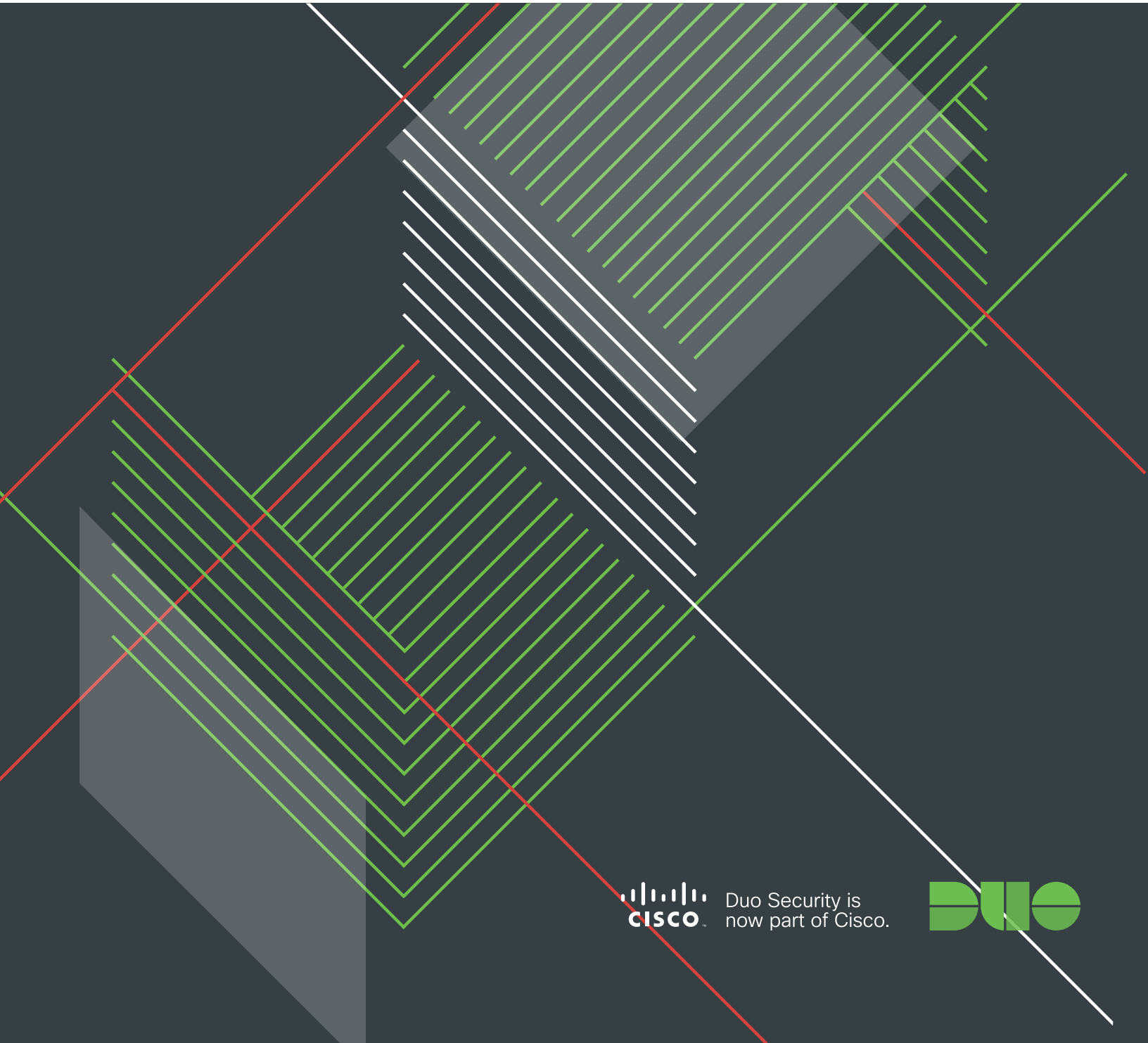
The 2017 Duo

Trusted Access Report

The Current State of Enterprise Endpoint Security



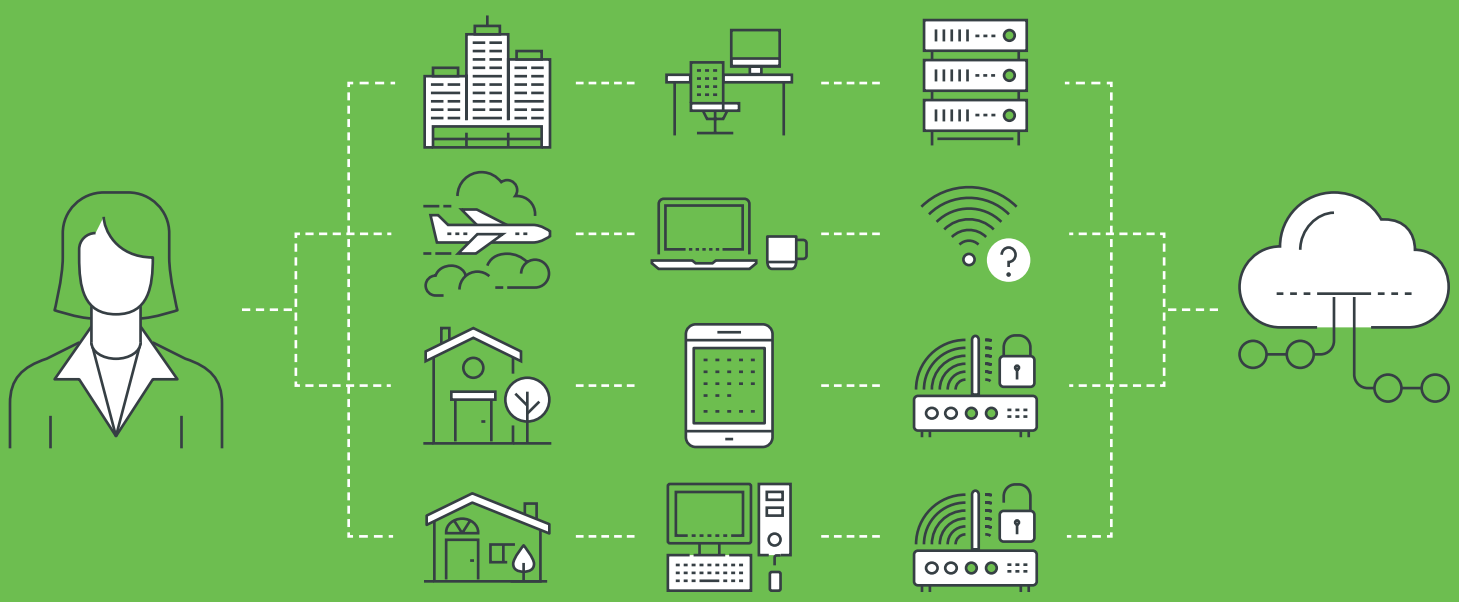
This page intentionally left blank.

AUTHOR
THU T. PHAM

RESEARCHER
KYLE LADY

DESIGNER
CHELSEA LEWIS

PRODUCER
PETER BAKER



The Evolution of Enterprise Security

Networking has expanded over the past three decades as technology evolved to increasingly rely on the Internet, cloud services and mobile devices, introducing more complexity into enterprise information technology.

Traditional enterprise security models were built around protecting a trusted, internal network from external threats by using security solutions like firewalls. Enterprise data was safely contained within the perimeter of this secure environment, defined by physical boundaries.

The enterprise perimeter has been redefined by new networking models – and with new tech, come new security risks.

But that perimeter has been redefined, or removed altogether, with new tech emerging to meet consumer demand for mobility, flexibility and usability. In turn, that consumer demand has blurred the lines between personal tech and the workplace.

Modern employees are now untethered ones; often working outside of the office walls using personal laptops, tablets and smartphones to connect to work applications via different networks – one day, from a coffee shop; the next day, from their homes.

As a result, enterprises no longer have distinct boundaries defined by inside and outside the firewall. Information sharing and processing requires access from many different endpoints, networks and users. And with these new networking models and new tech come new security risks.

