MobileIron

MOBILE SECURITY AND RISK REVIEW

THIRD EDITION

EXECUTIVE SUMMARY

Welcome to the third edition of the Mobile Security and Risk Review. This bi-annual review provides IT security leaders with timely information about the mobile threat landscape and the emerging risks facing their organizations.

THIS EDITION INCLUDES:

REGIONAL DATA

from Australia, Belgium, France, Germany, Japan, the Netherlands, Spain, the United Kingdom, and the United States

INDUSTRY-SPECIFIC

data for financial services, government, and healthcare

STATISTICS

on the adoption of Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP)

THE MOST POPULAR

enterprise apps

THE TOP BLACKLISTED

mobile apps

SEVERAL AREAS SAW LITTLE CHANGE OR IMPROVEMENT OVER THE LAST SIX MONTHS:

29%

of companies had outdated policies

ONLY

55%

consistently enforced security policies

LESS THAN

5%

deployed mobile anti-malware

To help IT organizations make risk mitigation part of their mobile security routine, we developed the Security Hygiene Priority Checklist.

THE MOBILE THREAT LANDSCAPE

NEW THREATS AND TRENDS

Almost immediately after we published the second edition of this report, high profile vulnerabilities and new malware families began appearing. The Godless malware, identified in late June 2016, managed to infect an estimated 850,000 devices. Initially discovered in February 2016, Hummingbad was more widely analyzed in July, and it appears it was created by Yingmob, the group behind the YiSpectre iOS malware that made headlines last year. Hummingbad succeeded in infecting nearly 85,000,000 devices. The apparent goal of both malware families was to drive fraudulent ad revenue. However, what is more more notable — and sinister — is that they contained exploits that attempt to "root" devices over the air without the user's knowledge, thus giving attackers full control of an infected device.

"HUMMINGBAD SUCCEEDED IN INFECTING NEARLY 85M DEVICES."

Later in the summer, a series of four vulnerabilities named "QuadRooter" were identified in the Android firmware for Qualcomm baseband chipsets. The vulnerabilities affected an estimated 900,000,000 devices but were largely mitigated by the Verify Apps feature of Google Play and Android.

iOS had its highest profile and most dangerous vulnerabilities and malware to date in Trident/Pegasus, a series of three vulnerabilities that needed to be exploited together. Like Godless and Hummingbad, the Trident vulnerabilities gave attackers a method to "jailbreak" devices over the air and then install the Pegasus spyware, which was capable of intercepting virtually all communications to and from a device.

Later in the fall, Android exploits for a long-standing Linux Kernel vulnerability known as "Dirty COW" (CVE-2016-5195) began circulating, continuing a long-running trend of Open Source Software vulnerabilities that affect mobile devices and apps. Shortly after, a malware family called Gooligan compromised a million Google user accounts using apps that were downloaded from third-party app stores. Like other malware families, Gooligan would "root" infected devices and harvest authentication tokens allowing attackers to access user data from a variety of Google services.

Finally, the Adups agent compromised handsets from manufacturer BLU by transmitting call logs, SMS messages, location info, and more to servers in China. Adups positions itself as an Android firmware provisioning tool but the Android Compatibility Test Suite (CTS) has blacklisted it.

[1] Identified by Trend Micro, http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/

[2] Identified by Check Point Software Technologies, http://blog.checkpoint.com/2016/07/01/from-hummingbad-to-worse-new-in-depth-details-and-analysis-of-the-hummingbad-andriod-malware-campaign/

[3] Identified by Check Point Software Technologies, http://blog.checkpoint.com/2016/08/07/quadrooter/

[4] Identified by Lookout and Citizen Lab, https://blog.lookout.com/blog/2016/08/25/trident-pegasus/

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195

[6] Identified by Check Point Software Technologies, http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/

