

The CIO's Guide to Mobile Threat Defense

The Case for Conditional Entitlement

THE CIO'S GUIDE TO MOBILE THREAT DEFENSE

How to Ensure Robust Mobile Device Security
and Maximize User Productivity Using
Conditional Entitlement



Executive Summary

As professionals throughout the corporate world enthusiastically embrace a mobile-first approach to getting things done, mobile devices are poised to become the primary vehicle for worker productivity. The challenge is that **mobile device security has not kept pace with mobile application consumption**. More and more workers are accessing more and more corporate resources on mobile devices that are becoming bigger and bigger targets for cybercriminals.

The threat that mobile devices pose to IT security is real, omnipresent and increasing. That is the impetus for the creation of the conditional entitlement framework described in this eBook. The framework takes into account the unique relationship between users and their mobile devices both in terms of their role as device administrator and in terms of their strong affinity for, and high expectations of privacy on, their mobile devices.

By enabling protection from **zero-day threats**, **enabling enterprise scalability**, **leveraging machine-learning-driven autonomy** and **providing on-device immediacy**, the conditional entitlement framework allows businesses of every size to balance the needs of users to access corporate resources via mobile devices and the need to ensure robust security for those mobile devices.



DEFINITION OF TERMS

Conditional entitlement: A framework for balancing, in an automated and real-time fashion, the needs of users to access corporate resources via mobile devices and the need for ensuring robust IT security

Dynamic risk score: A real-time quantification of the amount of risk posed by a device, taking into account key characteristics of the user

Machine learning: The capability that enables Zimperium's on-device agents to protect devices from threats- including new/unknown and zero- day threats- autonomously

Mobile access entitlement groups: Sets of devices whose users have similar access network requirement and other commonalities

On-device agent: An agent that operates autonomously on a mobile device, requiring no continuous network access

Table of Contents

Chapter 1

Businesses Cannot Compete Without Robust Support for Mobile Devices 4

Chapter 2

Mobile Devices Are Here to Stay—So IT Has No Choice but to Adapt 11

Chapter 3

Learn to Balance Productivity and Security using the Conditional Entitlement Framework 14

Chapter 4

Know the Characteristics Required to Enable Conditional Entitlement Capabilities 23

Chapter 5

Learn Best Practices for Implementing Conditional Entitlement 26

Chapter 1

Businesses Cannot Compete Without Robust Support for Mobile Devices

Desktop and laptop PCs have long been a fundamental component of productivity in the enterprise. But technology has evolved, and mobility is now a defining characteristic of the workforce. Today, mobile devices—based on iOS, Android and Windows Mobile—share the role of driving productivity.

The research makes it clear. Forbes reported that enabling the mobile workforce drives 30% better processes and 23% higher productivity¹. This has led to a **sharp increase in demand for mobile apps**. Gartner predicted that demand for enterprise mobile apps will grow five times against the development capacity in 2017².

Without robust mobile solutions, businesses will be at a severe competitive disadvantage, missing the opportunity to better serve customers, support employee productivity, and ultimately, grow revenues.

71% of enterprises regard mobility as a top priority. The risk to businesses that fall short in meeting employee mobility needs has impacts across the enterprise³.

¹ Forbes. <https://www.forbes.com/sites/danielnewman/2016/03/29/is-mobility-the-answer-to-better-employee-productivity/#2d09d0e8131c>