Administrators of modern environments are faced with new security challenges as they attempt to secure hundreds and thousands of modern employees' access to the new enterprise network:

- **Personal, unmanaged devices** used by employees to connect to company applications and networks may introduce new risks, as admins lack insight into their software, device and security health
- **Remote access** to enterprise applications is convenient for both users and online criminals that target user credentials and exploit known vulnerabilities targeting out-of-date devices to gain access to enterprise data
- **The adoption of cloud-based services** results in the dissolution of the traditional enterprise perimeter; requiring security that focuses on protecting access to the data itself, rather than building walls around the systems upon which that data resides

Securing the new enterprise network requires a new approach – one that focuses on securing user and device access to applications and data.

Trusted Acces

To protect access to company data, enterprises must find a way to:

Verify the identity of the user

Is the user really who they say they are, and not an attacker that has stolen their username and password to access your enterprise environment?

How can you truly verify their identity using the most secure methods?

Verify the security health of a device

Is the device company-issued or managed by your IT department, or is it your employee's personal laptop, tablet or phone?

Is the device running the latest software that has patched known vulnerabilities?

Does the device have security features enabled or disabled?

ss

IN ORDER TO:

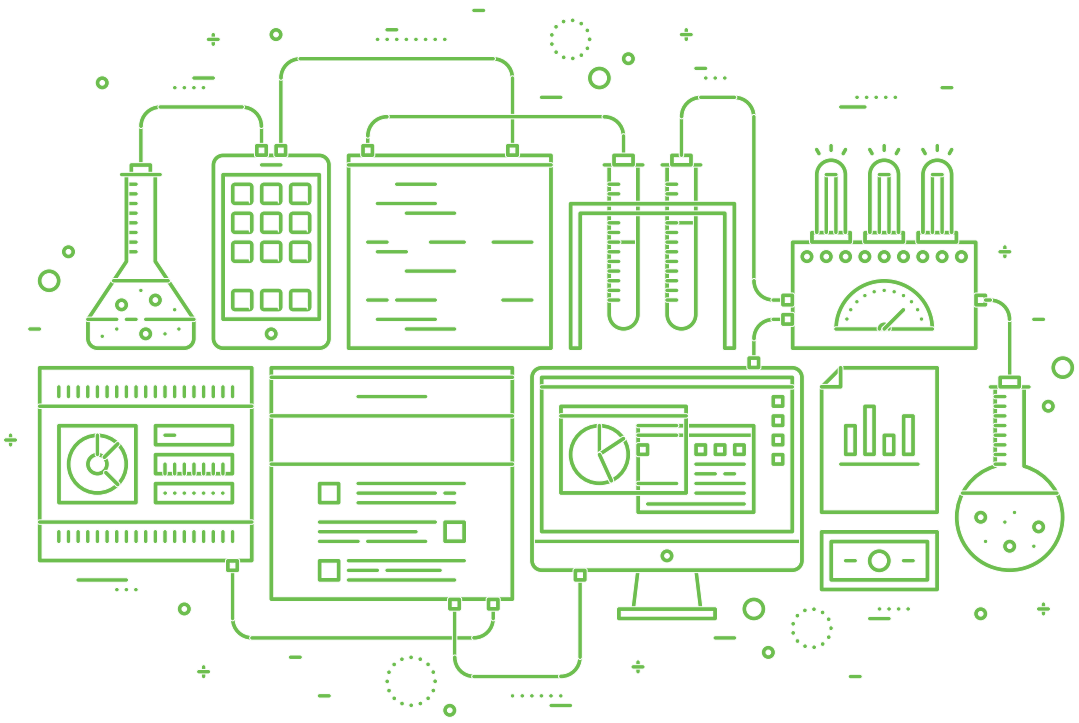
Grant secure, simple access to work applications.

Does the employee have access to only the applications needed to do their job?

Based on the security health of the device used, does the employee have the appropriate level of access to certain applications and data?

Can they securely log into applications, from anywhere, without adding more friction to their workflow?

This new approach to security requires the combination of a number of factors before access is granted – including indicators of trusted devices and indicators of a trusted user.



We looked at key indicators of device security health of 4.6 million endpoints.