THE STATE OF MOBILE ENTERPRISE SECURITY

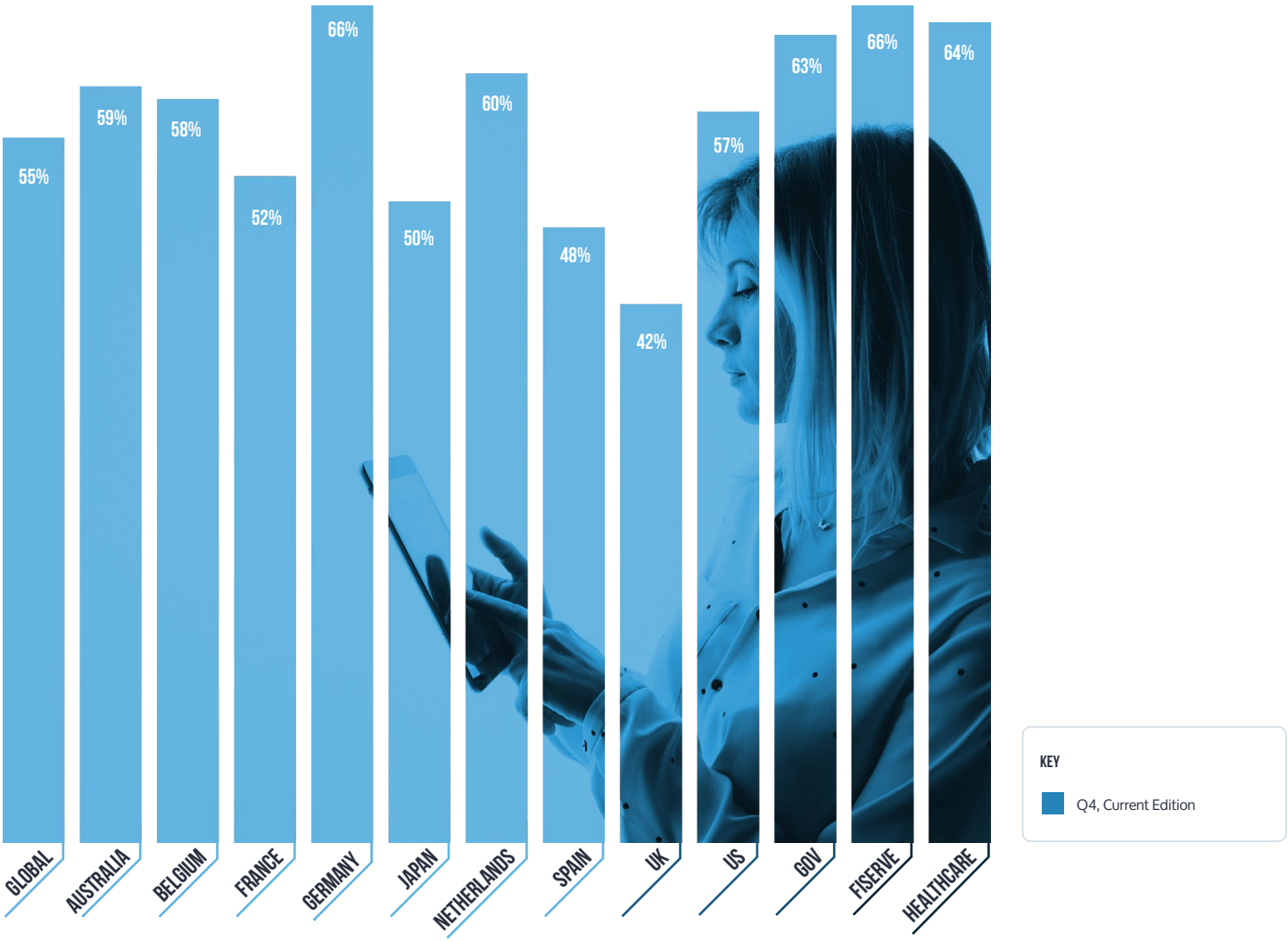
POLICY ENFORCEMENT

IT organizations spend time and resources to configure mobile security policies, but they are not always consistently enforced. In the latter part of 2016, nearly half of companies did not enforce device policies, a figure which was consistent with Q2. Germany had the highest percentage of companies enforcing security policies (66%) while the UK had the lowest (42%). Regulated industries enforced policies (64%-66%) at a rate well above the global average of 55%. Spain saw the largest increase with the number of companies enforcing policies jumping to 48% from 40%.

RECOMMENDATION:

Ensuring policy compliance is just as important as creating the policy in the first place. Organizations need to ensure they have a methodology in place to bring non-compliant devices back into compliance or prevent them from accessing resources altogether. For instance, if a device violates a passcode policy, IT can prevent the user from accessing corporate apps and data on that device until the passcode requirements are met.

PERCENT OF COMPANIES ENFORCING POLICIES



MobileIron

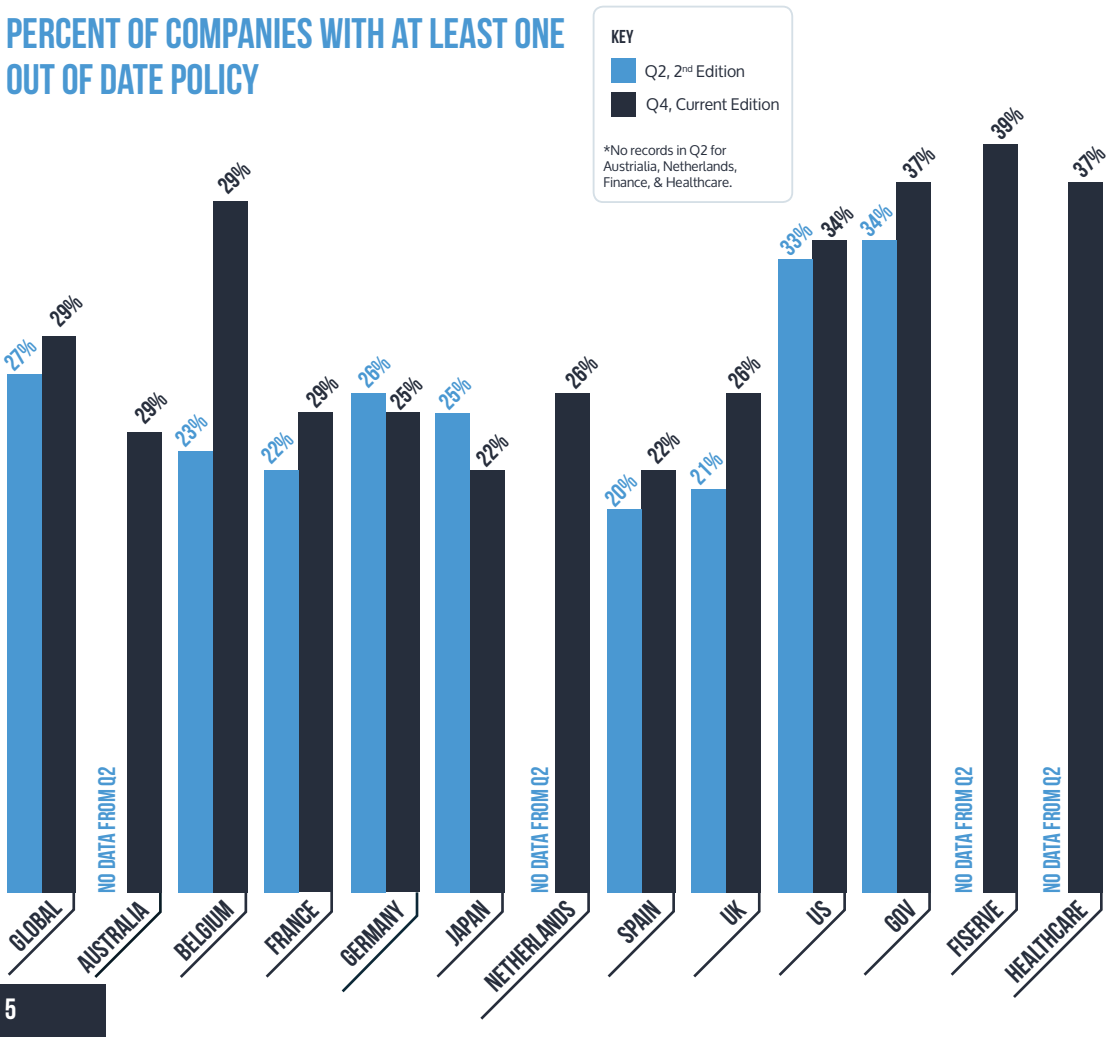
OUTDATED POLICIES

Nearly 30% of companies have at least one outdated policy, a trend that has not changed since the previous report. Out-of-date policies happen when the mobile IT administrator has changed a policy on the console but that change has not been propagated to all of the devices being managed. This is usually a result of user behavior. For example, users may have a device that they use infrequently or receive a new device and stop using their old device, resulting in scenarios where a device either connects infrequently or "fades away," preventing it from receiving updates. Most regions saw an increase in the percentage of companies with outdated policies, although Japan and the Netherlands experienced a decrease. Spain and Japan had the fewest organizations with outdated policies (both at 22%), while companies in Belgium had the most, at 36%. In fact, Belgium jumped from 23% in Q2 to 36% in Q4. The three industries had higher rates of out-of-date policies than most individual regions.