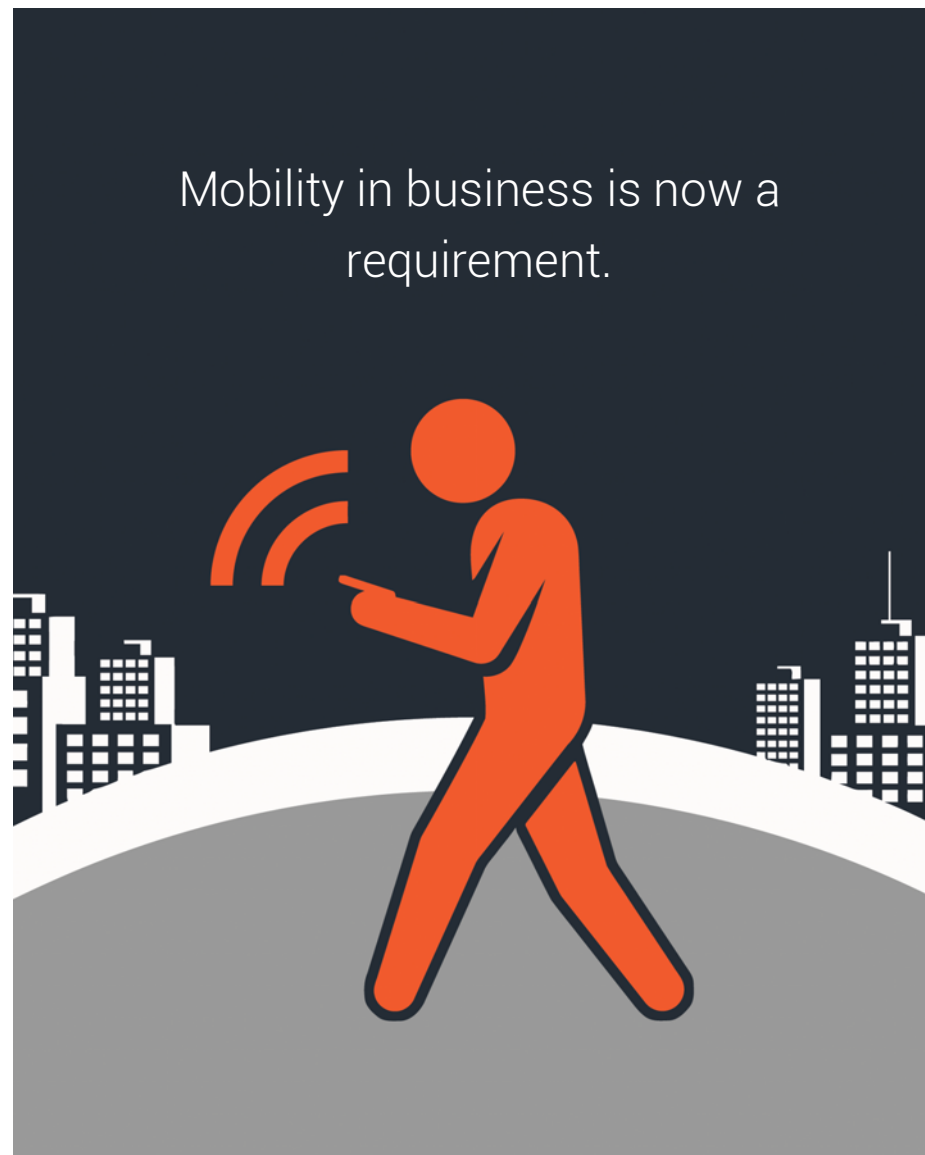
² KonstantInfo. <https://www.konstantinfo.com/blog/demand-for-enterprise-mobile-apps-will-grow-five-times-against-the-development-capacity-in-2017-gartner-report/>

³ Fingent. <https://www.fingent.com/blog/enterprise-mobility-trends-and-challenges-in-2017>

