LMNTRIX

BE THE HUNTER | NOT THE PREY

PROTECTING YOUR MOBILE ENVIRONMENT

UNVEILING THE POWER OF LMNTRIX MOBILE THREAT DEFENSE

Safeguarding your devices, data, and users in the mobile era

LMNTRIX USA.
333 City Blvd West,
18th Floor, Suite 1805
Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX INGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65 3159 0639

LMNTRIX HONG KONG.
14F, Manning House, 38-48
Queen's Road Central, Central,
Hong Kong
+852.580.885.33

LMNTRIX AUSTRALIA.
Level 32, 101 Miller Street,
North Sydney NSW 2060
+61.288.805.198

LMNTRIX INDIA.
VR Bengaluru, Level 5,
ITPL Main Rd,
Devasandra Industrial Estate,
Bengaluru, Karnataka 560048,
Email: sales@lmntrix.com
+91-22-49712788

WHITE PAPER **2023**

lmntrix.com

EXECUTIVE **SUMMARY**

The performance capabilities of mobile devices offer businesses benefits in improved employee responsiveness and productivity when away from their typical working environment. However, mobile devices require connectivity and integration into corporate systems to maximize benefits. Consequently, there has been a significant escalation in the volume and type of malware developed to attack mobile devices. This increase is partly due to mobile devices being seen as an insecure backdoor into corporate networks allowing attackers to bypass robust boundary security controls on other ingress paths. This weakness is particularly prevalent where employees use personal mobile devices to connect with corporate infrastructure.

Such use offers businesses cost savings from device procurement, maintenance, and support. In addition, they have benefits in employees being more likely to respond out of regular working hours. Corporate-owned-personally-enabled mobile devices can be seen as a benefit for employees while allowing greater control over device configuration.

However, the encouragement of the Bring Your Own Device culture, where employees use their personal mobile devices rather than a corporate-supplied and controlled device, fuels these security weaknesses due to more significant vulnerabilities.

The increasing levels of security risk that result from these practices have created the need for businesses to implement effective mobile security solutions within the corporate environment to accommodate vulnerabilities and weaknesses in mobile endpoint devices.

This white paper explores the issues around integrating mobile devices into corporate systems and options for protecting these systems using mobile security solutions. The aim is to help you determine your cyber security protection requirements to select the appropriate managed security solution for your mobile technology systems.

CONTENTS

OVERVIEW OF **MOBILE SECURITY**

GENERAL INTRODUCTION TO MOBILE SECURITY

This paper will explore the cyber security issues around using mobile devices in a business environment and the measures you can take to protect your IT systems against cyber attacks. These threats can originate from various sources, such as lost or stolen devices, malware introduced onto devices, or the intercept of communications between the device and the business's IT infrastructure. Attacks can result in security incidents with the potential to cause significant reputational damage and financial loss.

FIGURE 1 - Mobile Device Threats

Mobile devices are now a ubiquitous part of the workplace environment as employees carry and use personal devices throughout the working day. Even if these devices are used solely for personal use, they often connect to workplace networks to affect connectivity with the outside world, accessing the corporate infrastructure within the protective perimeters of boundary controls.

When it comes to protecting corporate information on mobile devices, this is not just restricted to the contents of emails and their attachments. Users often take photographs to capture information on whiteboards or other presentation media. This can include commercially sensitive data. In addition, answer phone messages and voice memos, local copies of documents downloaded from shared drives, document scanner applications, and other sources may all be present on the device.

MOBILE-SPECIFIC SECURITY CONSIDERATIONS

Traditional security solutions focused on protecting endpoints within corporate facilities and the networks that connect these devices. Security controls are positioned around the perimeter of the systems with the intention of protecting against attacks attempting to breach the border. However, the increasing adoption of mobile devices for business use has disrupted this model. Now devices outside the perimeter are permitted authorized access across the boundary and into the corporate network. Often, these devices are owned by the users rather than the business. The increasing use of mobile applications and the need for the remote working drive this adoption of mobile technology.

One key difference between mobile devices and traditional endpoint computers is limited computational processing power and storage memory resources. These, in turn, limit the sophistication possible in endpoint security solutions for mobile devices. Similarly, battery limitations also restrict how any security solution can operate.

While Enterprise Mobility Management (EMM) solutions are available to manage devices, these solutions do not provide the security controls needed to protect business systems. Instead, mobile security solutions offer a solution for delivering endpoint protection for mobile devices. This term covers computational equipment with network connectivity, including smartphones, tablets, and laptops that are used outside of corporate-managed facilities using network connections outside the control of the business.

It's important to note that allowing employees to use personal mobile devices means that the corporate network security solution needs to be capable of managing a diverse range of endpoints. Each connected device potentially has a unique configuration in terms of hardware, operating system, application software, and settings.

Personal mobile devices are also more likely to have an out-of-date operating system or applications where users neglect to install updates in a timely manner. Threat actors can exploit this weakness in user behavior to gain control of devices as an entry point into corporate systems for further lateral movement to more valuable targets.

MOBILE SECURITY EXPLAINED

Mobile security is the term for any technological control that protects corporate systems from threats from using mobile devices. There are three critical aspects of mobile security:

- They protect the mobile device and any data it holds from threats such as downloading malware, installing vulnerable or compromised apps, and exploiting operating system vulnerabilities.
- They protect the network connection between the mobile device and the boundary of the corporate systems from threats such as man-in-the-middle attacks.
- They protect the corporate systems from unauthorized access by mobile devices using identity and access management solutions to protect against threats such as impersonation or cloning of mobile devices.

Any mobile security solution should have the capability to detect threats, analyze attacks and remediate the damage. A key element of mobile security is the capability to protect personal and corporate information stored on lost or stolen mobile devices through remote deletion mechanisms.

THE BUSINESS CASE FOR MOBILE SECURITY

Mobile devices have become critical tools for businesses to enable employees to work remotely from home, on the move, or within third-party premises. They encourage employees to be available when needed by blurring the line between work and leisure while offering greater flexibility in where and when work activities are undertaken. As a result, the adoption of mobile device integration into corporate systems is growing significantly due to business continuity benefits. However, mobile devices bring with them security risks.

2022

466% increase in attacks that exploited zero-day vulnerabilities against mobile endpoints.
97% of Businesses faced Malware Threats.
80% Increase in Android Banking Malware Threats.
50 times more Android than iOS Malware.
47% of Free Android Anti-Virus Apps are Ineffective.
Credential Stealing Malware is available for Criminals to Rent.

FIGURE 2 - Mobile Business Threats

Where personal mobile devices are permitted to store corporate information, personal and corporate data segregation can be compromised through weak controls or poor user practices. This weakness can compromise the confidentiality and integrity of corporate and personal data. From the business's perspective, Automatic or manual synchronization of data held on a personal mobile device with either cloud backup solutions or other personal devices significantly increases the opportunity for threat actors to discover and compromise corporate information. This issue is a particular concern for data subject to regulatory control, such as financial or personal information.

A breach of information security that compromises corporate data held on a mobile device or allows an attacker to use the device's connectivity to gain access to a business network can have serious consequences, including reputational damage, financial loss, or regulatory penalties. Any business that includes the use of mobile devices for business purposes must protect against the unique security threats that such devices enable. New mobile device-specific threats include SMiShing, a phishing scam that uses SMS messages to deliver phishing content, including malware-laden attachments or links to malware.

A successful attack on a mobile device may alone be sufficient to compromise business operations or cause damage to the viability of the business. A successful attack on corporate systems using a mobile device as the access point for the attack has the potential to halt business operations or irreparably damage the business leading to loss of trading and job losses.

The business case for a mobile security solution starts with protecting the business from unacceptable harm. However, many factors must be considered when searching for the correct answer.

- Mobile security must seamlessly integrate with existing corporate security controls, critically not introducing new weaknesses and vulnerabilities into the business systems. The overhead of managing mobile security should not adversely impact corporate security management as a whole.
- Mobile security must protect devices and connected networks from attacks, including malware, vulnerability exploitation, and social engineering. In addition, the solution must be flexible and adaptable, able to detect and respond to complex evolving threats and novel attack vectors.
- Mobile security must ensure that regulatory and legislative compliance is not adversely affected by the business use of mobile devices.

- Mobile security must protect corporate systems against data leakage or compromise data confidentiality, integrity, and availability.
- Mobile security must support incident analysis, response, and forensic investigation processes to contain and counter-attacks.
- Mobile security must align with corporate policies and business processes, including device management.
- Mobile security must not hinder the productivity benefits that mobile devices bring to the company by enabling secure remote connections to corporate networks.
- Mobile security must support all permitted mobile device makes and models equally.

Mobile security solutions deliver improved security posture to the organization's systems through risk management. The key driver for implementing mobile security is the rapid increase in risk levels. Threats are not just becoming more widespread, but the impact of successful attacks is growing. For example, malware is now increasingly used to exfiltrate sensitive information from mobile devices that can be used to leverage different attack vectors, including infiltration of corporate networks and targeted phishing. In addition, the risk of corporate data leaks is growing as more mobile devices access corporate systems and handle both personal and business information.

Mobile security solutions need to enforce the trust relationship between users and corporate systems, a user base that embraces security controls will create more robust system security. The key to achieving this is the premise that the mobile security solution will protect the users and their personal information as well as protect business systems and corporate data. Creating mutually beneficial security will promote adoption and prevent users from bypassing overly restrictive limitations. It also incentivizes everyone to protect mobile devices. This security then needs to be balanced with device usability to ensure that security controls do not compromise the productivity gains that come from mobile device users.

Choosing the right mobile device security solution starts with finding vendors with a track record of providing such solutions to similarly sized businesses in the same industry vertical. Critical criteria to focus on are the vendors' success in integrating their solution into their client's business systems, the available operational support, and the ability to support compliance and governance issues.

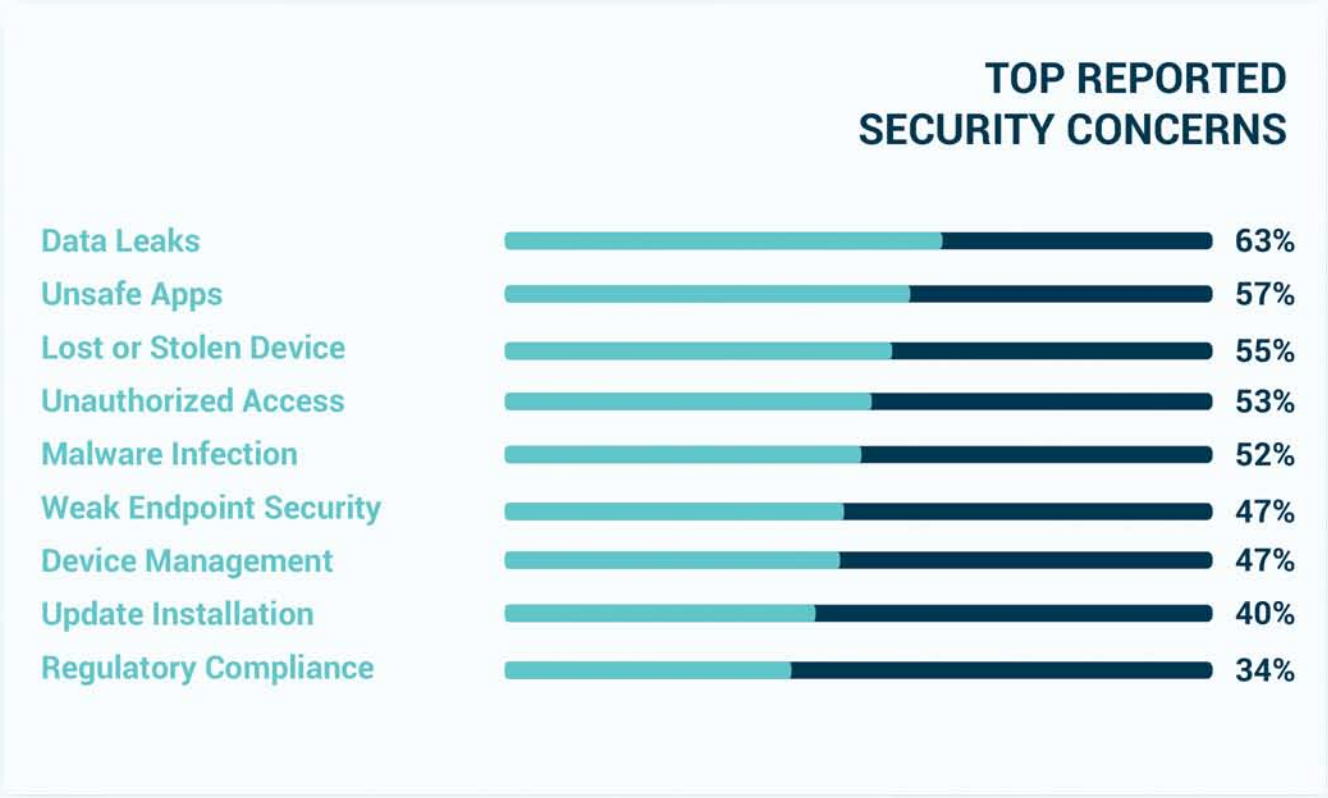


FIGURE 3 - Main Mobile Device Security Concerns

MOBILE SECURITY **OVERVIEW**

MOBILE SECURITY THREATS

OVERVIEW

The threat landscape for mobile devices is expanding and evolving rapidly as the value of compromising these devices grows. Mobile apps now manage sensitive operations such as financial transaction management and authentication processes in addition to handling communications. The ability to compromise a mobile device offers attackers a range of exploitation options, from simple theft of sensitive information to hijacking the device to launch broader attacks.

2022

30% of zero-day vulnerabilities uncovered in 2022 targeted mobile devices.
75% of the phishing sites analyzed specifically targeted mobile devices.
42% of New Mobile Malware is Adware.
40% of mobile devices contain hardware vulnerabilities.

FIGURE 4 - Mobile Malware Statistics

Advanced persistent threats are also exploiting mobile device weaknesses for sophisticated attacks. For example, the Pegasus spyware deployed by the NSO Group has been found on the mobile devices of government officials, journalists, and human rights activists across the globe. The success of this software has now seen some other equally sophisticated spyware products being deployed, whose reach and functionality are still subject to research.