RECOMMENDATION:

Since devices with out-of-date policies don't conform to the current configuration standard, IT should configure the management platform to automatically notify users with steps to quickly update or refresh outdated policies and configurations. Depending on the security requirements, IT may consider restricting device access to enterprise resources until the issue is diagnosed and resolved.

PERCENT OF COMPANIES WITH AT LEAST ONE OUT OF DATE POLICY



"30% OF COMPANIES HAVE AT LEAST ONE OUTDATED POLICY"

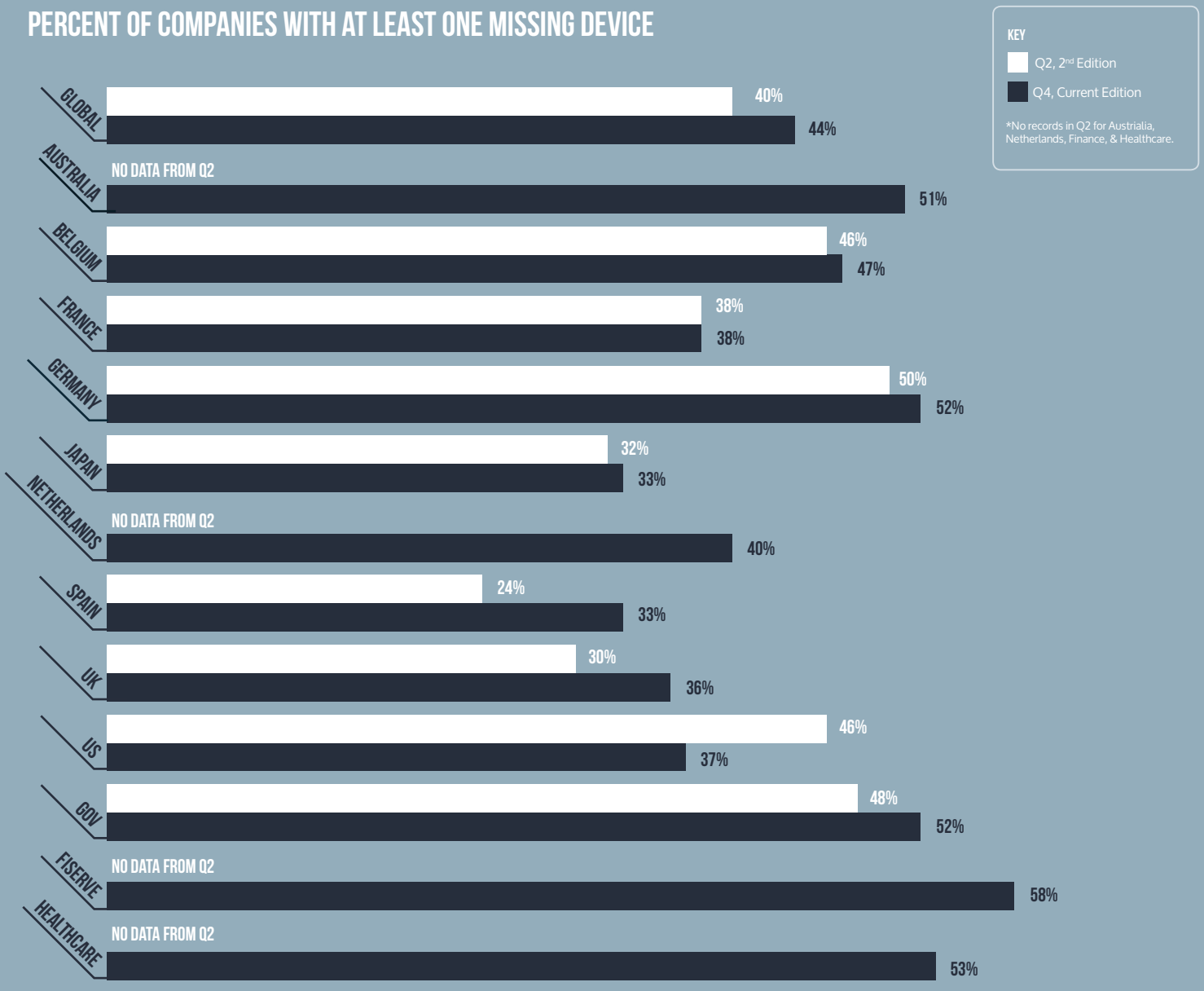
MISSING DEVICES

The percentage of companies with at least one missing device rose from 40% to 44% worldwide. This can be attributed in part to the global enterprise expansion of mobility and the greater number of mobile devices under corporate management, but the implications are extremely serious. When an enterprise device is lost or stolen, the company risks losing much more than just the cost of the hardware. If enterprise data, such as personal employee or customer data, company financials, or other confidential information, falls into the wrong hands, the organization can face tremendous legal, monetary, and reputation costs. Every region except for the Netherlands experienced an increase in the percentage of companies with at least one missing device. Spain had the largest increase in the percentage of companies with at least one lost mobile device — from 24% to 33%. More than half of all the industries had at least one company with a missing device; financial services had the highest occurrence with 58%.

RECOMMENDATION:

Enterprises will always have to deal with lost or stolen devices but data loss can be prevented. Organizations should have an EMM solution in place that allows IT to remotely wipe corporate data and apps from stolen or misplaced devices. The ability to remotely track a lost device and deny access to unauthorized users is also a critical capability to ensure data never falls into the wrong hands — even if the device itself does.