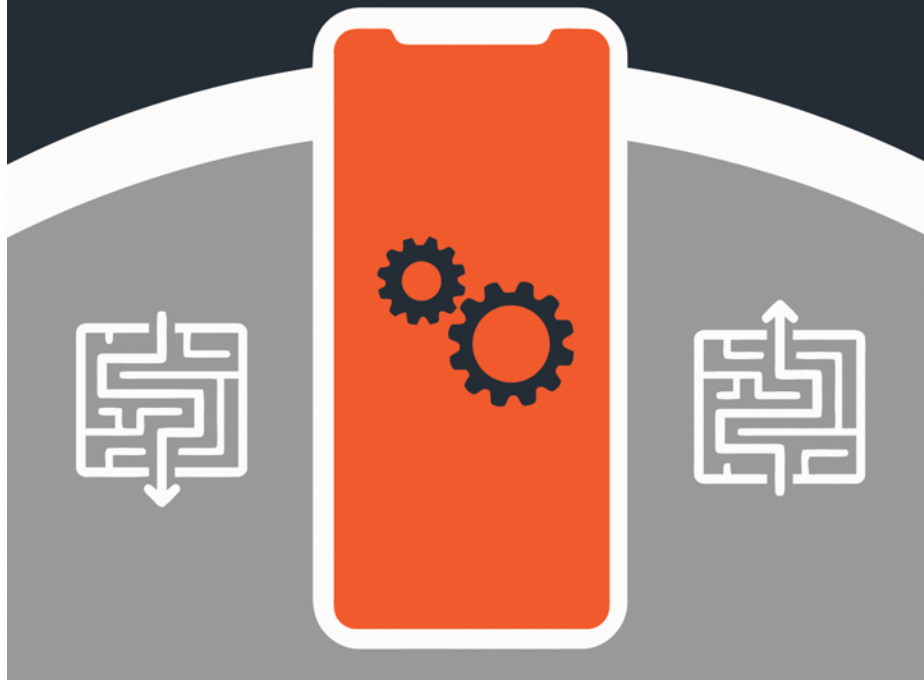
There is no doubt that enabling mobility is an absolute requirement in the enterprise, and yields tangible benefits. What is equally certain, though, is that gaining those benefits comes at a price. This is because mobile devices pose unique IT security challenges to the enterprise.

In this eBook, we will look at those challenges and identify strategies for overcoming them.

Mobility in business is now a requirement.



Mobile devices power productivity – and drive IT and security professionals crazy.



To understand why mobile poses unique challenges, it is important to realize that enterprise IT interacts with mobile devices differently than other devices. This difference requires IT to take a unique approach to managing mobile devices and the risk they represent.

Mobile devices such as smartphones are fundamentally different from other enterprise devices such as desktops and laptops in this vital respect: **IT does not administer the device—the user does.**

This is problematic for a number of reasons. For example, without administrator access to mobile devices, IT cannot actively update patches on end-user smartphones. The business has to count on the mobile device owners to do that for themselves.

A similar challenge arises regarding the apps that users put on their mobile devices. IT has long been able to monitor and manage the software that users put on their PCs. But with users administering their own mobile devices, **IT cannot prevent users from downloading potentially risky apps.**

IT's difficulties managing risks associated with mobile devices extend beyond app management. IT also cannot prevent users from connecting their mobile devices to random and unsecured Wi-Fi networks. That means users are more susceptible to rogue Wi-Fi network attacks. In spite of all of these security issues, however, users still want to connect their devices to the corporate network. That's the first part of the challenge.



With an eye toward security, it may seem like a viable option to require that users grant IT administrator rights to their mobile devices in exchange for the ability to access corporate networks and resources. But that leads to the second part of the mobile device challenge.

Users tend to have a particular perspective relating to mobile devices—a perspective that makes it much harder for IT to secure those devices. Specifically, users are highly protective of their mobile devices. Users that happily accept automated patching and application restriction on their desktops and laptops resist having those same measures being applied to their smartphones.

Moreover, when businesses do attempt to exercise direct control over user devices for security reasons, the reaction has been strong. Many experience “backlash from some employees, who are upset that their company now has the capability to remotely wipe their personal smartphone or laptop if it suspects a security breach⁴.”

Users have strong feelings about their mobile devices – which can be bad for security.



⁴ Ars Technica. <https://arstechnica.com/information-technology/2016/01/how-the-smartphone-changed-everything-or-the-rise-of-byod-in-the-workplace/>

User concerns around privacy on mobile devices are high – even for company-owned.



The issues around mobile device security are especially significant because **the number of attacks on mobile devices is growing**. One recent survey found that one in five companies reported mobile device breaches, with almost 80% acknowledging that it can be difficult even to determine that a breach has taken place⁵.