Mobile devices offer security controls such as device-level encryption for data at rest, providing a layer of protection. However, this configuration of protective measures is outside the control of the administrators of corporate systems and may not be robust enough to reduce risks to an acceptable level.

APPLICATION THREATS

App-based threats can result in malware being installed on the device. The apps themselves may introduce malware due to inherent security weaknesses or an attacker compromising the app. Malware can also be introduced through adverts provided through an app where the source advert is compromised to introduce malware. Malware can also be introduced when browsing a compromised or malicious website directly by the website or using sideloading techniques.

Messaging apps such as SMS or email can also be exploited by sending malware-laden messages that are not detected and quarantined.

Apps may intentionally or inadvertently collate data that may subsequently leak out of the device due to poor security practices. This issue may allow unauthorized third parties, such as app developers, access to sensitive personal or corporate information. In addition, compromised or malicious apps may also intentionally access or collect corporate data and leak this information out of the device through messaging or network connectivity to an attacker in control of the app.

DEVICE THREATS

Device-based threats come from vulnerabilities in the operating systems of mobile devices such as Android and iOS. Persistent threat actors have the capability to research and uncover flaws that may grant access to devices by exploiting such weaknesses. Furthermore, these weaknesses are made more accessible if users fail to keep their services updated to include the latest security patches allowing attackers to use the known and documented vulnerabilities that the patches resolve. A mobile operating system vulnerability that gives an attacker root or kernel-level privilege escalation will allow the attacker to take complete control of that device able to bypass device and app-level security controls. This opportunity is made easier for attackers by the number of out-of-date operating systems with known vulnerabilities still in use.

Statistics show the scale of the problem. The Android operating system is used on around 43% of mobile devices. Of the rest, Windows is used by around 29%, iOS by about 18%, macOS by approximately 6%, and Linux by about 1%. When looking at smartphones, there are currently around 4.2 billion Android and iOS users worldwide. Android is used by approximately 71% and iOS by nearly 28%. Looking at which versions of each operating system are used highlights the sheer scale of the issue of out-of-date and vulnerable systems.

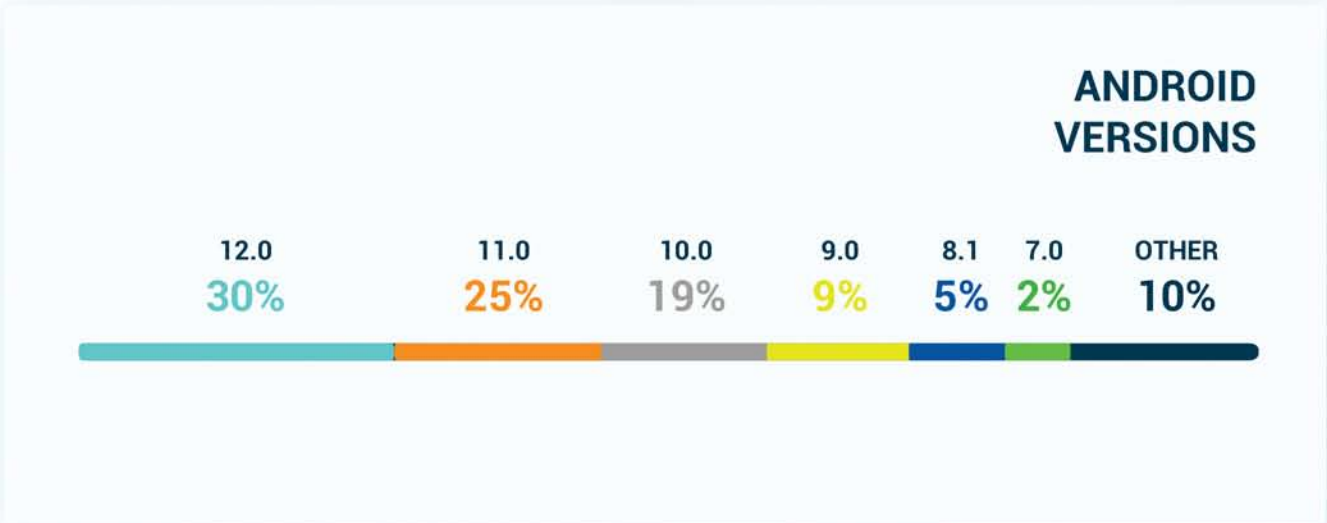


FIGURE 5 - Android Versions in Use

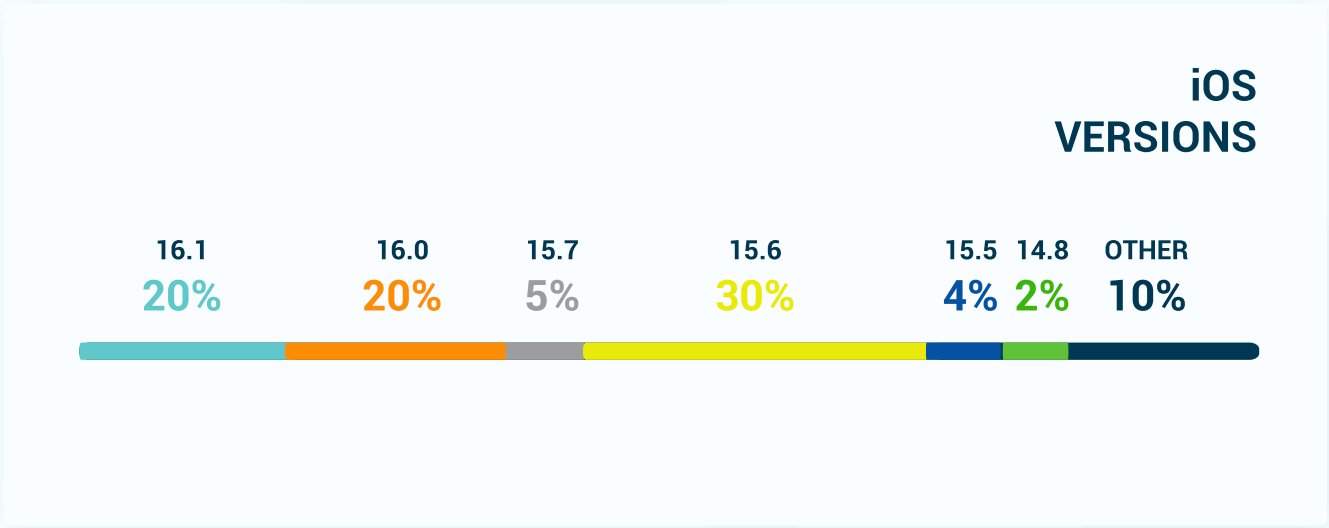


FIGURE 6 - iOS Versions in Use

Mobile devices are easily lost, left behind on a table, or fall out of a pocket. Their small size and light weight mean that the owner may not be aware of the loss for some time. Mobile devices are also particularly susceptible to theft, either while being carried or left in a vehicle or at home. Weak access controls on the device may allow its holder to readily and quickly gain access and exploit connectivity before the device is reported stolen and disabled. Attackers may specifically target employees of an organization as part of a targeted attack on that business's systems where the potential rewards exceed the risk. Theft of mobile devices is seen as a relatively low-risk venture with a low likelihood of law enforcement investigation.

Malware on home computers or unpatched vulnerabilities can also provide an attack vector to compromise any personal mobile devices that are directly connected to or synchronized with the infected computer.

NETWORK THREATS

Network-based threats come from attackers re-directing network traffic flow by exploiting vulnerabilities or installing malware to alter network configuration settings. These techniques allow attackers to direct traffic to a malicious endpoint, implement a man-in-the-middle attack to steal corporate data, or provide an access point to launch an attack on the corporate systems. Such threats can not only intercept network traffic but also compromise the robustness of any encryption, such as SSL, to make it easier to decode traffic to compromise the confidentiality or integrity of messages.

Compromising the trusted root certificate authority stored within the device allows attackers to add their malicious certificate authority for secure connections. Additionally, links that appear as HTTPS configured traffic can transmit data using weak or no encryption, compromising security.

FIGURE 7 - Mobile Malware Statistics

For example, the 'NotCompatible' malware targets Android mobile devices by mimicking a system update to lure users into installing the executable, typically distributed through compromised web adverts. The malware creates a web proxy on the infected device to gain access to network traffic, managed by a command-and-control server at the address notcompatibleapp.eu, hence the name.

The Malapp.d malware also targets Android mobile devices but with a more comprehensive set of attack options. These include capturing keyboard inputs to steal authentication information such as passwords, the ability to terminate processes such as security applications, and deleting data or launching Denial of Service (DoS) attacks. It can also manage remote access connections, allowing attackers to exfiltrate corporate data or launch further attacks.

ROOTING AND JAILBREAKING

The security of mobile devices is significantly affected where personal devices are rooted or jailbroken. Rooting is a process where Android mobile devices are modified to allow the user privileged access to all operating functions, also known as root access. While this process gives users control over their devices, it also disables the in-built security functions of the Android operating system.

Similarly, jailbreaking is the term for modifying the iOS operating system to remove all security restrictions, making the device's features easier to access. For example, users typically jailbreak devices to allow the installation of apps that Apple has not approved for inclusion in the App store. Both these techniques create vulnerabilities that attackers can exploit far more straightforwardly than if the device is not rooted or jailbroken.

MOBILE RISK ASSESSMENT

OVERVIEW

Risk assessment techniques identify unacceptable levels of risk, single points of failure, and opportunities for continual improvement. Risk assessment information and methods help businesses to evaluate the risk of disruption or compromise.

Business risk assessment and mitigation measures typically focus on the organization's prioritized activities and supporting resources. While this approach maximizes the benefit of any investment in risk treatments to reduce the frequency or impact of disruptions, it may omit to consider enabling technologies such as mobile devices that.

Mobile risk assessment typically involves methods to identify, analyze and evaluate various risks relevant to the organization's use of mobile devices in its business processes. Risks are considered using measures of the likelihood of the risk materializing and its impact on the business. Mobile risk assessment methods can be effective when analyzing known and anticipated risks. However, there are limitations to risk assessment techniques for complex and emerging risks as threats.

Risk assessment methods typically consider time frames relevant to the organizational planning process and business objectives. An important consideration is that mobile devices, in particular, have limited operational timespans before they become obsolete compared with traditional IT equipment.

RISK IDENTIFICATION

Risk identification starts with listing the known and anticipated internal and external risks for each of the activities for which mobile devices are used. Sources of useful information include previously reported incidents within the relevant industry sector or geographical location, along with publicly available information or reports relating to threats and past disruptions.

Threat intelligence can provide indications of the prevalence of particular threats for an organization, with threat levels typically affected by the nature of the business, its ownership, and its areas of operations. For example, certain companies in certain countries will face more significant threats due to geopolitical factors.

RISK ANALYSIS

Risk analysis is determining the likelihood of each risk occurring and the most credible worst-case impact to provide a rating of the risk level. Typically impacts can be categorized by looking at effects on financial, legal, and reputational implications. This granularity will aid the prioritization process, mainly where regulatory compliance is critical.

The information from the risk assessment process will allow the identification of opportunities to mitigate each risk identified by seeking to reduce the likelihood of the risk materializing or lowering the impact of the risk on the organization.

Risks at a level within the risk appetite of the business may be accepted with no further work required. Typically, these are risks that are unlikely to occur within the operational life of the business process or whose consequences are so minor they will not adversely affect the business.

Credible risks at a level beyond the risk appetite of the business will require action to eliminate the risk or reduce its assessed level down to an acceptable level. For example, risks can be reduced by introducing technological controls such as a firewall or monitoring software. Alternatively, procedures can be introduced to prevent mobile devices from being used in a manner that the risk can exploit. Calculating risk levels allows the business to prioritize risk reduction and concentrate on the most significant risks first to gain a rapid improvement in the company's security posture.

An important consideration when implementing security controls on mobile devices is that if the rules noticeably restrict or impede the use of the device, users will either not use it or try to find ways to work around or bypass the security controls entirely.

MOBILE SPECIFIC RISKS

One critical mobile-specific risk is storing sensitive corporate data in locations other personal apps can access, such as contact information or email attachments. The risk to corporate information is directly affected by the weaknesses and vulnerabilities of non-corporate applications.

Mobile devices also record and store position-tracking information from sources such as mobile phone mast triangulation and GPS sensors. This information can provide attackers with valuable information for further attacks, such as locations where employees congregate where eavesdropping may be undertaken or the physical location of a sensitive site such as a data center.

Other typical risks associated with the use of mobile devices include:

- A user-initiated data leak is caused by copying corporate data into a personal app
- The compromise of corporate data confidentiality through sharing a personal mobile device with a third party, such as friends and family.
- Unintentional data loss through accidental deletion of information stored on a mobile device.
- Unintentional data loss through the uninstalling of an app on a mobile device..
- The use of a refurbished or second-hand mobile device of unknown configuration status or which has a malware infection.
- A mobile device owned by a user who has left a business through resignation, redundancy, or other termination of employment that retains corporate information, including data, network configuration settings, or apps.
- The use of mobile devices with unpatched or unsupported operating systems and apps with known vulnerabilities.

- The occurrence of unreported security incidents involving the compromise of a personal mobile device that the user is unaware of or unwilling to report due to fear of consequential actions.
- An inability to detect malware infection on a personal mobile device can lead to the compromise of corporate authentication credentials using keylogging of screen scrapping technology.
- Unreported compromise of corporate information when a damaged personal mobile device is given to a non-reputable repair service provider.
- Simultaneous connectivity with both a corporate network and an insecure public network results in data leaking across connections.

A complete set of candidate risks for consideration can be obtained from publicly available sources to ensure the list of considered risks is complete. A list of the typical mobile security risks identified by the OWASP® Foundation, including explanations, is provided at the end of this paper for reference.

MOBILE DEVICE MANAGEMENT

Enterprise Mobility Management (EMM) solutions are commonly used in the corporate environment for managing devices. They allow businesses to track mobile devices, implement authentication and access management, oversee their configuration, and protect data held on the device. EMM was developed to control which devices were permitted to connect to a business network.

They manage how the connection is made and what permissions the device has once connected. However, it is vital to note that EMM solutions alone do not offer complete mobile security. They help protect information stored on devices against loss or theft. However, they do not provide comprehensive threat detection and response capabilities and offer limited protection against knowledgeable or advanced persistent threats.

Lost and stolen device management services should include blocking future access to corporate systems and remotely wiping data from the device, even following a change to the SIM card in an attempt to hide the device.