Methodology: Duo's Data Analysis

To give you insight into the current security health of devices used to access the enterprise environment, we've analyzed our rich dataset of customers from every industry and size, including:

200 million+
Authentications per month

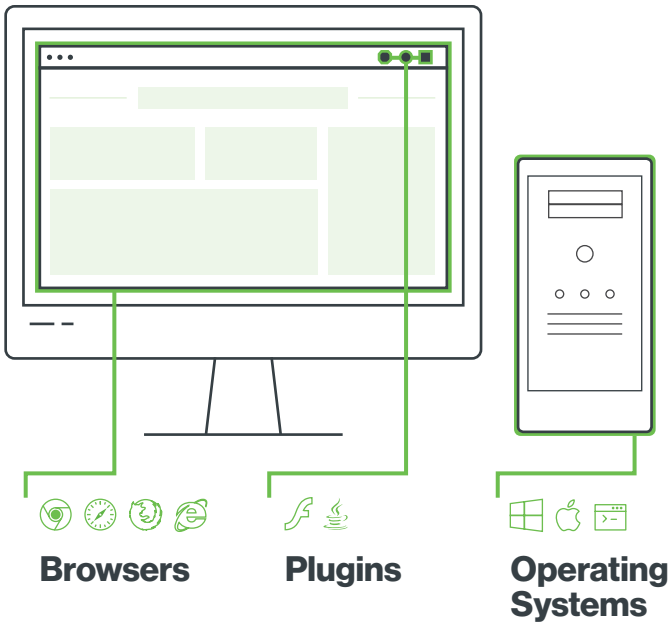
3.5 million
Mobile phones used for authentication

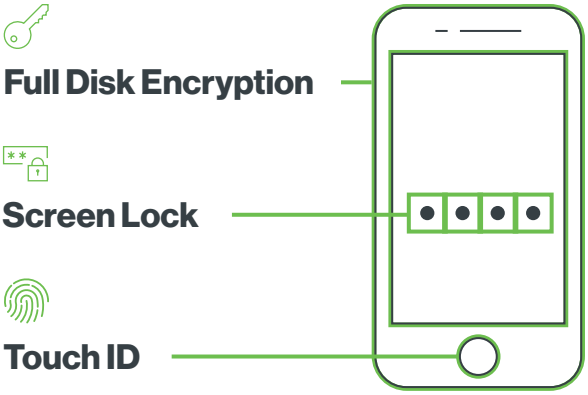
4.6 million
Endpoints used by businesses worldwide

The majority of the data analyzed in this report covers business use cases from the North American and Western European regions. Nearly three million users securely access thousands of applications and services across the globe with the help of Duo's **Trusted Access** platform.

Device Security Health, Explained

We looked at key indicators of device security health of 4.6 million endpoints across many different industries and geographic regions. These key indicators include **out-of-date operating systems, browsers and plugins** that make endpoints more susceptible to vulnerabilities, and potentially risky points of access to your enterprise applications.





We also analyzed which mobile devices have security features enabled, such as **full disk encryption, screen lock and Touch ID/fingerprint authentication**.

Finally, we reveal insights gleaned from our data from simulated phishing campaigns conducted by enterprises using **Duo's phishing tool**.

At a Glance:

Key Findings

A high-level overview of the top findings from our data research and analysis

Overall Device Security Health

Things are looking up for Microsoft operating systems (OS) – 31% of endpoints are running the latest OS version, Windows 10, compared to last year's 15%. Enterprises are slowly migrating to the most up-to-date and secure version two years after its release.

However, 13% of endpoints are browsing dangerously on an unsupported version of the Internet Explorer browser that is no longer receiving security updates.

The percentage of endpoints running an out-of-date version of Flash has increased from 42% in 2016 to 53% in 2017, meaning more than half of enterprise endpoints are not protected against the latest known vulnerabilities.

We also found that 21% of endpoints are running version 24.0.0.194 of Flash, which has 11 listed critical vulnerabilities published in February 2017.

U.K. & EMEA

Compared to North America, EMEA (Europe, Middle East and Africa) countries are slightly more up to date.

In EMEA, 40% of endpoints were running the latest Windows 10, compared to 31% in North America. In the U.K., 37% of endpoints were running Windows 10.

The U.K. is also slightly more up to date when compared to the global average – except for when it comes to Flash.

By Industry

The technology industry has the highest number of endpoints running the latest Windows 10 operating system (OS), while machinery and healthcare have the lowest percentage of endpoints on the latest version – meaning these industries may be susceptible to vulnerabilities affecting older, unpatched OSs.

Fifty-seven percent of environmental endpoints are running an up-to-date macOS version, while 76% of state and local government's endpoints are running a two-year-old version of macOS.