The resistance doesn't just apply when the user owns the device, and brings it into the corporate environment under a 'bring your own device' (BYOD) policy. They feel the same level of protectiveness with a device the company owns.

Mobile device users are extraordinarily sensitive to privacy issues. Similarly, users expect to have much more privacy in the way they use their mobile devices than they expect on corporate desktops and laptops.

Few users are surprised if they get a notification from IT security that unauthorized software has been detected on their laptop, and that the user needs to remove the software. But users react very differently when notified that they must remove a particular app from the mobile device.

⁵ CSO Magazine. <https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html>

The difficulty identifying breaches is particularly telling. The fact is that compromised mobile devices often go completely unnoticed. Often, **IT has no visibility at all into the state of the unmanaged or user-managed devices** accessing corporate networks.

That opens up significant opportunities for cybercriminals to perform various attacks and compromises without the user—or corporate IT—having any knowledge of the attack.



IN SUMMARY

Mobile devices are vital to increasing user productivity, but the devices are typically unmanaged, vulnerable and potentially compromised.

A growing number of these mobile devices are connecting to corporate networks and putting corporate data and resources at risk. The enterprise must act quickly and decisively to mitigate the risk.

Chapter 2

Mobile Devices Are Here to Stay—So IT Has No Choice but to Adapt

Mobile devices are ensconced as a permanent part of the corporate IT landscape, at least until technology evolves beyond them. Enterprise IT organizations must therefore find a way to mitigate the information security risk the devices pose.

One option that is pretty firmly off the table is simply locking mobile devices out of the network. That approach would inevitably create cultural backlash and reduce productivity, defeating the purpose of enabling mobility to begin with.



This is particularly true for recent entrants to the workforce. Millennials, for example, are largely digital natives that strongly favor a **mobile, collaborative working environment**⁶.

The opposite approach is equally untenable. Enterprise IT cannot simply allow users with inadequately managed devices open access to the business's network and resources. That would remove many obstacles to user productivity, but would create unacceptable risk. The ideal approach would **meet the needs of users while protecting the business's data**. More particularly, it would allow IT to simultaneously and continuously minimize mobile device risk while broadly enabling user access and productivity.



⁶ Sencomm. <http://www.sencomm.com/single-post/2017/05/17/Millennials-The-Mobile-Collaboration-Generation>



Zimperium has developed the ideal approach, which we refer to as '**conditional entitlement.**' Under conditional entitlement, IT gives mobile devices access to the specific resources their respective users need in order to be productive. However, that access is contingent on the risk profile of the device and the user, determined in real-time.

That means that devices maintain their access to the corporate network only as long as the devices meet specified standards of risk acceptability. The second that a device fails to meet the standard of risk acceptability, though, remediation measures kick in, automatically blocking potential attacks against the network.

When corrective measures have been applied and the device again meets the specified standard, the device automatically regains the access that the user needs to be productive.

For conditional entitlement to function as described, a number of technologies, processes and polices must be in place. We will describe those requirements in the following chapter.

Chapter 3

Learn to Balance Productivity and Security using the Conditional Entitlement Framework

Conditional entitlement is a framework that creates an ideal balance of productivity enablement and risk mitigation for mobile devices in the workplace.

IT and Security Benefits	Users Benefits
<ul style="list-style-type: none">• Scalability allows IT to manage massive numbers of mobile devices• Automation removes burden of hands-on mobile device management• On-device technology avoids dependence on cloud-based resources for threat detection• Machine learning enables protection from zero-day threats	<ul style="list-style-type: none">• Gain the corporate network access they need in order to achieve maximum mobile productivity• Receive the levels of privacy they expect on their mobile devices• Gain enhanced security for personal data as well as corporate data• Retain administrative control of their device

Successfully implementing conditional entitlement requires processes and policies, as well as technology with specific capabilities. In addition, conditional entitlement requires that those capabilities have specific characteristics. We'll take a closer look at the processes, policies, capabilities, and their characteristics.