The core capabilities of conventional EMM solutions include the following:

- Mobile Device Management (MDM) services for device life cycle management. This service supports the configuration, provisioning, and management of content. It also enables remote viewing and data wiping.
- Mobile Application Management (MAM) services apply policies and control functionality of individual applications, which are delivered via an app store. It also provides usage analytics for resource monitoring.
- Mobile Identity (MI) services provide access control for trusted devices and users.
- Mobile Content Management (MCM) services define and enforce access rules for content download, upload, and distribution on mobile devices.

Note that an Over the Air (OTA) provisioning capability will be particularly important for remote device management where users infrequently or never are present within a corporate-managed facility.

MOBILE SECURITY POLICY

A foundation of effective mobile security in any organization is publishing a mobile security policy. The mobile security policy lays down the rules that protect an organization and all the individuals within the scope of using mobile devices that connect with the business's information systems. These rules should be designed not only to protect the users of the systems but also to ensure that all the users behave the way the business and other users expect them to. These rules must be fair and non-discriminatory. Any restrictions must not be perceived to be unjust or fall into disrepute if they are to be effective. They must not benefit a minority but equally must not benefit the majority at the expense of a minority.

The mobile security policy must embody several important interrelated ideas. First, there should be clear limits to the scope, restrictions, and consequences set down in the policy. Second, an organization should exercise its authority through the published policy enforced in accordance with set procedures. No one within the organization should be exempt from the policies, and the policies should protect the rights of all the individuals within the organization. Third, the published policies must be endorsed at the organization's highest level and subject to formal authorization and publication processes. Finally, all personnel subject to the policies should not only have access to their content but should explicitly acknowledge that they have read, understood, and have explicitly agreed to abide by the responsibilities placed upon them by the policies.

The rise in the use of personal mobile devices in the workplace environment also needs to be reflected in associated acceptable use policies. Mobile devices are often used for social networking, which creates new threats to businesses. This popularity in social networking means increasing numbers of people regularly publish information for the world to access.

However, even if the post is made from a personal device, if it is connected via a business network, the organizations providing the infrastructure have a legal responsibility for any content they publish. This liability applies to postings to a blog, a social networking site, a forum, or any other medium. Therefore, the policies should not only remind users of their responsibilities but also seek to indemnify the organization providing the information system against any liability arising from any breach of legislation. This will include confidentiality, copyright, or other intellectual property rights as a result of material published by the user and against all damages, losses, claims, and costs arising from any such publication.

Users must be explicitly instructed not to make defamatory or obscene statements, seek to incite racial hatred, or otherwise break applicable laws. Organizations have wide-ranging discretion to monitor the users' activities of their information systems. Without the appropriate policies and procedures, this monitoring may be, at best ineffective and, at worst illegal. Monitoring, however, is only effective if it is done comprehensively and systematically with processes in place to ensure appropriate and secure monitoring is coupled with enforcement, disciplinary, and remediation procedures. The complete list of potential breaches of legislation that a user may knowingly or unwittingly undertake is extensive, and each should be addressed. Examples include using the information system to send offensive or harassing material or in any way that breaches applicable legislation or regulation to perpetrate or promote any unlawful activity such as fraud, software, film or music piracy, or any other breach of copyright.

Mobile security policies help protect both the organization and the individuals within the organization but only if they are comprehensive, consistent, correct, proportionate, reasonable, enforceable, and appropriate.

SECURE APP DEVELOPMENT

OVERVIEW

Statistics show there are over 6 billion active smartphone subscriptions worldwide, forecast to surpass 7 billion by 2024. In addition, each smartphone will, on average, have more than 80 apps installed, of which around 30 will be used in a typical monthly period. These numbers demonstrate the scale of the attack surface that hackers have when looking to compromise a mobile device through app weaknesses. Consequently, mobile app security has become a critical factor in protecting mobile devices.

Research shows that most available apps include an exploitable security flaw, and business apps are more likely to leak data than an average mobile app. Consequently, there is now a perceptible shift in mobile application development towards better security and safeguarding of data.

Mobile application security must be an integrated part of the development process to be effective. Security controls added after development is complete as a protective wrapper against implementation weaknesses will never be as effective as eliminating those weaknesses during the development lifecycle.

IMPORTANCE OF MOBILE APP SECURITY

Business productivity and financial management apps are prime examples of the critical nature of mobile app security. Attacking a mobile device through an app weakness will allow the attacker access to information the user holds on their device. Additionally, the ability of an attacker to compromise a business app offers the potential to launch an attack on the business systems that host the server-side app software, providing the capability to access the data for all users and act as an entry point into the business's infrastructure.

Business apps developed in-house are statistically more likely to include high-risk security weaknesses as they are typically only intended for use by employees with the assumption that no one outside of the business will have access to the app. As a result, such apps are an attractive target for attackers looking to access corporate systems or cause reputational damage.

Attackers can access such apps through the loss of stolen mobile devices. However, more sophisticated attackers undertaking a targeted attack on a business may access the app itself relatively quickly. Tools that make the task of reverse engineering an app executable into understandable code straightforward are available. In addition, knowledgeable attackers can identify exploitable weaknesses in the code.

APP DEVELOPMENT THREATS

The more common mobile security threats created by app development processes include the following:

- Weak user authentication processes allow an attacker to impersonate a legitimate user and gain access with their permission.
- Poor role-based access controls allow a user with regular access permissions to gain access to administrator functions with privileged access permissions.

- Failure to check parameter validity and filter invalid data creates injection flaws where an attacker can pass malicious commands within message data. Typical attacks include Structured Query Language (SQL) injection on a database server or Lightweight Directory Access Protocol (LDAP) command injection on a directory server.
- Poor data security through the use of plain text messaging and storage or implementation of weak encryption algorithms with known vulnerabilities.
- Poor encryption management where passwords and encryption keys are accessible in plain text or stored using weak salting and hashing algorithms.
- Use of open-source and third-party components and libraries with known security vulnerabilities.

MOBILE SECURITY SOLUTIONS

Enterprise mobile security solutions are available with wide-ranging capabilities to support businesses of all shapes and sizes. The ideal solution should be capable of supporting a sizeable remote workforce using diverse types of mobile devices with minimum overhead for the business IT support team.

The principal goal of the solution is to protect business systems, including corporate apps and sensitive information accessed by mobile devices. Additionally, the security solution should protect mobile devices from threats.

Any solution should be straightforward to deploy, integrate with existing security solutions, and be simple to operate. In addition, it is critical that the solution does not impede business processes or deter the use of mobile devices through restrictive controls. Cloud-based unified endpoint management (UEM) solutions offer an excellent alternative to traditional EMM solutions as part of a mobile security solution.

The critical elements of a mobile security solution are:

- Proactive threat detection and response with continuous monitoring and alerting combined with automated remediation of business networks, apps, and devices.
- Threat hunting capability using remote device intelligent search functionality.

- Customizable watch lists that enable threat tracking and alerting.
- A centralized inspection, audit, and compliance management for remote devices with alerting and reporting functions and inventory management facilities.
- Identity and access management (IAM) for mobile devices to secure connectivity and manage device, data, and app access, including management of single sign-on (SSO) and multi-factor authentication strategies and enforcement of authentication complexity rules.
- Encryption management, including policy enforcement and critical management functions.
- Central unified mobile device management through policy deployment and enforcement, including onboarding of new devices, decommissioning of devices, removal and wiping of lost and stolen devices, along with the configuration of connections, devices, and apps, and enforcement of usage restrictions.
- Vulnerability reporting functions using threat intelligence referenced against device firmware and software configuration information.
- Provision of an enterprise application catalog for the secure distribution and management of corporate apps and approved third-party apps.
- Granular access controls using role-based permissions and group policies.

EFFECTIVE **MOBILE SECURITY**

OVERVIEW

Effective mobile security should go beyond detection and response to incidents and assure the business that it can operate mobile devices without the risk of business disruption or data breaches.

It's critical to remember that the threats to mobile devices are significantly different than other endpoint equipment due to the combination of functionality built into a standard mobile device and the manner in which it is operated. Therefore, security policies and processes for mobile devices need to reflect these differences for mobile security solutions to be effective.

The following statistics from the last ten years show the scale of the problem regarding users keeping their mobile devices secure.

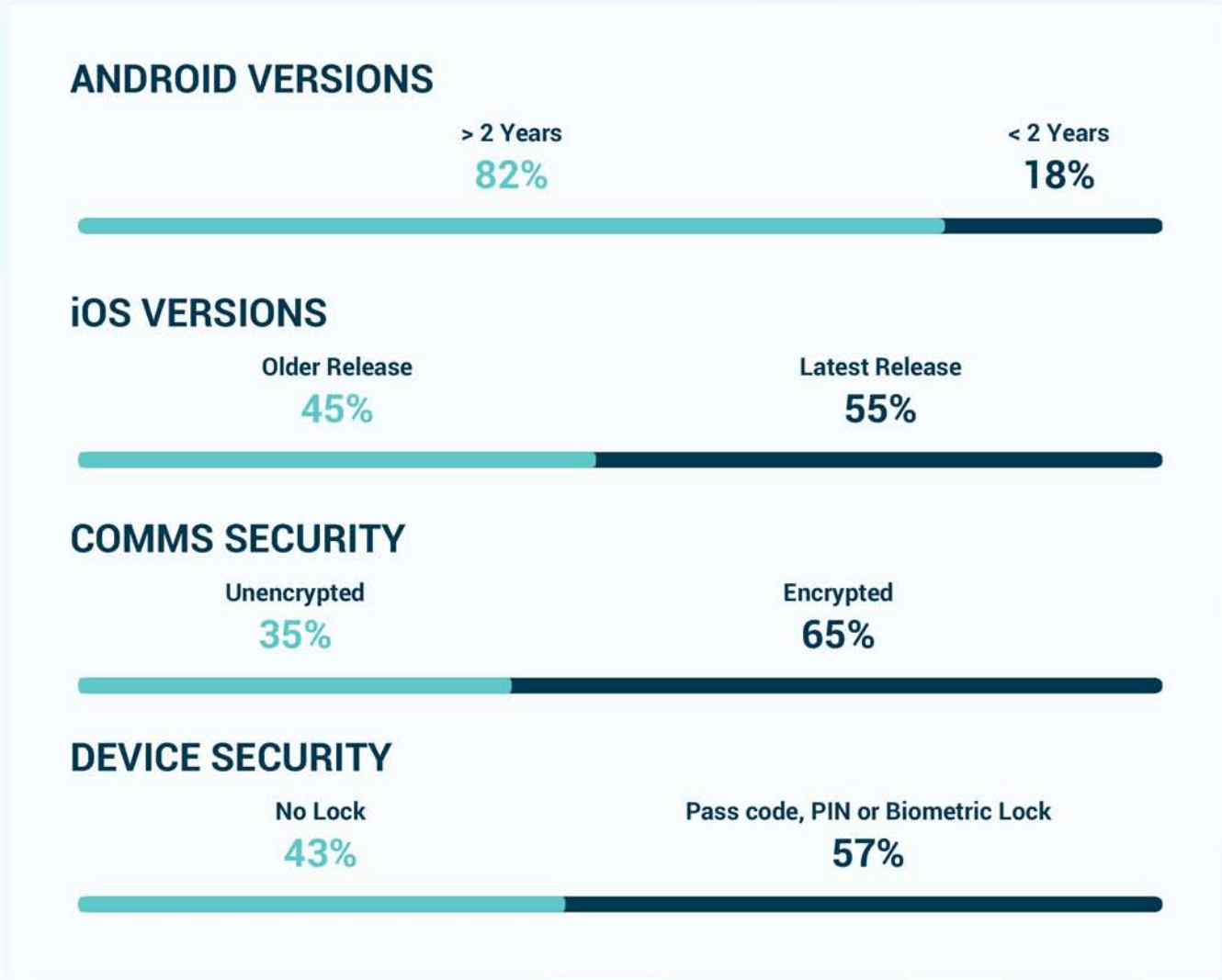


FIGURE 8 - Mobile Security in Pictures

LMNTRIX
BE THE HUNTER | NOT THE PREY

MOBILE SECURITY SOLUTIONS

Mobile devices offer businesses productivity benefits beyond remote working. For example, in a customer-facing environment, employees issued with mobile devices can serve customers quicker by collecting payment and delivery information from anywhere within the retail space rather than returning to the location of a fixed point of sale equipment. However, this model will only be effective if those customers have an assurance that their personal information will be kept secure.

From the business's point of view, there is an additional security overhead to secure the flow of sensitive information from potentially many mobile sales devices in place of a few fixed devices. The implementation of mobile technology will play a critical part in device security. The business use case may require the development of bespoke native mobile apps or web-based apps. Alternatively, off-the-shelf apps may be available. Each use case places unique security demands on the business.

These demands are most acutely realized when businesses allow the integration of user-owned devices into the corporate network under a Bring Your Own Device (BYOD) model. Managing diverse ranges of different consumer-grade technology can be challenging for businesses used to managing enterprise equipment. In addition, such devices have inherently lower security standards, requiring more effort to bring up to an enterprise standard.

Mobile security solutions must address such security challenges while recognizing that the adoption of mobile technology will inevitably increase while the diversity of devices will also grow. Therefore, the goal of any effective mobile security solution should be to protect corporate systems and data security without disrupting normal business operations.

KEY FEATURES

The key features of a mobile security solution are the ability to detect and respond to mobile specific threats that encompass:

- Use of vulnerable or misconfigured apps.
- Installation of sideloaded apps.
- Installation of compromised apps.
- Installation of mobile malware.
- Compromise of the operating system vulnerabilities.
- Exposure to network-based attack.

Additionally, the mobile security solution must integrate with existing EMM solutions without compromising overall security. EMM device provisioning will need to ensure that the endpoint agent of the mobile security solution is installed and operating before the device is permitted to join the corporate system.

The mobile security solution's threat detection and response processes need to integrate with the EMM's processes for blocking access, quarantining, or remote data wiping in line with the required response for any particular threat.

Also, threat intelligence information from the mobile security solution needs to be incorporated into the EMM processes where necessary to allow business processes for managing mobile devices to adapt to emerging or evolving threats.