PERCENT OF COMPANIES WITH AT LEAST ONE MISSING DEVICE



MobileIron

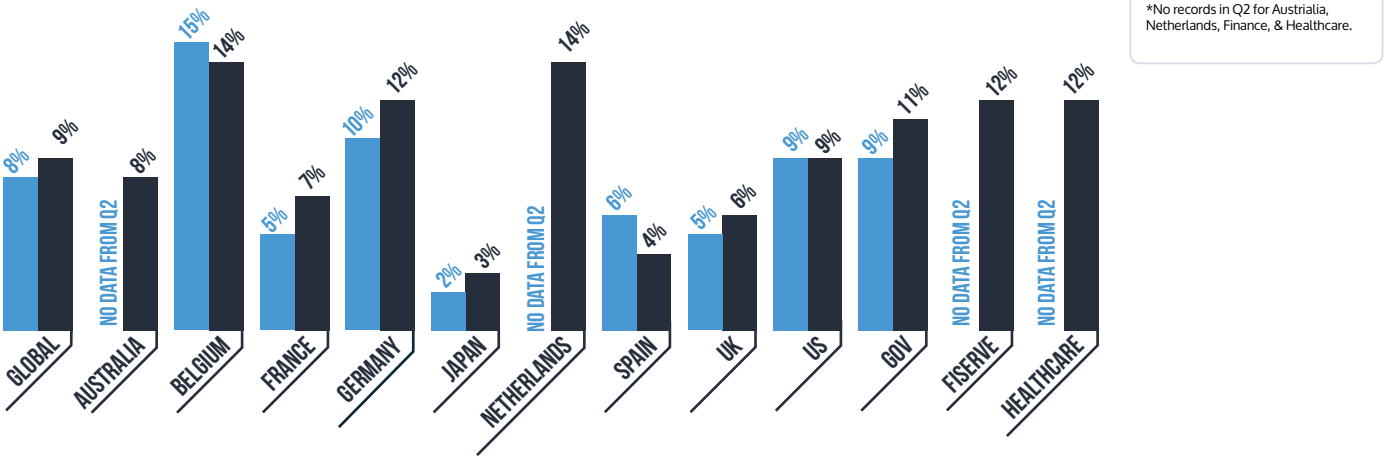
ENFORCING OPERATING SYSTEM UPDATES

OS vendors know that hackers have mobile devices and apps in their crosshairs. These threats continue to evolve rapidly, so vendors are working harder to deliver security patches in the form of OS updates to protect users and data from the latest attacks. Of course, in order to be effective, these updates must be installed. Fortunately, 2016 saw a positive trend in this direction because the number of organizations enforcing OS updates increased from 7.5% to 9%. While the numbers are still low it's good to see the increase. Security-focused industries such as financial services (12%), government (11%), and healthcare (12%) are enforcing OS updates at a greater rate than the global average of 9%. Companies in the Netherlands (14%) and Belgium (12%) were the most likely to enforce OS updates. Japanese companies (2.5%) were the least likely.

RECOMMENDATION:

Enforcing OS updates is one of the easiest and most cost-effective ways to prevent attacks from exploiting holes in older operating systems. Security patches address these specific vulnerabilities and, as a result, enforcing updated OSs provides one of the best protections against mobile threats. For very little effort and expense, patching offers a tremendous security advantage. For iOS devices, Apple's DEP Supervision simplifies this process. If a device runs iOS 9 or higher and is supervised over-the-air using Apple's DEP program, an EMM platform can trigger downloads and updates of the latest iOS release. There's simply no reason not to ensure OSs are consistently updated. Think of the 80/20 rule; organizations can reap 80% benefit with just 20% effort.

PERCENT OF COMPANIES ENFORCING OS UPDATES



MobileIron

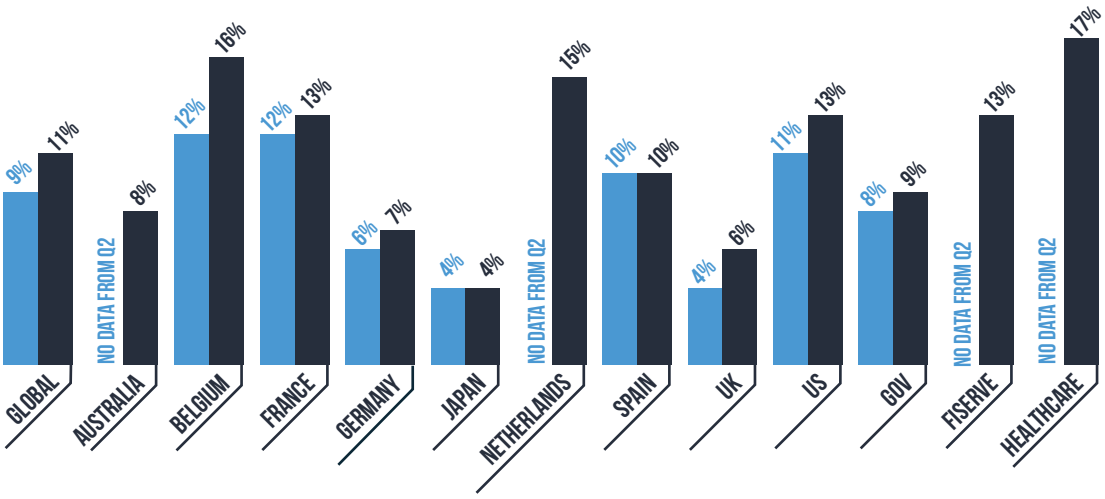
DEVICE COMPROMISE

Users are always looking to get the apps and contents they want in order to do their job — even if it sometimes means circumventing security controls. With Android, there have always been tools to root the device, whereas iOS requires "jailbreak" software to bypass certain device controls. Although Pangu, the maker of some of the most popular jailbreak tools, delivered updates on the heels of the initial release of iOS 9, Apple was quick to patch, and further Pangu updates were not available until iOS 10 was in Beta. Despite this "drought," the rate of jailbroken devices has continued to rise. The rate of compromised devices increased from 9% to 11% across all regions and industries. Financial services (13%) and healthcare (16.5%) experienced higher rates of device compromise than government (10%). Belgian companies experienced the highest increase from 12% in Q2 to 16% in Q4. At just 4%, Japanese companies had the fewest incidents of compromised devices.