Capabilities Required for Conditional Entitlement Success

The process, policy and technology requirements for a conditional entitlement framework fall into 4 categories:



Group creation and management



Dynamic, automated risk quantification/scoring



On-device monitoring of devices, networks and apps



Real-time, automated entitlement granting and revocation

Create custom groups to
enhance scalability.



The ability to create groups with similar mobile device access characteristics, i.e. sets of devices whose users have similar network access requirements, contributes to the scalability of the conditional entitlement framework. The goal is to create mobile access entitlement groups that provide access to selected resources **based on user productivity needs**.

For example, one group might consist of sales users, who require access to corporate email, a sales automation tool and product literature. Another group might be for customer service users, who require access to email and a CRM solution.

Once groups are in place, it is a simple matter to add users and devices to the appropriate mobile access entitlement groups so that the users can access the tools they need to be productive.

Quantify risk to support
automation.



Conditional entitlement requires that a business have the capability of establishing and monitoring, in an automated fashion, the relative risk that a device poses to the business's network and data.

The use of **dynamic risk scores** sets the groundwork for automation within the conditional entitlement framework. A risk score quantifies the amount of risk posed by devices and their users. A device's risk score reflects characteristics of both the device and the device's user. Higher risk scores indicate higher relative risk, and lower risk scores indicate lower relative risk.

To illustrate, a particular device's risk score might be higher or lower depending on whether the device has as an adequate password; has all current recommended operating system and app patches and updates; has non-approved apps or prohibited apps; or has specified configuration characteristics.

Similarly, a device's risk score will reflect user-related factors such as whether the designated user is an executive; is a remote worker; connects the mobile device to untrusted networks; etc.

Risk scores are dynamic. This means that an individual device's **risk score can change over time**. In fact, many of the factors comprising a risk score can change quite rapidly. Simply adding an unauthorized app to a mobile device, for example, will change that device's risk score significantly.

Here is where risk scores and mobile access entitlement groups intersect: the business must **determine acceptable risk scores for each group**. That entails defining in advance the specific score at which a device loses its membership in the group and, by extension, the network and data access that group membership provides.



Specifying these thresholds makes it possible to automate the granting and revocation of network access.

Monitor on-devices to combat zero-day and custom threats.



Among the most fundamental capabilities required of the conditional entitlement framework is the ability to monitor mobile devices on-device, in real-time, for threats and attacks.

Under conditional entitlement, the on-device agent must be capable of monitoring and analyzing relevant data relating to apps that are added to, removed from, or modified on the device.

The agent must also be able to detect any modifications to the device's operating systems. And, of course, the agent must have the ability to monitor and analyze characteristics of networks to which the device connects.

Since conditional requirement requires a device-resident agent that operates continuously and autonomously, that means that the agent **must not depend on sending data to an external cloud resource** for identification or analysis.

Instead, the agent must be capable of identifying threats independently, including **zero-day threats**. Moreover, the agent must leverage machine learning to identify threats that would otherwise be undetectable.



Grant and revoke access
automatically, in real time.