VULNERABLE AND MISCONFIGURED APPS

The most common threat for mobile apps is the presence of security weaknesses and vulnerabilities in legitimate apps, particularly apps used for business processes. Apps are regularly updated to patch known vulnerabilities and correct implementation errors. Once an update is made available, sophisticated attackers will analyze the updates to determine if it identifies any weaknesses that can be exploited in the unpatched code. Attackers can then use this information to seek out and attack any mobile devices using an unpatched app version.

Additionally, advanced persistent threats have the resources available to analyze the code of popular business apps to find exploitable weaknesses unknown to the developer. Identifying zeroday vulnerabilities allows threat actors to launch attacks that may evade existing detection controls.

Solutions for detecting exploitable App vulnerabilities should monitor mobile devices for abnormal behavior that indicates that the app has been compromised. Advanced behavioral monitoring has the potential to identify the threat early in its attack cycle, implement a system-wide response for all mobile devices and provide valuable threat intelligence to the broader community.

SIDELOADED APPS

One of the critical methods of ensuring the legitimacy of mobile apps is using official app stores for centralized distribution of the app executable. Sideloading is the action of loading an app executable from a non-approved source. This operation may occur for many reasons. For example, the user may wish to install a popular app not available in their geographic region for licensing issues, or the acceptable usage restrictions of an EMM may block the app. Sideloading also allows streaming media to be permanently stored for offline use and can help avoid downloading via mobile networks in the event of bandwidth limitations.

The issue with sideloading is the higher risk that the app contains malware or has otherwise been compromised. This loading method is also a common technique employed in phishing attacks to introduce malware onto a device by appearing to offer access to a legitimate app. Advanced attacks may also use this technique to introduce an app onto a target's mobile device that does not contain malware but which, at a future date, may introduce malware through an update for the app. This approach allows the compromised app to avoid detection using signature scanning and behavioral analysis techniques until the malicious payload is deployed later.

Sideloaded app detection solutions should monitor mobile devices for apps that either appear on a deny list or do not appear on an allow list, depending on the corporate policy. App management can either impose restrictions on user actions to prevent sideloading or rely on reporting mechanisms to advise the removal of unauthorized apps.

COMPROMISED APPS

Sophisticated attackers may seek to develop apps that appear legitimate but include the inbuilt capability to act as an attack facilitator. Advanced persistent threats have the resources to build apps and complete the steps necessary for their inclusion in official app stores. In addition, the development and distribution of apps are now relatively low-cost and straightforward, making such attacks credible. The main effort involved is the social engineering campaign necessary to persuade target users to install the app.

Compromises app detection solutions should monitor mobile devices for apps that either appear on a deny list or do not appear on an allow list, depending on the corporate policy. However, the former deny list approach will only be effective once threat intelligence information identifies the app has been compromised. On the other hand, malware detection using signature and behavioral monitoring has the potential to detect the threat early in its attack cycle and implement a systemwide response for all mobile devices.

MOBILE MALWARE

Malware detection solutions should use signature and behavioral-based detection to offer the best levels of protection using a reinforcing approach that compensates for the weaknesses in each method.

Signature scanning can detect known and static malware code quickly and effectively. However, it cannot uncover novel (zero-day) or dynamic code until its signature is added to the malware library by the scanning solution provider after this new malware is detected and analyzed.

Behavioral analysis overcomes the limitations of signature scanning by attempting to recognize the presence of malware through its effects on the device. This approach can detect threats for which there is no known signature before they exhibit malicious behavior.

To be effective, it requires distinguishing between normal user behavior and abnormal malware behavior. This challenge necessitates access to as much information as possible to minimize the potential for false alarms while maximizing the potential for threat detection. Additionally, behavioral analysis needs to be undertaken at a corporate system level that includes all connected mobile devices rather than focused on each separate device.

This information collation and analysis must be performed in real-time to deliver timely detection that allows threat response before the threat has caused irreparable damage or moved deeper into the corporate systems. Again, machine learning techniques and big data handling make this approach more efficient.

OPERATING SYSTEM VULNERABILITIES

Ultimately an attacker will seek to root or jailbreak the operating system to gain complete control over the mobile device. Achieving this allows the attacker to bypass all security controls and access any information of value held on the device. Auto-rooting malware that presents an attacker with access to a fully compromised device following malware infection is increasing in prevalence.

Protecting against rooting or jailbreaking uses digital fingerprinting techniques to compare a device's operating state against a previously known secure state to detect differences due to the effects of the malware. This fingerprint will encompass the operating system software, configuration settings, and other relevant firmware and software information to provide a complete picture of the device's health.

NETWORK-BASED ATTACKS

Information in transit between mobile devices and their interface with the boundary of corporate systems offers an attractive target to attackers able to intercept or eavesdrop on communications.

The widespread use of Wi-Fi connectivity.

Setting up a compromised mobile phone mast or Wi-Fi network in an area frequented by mobile device users is a relatively straightforward proposition for a sophisticated threat actor. Any device connecting to the attacker-controlled network can then be targeted for compromise through various attack vectors.

- The attacker can bypass any missing or inadequate access controls to gain access to resources or information using the credentials of the mobile device.
- An attacker can bypass any missing or inadequate authentication controls to assume the identity of a legitimate user and gain access to system resources using their assigned privileges.

- An attacker may be able to introduce malicious code into the corporate system by inserting it into the network messages where any application programming interface (API) is present. This attack will be successful if the API cannot detect malicious code and where the parsing or processing of the compromised message may execute the code.
- An attacker may use the compromised network traffic to launch a distributed denial of service (DDoS) on the corporate system, halting operations by consuming processing resources or filling available memory.
- An attacker may be able to launch a Man-In-The-Middle (MITM) attack by eavesdropping on network messages or intercepting and altering messages to either steal information within the messages or perform some action of benefit to the attacker.
- An attacker may launch a replay attack by recording a valid message and resending it, either unaltered or with modified content, to generate a response or perform an action.

The encryption of network traffic offers confidentiality protection against eavesdropping, interception, and modification of network messages. However, encrypted messages also allow attackers to hide their actions on a network by using the same encryption techniques to defeat simple network message monitoring methods used in security solutions. However, advanced mobile security solutions can use behavioral analysis of metadata from message packets combined with machine learning processes to detect hidden and unknown traffic attributable to an attack in realtime irrespective of if the traffic is encrypted.

Protecting against the compromise of network connectivity involves interrogation and analysis of connection configuration, including security certificates and Transport Layer Security (TLS) settings. Comparison against standard configuration data allows the identification of compromised network connections before the connection is established. Connectivity can then be denied at the corporate system boundary.

ELEMENTS OF A MOBILE SYSTEM

Critical elements of an effective mobile security solution are:

USER SECURITY AWARENESS

All users of mobile devices should receive security awareness education through informal briefings, teaching sessions, or formal training packages. The goal should be to ensure all users know the security threats and understand their responsibilities in minimizing risks.

SECURITY PATCHING

All devices should be kept up to date with the latest security patches installed within a defined period from their availability to minimize the window of opportunity for attackers to exploit known vulnerabilities. Ideally, update installation should be automatic to ensure ongoing compliance.

USER CREDENTIALS

All devices and applications should be protected from unauthorized access using robust user credentials such as complex passwords, biometrics, and multi-factor authentication controls. Additionally, password complexity should be automatically enforced to ensure user compliance.

DATA PROTECTION

Personal and corporate information should be segregated using containerization technology where possible and protected using robust encryption processes for both data at rest and in transit to minimize the risk of data leakage.

Virtualization techniques can separate personal and corporate applications and data where the mobile device can support such technology. Issues come when a device operating in one mode receives an interruptive event from the other, such as receiving a work phone call when using the personal virtual environment.

This segregated approach to mobile security uses virtual containers on the device to segment personal apps from corporate data and apps protected with authentication for access management and protective encryption technology. Hence, creating virtual containers allows users to have separate personal and work environments on their mobile devices.

DEVICE MANAGEMENT

MDM solutions are available to manage corporate control of mobile devices. In the case of a personal mobile device, the owner must agree and permit the onboarding of their device into the MDM solution. MDM tools monitor mobile device usage to support security detection and response processes using behavioral monitoring. They should also provide the capability to prevent lost or stolen mobile devices from connecting to corporate systems and enable remote data wiping and disabling to minimize the risk of exploitation of the device or any information on the device.

MDM solutions allow corporate administrators to define and impose security rules and policies that limit what the user can do with the device. For example, include restrictions on installing, launching, and uninstalling applications and changing configuration settings. In addition, integrated solutions include security controls, including data encryption.

This approach requires users to accept that a specific personal application may be prohibited if they present a risk to corporate data held on the device or connectivity with corporate systems. Depending on the sensitivity of the data and the risk appetite of the business, prohibition may be based on a deny list for known insecure applications or an allow list of those applications with evidence that they do not pose a risk. Choosing the correct approach will depend on the company's employees' cultural, behavioral, and sociological approaches.

USAGE MANAGEMENT

Mobile device management should support enforcement of usage controls for website access and app installation using the principle of an allow list or deny list based on the corporate policy and risk appetite. Alternatively, the business may choose to restrict app installation to using an enterprisemanaged trusted app store in place of public app stores where this approach is appropriate for corporate-issued and managed devices.

MALWARE PROTECTION

Anti-malware applications using signature-based detection or a more advanced heuristic-based behavioral monitoring approach can provide device-level protection. In addition, device restrictions that prevent downloading and installing unapproved executables from websites, app stores, external connections, or removable media will limit the ability for malware infection. Where cloud services are used, anti-malware protection can also be added within the cloud-based infrastructure to provide additional detection capabilities.

SECURITY AUDIT

Periodic audits of mobile device configuration and fingerprint processes will provide ongoing assurance of the integrity of security controls and compliance with the security policy.

DEVICE PROTECTION

Critical features for protecting mobile devices include:

MALWARE PROTECTION

Mobile devices allow users to install apps from a range of sources depending on the type of device and its operating system. In addition, anti-malware scanning can protect devices by checking executable files against known malware signatures when files are downloaded via network connectivity and uploaded on removable media using a wired or Bluetooth connection.

NETWORK ENCRYPTION

Network connectivity can include an additional layer of message encryption using Virtual Private Network (VPN) technology to protect against interception or eavesdropping-based attacks. A VPN tunnel is established between each mobile device and infrastructure managed by the business to safeguard communications outside the corporate infrastructure's boundary. For example, this prevents message traffic interference if a mobile device connects to a maliciously operated cell mast or Wi-Fi hotspot.

CREDENTIALS MANAGEMENT

On-device credentials management synchronized with a centralized vault can prevent the use of weak or compromised access credentials by ensuring all web and app access use strong and unique identity credentials, including passcodes, passwords, and usernames. This control reduces the risk of compromise using brute force attack methods while ensuring the availability of credentials across multiple user devices where necessary.

URL FILTERING

URL filters can protect mobile device users from accessing URLs that link to malicious content, such as malware executables, by cross-referencing libraries of known bad links. In addition, protection needs to include the ability to check URLs embedded within imagery, such as QR codes.

A complete solution will also need to place controls on which internet addresses the device can access using browsers. They may use techniques such as scanning for malware before access, imposing deny lists for websites that do not fall into acceptable use guidelines, or the more restrictive allow list for approved sites. However, technologically knowledgeable employees can bypass security controls that are too restrictive using services such as proxy, virtual network access, or other well-known techniques.

REMOTE MONITORING

Remote monitoring functions that access device features, including the microphone and camera, and provide real-time device location information, can support investigation and recovery activities in the event a device is misplaced or stolen.

REMOTE WIPING

If a mobile device is stolen, remote deletion of content can prevent an attacker from subsequently gaining access to helpful information from the device once they have defeated any access controls. Consequently, remote wiping should cover applications and configuration settings that would be useful for an attacker in addition to personal and corporate data. Ideally, the remote wipe will reset the device to its factory default state or leave the device permanently inoperable.

SERVER PROTECTION

The corporate interface with mobile devices provides a single line of defense for business systems against compromised devices. Interfaces are typically implemented using API calls consumed by apps on the mobile device or web services accessed by the device.

Weak server-side controls provided the most significant risk that an attacker using a compromised device or able to impersonate an authenticated device can gain access to corporate systems. The typical cause of vulnerabilities in exposed services and API calls is the failure to integrate security into the development process, resulting in insecure coding techniques.

Typical reasons for high-risk vulnerabilities are a failure to define robust security requirements in outsourced development or a lack of security knowledge in the development process for in-house development. Other factors include business pressures to deploy solutions quickly and poor budgeting to allow thorough security implementation in mobile applications.

Segregation of mobile services from other business systems using virtualization and containerization technology can help contain threats originating from mobile devices. Extended Detection and Response (XDR) can be applied to provide automated attack validation, investigation, containment, and remediation services that protect corporate systems.

THREAT INTELLIGENCE

Typical mobile security solutions protect against known threats, but without knowledge of adversary behavior and intent, it is difficult to provide comprehensive defense against malicious activities. In addition, attackers constantly develop new tactics, techniques, and procedures to bypass the current threat detection mechanisms and technologies.

Mobile threat intelligence is necessary to gain insight into the current and forecast mobile threat landscape. Intelligence should be delivered in real-time using automated information feeds to inform detection and response processes. As threat intelligence reveals new exploits, intelligent asset management can automatically highlight those vulnerable network assets to initiate a risk based decision process to update, replace, or retain affected devices.

Mobile threat intelligence can also provide new insights into attack patterns that allow previously undetected abnormal events to be retrospectively identified. Thus, a previously undetected attack can be deduced, and a response initiated based on this examination of old data with new knowledge. The retention of mobile device activity records enables the use of threat intelligence to identify novel persistent threats sophisticated enough to evade behavioral analysis.

MOBILE **DEVICE DEPLOYMENT**

WEB BROWSER DEPLOYMENT

The simplest method of deploying mobile devices is to provide access to corporate data and services through the web browser. This approach can use the standard web authenticate technology and session management functions to provide secure access. In addition, this approach has the benefit that it will function on unstable network connections and manage the outages typically experienced when using a mobile device on the more.

FIGURE 9 - Web Browser Deployment

This simple and versatile approach is ideal for simple corporate email access. However, it offers the lowest level of security management. Mobile security solutions cannot prevent data loss or access from insecure services or compromised devices. An attacker could use the device to access the browser cache, session credentials, and security tokens with relative ease.