Biotech comes in last for mobile security features, with the lowest amount of mobile devices with screen lock or encryption enabled, meaning they lack mobile device security. Tech (consumer web) has the highest adoption of Touch ID/fingerprint authentication and encrypted phones, meaning they have the most secure mobile devices compared to other industries.

Healthcare

The percent of healthcare endpoints running Windows XP has increased from 2% to 3%, which is higher than the 1% of overall endpoints. This is troubling to see, as Microsoft ended security support for Windows XP in 2014, and running the OS could run afoul of HIPAA.

Mobile Security Health

Twenty-seven percent of Android phones are running the latest major OS version, and 73% of iPhones were running the latest major version, iOS 10 and above. Monthly patches for Android devices do protect against known vulnerabilities, but each new major OS version also adds security features to proactively protect users. Both are important pieces that help complete the security puzzle.

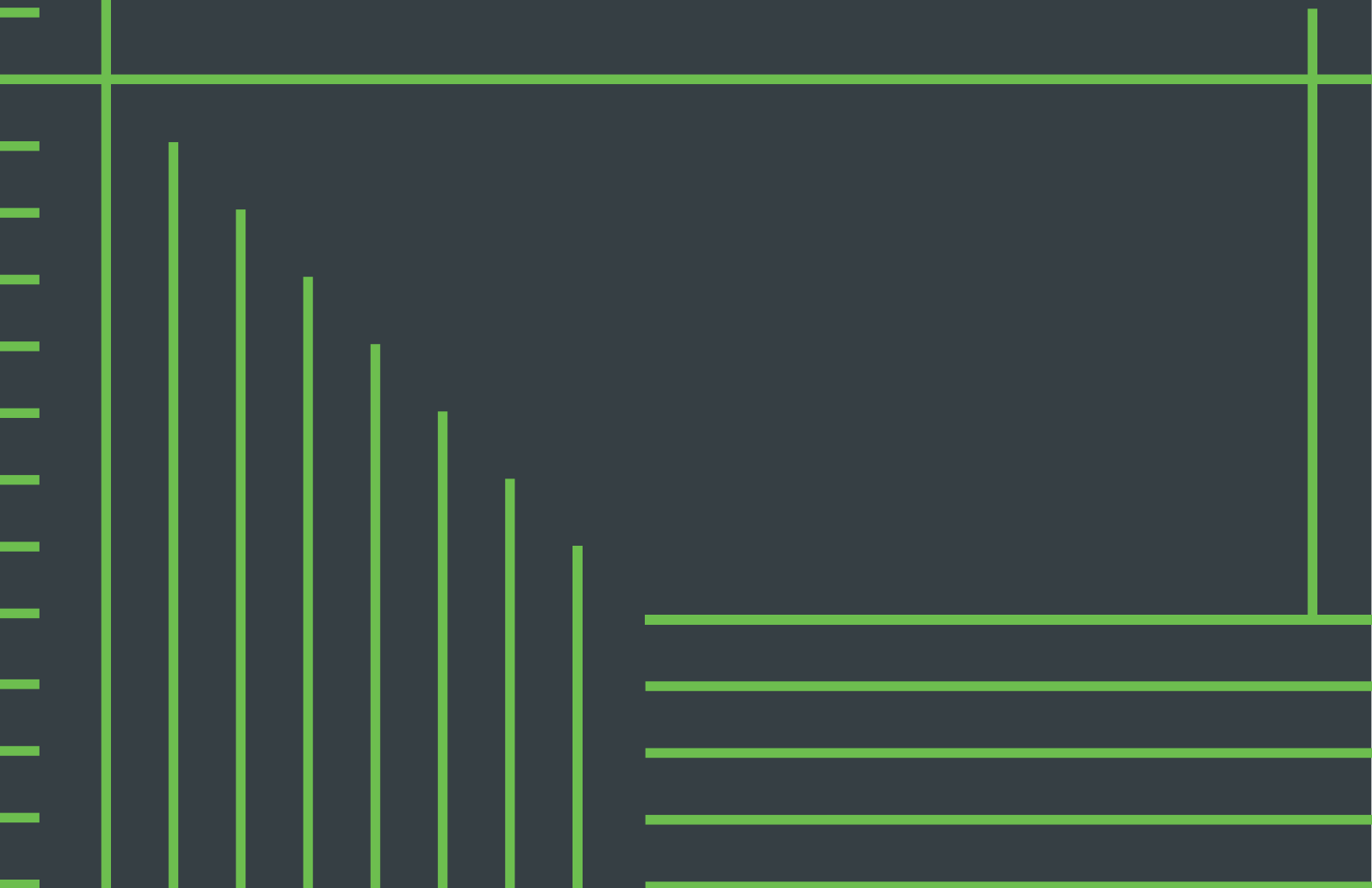
Five percent of phones are using Duo's two-factor authentication for personal use, or for a small number of users (less than 10), and 96% of those are Android devices. Jailbreaking or rooting can potentially expose devices and sensitive data to malicious apps, as well as undermining the device's overall security model.