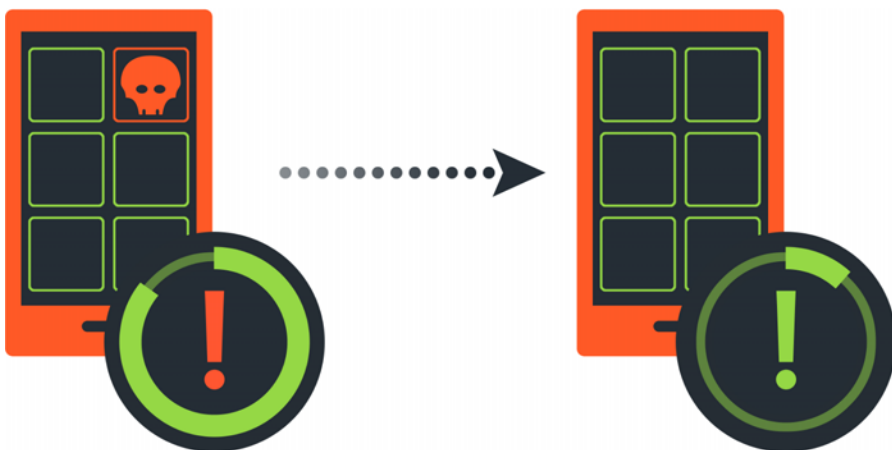


Earlier we described capabilities relating to group creation and management, dynamic risk quantification and on-device monitoring of mobile devices. Each of those capabilities combines in the conditional entitlement framework to enable automated, real-time granting and revocation of network access.

To describe this at a high level, any time a device's risk score increases and exceeds the group's risk score threshold, a pre-determined preventive measure is instituted **instantly**. For example, a salesperson with a compromised device could be automatically denied access to the company's SFA solution.

This would **block any potential attacks on corporate resources**. Alternatively, the preventive measure might be instantly wiping the contents of the device.

This automation and instant response reflects the fact that risk scores change in real-time. For example, a device might at any point become compromised or jailbroken/rooted, all of which increase the device's risk score. As we mentioned earlier, a user might add a prohibited app to their device, again increasing the device's risk score. Similarly, any time that a user connects a device to an untrusted network, the device's risk score increases.



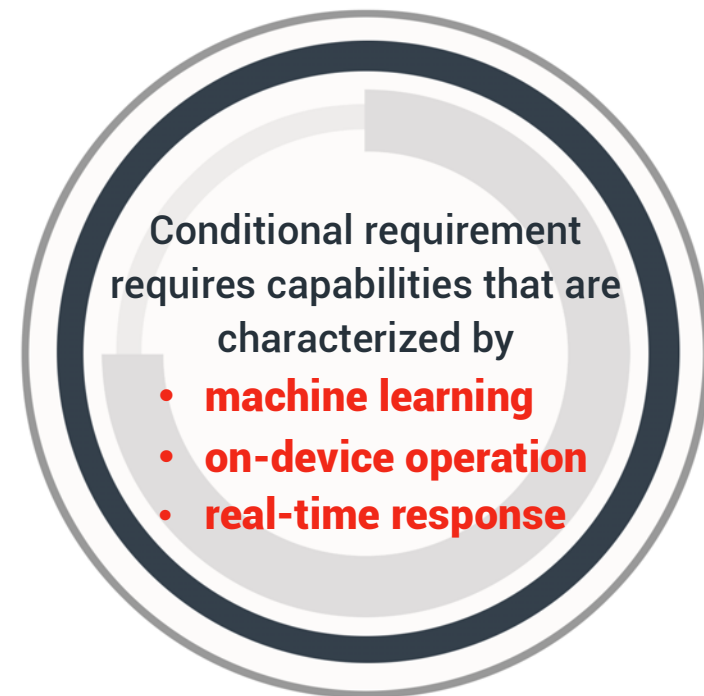
This automated change works in the reverse direction as well. Just as a user might add a prohibited app, the user might also rapidly remove that app; the on-device agent will register the change. Once the cause of the increased risk score has been remediated, the device would automatically be returned to the group of which it was originally a member. This restoration of access takes place in real-time without requiring human intervention.

Chapter 4

Know the Characteristics Required to Enable Conditional Entitlement Capabilities

Having described the capabilities required for successful implementation of the conditional entitlement framework, we will now look at the characteristics those capabilities must have.

First, conditional entitlement **must leverage an agent that is capable of machine learning**. This is because machine learning enables the agent to detect anomalous behaviors of apps and/or Wi-Fi networks. That is critical to the agent's ability to protect against zero-day attacks as well as custom attacks targeted towards specific individuals.



Next, the machine-learning agent must operate directly on the mobile device. This is for several reasons. On-device operation avoids risks and delays of cloud-sourced threat detection, and allows protection to continue **even when no network is available**.