The deployed mobile security solution should enforce strong authentication controls on corporate services, including multi-factor authentication. It should also ensure any Cloud Access Security Brokers (CASB) used to control session-level privileges in corporate services have permissions set appropriately.

REMOTE VIEW DEPLOYMENT

Remote viewing technology can provide the user of a mobile device with an interactive view of the corporate environment with access to an enabled suite of business applications. Commercial remote viewer solutions running on a remote server provide a virtual desktop image to the mobile device. This approach minimizes the quantity of corporate data cached on the mobile device that would be at risk of compromise in the event that the device is lost or stolen.

FIGURE 10 - Remote View Deployment

The robustness of this approach's security relies on the integrity of the communications channel between the server and the remote endpoint. Therefore, the incorrect configuration will create an exploitable vulnerability that will undermine the security of the mobile device solution.

In addition, malware on the mobile device will create a risk to the business applications. This risk can be minimized by using a thin client implementation of corporate services to limit access. However, there will still be a residual risk from screenscape and keylogging malware or an attacker's injection of keystrokes/mouse movements to execute commands on the remote server using a command-line shell. The latter has the potential to act as the initiator for attack escalation of the exfiltration of corporate data. Therefore, the mobile security solution should also manage mobile device and app compliance checking to minimize risk.

The mobile security solution should ensure that robust authentication methods are enforced for remote viewer solutions and manage revocation of access in the event a device is reported lost or stolen. The security solution's detection and response focus on protecting the virtual desktop image within the corporate network boundary, where controls can be applied independently from the mobile device. This control should prohibit copying or rendering corporate data outside the virtual environment to limit data leakage risks.

The benefit of the remote viewing deployment of mobile technology is it allows the mobile security solution to focus on securing the corporate infrastructure and resources within the control of the business's IT security team instead of the mobile device, which is outside their control.

One significant performance consideration is that this solution relies on access to a stable connection with sufficient bandwidth and throughput to support connectivity with the remote environment.

The deployed mobile security solution should limit exposure of corporate resources on a need-toknow basis when required using Role Based Access Controls (RBAC). Access should be denied at all other times. It should also enforce strong authentication controls on corporate services, including multi-factor authentication, and implement robust network traffic encryption between the mobile device and the corporate systems. The solution should also prevent access using weak or vulnerable protocols such as Remote Desktop Protocol (RDP) and prevent multiple user sessions from limiting the impact of device compromise.

The deployed mobile security solution should also limit which corporate resources are available to a mobile device and prevent unnecessary corporate data transfer from the virtual desktop to personal apps on the device. It should also control what apps are installed on the virtual desktop.

BOOTABLE CORPORATE OPERATING SYSTEM DEPLOYMENT

A secure deployment option is to implement dual boot technology into the mobile device so the user will either boot using the native operating system for personal use or the separate corporate managed operating system for business use. This approach requires the mobile device to have access to bootable media such as a USB drive. Configuration of the device and its bootable operating system is potentially complex but offers businesses the lowest risks. However, the downside is the need for users to undertake a reboot process every time they switch between personal and business use of their device.

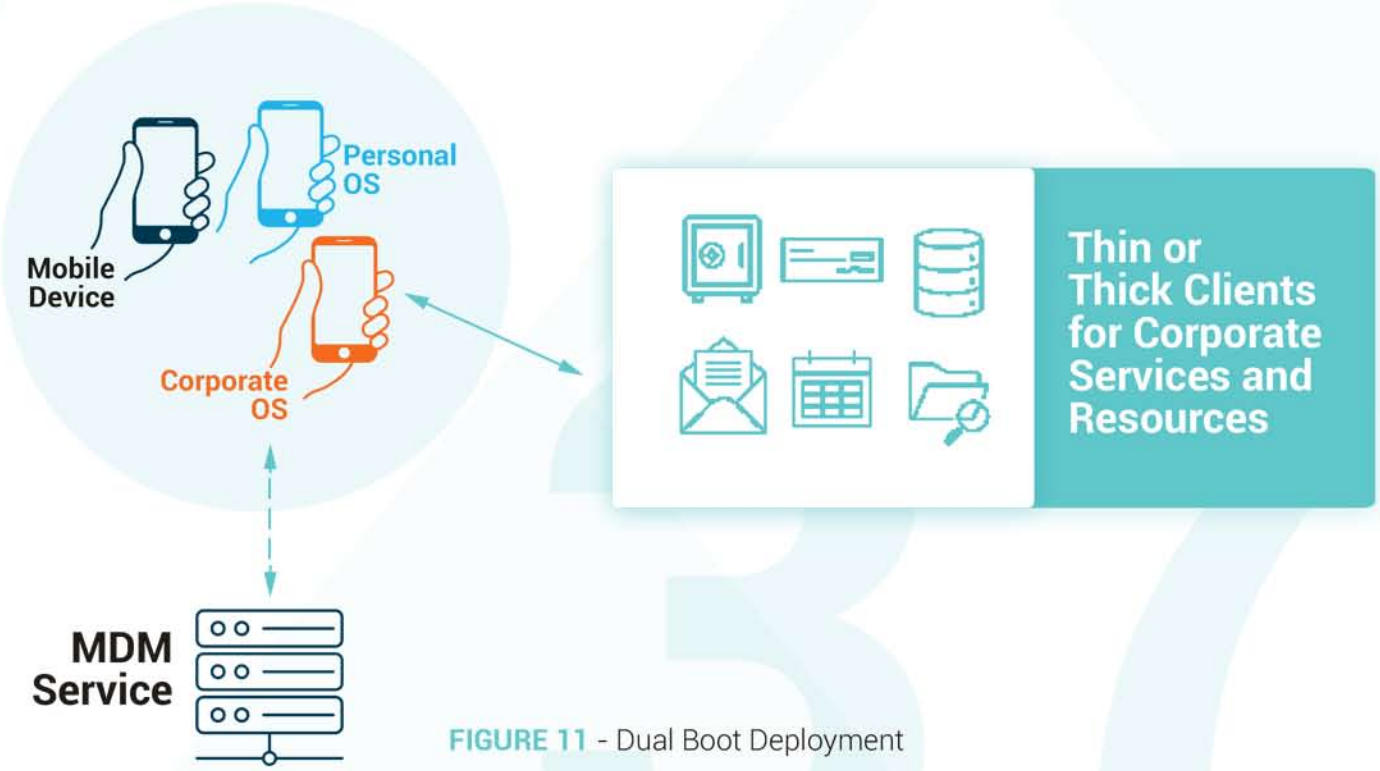


FIGURE 11 - Dual Boot Deployment

The deployed mobile security solution should enforce full volume encryption of the corporate environment to protect data from compromise or theft and enforce the installation of security patching to ensure the bootable operating system is up to date.

MOBILE DEVICE MANAGEMENT DEPLOYMENT

MDM solutions enable the enrollment of personal mobile devices into corporate systems to provide the business with limited control of device configuration and settings using a partly managed approach. The benefit is all popular mobile device operating systems support MDM solutions, though with different levels of control over the application of security controls.

The mobile security solution must integrate with the MDM application to enforce device-specific security policies through configuration policies. This approach offers businesses greater assurance of device security but with less control over device usage.

MDM solutions offer businesses reporting and monitoring facilities for mobile device states to provide a view of security integrity based on the viewpoint of the MDM application. However, sophisticated malware can mask malicious activities from MDM solutions. Also, any compromise of the operating system by malware would compromise the integrity of any MDM-applied security controls.

The benefits of using a mobile security solution based on an MDM deployment is that strong authentication can be enforced and controls for security policies are implemented and enforced at the platform level. In addition, they can also implement a corporate app store to manage approved app installation and ensure updates are promptly installed as necessary.

The downside for users is that security controls may restrict the personal use of the mobile device. At the same time, for businesses, there are risks associated with corporate data being stored on the device and the ability of users to bypass or remove security controls.

MOBILE APPLICATION MANAGEMENT DEPLOYMENT

Mobile Application Management (MAM) solutions allow the owner of a mobile device to retain complete control over its configuration and use, except for business applications. These apps are segregated using containerization technology held on the device and managed by the business. This approach gives the company complete control over the corporate apps and the data they access, applying security controls at the app level.

The benefit of this approach is better protection of corporate data from leakage into personal apps by preventing any direct copies or screenshots of corporate data from being transferred outside the segregated container. The downside for the business is that a mobile device poorly configured or compromised by malware will undermine the integrity of the app-level security controls. Malware will be able to gain access to corporate data and the security tokens for services accessed on the device.

A potential benefit to the device owner is that corporately managed processes to access or remote wipe are limited to the data within the segregated container. Likewise, personal information outside the segregated container is separated from the corporately managed solution.

LMNTRIX
BE THE HUNTER | NOT THE PREY

MOBILE **SECURITY REQUIREMENTS**

OVERVIEW

The first step in deploying a mobile security solution is defining the mobile system's goals, objectives, and scope to ensure that the deployed solution meets the correct requirements.

Mobile device use in corporate systems creates security challenges that include:

- Ensuring users of personally owned mobile devices comply with applicable policies and procedures.
- Support a diverse range of device types, configurations, operating systems, and apps.
- Protecting corporate infrastructure and data.
- Protecting users' personal data.
- Maintaining regulatory and legal compliance.

How mobile devices are used for business activities will significantly impact threat types and risk levels. Therefore, it is critical that usage is strictly defined and scoped before risk assessment and that no creep in scope is permitted without revisiting the risk assessment process. For example, integrating mobile devices with centralized calendars and appointment systems creates significantly lower risks than access to file-sharing systems.

What mobile devices will be supported will also influence the security solution deployment. Mobile devices can include laptops, tablets, and smartphones; these may be corporate-supplied devices or users' personal devices. These may have a broad range of operating systems and utilize various connectivity options, including cellular or Wi-Fi networks.

Where mobile devices will be used will also have an effect. Devices brought onto business premises may connect with trusted networks within the boundary of the perimeter security controls of the corporate IT systems. Equipment used in different countries may be subject to more significant risks or require a security solution that complies with local legal requirements. This consideration is particularly relevant for encryption-based controls where some countries have specific legal restrictions on the use of encryption.

Policy enforcement is a critical consideration in assessing risk. Policies enforced using automated technological controls are more robust than policies that require users to follow procedures to maintain security manually. In turn, the effectiveness of technical controls will depend on the type of device, particularly the operating system and its configuration.

ROLE-BASED PROTECTION

The business requirements for mobile devices may have role-based conditions that affect any security solution. For example, senior executives may need to handle sensitive corporate information where restrictive security controls may be necessary to reduce risks to acceptable levels. Conversely, administrative employees may not require access to corporate data, using mobile devices for appointment setting and messaging. In this latter case, restrictive security controls may discourage using corporately managed mobile devices, impacting productivity.

How mobile devices are used for different roles within the business will impact security control requirements and should be defined and scoped before risk assessment. This approach ensures no creep in usage for each defined role is permitted without revisiting the risk assessment process to determine the minimum controls needed. In addition, each role-based group's priorities and needs must be balanced against corporate security requirements.

ACCESS SCOPE

The security solution will be influenced by the scope of the business services accessible using mobile devices. For example, a system replicating the complete corporate environment on a personal mobile device will have more stringent requirements than a system that only provides a controlled subset of business processes. This scope limitation may include providing a subset of functionality for a business process. For example, a financial administrator may be permitted to authorize payments to existing suppliers but not allowed to change or add new payment details using a mobile device.

Similarly, users with privileged or administrative-level access to business systems on corporately managed devices requiring equal access from a personal device will require stringent and robust security controls. A business may provide such users with corporately managed mobile devices or limit access when remote working to implement a more effective mobile security solution.

MOBILE DEVICE OWNERSHIP

There are various options available for businesses looking to introduce mobile devices into corporate systems:

- Bring Your Own Device (BYOD), where employees use a personal mobile device for business use.
- Corporately Owned Business Only (COBO) devices offer the most robust security but require employees to carry a separate personal mobile device. Unfortunately, this often results in employees using the personal device for business purposes and the COBO device being under-utilized, losing any potential productivity benefits.
- Corporately Owned Personally Enabled (COPE) devices allow the business to maintain control over mobile devices while allowing employees to undertake limited personal use subject to security restrictions.
- Personally Owned Corporately Managed (POCM) devices allow employees to choose which mobile device they use with limited personal use subject to any security restrictions while allowing the business to maintain control over mobile devices.

The success of COBO, COPE, and POCM schemes will depend on the nature of the security restriction imposed on users and how willing employees are to accept the limitations in return for the benefits of remote working using the mobile device. Security controls adversely affecting mobile device usability will drive down mobile device adoption and risk undermining the business approach. In addition, overly restrictive controls can encourage employees to use workarounds that undermine security controls.

Where role-based protection is necessary, businesses may implement different schemes for each role. For example, where access to sensitive corporate data is deemed too high risk to allow BYOD, a COPE scheme may be necessary for that role.

FIGURE 12 - Role-Based Mobile Ownership

PROCEDURAL CONTROLS

Where a mobile security solution relies on procedural controls to be fully effective, these must be communicated to all relevant employees effectively. Employees' training and awareness sessions may be needed to support the documented security procedures. All employees must understand their responsibilities and agree to abide by the controls.

While procedural controls are essential for all business security solutions, mobile device procedures face additional challenges when employees are expected to follow corporate guidelines when using their personal devices. In addition, cultural and sociological barriers may need to be overcome during the education process to ensure that employees follow procedural controls at all times, particularly when utilizing the device for personal use.

Device monitoring and regular audits may be necessary to provide evidence of compliance and limit the window of opportunity for threats when a device is misused or procedural controls are ineffective.

LEGAL CONSIDERATIONS

Using a personal mobile device for corporate use has legal implications from a data protection point of view in certain jurisdictions that need to be addressed by the mobile security solution. For example, the responsibility for protecting the personally identifiable data of citizens of the European Union lies with the business's data controller rather than the mobile device owner, even when that data is stored on their mobile device. However, the mobile device owner is responsible for taking reasonable measures to protect that data against unauthorized or unlawful processing while it is on their device.

Another consideration for the business is that where a personal mobile device is under corporate control through the mobile security solution, the device owner is entitled to a degree of privacy, such that the business should not access or process the device owner's personal information without permission.

Regulated industries will also have restrictions and limitations on how mobile devices can access, process, and store information that depends on the industry and the nature of the data. A final consideration is that commercial or partner agreements may also include clauses relating to the handling and processing of information that may affect the use of mobile devices and the implementation of a security solution.