Phishing

Phishing is a type of fraud – by sending an email pretending to be from a credible source, the attacker attempts to obtain sensitive data (like passwords) from unsuspecting users. Attackers may also send malware email attachments to check users' devices for software vulnerabilities, then infect them.

Of all the phishing simulation campaigns, 25% of recipients clicked on the link within a phishing email and another 13% entered their credentials – which, in an actual phishing attack, could potentially expose them and their company to malware and password theft.

Overall Device Security Health

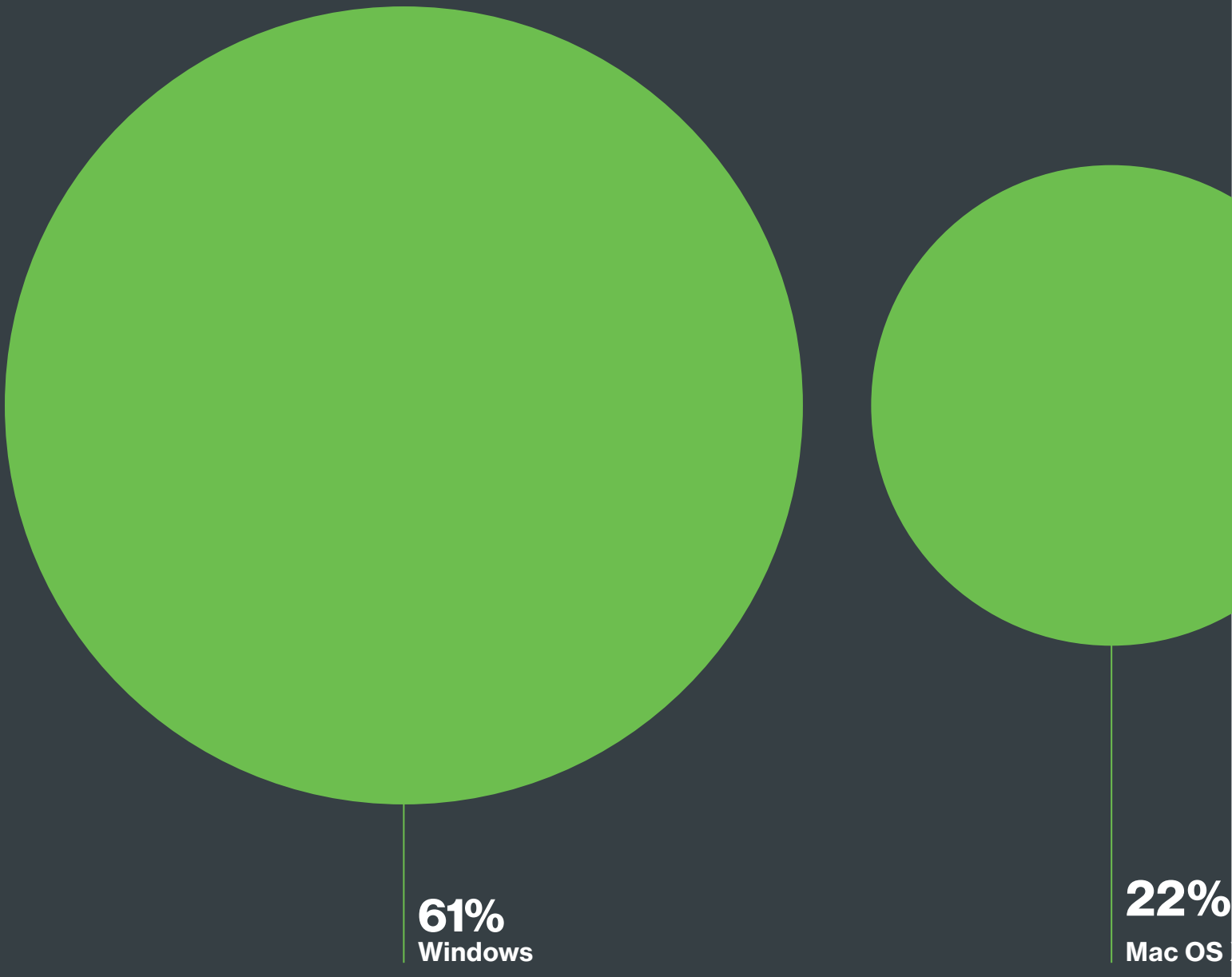


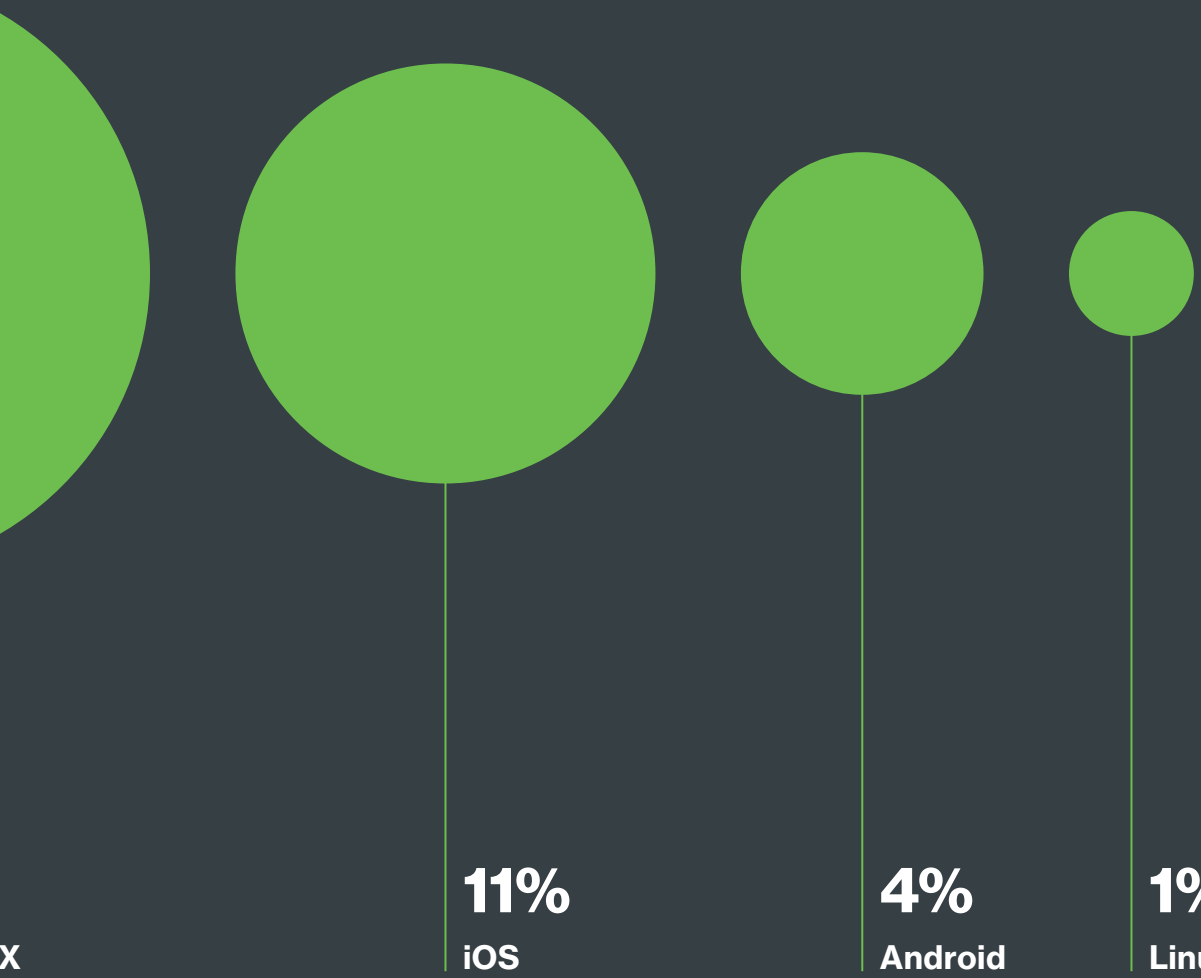
The latest year-over-year trends across operating systems, browsers, Flash and Java. Here's the current security state of enterprise endpoints.