RECOMMENDATION:

After patching, ensuring device compliance is the most important security precaution IT organizations can take. With the right EMM solution, IT can prevent compromised or non-compliant devices from accessing corporate resources until the issue is resolved. Preventing device compromise is critical to keeping enterprise data secure because rooted or jailbroken devices are highly vulnerable to attacks.

PERCENT OF COMPANIES WITH AT LEAST ONE COMPROMISED DEVICE



KEY

Q2, 2nd Edition

Current Numbers

*No records in Q2 for Austrialia, Netherlands, Finance, & Healthcare.

MobileIron

SECURITY HYGIENE

Mobile malware has evolved beyond data exfiltration and can now take over the whole device. Although mobile devices have many inherent security features, such as sandboxing, some types of attacks can bypass those features. These types of malware effectively take control away from the user and put it into the hands of the attacker. Despite the rise in high-profile mobile malware attacks, anti-malware adoption continues to remain flat with a global adoption rate of less than 5%.

Although some types of mobile malware attacks are difficult to propagate on a mass scale (for now), IT needs to maintain good security hygiene to protect their corporate apps and data from the next wave of mobile malware attacks. Some of the most effective security hygiene practices are easy and very cost-effective to deploy, so they should be part of every IT organization's toolkit.

PRIORITY CHECKLIST

1. CONTROL RISKY USER BEHAVIOR.

Risky employee behavior is on the rise. Globally, 11% of companies had at least one compromised device that was able to access company data in Q4, up from 9% in Q2. In addition, 44% percent of companies reported missing devices, up from 40% in Q2. To protect against unauthorized access to corporate resources, IT organizations need to improve policy enforcement and device compliance. However, when IT tries to enforce security policies, they can create additional steps that users may try to circumvent by taking unauthorized actions such as "rooting" or "jailbreaking" their devices. Heavy-handed device management is not the best approach to mobile security, but to ensure some measure of protection for enterprise services, the security state of the device and apps must be verified on a frequent basis.

2. ENSURE THE OS IS CONSISTENTLY UPDATED.

Although corporate security hygiene trends remained flat between Q2 and Q4 2016, IT organizations did increase their enforcement of OS updates to ensure critical security patches were deployed on mobile enterprise devices. Ensuring that OS updates are applied is a low-effort, high-payoff way to ensure that devices are protected against ongoing security threats. Patching is one of the easiest and most essential security hygiene practices, which may explain why globally, 9% of companies enforced patching in Q4, up from 7% in Q2. The reason for this extremely low percentage may be that many companies have not yet operationalized this standard security practice for their mobile deployments. Organizations should require that [device] operating systems be no older than the second most current version, including minor versions and patches. For example, if the latest version of Apple iOS is 10.2, no devices running a version older than iOS 10.1.1 would be allowed to access corporate resources. The update rollout and schedule for Android is slightly different and as such the approach to monitoring Android versions may differ. As a rule of thumb, existing Android versions continue to receive security updates for a period of at least three years from their initial release, while new major releases are made available annually. At the time of writing, Android v4.4.x, Android 5.x, and Android 6.0 were all widespread; Android v7.0 was also generally available. Android has also moved to a monthly security patch release cycle. Despite the greater variations in OS version and patch levels, the same basic N-1 logic applies: for each Android version in an environment, devices should be at the latest available major/ minor version and not more than one month out-of-date on the security patch level. For example, devices should be running v4.4.4, v5.1.1, v6.0.1, or v7.1.1 and have a Security Patch Level no older than 2016-12-01 or 2016-12-05. It should be noted that Google does not currently provide security updates for Android versions older than v4.4.4, so additional measures may need to be taken to ensure the integrity of the device and that data on the device is sufficiently protected .

[7] Source: https://developer.android.com/about/dashboards/index.html

3. DENY ACCESS FROM COMPROMISED DEVICES.

Compromised operating systems have long been a prime target for mobile attackers, as they bypass important security features, making them easier targets. We now see an emerging trend of mobile malware incorporating exploits to compromise the OS without the user being aware of the compromise. As this trend continues, the risk from these vulnerabilities changes from isolated cases driven by user action to broader attacks triggered by more organized threat actors. For this current period, companies with at least one compromised device attempting to access corporate data increased from 9% to 11% globally. Organizations need to ensure they are monitoring for compromised devices and blocking access to all enterprise resources from these devices.

4. PREVENT UNAUTHORIZED CONFIGURATION AND APP MODIFICATIONS.

Many mobile security threats originate with social engineering and techniques designed to trick users into installing malicious configurations, software, or both. These threats often originate in unauthorized sources such as websites or third-party app stores. Organizations should control sideloaded configurations and apps by monitoring for "unmanaged" Configuration and Provisioning Profiles on iOS; for Android, disabling "Allow Untrusted Sources" as well as monitoring app permissions (e.g., blacklisting apps that request the Device Admin permission) will reduce risk of unauthorized changes to configurations and apps. However, the latest research shows that while most organizations spent time creating policies, nearly half of the companies surveyed did not take an action such as blocking network access. This may be because in many low-risk scenarios low-risk scenarios the action is to alert the employee or IT administrator in order to request manual remediation. However, manual remediation is not immediate nor does it require the employee take corrective action. Therefore, our recommendation is to automate policy enforcement. Organizations will need to consistently update policies to protect against future mobile attacks.