As well, on-device protection allows the agent to forego sending potentially private information off of the device, while still detecting any changes that impact the device's risk score. By operating autonomously, the **agents avoid need for human intervention**. Given the number of mobile devices in use in typical business, requiring human intervention would simply be unworkable.



And perhaps most importantly, the on-device agent must respond in real-time to changes in the device's risk score, taking appropriate action. The real-time nature of these adjustments not only avoids potential delays that could reduce user productivity, but also proactively **blocks attacks**.

As observed earlier, real-time response by the on-device agent avoids the need for human intervention. Enterprises typically do not have enough security professionals on staff to deal with alerts and make decisions on a per-instance basis, and certainly not enough to do so in real-time.

In summary, conditional entitlement first requires a solution that enables group creation and management, dynamic, automated risk quantification, on-device monitoring of networks, apps and OSs, and real-time, automated entitlement granting and revocation. These capabilities must leverage machine learning, operate on-device and respond in real time.



Chapter 5

Learn Best Practices for Implementing Conditional Entitlement

In the preceding chapter, we described some of the basic components of a fully realized CE framework. Although full implementation is the ideal state, we recognize that most companies will make the journey to that state in steps, rather than all at one time. Here, we will note some of the **best practices** that we have identified at successive stages of the process as we have helped businesses move toward full CE. Entitlement iterates at each step.



1. Establish preliminary groups



2. Assess mobile operating systems and application risks



3. Assess device risk



4. Detect active threats



5. Perform ongoing, real-time conditional entitlement

Step 1: Establish preliminary groups

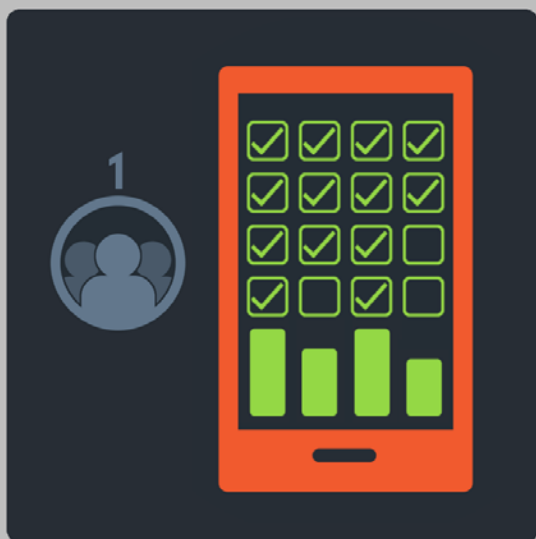


Resources: May leverage existing groups as a starting point

The first step is determining which users require protection for their mobile devices. One approach is to set up representative user group types, such as executives, sales, etc. The goal is to **identify commonalities among groups of users** from the perspective of the resources to which they require access via mobile devices.

The group creation process can begin as a net-new grouping, but many organizations simply overlay groups that are already present in mobile device management, active directory or cloud access security broker (CASB) solutions. Note that the preliminary groups need not be comprehensive; it is common to refine groups over time.

Step 2: Assess mobile operating systems and application risks



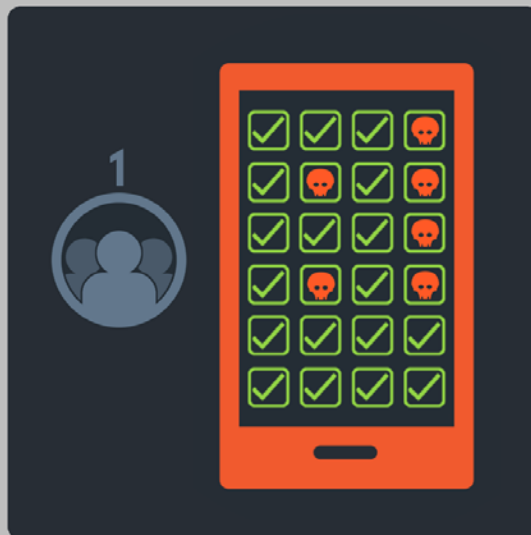
Resources: Utilizes an existing Mobile Device Management (MDM) solution

With preliminary groups in place, the next step is to **assess risk**. This entails scanning the mobile devices in each of the groups through an MDM solution to identify both mobile OS risks and application risks.

