-for-businesses)

A lack of mobile security can lead to compromised employee, business or customer data. If an employee leaves a tablet or smartphone in a taxi or at a restaurant, for example, sensitive data, such as customer information or corporate intellectual property, can be put at risk.

IT pros should keep an eye out for these mobile threats.

[Application security](https://www.techtarget.com/searchsoftwarequality/definition/application-security) is also a mobile security concern. One problem is mobile apps that request too many privileges, which allows them to access various data sources on the device. Leaked corporate contacts, calendar items and even the location of certain executives could put the company at a competitive disadvantage. Another concern is malicious software or [Trojan](https://www.techtarget.com/searchsecurity/definition/Trojan-horse)-infected applications that are designed to look like they perform normally, but secretly upload sensitive data to a remote server.

Malware attacks are a common mobile security concern. Experts say Android devices face the biggest threat, but other platforms can attract financially motivated cybercriminals if they adopt near-field communications and other mobile payment technologies.

### How does mobile security work?

As is the case with securing desktop PCs or network servers, there is no one single thing that an organization does to ensure mobile device security. Most organizations take a layered approach to security, while also adapting longstanding endpoint security best practices.

Some of these best practices pertain to the way the device itself is configured, but other best practices have more to do with the way the user uses the device.

**Device security.**From a device configuration standpoint, many organizations put policies into place requiring devices to be locked with a password or to require [biometric authentication](https://www.techtarget.com/searchsecurity/definition/biometric-authentication). Organizations also use mobile device security software that allows them to deploy matches to devices, audit the OS levels that are used on devices and remote wipe a device. For instance, an organization may want to remotely wipe a phone that an employee accidentally leaves in public.

**End-user practices.**Some end-user mobile security best practices might include avoiding public Wi-Fi or connecting to corporate resources through a virtual private network (VPN). IT staff can also educate users on mobile threats such as malicious software and seemingly legitimate apps that are designed to steal data.

### What are the benefits of mobile security?

The most obvious benefit to mobile security is preventing sensitive data from being leaked or stolen. Another important benefit, however, is that by diligently adhering to security best practices, an organization may be able to prevent ransomware attacks that target mobile devices.

At a higher level, a solid mobile device security plan can help to ensure regulatory compliance. A strategy also makes mobile devices and the software that runs on them easier to manage.

### What are the challenges of mobile security?

One of the biggest challenges to mobile device security is the sheer variety of devices that employees potentially use. There are countless makes and models of smartphones, tablets and other mobile devices. Mobile device management (MDM) software generally supports the more popular devices and the latest mobile OSes, but not all security policy settings work on all devices.

Another challenge to mobile device security is the constantly evolving threat landscape. At one time, there were relatively few mobile threats for organizations to worry about. As devices became more widely adopted, however, cybercriminals began increasingly targeting mobile platforms.

### What are the types of mobile device security?

Mobile device security often centers around the use of MDM. MDM capabilities are often available in enterprise mobility management and [unified endpoint management tools](https://www.techtarget.com/searchmobilecomputing/opinion/Mobility-management-systems-evolve-from-MDM-to-EMM-to-UEM), which evolved from the early device-only management options.

However, organizations typically use other security tools to enhance their mobile device security. This might include VPNs, antimalware software, email security tools that are designed to block phishing attacks and endpoint protection tools that monitor devices for malicious activity.

### Mobile device security vendors and products

There are several vendors that offer mobile device management and security tools. Some of the tools available include:

* Scalefusion
* Hexnode Unified Endpoint Management
* Microsoft Enterprise Mobility + Security
* VMware Workspace ONE Unified Endpoint Management
* Google Endpoint Management
* N-able Remote Monitoring and Management