VPP AND DEP ADOPTION

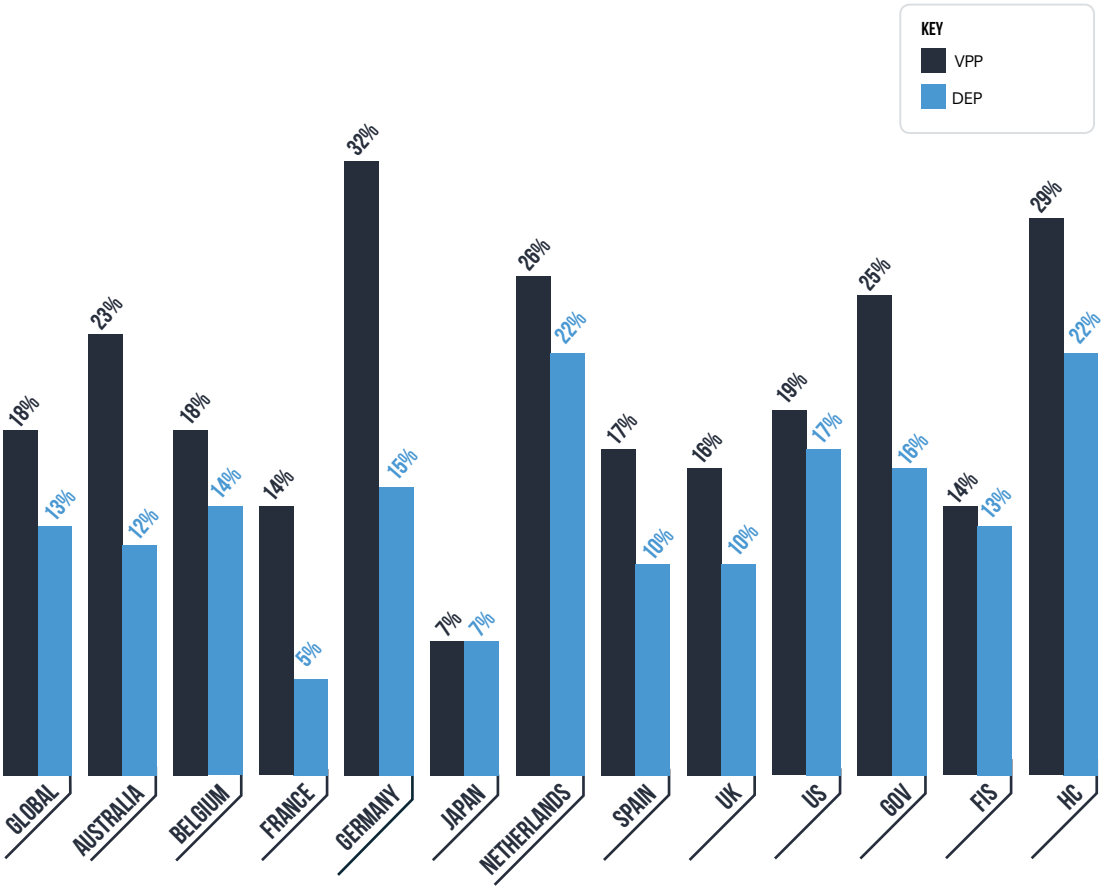
For the first time, this report measured the global adoption of Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP).

VPP was launched in 2011 and it gained momentum with the introduction of the DEP corporate fleet program because, together, they give organizations the tools to manage iOS device fleets and the apps that run on them.

Nearly one in five organizations is currently using VPP to streamline enterprise app deployment to users. The rate is significantly higher in healthcare (29%) and government (25%). At 32%, Germany had the most organizations using VPP. At just 7%, Japanese companies had the lowest use of VPP.

Organizations are also increasing their adoption of DEP because it gives them more control over their mobile fleets. With DEP, enterprises can enforce tighter restrictions on corporate-owned, supervised devices. For instance, tablets can be restricted to single-app kiosk mode to prevent users from downloading unauthorized apps. Currently, nearly 13% of organizations around the world are using DEP. Companies in the Netherlands recorded the highest use of DEP at 22%, while their counterparts in France had the lowest at just 5%. Nearly one-quarter (22%) of healthcare organizations are using DEP today.