MOBILE DEVICE BEST PRACTICES

A deployed mobile solution can include various best practices to minimize business risk. Examples include:

- Personal mobile devices should only be used for a defined set of business processes compatible with the level of risk that this use creates.
- Mobile device users must be explicitly aware of their responsibilities and obligations for keeping corporate data secure and how this differs from standard IT security awareness.
- Businesses enabling personal mobile devices for business processes must explicitly understand their responsibilities and obligations to the device owners.
- User permissions and service access policies should operate on the principle of least privilege and offering the minimum visibility of corporate data necessary for the user to perform their required duties.
- Mobile security solutions must maintain a balance between security and usability for personal mobile devices while maintaining business risks at an acceptable level.
- Mobile security solutions must not rely on device-hosted technical controls such as encryption and containerization that can be compromised by malware on the device.
- Mobile security solutions must employ robust multi-factor user authentication methods to counter the increased risk of mobile device usage while maintaining device usability by adopting single sign-on and password-less techniques.
- Device authentication should be employed to create trust relationships when onboarding a new device using additional factors such as access from within the boundary of corporate systems or from an alternate verified location.
- The mobile security solution should employ risk-based authentication and access control to ensure controls are proportionate. This approach will make access permission decisions based on meta-identity data, including the device, its location, and the nature of the resource request. Additionally, the security solution should automatically limit access and raise alerts when the risk is deemed higher than the permitted level for the business.
- Where technology permits, mobile device access should use different passwords to unlock the device and access corporate services and data. Where it is not possible to apply sufficient technical controls, the security solution should restrict access to that subset of corporate data and services that meet the acceptable risk level for the business.

- The security solution should automatically deny access to any mobile device that does not comply with the mobile security policy, such as a change to the configuration, the installation of unapproved apps, or abnormal behavior.

- The mobile security solution should capture sufficient event and usage information to enable threat detection and response processes and support investigation and analysis activities. Typical information should include event times, source IP addresses, device details, successful and failed authentication and authorization events, data and service access requests, and network configuration information.

LMNTRIX
BE THE HUNTER | NOT THE PREY

MOBILE **SECURITY DEPLOYMENT**

DEPLOYMENT SCOPE

Successfully deploying mobile security technology requires a clear definition of its objectives to provide sufficient coverage to be effective. Then, the deployment can be implemented with the understanding of what the solution needs to monitor to achieve its goals. There must be a clear definition of what mobile device endpoints are in scope and which locations on the corporate network require traffic data to be collected and analyzed.

DEPLOYMENT OBJECTIVES

The questions that need answering are:

- What are the mobile devices that an attacker could target?
- Where is the critical network traffic that an attacker could target?
- What ingress and egress points to the corporate network could an attacker target?
- What Internet traffic must be monitored to detect an attacker's command and control connections, data exfiltration, or other interactions with the outside world?
- What mobile-to-corporate network traffic must be monitored to detect any reconnaissance, data acquisition, or exfiltration an attacker performs?
- What mobile-to-mobile traffic must be monitored to detect any reconnaissance, lateral movement, data acquisition, or exfiltration an attacker performs?
- What mobile to authentication server traffic must be monitored to detect brute force access attempts or lateral movement?
- What network traffic within corporate systems do I need to collect to provide a complete record of an attacker's actions?
- What network traffic within corporate systems do I need to collect to provide sufficient intelligence about an attack profile?

With the objectives of the mobile security solution defined, the solution can be deployed.

DEPLOYMENT PROCESS

ENDPOINT SENSOR DEPLOYMENT

Mobile devices connected to business systems require equal protection as other corporately managed devices that operate as endpoints on the corporate network. Lightweight endpoint sensors provide rapid deployment of detection capabilities that minimize the impact on mobile device operations. Endpoint monitoring captures detailed state information and prevents exploits, malware, file-less attacks, malware-less attacks, phishing, injection, macro-based attacks, ransomware, credential theft, and adversary tradecraft prevention.

NETWORK SENSOR DEPLOYMENT

The location of physical and virtual network sensors determines what data is collected and what information is available to the security solution's behavioral analysis algorithms. In addition, each mobile device endpoint on the corporate network has a distinctive pattern of behavior that describes their everyday operations. Therefore, sufficient information must be gathered to allow the modeling of this behavior for every mobile device endpoint and user to ensure complete coverage for protective systems.

- Physical appliances use port mirroring and network tap techniques to provide monitoring capabilities on physical infrastructure. Coverage requirements will govern their location, and peak packet transmission rates will drive the number needed. Network placement of the SPAN and TAP points across a network is critical to ensure sufficient coverage of network traffic to detect attacks of all phases quickly and efficiently.
- Virtual sensors in the form of lightweight agents provide metadata capture capabilities for virtual infrastructure.
- Cloud sensors in the form of lightweight agents provide full packet capture capabilities for cloud-based infrastructure and for situations where access is unavailable for the placement of physical sensors.
- Application sensors provide connection monitoring for third-party Security-as-a-Service (SaaS) solutions outside the reach of other sensor types.

Caution should be observed when implementing port mirroring due to the additional loading on switching devices that can adversely impact network performance and affect business services. Therefore, capacity planning and loading assessments are a necessary part of the planning process for sensor deployment planning.

NETWORK DATA CAPTURE

Different segments of the network provide access to the different traffic types considered by the objectives of the deployment. Monitoring points should be placed at strategic locations across the internal network within the perimeter controls to collect as a minimum:

- Mobile device authentication traffic.
- Indirect traffic to and from the Internet via mobile device endpoints.
- Mobile device endpoint traffic to server application services, including file services, print servers, web portals, and others handling sensitive information.
- Traffic from mobile device endpoints to and from cloud-based systems and services.
- Traffic between mobile device endpoints via the corporate network.

CONFIGURATION

Once the mobile security solution is deployed, it will require configuration to ensure necessary coverage. For example, all network traffic monitoring must be bidirectional, either using a single port capturing transmitted and received packets or two ports capturing traffic in each direction separately. The capture of bidirectional traffic is preferable to prevent duplication of recorded traffic that can negatively impact processing and storage requirements for captured packets and switch loading.

MONITORING

An implemented and deployed mobile security solution provides the means for detecting in-network threats to inform the response and recovery processes and allow post-incident forensic analysis and threat intelligence gathering. The implemented solution will therefore need to record the information necessary to achieve these goals

The monitoring requirements form part of maintaining the mobile security solution and ensuring it provides the required coverage. In addition, operational experience and post-incident lesson-learned exercises would allow the placement of network monitoring facilities to be refined as part of the standard improvement processes

MEASURING

Mobile security solutions provide a mechanism to measure the effectiveness of corporate security controls for crucial performance indications and metrics generation. For example, the efficacy and reliability of existing security controls can be quantified using information gathered from tracing an attacker's ingress path and actions. The results from this stage can drive security control improvements and refine the incident response playbooks as part of the continuous improvement process.

USE **CASES**

DATA LEAKAGE

TMobile apps are frequently responsible for unintentional data leakage due to undocumented data collection for advertising and marking purposes. It is common for free apps available from official public app stores to generate revenue by acquiring data from mobile devices and exfiltrating it to a remote server. The primary intention is to collate information that advertisers can mine to allow the generation of targeted adverts. However, this data is also available to attackers looking for information of potential value to support an attack. This attack may be an untargeted malware release or a more targeted phishing or ransomware attack.

The low-cost nature of the development of these free apps means that they may unintentionally collect corporate data held on a mobile device in addition to the personal information they primarily want to collect.

Data leakage can also occur through malicious enterprise-signed mobile apps that are designed to collect and exfiltrate data across corporate networks undetected.

Mobile security solutions should assign access controls to apps on a least-access basis to limit the potential for data leakage.

UNSECURED WI-FI

Personal mobile device users are significantly more likely to connect to a wireless hot spot in preference to using cellular data when accessing business applications to manage data usage and charging. However, public wireless hot spots are typically unsecured, allowing connections to be exploited by an attacker.

Mobile security solutions should ensure that corporate applications and data cannot be accessed over an unsecured network by disabling this functionality or through the application of a secure communications tunnel over the unsecured connection.

NETWORK SPOOFING

Mobile device users employed by high-value target organizations such as financial institutions or government bodies are vulnerable to targeted attacks using network spoofing technology. Sophisticated attackers can create fake network access points that mimic cellular or Wi-Fi networks in a location frequented by these users. High-traffic public locations such as airports, railway stations, and coffee shops near business centers are prime targets.

These networks may be disguised as free public networks or given a name that encourages users to believe they are signing into a legitimate service.

Mobile security solutions should ensure that corporate applications and data are protected using a secure communications tunnel over any connection outside the corporate system security boundaries.

PHISHING ATTACKS

Mobile devices are popular targets for phishing attacks due to the nature in which they are typically used. Successful phishing relies on recipients responding immediately to a compelling instruction without studying the wording of the message too closely, checking the integrity of any web links, or confirming the message was sent by the person who appears to be the originator. Mobile device users are more likely to see messages as soon as they are received. It is also more challenging to check web links on a small touchscreen, whereas on a computer, simply moving a mouse pointer over the link will reveal its actual structure. The touchscreen technology of mobile devices makes it far more likely that the recipient will unintentionally press a web link as they scroll through the message.

Mobile security solutions should monitor incoming messages of all types and quarantine those that contain suspicious links or match the pattern of a phishing message.

SPYWARE

A common type of malware found on personal mobile devices is spyware that tracks the activity and location of the mobile device to allow someone to monitor the device owner closely—installed by partners, close acquaintances, or employers, the malware facilities stalking behavior. Spyware is designed to be invisible once loaded on the target's device without their knowledge. The difference from other types of malware is that the application is intentionally installed on the mobile device. The risk to businesses is spyware installed on an employee's device may unintentionally collect and disclose corporate information. Spyware, by its nature, is produced by unscrupulous developers and may also contain other types of malware that may compromise corporate systems.

IMPROPER SESSION HANDLING

Mobile apps commonly use tokens to enable a single identity authentication event to be applied to multiple transactions to make using the app more straightforward and quicker. Tokens are generated to identify and validate the app to the service the app connects with for the session duration. Unfortunately, poor coding practices may allow attackers to access a token and use it for their own interactions, impersonating the previously authenticated device.

Improper session handling includes the unintentional sharing of session tokens by apps that enable a malicious actor to intercept and replay the time and impersonate a legitimate authorized user. Other examples are sessions that remain open after the mobile app has been closed, allowing an attacker to hijack the open session and avoiding the need to authenticate their own device.

THREAT **CASE STUDIES**

ZERO CLICK ATTACKS

One of the most significant threats to mobile devices is the zero-click attack vector, where an attacker can introduce malware onto the device without requiring the user to perform any action. This attack type is possible where existing exploitable vulnerabilities are present on the device in applications that automatically accept and process data, such as email or instant messaging apps.

The best example of this attack type is the Pegasus spyware used by nation-state threat actors to target high-profile targets, including rival politicians, human rights activists, journalists, and dissidents. The NSO Group, which produces and distributes the Pegasus spyware on behalf of their clients, was able to exploit a number of zero-click vulnerabilities. These included an iOS vulnerability in some older releases and a WhatsApp vulnerability on the Android version.

The later versions of Pegasus rely on exploiting iPhone iMessage zero click vulnerabilities or using other attack vectors, such as phishing attacks, for installing the malware via a compromised URL or network attacks. A fix to prevent the zero-click vulnerability in iOS was subsequently deployed in iOS version 14.8.

The Pegasus spyware allows attackers access to text messages and the device's microphone and camera. It also enables the tracking of calls, collection of passwords, location tracking, and collection of data from apps installed on the device. The iOS version of Pegasus was particularly noteworthy because it implemented a sophisticated zero-click remote jailbreak of the target device to perform its malicious surveillance functions.

One of the critical factors for the success of Pegasus was the ability of the cyber security black market to financially incentive security researchers to sell newly discovered vulnerabilities to the criminal community rather than the original developers of operating systems and applications.

SMISHING ATTACKS

Smishing, or SMS Phishing, is the technique where SMS messages are employed as the attack vector for malware distribution rather than the traditional use of email. SMS messages have an improved chance of success over email due to the novelty of the technique and the ability to imitate personal contacts or other trusted parties.

Smishing is particularly useful once a mobile device has been compromised by other means, and the attacker can use the contacts from that device to launch a targeted Smishing attack that impersonates the owner of the compromised device. Each successful Smishing attack will generate additional contacts that can be used in subsequent attacks, allowing a cascade approach to a targeted campaign.

An example of a Smishing attack is the deployment of the FluBot malware from December 2020 onwards, which targeted Android devices. The malware was installed via a malicious link embedded in a package delivery tracking message. Recipients were encouraged to select the link to listen to a voice message or install a courier's tracking application. Once installed, the malware was designed to steal banking app credentials and cryptocurrency account details. In addition, the malware would also use the infected device's contact details to propagate its spread.

The FluBot attack was one of the fastest spreading Smishing attacks, initially spotted in Australia before spreading across much of Western Europe. The attack was halted when international police cooperation resulted in the seizure of the command and control server in the Netherlands.

However, the investigation into the FluBot attack has identified a similar Android malware called MaliBot which also targets online banking and cryptocurrency apps in Italy and Spain. MaliBot typically disguises itself as a cryptocurrency mining app though other variants have been observed. The most significant risk is that Malibot can steal and bypass multi-factor authentication codes.

APP STORE MALWARE

Official app stores give mobile users a degree of trust that the listed apps are free of malware due to the review process submitted apps follow before listing. Figures for 2021 indicate that Apple rejected 1.6 million suspicious apps while Google blocked 1.2 million. However, official apps store remain a target for well-resourced criminals looking to have apps listed that will pass review checks with their malicious intent disguised.

For example, the SharkBot malware that targets banking apps on Android devices was found in several Anti-Virus solutions and device cleaner applications listed on the Google Play Store with a few thousand downloads. Similarly, the Android banking Trojan named Xenomorph was on the Google Play Store masquerading as a device performance improvement tool with over fifty thousand downloads.

Social media accounts are also an attractive target for hackers due to the further potential for attacks that access to a compromised social media account presents. For example, Meta has identified over 400 malicious apps on Google Play Store and Apple's App Store specifically designed to steal Facebook account access credentials. These apps are disguised as a broad range of legitimate app types, from VPN services to photo editors, performance improvement tools to games.