With respect to the OS, the goal is to determine whether any given device has an OS version that is dated or that lacks a known, required patch.

With respect to applications, the goal is to determine if any devices are running one or more applications that are known risks, such as apps that are known to include insecure code.

Step 3: Assess device risk

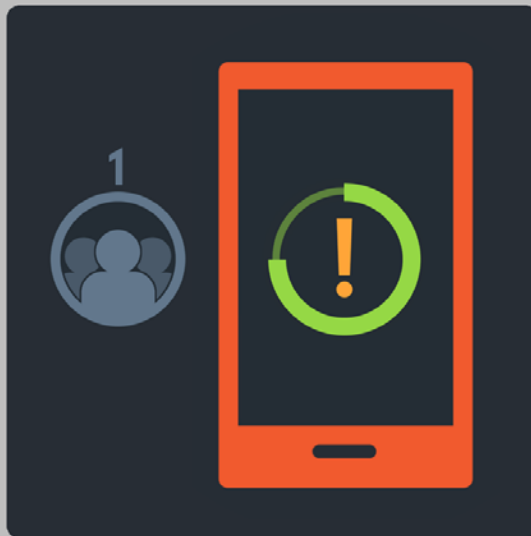


Resources: Utilizes the Zimperium
on-device agent

To gather the data required for a comprehensive risk assessment, the next step is to **identify risks** associated with the device.

This step identifies, for example, iOS devices that are jailbroken or Android devices that are rooted. This level of risk assessment requires that the device have an agent resident on it. That agent identifies device risks and passes that information on to the MDM solution.

Step 4: Detect active threats



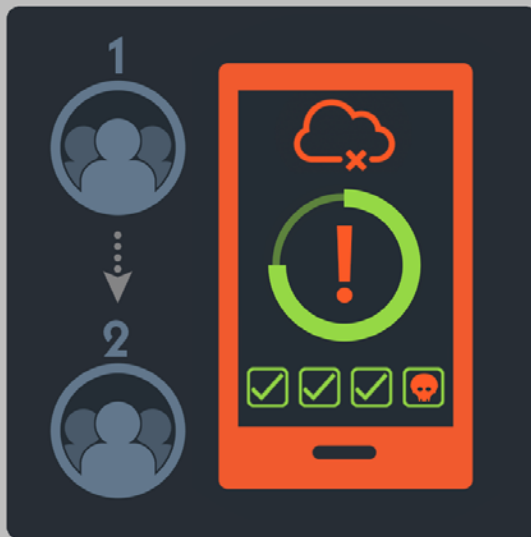
Resources: Utilizes the Zimperium on-device agent and may also use an existing MDM solution

The data from previous steps, combined with the access requirement characteristics for each entitlement group, now establishes a baseline **risk score** for each device.

The on-device agent monitors the device continuously for active threats. Devices that have active threats on them will be handled automatically according to the policy set for the group to which the device belongs.

Otherwise, as long as the device's risk score is within the established threshold for the assigned group, the user will have access through the device to the resources the user needs to be productive.

Step 5: Perform ongoing, real-time conditional entitlement



Resources: Utilizes the Zimperium on-device agent and may also use an existing MDM solution

This step is the longest-term of the steps in the process, yet in most ways requires the least active participation from IT professionals. The autonomous agents on mobile devices provide continuous protection whether or not the device is connected to a network, and protects against novel and heretofore unknown threats as well.

Over time, businesses may modify the policies for remediation actions and/or modify the access for particular groups, and may also re-assign users and their devices to different groups if the user's role in the business changes.



ZIMPERIUM[®]

If your business could benefit from maximum mobile productivity and robust mobile security, the conditional entitlement framework may be right for you. Give us a call at 844.601.6760 or visit <http://www.zimperium.com> to learn more.