PERCENT OF COMPANIES USING VPP AND DEP



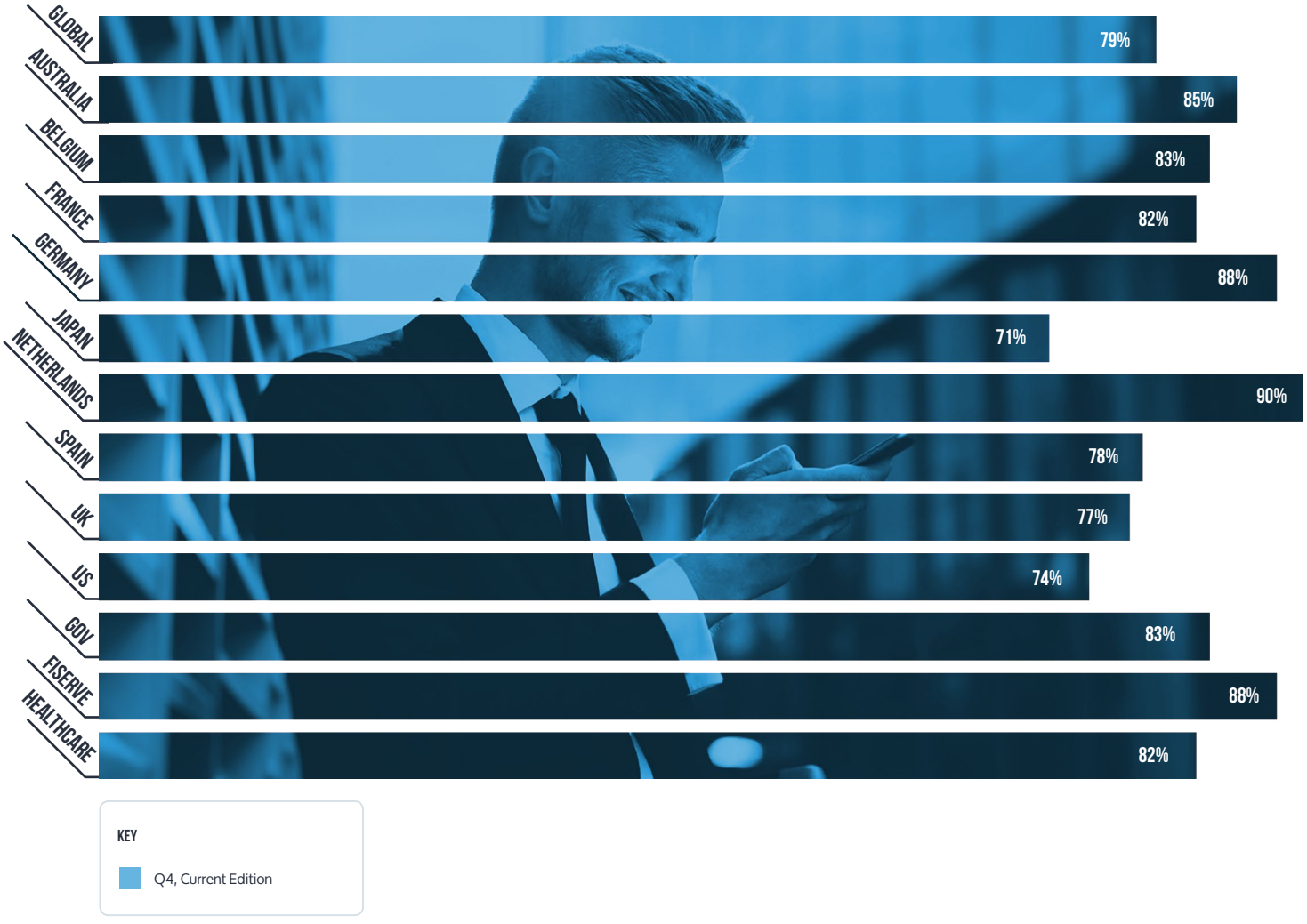
MobileIron

STATE OF ENTERPRISE APPS

FOUR OUT OF FIVE ORGANIZATIONS HAVE 10 APPS OR MORE

MobileIron's global customer base has installed more than 70,000 managed enterprise apps, and nearly 80% of these organizations have more than 10 enterprise apps installed. Organizations in the Netherlands (90%) are most likely to have an average of more than 10 apps installed, while organizations in Japan (71%) are the least likely. The rate is also high in the vertical industries. Among financial services organizations 88% were likely to have more than 10 apps installed, with government (83%) and healthcare (82%) not far behind.

PERCENT OF COMPANIES WITH MORE THAN 10 APPS INSTALLED



MobileIron

TOP INSTALLED APPS

	GLOBAL	AUSTRALIA	FRANCE	GERMANY	JAPAN	BELGIUM	NETHERLANDS
1	Webex	Anyconnect	File Manager	Arm	Google Maps	Touchdown	Chrome
2	Anyconnect	LinkedIn	WIT Mobile	Keynote	Webex	Pulse Secure	Whatsapp
3	Concur	Edge	Canet	Numbers	Chrome	Webex	Word
4	Adobe Acrobat	VIP Access	MA Banque	Pages	Salesforce	Pages	Adobe Acrobat
5	Pulse Secure	Entertain	Annuaire	Adobe Acrobat	Smart Catalog	ECAS Mobile	QuickSupport for Samsung
6	Keynote	Telstra 24x7	Ma Carte	Excel	Web Directory	Evernote	YouTube
7	Numbers	Chrome	Google Maps	DB Navigator	box	Word	Excel
8	Pages	Google Maps	Les Infos	Word	Jabber	Excel	LinkedIn
9	Google Maps	Citrix Receiver	Adobe Acrobat	Companion	Word	Salesforce	Google Maps
10	Word	Concur	Smart TPE	Webex	Powerpoint	File Manager	Evernote

	SPAIN	UK	US	GOV	FISERVE	HEALTHCARE
1	Numbers	Chrome	Webex	Adobe Acrobat	Webex	Webex
2	Keynote	Google Maps	Concur	Pages	Ma Banque	Concur
3	iMovie	Adobe Acrobat	AnyConnect	AnyConnect	Canet	Pulse Secure
4	Alertas	Word	Adobe Acrobat	Numbers	RSA SecureID Software Token	AnyConnect
5	Whatsapp	Excel	Pulse Secure	Keynote	Adobe Acrobat	Keynote
6	Pulse Secure	Keynote	Jabber	Pulse Secure	Pulse Secure	Excel
7	Citrix Receiver	Gmail	box	Google Maps	Google Maps	Word
8	Kaspersky Endpoint Security	YouTube	Keynote	YouTube	Citrix Reciever	Powerpoint
9	Microstrategy	Nervecentre	Numbers	RSA SecureID Software Token	Any Connect	box
10	YouTube	Pages	Pages	Evernote	Word	Numbers

TOP BLACKLISTED APPS

The list of top blacklisted apps might be considered a badge of honor for highly popular consumer apps that have gotten the attention of IT security teams. Due to their widespread use and the perceived risk they may pose, organizations around the world are increasingly blocking apps such as WhatsApp, Netflix, and Outlook in addition to longstanding ones such as Angry Birds and Twitter. For the first time, companies in Australia blocked Tinder. Other apps such as Evernote, OneDrive, Box, and Line dropped off the list, in part due to their increasing use for enterprise business.

TOP BLACKLISTED APPS

	GLOBAL	AUSTRALIA	BELGIUM	FRANCE	GERMANY	JAPAN	NETHERLANDS
1	Angry Birds	Angry Birds	Facebook	Facebook	Dropbox	Line	Dropbox
2	Dropbox	Facebook	Dropbox	Angry Birds	Facebook	Dropbox	CamScanner
3	Facebook	Hipster Pawslez	WeChat	Dropbox	Whatsapp	Evernote	Cydia
4	Whatsapp	path	Angry Birds	Twitter	Angry Birds	Skype	Winzip
5	Twitter	Dropbox	PDF Reader	Outlook	OneDrive	Team Viewer	CamCard
6	Skype	Twitter	Winzip	Cydia	Outlook	Twitter	OPlayer
7	OneDrive	2Day FM	Google Drive	Candy Crush	Google Drive	One Drive	WeChat
8	Outlook	Pandora	CamCard	YouTube	Twitter	Facebook	Outlook
9	Netflix	xCon	Mercury	Clash of Clans	Sugarsync	Viber	PDF Reader
10	Google Drive	Google Drive	Twitter	Skype	Skype	Tunnelbear	Mobile Ticket

	SPAIN	UK	US	GOV	HEALTHCARE	FISERVE
1	Angry Birds	Dropbox	Angry Birds	Angry Birds	Angry Birds	Dropbox
2	Facebook	Angry Birds	Dropbox	Dropbox	Dropbox	Angry Birds
3	Twitter	Facebook	Facebook	Facebook	Facebook	Facebook
4	YouTube	Twitter	Netflix	Outlook	Netflix	Outlook
5	Pokemon GO	Whatsapp	Pandora	Whatsapp	Twitter	box
6	Cydia	box	Outlook	box	Outlook	Twitter
7	Viber	Outlook	box	Cydia	Skype	Instagram
8	Soduku	OneDrive	Twitter	Snapchat	Google Drive	Sugarsync
9	Powerpoint	Skype	YouTube	vShare App Market	OneDrive	box
10	LINE	SugarSync	OneDrive	Google Drive	Whatsapp	YouTube

INDUSTRY SPOTLIGHT: GOVERNMENT

Government organizations around the world are often hamstrung by bureaucracy and funding challenges. They frequently struggle to hire and maintain people, deploy new technologies, and keep them updated in a timely manner. Despite these obstacles, government IT organizations are overall maintaining good security hygiene practices. However, government users are more complacent and their lack of vigilance can put government data at risk on mobile devices.