APP VULNERABILITIES

The SHAREit App, with over 1 billion downloads, was one of 2019's most popular apps on the Google Playstore. This file-sharing app gained popularity due to its compatibility with a wide range of devices and platforms, including Android, iOS, macOS, and Windows-based devices. However, a high-risk vulnerability was found in February 2021 that would allow an attacker to perform remote code execution on the device using this app. The vulnerability was subsequently patched to eliminate this risk.

The Klarna Payment App is an example of poor development practices that led to authorized users being granted random read-only access to another user's personal information. This flaw included access to see payment details and limited credit card information. The defect was traced to a fault in a configuration update in the app due to a human error. The error was present in the live app environment for approximately 30 minutes before it was identified and the app disabled. The issue was resolved, and access to the app was restored after a downtime of nearly seven hours. However, this episode demonstrated the weakness of the development and testing processes. Not only did they allow the error to occur, but it was not detected until the change to the app had been released to the public.

The Amazon Ring Neighbors App is designed to enable users of Amazon's Ring smart doorbell to be used as a neighborhood watch information exchange by sharing an alert with app users within a set distance of the alarm. However, it was found that the app would leak the users' personal information, including the exact location of their homes.

The Parkmobile App, which provides a cashless payment of parking charges in the United States, was discovered to have revealed the personal information of its 21 million registered users when the stolen information was found being sold on the dark web. However, it is reported that the data breach did not compromise passwords and financial information.

LMNTRIX
BE THE HUNTER | NOT THE PREY

ABOUT **LMNTRIX**

OVERVIEW

Your mobile security solution should provide peace of mind that adopting mobile technology will not compromise corporate systems in business processes. Typically, the difference between preventing a cyber attack and falling victim is understanding how and where to seek compromise indicators. Even the most advanced attackers leave traces of their presence, so an effective defense must not only be vigilant but also ever-adaptive in response to changes in attacker tactics. A critical element in this age of constantly evolving threats is a detailed view of an organization's entire potential attack surface.

Unfortunately, log collection solutions are simply outgunned against today's advanced threat actors as they either lack the data or the ability to analyze their data in a manner that allows rapid attack detection.

LMNTRIX has reimagined cybersecurity, once again turning the tables in favor of the defenders. We have cut out the bloat of SIEM, log analysis, false positives, and associated alert fatigue and created new methods for confounding even the most advanced attackers. We combine deep expertise with cutting-edge technology, leading intelligence, and advanced analytics to detect and investigate threats with great speed, accuracy, and focus. We believe that in a time of continuous compromise, you need continuous response – not incident response.

As a company, we stand in defiance of the unwanted human presence within corporate networks by attacking the root of the problem—the adversary's ability to gain entry and remain undetected. Our real-time hunt operations identify signs of planned and active attacks and take action to neutralize them, forming the basis of our comprehensive Active Defense approach to limiting security exposure.

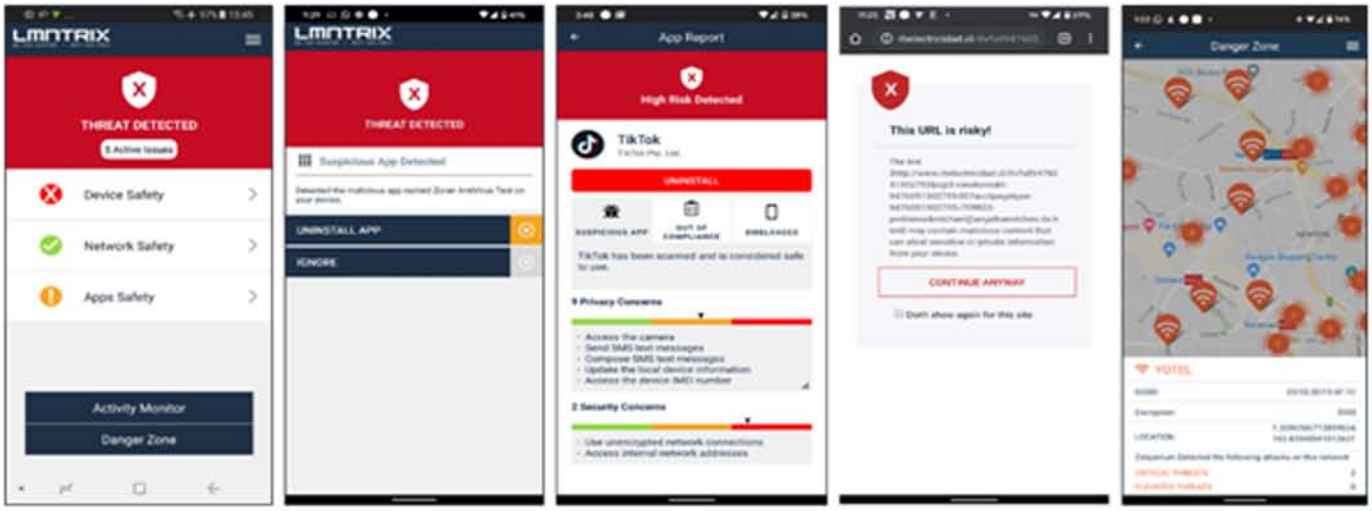
We are a partner who becomes an extension of your internal team, can augment your MSSP, or be a full-service SOC as a service security solution.

LMNTRIX MOBILE SOLUTION

MOBILE ENDPOINT SECURITY

LMNTRIX's mobile solution allows businesses to secure their mobile endpoints using a privacy-first approach to data processing, providing mobile device users with secure access to business-critical systems and sensitive corporate data.

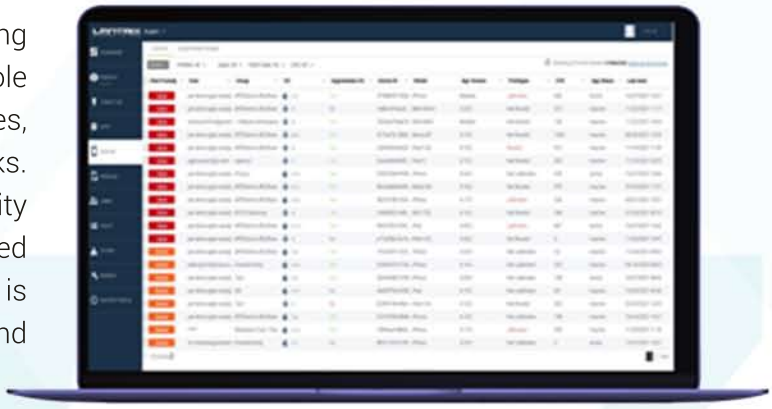
In addition, our solution implements on-device, machine learning-powered detection capable of scaling with business needs.



The cloud-based machine learning engine uses billions of data points to understand mobile risks and threats and keep mobile endpoints secure using real-time, on-device protection. The model is delivered to the endpoint, giving it the power of on-device protection even when the device has no network connectivity. This state-of-the-art solution secures mobile devices against the most advanced threats.

END-TO-END PROTECTION

LMNTRIX's mobile solution is managed using an advanced cloud-native management console that enables businesses to manage policies, monitors for threats, and mitigate mobile risks. This enterprise-focused, advanced mobile security solution integrates with LMNTRIX's Extended Detection & Response (XDR) platform and is deployable on any cloud, on-premises, and air gapped environments.



This approach provides security operations and incident response teams with the critical mobile threat and risk data necessary to support modern Zero Trust architectures. The unmatched threat forensics and risk intelligence data feed can be integrated with leading enterprise mobility management (EMM) and unified endpoint management (UEM) in addition to LMNTRIX's security operations (SOC) and incident response (IR) solution.

LMNTRIX

BE THE HUNTER | NOT THE PREY

TRULY MOBILE MACHINE-LEARNING-BASED PROTECTION

LMNTRIX MOBILE provides comprehensive protection for mobile devices. It provides the risk intelligence and forensic data necessary for security administrators to raise their mobile security confidence. As the mobile attack surface expands and evolves, so does LMNTRIX's on-device, machine learningpowered detection. LMNTRIX MOBILE detects across all four threat categories — device compromises, network attacks, phishing and content, and malicious apps.

With LMNTRIX MOBILE, the LMNTRIX MDR team gains complete visibility into mobile threats and risks through native integration with LMNTRIX XDR. The unmatched forensics provided by LMNTRIX MOBILE prevent a compromised device from turning into an outbreak. By collecting forensic data on the device, network connections, and malicious applications, the LMNTRIX MDR team is able to review forensics to minimize risk exposure.

KEY FEATURES AND ENTERPRISE-GRADE CAPABILITIES

LMNTRIX MOBILE's on-device, machine learning-powered detection is capable of evaluating the risk posture of a user's device, securing the enterprise against even the most advanced threats.

With a privacy-by-design approach, LMNTRIX MOBILE provides users with a transparent experience by delivering customizable user settings and insight into what data is collected and used for threat intelligence.

Built with advanced threat security in mind, LMNTRIX MOBILE meets the mobile security needs of enterprises and governments around the world.

- **Powered by Machine Learning:** Machine learning-based detection provides prevention against the latest mobile threats, including zero-day malware.
- **Critical Data, Where You Need It:** Native iintegration with LMNTRX XDR and option to integrate with 3rd party SIEM, IAM, UEM, and XDR platforms, administrators always have the visibility they need.
- **Deploy Anywhere:** Address local data laws and compliance needs by deploying to any cloud, on-premise, or air-gapped environments.

- **Zero-Touch Deployment:** Deploy and activate LMNTRIX MOBILE on your employees' and contractors' mobile endpoints without the need for complicated activation steps by the end user.
- Access to Critical Data: Comprehensive device attestation enables enterprises to have a complete picture of their mobile endpoint security and shores up Zero Trust architectures through existing integrations.
- Access to Critical Data: Comprehensive device attestation enables enterprises to have a complete picture of their mobile endpoint security and shores up Zero Trust architectures through existing integrations.

LMNTRIX ACTIVE DEFENSE

LMNTRIX Active Defense is a three-tier outcome-based solution (Industry refers to it as Managed Detection & Response (MDR) and our platform as Extended Detection & Response (XDR).

1) **LMNTRIX XDR** (AWS Data Lake and Platform).

2) **LMNTRIX TECHNOLOGY STACK** (Deployed deep within Customer Networks).

3) **LMNTRIX CYBER DEFENSE CENTRE** (Security Analyst Driven).

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, UEBA, and Deception Everywhere with completely automated attack validation, investigation, containment, and remediation on a single, intuitive platform. Backed by a 24/7 Managed Detection and Response service at no extra cost, LMNTRIX provides comprehensive protection of the environment for even the smallest security teams. In addition, it is a single investigative platform for insights into threats on enterprise, cloud, hybrid, and industrial control systems (ICS) networks.

The LMNTRIX XDR delivers unique advantages over current network security solutions. It is a holistic and multi-vector platform with an unlimited retention window of full-fidelity network traffic, innovative security visualizations, and the ease and cost-savings of an on-demand deployment model.

LMNTRIX XDR is based on multiple detective, responsive, and predictive capabilities that integrate and share information to build a security protection system that is more adaptive and intelligent than any one element. The constant exchange of intelligence between the Active Defense components and the wider cybersecurity community enables LMNTRIX to keep abreast of the TTP of the most persistent, well-resourced, and skilled attack groups.

FIGURE 13 - LMNTRIX XDR

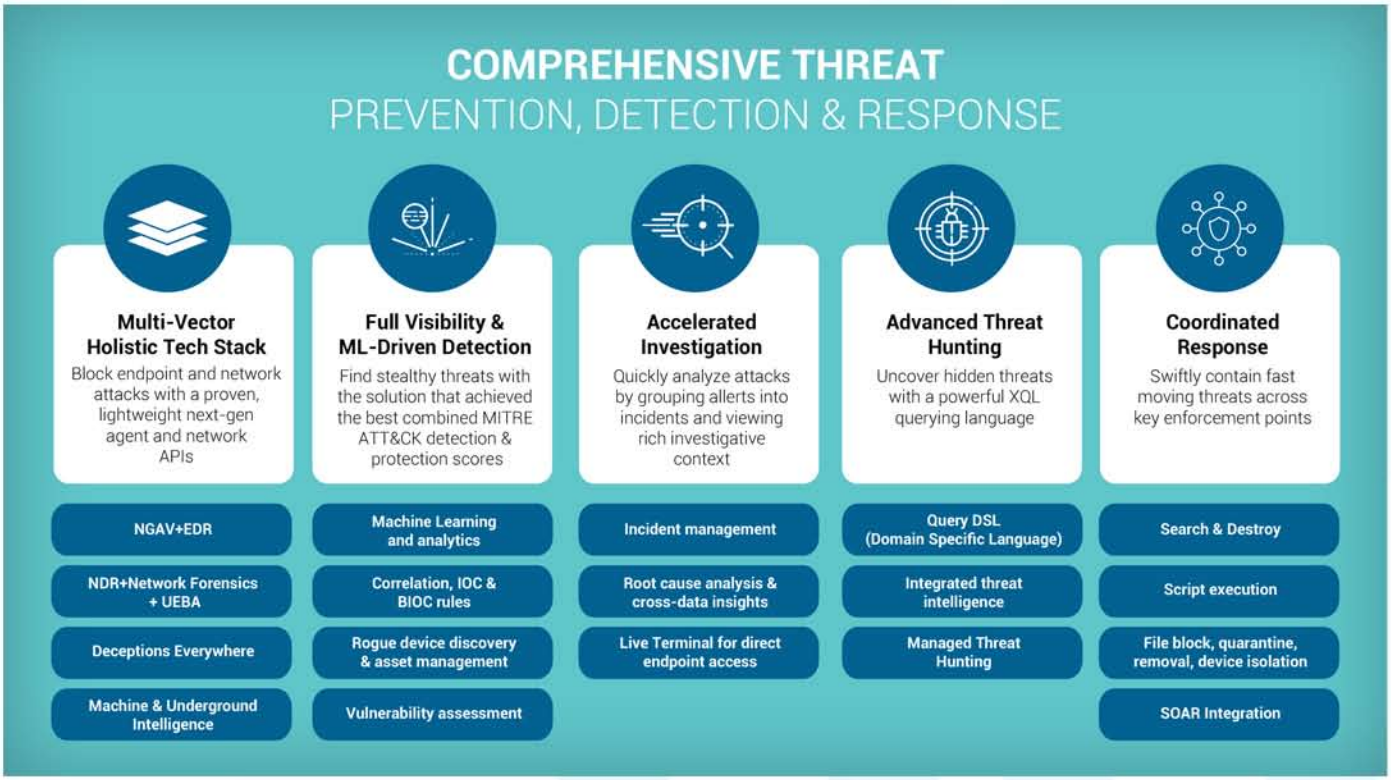


FIGURE 14 - LMNTRIX XDR Features

LMNTRIX TECH STACK

The LMNTRIX Tech Stack is a powerful, proprietary threat detection stack embedded within the client environment behind existing controls. TECHNOLOGY STACK comprises multiple detective systems, combining contextual threat intelligence and correlation, static-file analysis, user and entity behavior analytics (UEBA), and anomaly detection techniques to find threats in real-time. In addition, it eliminates alert fatigue, determining which alerts to escalate through multi platform consensus.

LMNTRIX CYBER DEFENSE CENTERS

LMNTRIX employs a global network of Cyber Defense Centers (CDC) comprising trained and certified hunters and intrusion analysts and provides constant vigilance and on-demand analysis of your digital assets and networks. Our intrusion analysts actively probe and monitor your networks and endpoints 24x7, using the latest intelligence and proprietary methodologies to look for signs of compromise. When a suspected breach is detected, the team performs an in-depth analysis of potentially affected systems to confirm the breach. Additionally, when data theft or lateral movement is imminent, our endpoint containment feature makes immediate action possible by quarantining affected hosts, whether they are on or off your corporate network. This significantly reduces or eliminates the consequences of a breach.

FIGURE 15 - LMNTRIX Cyber Defense Centre

APPENDIX A: MOBILE SECURITY RISKS

The following diagram summarizes the typical mobile security risks identified by the OWASP® Foundation. In addition, explanations are provided below for the labels M1 through M10 that describe the typical risks in more detail.

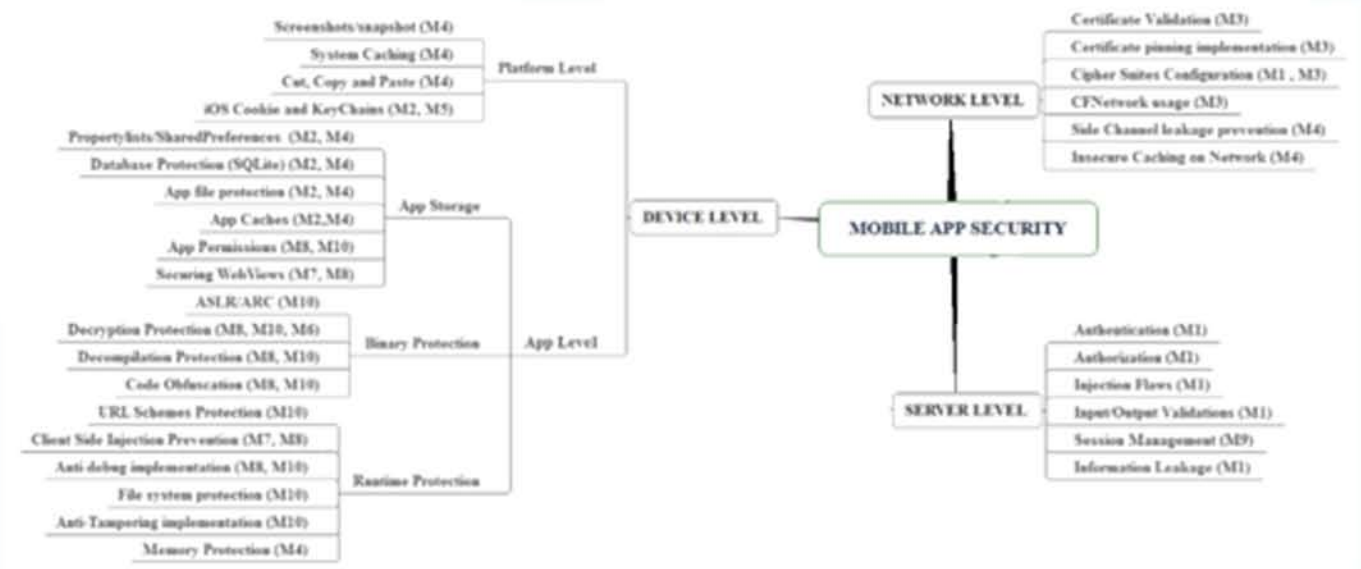


FIGURE 16 - Mobile Security Risks

M1: SERVER-SIDE CONTROLS

Weak server-side controls are common in app development due to insecure development practices. Typical root causes of weak controls are:

- The rush to market in a competitive marketplace.
- Inadequate security knowledge within the development team.
- Use of off-the-shelf development frameworks and tools that don't prioritize security.
- Lack of resources available for mobile applications.
- The assumption that the mobile OS will implement security controls.
- Weaknesses in cross-platform development and compilation processes.

This vulnerability will be exploitable when a web service, web server application, or API call consumed by a mobile app is exposed to an attacker. Consequently, insecure service or API call development practices create exploitable server vulnerabilities.

The typical attack method is to submit inputs containing malformed or malicious content or unexpected event sequences to the vulnerable server code. Protection requires using secure development, coding, and configuration practices on the server side of mobile applications.

M2: DATA STORAGE

Insecure data storage vulnerabilities occur when developers assume that apps on a mobile device will not have access to a device's file system or any stored sensitive information. A failure to protect data using robust encryption methods will allow data to be accessed by an attacker using standard tools.

An attacker may gain access to the data on the mobile device through physical inspection of a lost or stolen device or the use of malware or a compromised app to remotely access data. Additionally, rooting or jailbreaking a mobile device circumvents encryption protections rendering data unprotected against such threats.

Typical weaknesses in mobile device data protection can be found in the following functions that offer attackers valuable information for furthering attacks:

- URL caching (both request and response).
- Keyboard press caching.
- Copy/Paste buffer caching.
- Application backgrounding.
- Intermediate data.
- Logging.
- HTML5 data storage.
- Browser cookie objects.
- Analytics data sent to third parties.

M3: TRANSPORT LAYER PROTECTION

Mobile applications frequently offer insufficient protection of network traffic. Common weaknesses include sending message data in plain text or incorrectly implementing transport security.

Mobile applications commonly exchange data using client-server techniques, transmitting data across the internet via a mobile device's carrier network or Wi-Fi connection. Threat agents can exploit vulnerabilities to intercept sensitive data in transit by sharing the local network, such as a rogue cell tower or a compromised or monitored Wi-Fi network. Network traffic can also be intercepted using malware on the mobile device or the server-side infrastructure.

Weaknesses in transport layer protection can expose authentication details and sensitive data in transit, facilitate phishing and enable MITM attacks.

Typical controls include ensuring that all connections are correctly encrypted, SSL certificates are properly signed by a trusted provider and are in date, and encryption algorithms are sufficiently robust. In addition, sensitive information should be protected using a separate layer of encryption above the transport layer protection to provide a secondary defense against confidentiality compromise.

M4: DATA LEAKAGE

Unintended data leakage is the consequence of sensitive information or data being stored in a location on a mobile device that is easily accessible by other apps on the device. This risk typically results from insecure development practices or a failure to fully understand how the mobile device's operating system handles data used by the app. Poor data storage practices make sensitive information available to attackers via malware or compromised apps or through physical inspection of a lost or stolen device.

Unintended data leakage due to apps can also arise due to vulnerabilities within the device's operating system, the app development environment, compiler flaws, device changes that the developer is unaware of, or poor development practices.

For businesses, the theft of sensitive information may result in regulatory violations, reputational damage, or the commissioning of fraudulent activities.

M5: AUTHORIZATION AND AUTHENTICATION

Poor or missing authentication processes allow attackers access to mobile apps or server-side services. This risk is particularly prevalent in mobile services due to the weak security of typical mobile device form factors where four-digit passcodes are common. In addition, availability requirements tend to impose significantly weaker authentication schemes than other types of web applications. Mobile devices may regularly experience network connectivity and availability issues that apps must manage, whereas traditional web services assume connecting devices will have continuous connectivity. Consequently, mobile app authentication schemes include provision for offline authentication that creates security vulnerabilities. This risk is seen where mobile device apps make authorization decisions rather than server-side services.

Poor authentication practices will compromise logging and auditing by preventing the provable identification of which user performs which actions. This limitation will hinder any incident investigation and prevent post-incident forensic analysis activities used to avoid reoccurrence and to remediate any damage.

Authentication weaknesses can also expose underlying authorization vulnerabilities, allowing attackers to execute sensitive functionality anonymously. Any mobile device compromise could enable further corporate systems attacks through privilege escalation. The development of mobile applications should implement authentication processes that are as robust as an equivalent web application.

Authorization and authentication controls must be implemented on the server side whenever possible to counter the significant risk that an attacker can readily bypass mobile device controls. Local mobile device authentication can lead to client-side bypass vulnerabilities, particularly where operating system vulnerabilities exist, such as rooted or jailbroken devices, that allow run-time manipulation or modification of applications. Where mobile apps are required to support local authentication or authorization checks, local integrity checks should be employed to detect unauthorized changes.

Authentication tokens should be chosen to prevent the use of weak tokens, such as four-digit passcodes, or those with the most significant risk of spoofing, such as geolocation information. In addition, device-specific authentication tokens that can be revoked within the mobile app will reduce the risk of unauthorized access from a lost or stolen device.

Where persistent authentication (Remember Me) functionality is implemented within a mobile app, the authentication details must be stored on the server side and not on the mobile device to prevent compromise.

Application data should only be made available to a mobile device after successful authentication. Ideally, data should be encrypted using a key securely derived from the app access credentials to prevent bypass of authentication processes.

M6: CRYPTOGRAPHY

Insecure cryptography implementation is a common vulnerability in mobile apps. The exploitation of this risk requires an attacker to successfully return encrypted data to its original unencrypted form by taking advantage of weak encryption algorithms or flaws within the encryption process. This weakness will enable the unauthorized retrieval of sensitive information from the mobile device.

Attack vectors for exploitation include data decryption via physical access to the device, network traffic capture, or malicious apps on the device with access to the encrypted data.

Many cryptographic algorithms and protocols have known flaws or are insufficiently robust for modern security requirements. These include RC2, MD4, MD5, and SHA1, which are still in common use.

However, secure algorithms can also be compromised if encryption keys are not handled securely. Common issues include storing keys with encrypted content or other accessible locations, using hardcoded keys in app code, or allowing keys to be intercepted in transit.

M7: CODE INJECTION

Code injection is the execution of malicious code on a mobile device. Malicious code may be injected directly onto the device or delivered as data that the attacker inputs to a mobile app by exploiting a development weakness. This latter scenario relies on malformed data being accepted and processed by the app, where it is interpreted as executable code and allowed to run. This malicious code will run with the same scope and access permissions as the app running it unless it can also escalate its privileges, increasing the potentially harmful consequences.

Web browsers, office productivity tools, and database-based apps are all common attack vectors for introducing malware onto mobile devices. Protection techniques ensure that all mobile apps that receive data outside the device implement robust data validation that discards invalid or malformed data.

M8: UNTRUSTED INPUTS

Mobile devices often use hidden fields and parameter values for implementing privilege functions on the basis that knowledge of this confidential data is on a need-to-know basis. Typically apps use Inter-Process Communication (IPC) mechanisms for such calls. An attacker can easily intercept and analyze mobile app IPC calls to identify such data and exploit weaknesses in the implementation of the associated app. IPC calls should never include sensitive information, given its vulnerability to eavesdropping attacks. Parameter tampering can then be used to gain unauthorized access to functionality or perform privilege escalation. Poor development practices may even allow hidden parameters to bypass app security controls.

Apps should limit access to a list of trusted applications and restrict the use of IPC-triggered actions to require authenticated user interaction before authorizing any sensitive operation. These actions will prevent the exploitation of IPC call vulnerabilities. In addition, before acceptance, all data received from IPC entry points should also be subject to robust input validation.

M9: SESSION HANDLING

Mobile apps typically use session tokens to maintain state information when using stateless protocols like HTTP for implementing stateful transactions between the app and the server-side services. For example, authentication of the mobile app with the server establishes state information when the server application issues a session cookie to the mobile app. This session cookie supports the enforcement of authentication and authorization for the service requests of all future transactions.

An attacker gaining access to the session token during a transaction between the mobile app and the backend servers will allow that attacker to impersonate the authenticated user by submitting the token to the backend server to perform a malicious transaction. The impact of session token compromise will depend on the type of service that can be requested and the privileges of the impersonated user. However, the consequences are the same as poor authentication practices.

Session tokens can be captured using malware on the mobile device or network traffic capture. Typical poor development practice is failure to invalidate session tokens once a session is complete or only invalidating the session token on the mobile device app and leaving it open on the server side. These practices offer an attacker a window of opportunity to take over the session using HTTP manipulation tools. Therefore, session tokens should be closed at all points of the transactional chain-both when the session ends or after inactivity. This period will depend on the risk to the business of a compromised session balanced against user convenience; the higher the risk, the shorter the period.

Poor mobile app development practices may also result in insecure session token creation processes that create weak tokens susceptible to compromise using simple guessing or anticipation techniques. Developers should follow industry standards for producing sufficiently long, complex, and pseudo-random tokens.

M10: BINARY PROTECTION

Mobile apps are commonly deployed without binary protection due to device limitations. This lack of protection exposes the app binary to detailed analysis by attackers with technical knowledge and access to public domain tools. This omission allows attackers to reverse engineer the binary and uncover any security weaknesses inherent in the code. This risk is compounded by the typically poor

development practices employed in mobile app production that often omit security requirements. It will also reveal the presence of any hardcoded authentication details that an attacker can exploit.

An unprotected app binary may be examined to extract the intellectual property of the owner that can be incorporated into rival products, or it may be rebranded and marketed in direct competition on the app marketplace. A lack of binary protections will also allow attackers to modify to introduce exploitable hidden and compromised functions and redeploy the app binary onto the mobile app marketplace.

Binary protection will not prevent such attacks by capable and well-resourced attackers such as nation-states or organized criminals, but it will deter the more typical attackers.