SECURITY HYGIENE PRACTICES:

ENFORCING OS UPDATES IS UP FROM 9% IN Q2 TO

11%

IN Q4

25%

USE VPP

16%

USE DEP

63%

ENFORCED POLICIES IN Q4, UP FROM 61% IN Q2

37%

HAD OUTDATED POLICIES IN Q4, UP FROM 34% IN Q2

75%

HAD MORE THAN ONE SECURITY POLICY IN PLACE IN Q4, FLAT FROM Q2

43%

HAD MORE THAN ONE APPCONNECT POLICY IN PLACE IN Q4, DOWN FROM 45% IN Q2

RISKY USER BEHAVIOR:

9%

HAD A COMPROMISED DEVICE ACCESSING CORPORATE DATA IN Q4, UP FROM 8% IN Q2

52%

HAD MISSING DEVICES IN Q4, UP FROM 48% IN Q2

INDUSTRY SPOTLIGHT: HEALTHCARE

DEP makes device management compulsory, so it's ideal for enforcing security policies on corporate-owned devices. Healthcare organizations have started using DEP and VPP to protect highly confidential patient data and meet compliance regulations by automatically deploying proactive security controls. While the use of DEP and VPP is a positive security measure, healthcare organizations can improve other areas of security hygiene and risky user behavior.

SECURITY HYGIENE PRACTICES:

HEALTHCARE COMPANIES ARE THE MOST LIKELY OF THE VERTICALS MEASURED TO USE DEP (22%) AND THE SECOND-MOST LIKELY TO USE VPP (28%)

28%
VPP

22%
DEP

BUT ONLY

64%
ENFORCE POLICIES,

11%
ENFORCE OS UPDATES

37%
HAD OUTDATED POLICIES

77%
HAD MORE THAN ONE SECURITY POLICY

41%
HAD MORE THAN ONE APPCONNECT POLICY

RISKY USER BEHAVIOR:

17%
OF HEALTHCARE ORGANIZATIONS HAD AT LEAST ONE COMPROMISED DEVICE ACCESSING CORPORATE DATA — THE HIGHEST OUT OF ALL THE VERTICALS MEASURED

58%
REPORTED MISSING DEVICES

INDUSTRY SPOTLIGHT: FINANCIAL SERVICES

Financial services companies had the lowest DEP and VPP adoption rates. Given the regulatory requirements in this industry, DEP and VPP offer many advantages for achieving compliance. These organizations can also improve in other areas of security hygiene and risky user behavior.

SECURITY HYGIENE PRACTICES:

ONLY
14%
USE VPP

AND
13.%
USE DEP

THIS ADOPTION RATE IS LOWER THAN BOTH HEALTHCARE AND GOVERNMENT RATES

66%
ENFORCE POLICIES

BUT ONLY
11%
ENFORCE OS UPDATES

39%
HAD OUTDATED POLICIES

78%
HAD MORE THAN ONE SECURITY POLICY

49%
HAD MORE THAN ONE APPCONNECT POLICY

RISKY USER BEHAVIOR:

13%
HAD AT LEAST ONE COMPROMISED DEVICE ACCESSING CORPORATE DATA

58%
HAD MISSING DEVICES

SUMMARY AND RECOMMENDATIONS

In light of these findings, organizations should consider taking the following steps to improve their overall mobile security posture:

1. CONTROL RISKY USER BEHAVIOR.

Ensuring device compliance is critical to preventing unauthorized devices from accessing critical corporate resources. In addition, services such as web apps, enterprise Wi-Fi, and VPN will likely require additional configuration and policy enforcement to prevent access from unauthorized devices.

2. REQUIRE OS UPDATES.

Organizations should require that operating systems be no older than the second most current version, including minor versions and patches. For example, if the latest version of Apple iOS is 10.2, no devices running a version older than iOS 10.1.1 would be allowed to access corporate resources. The update rollout and schedule for Android is slightly different and as such the approach to monitoring Android versions may differ.

3. DENY ACCESS FROM COMPROMISED OPERATING SYSTEMS.

Organizations need to do more than just create policies. They need to consistently enforce and update security policies on every device accessing corporate resources. Devices that don't comply with current policy should either be barred from access or required to follow steps to quickly come back into compliance.

4. PREVENT OR MONITOR CONFIGURATION AND APP SIDELOADING.

Organizations should use management tools to ensure users cannot manually install configuration or provisioning profiles because this will prevent dangerous habits, such as tapping on a link to install certificates or in-house apps, that can be exploited by attackers. Organizations should also use their management tools to ensure users have not bypassed OS protections that prevent sideloading, such as enabling "untrusted" sources in Android or allowing unknown provisioning profiles to be trusted in iOS.

5. TAKE ADVANTAGE OF SECURITY AND MANAGEMENT CAPABILITIES OFFERED BY ENTERPRISE OWNERSHIP PROGRAMS.

As the enterprise use cases have become more common, mobile operating system vendors have begun offering more tools to improve the "user experience" for enterprises. The Apple Device Enrollment Program (DEP) and Google Android Device Owner Mode provide organizations with additional capabilities for securing their fleets of mobile devices, including mandatory EMM enrollment, and additional restrictions and configuration options.

METHODOLOGY

This data in this report is normalized, anonymous data collected between July 1 and December 31, 2016. We believe this is the largest set of enterprise-specific mobile device security analytics across the three most popular mobile operating systems: Android, iOS, and Windows.