Operating Systems Across the Enterprise

This year, we see most endpoints used in the enterprise are still running Microsoft's Windows operating system (OS), at 61%, a slight decrease from 63% in 2016. Another 22% are running macOS.

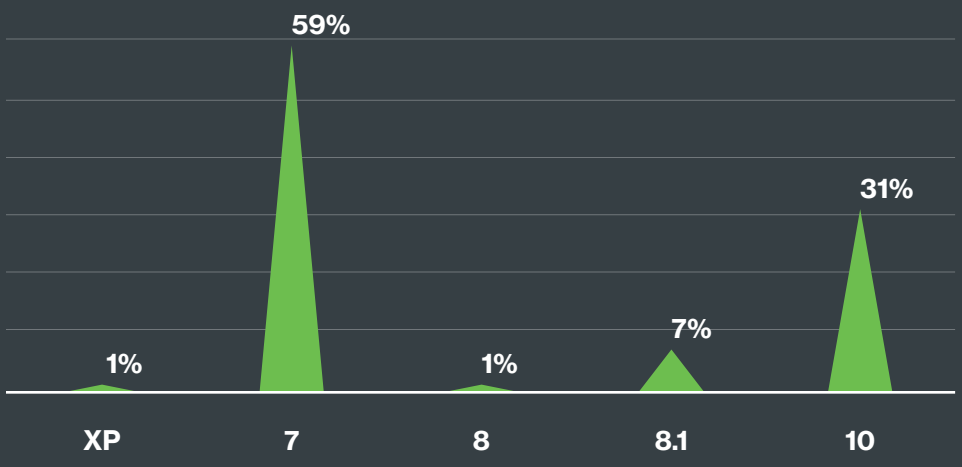
Operating System Distribution




X
11%
iOS
4%
Android
1%
Linux

Migrating Slowly to Windows 10

Windows OS Versions



More than double the number of endpoints are running the latest version Windows 10; 31% in 2017 compared to 15% in 2016. That means many more endpoints are secured against known vulnerabilities that may affect older Windows OS versions, although not the majority yet.

WHY MIGRATE **NOW?**

Windows 10 was released in 2015 and is the newest version of the Microsoft operating system. Two years later, we're seeing the start of the enterprise shift to the OS. Some analysts recommend 12-18 months to prepare – which may factor into the slow upgrade from Windows 7 or 8.1.[1]

Updating enterprise systems may mean a full software and hardware upgrade, which can be costly and require many resources. However, starting the migration now is key, as Microsoft will end support for Windows 7 in three years.

In order to prevent the installation of old versions of Windows on new processors, Microsoft has already blocked the installation of Windows 7 and 8.1 on systems with the Intel 7th Generation Core processors and AMD Ryzen systems. This means systems using these processors are no longer receiving security updates.[2]

Regular, timely patching is key to protection against known vulnerabilities. Microsoft fixed 45 vulnerabilities in its April update, including three bugs that were being actively exploited against users.[4]

In early April, the group known as the Shadow Brokers released a cache of hacking tools allegedly used by the NSA to the public, including what appeared to be several Windows zero-day vulnerabilities (previously unknown exploits without a patch).[5] However, Microsoft had already patched most of the vulnerabilities a month before the leak – showing that timely patching is key to keeping your environment safe in today's increasingly fast-paced threat landscape.

There's also a 13% decrease in endpoints running Windows 7, although it's still a relatively high percentage overall, at 59%.

Endpoints on Vista have also decreased by 57% from 0.96% in 2016 to 0.41% this year, a good trend to see as Vista has recently reached end of life. As of April 2017, the 11-year-old OS has reached end of life and will no longer receive security patches from Microsoft.[8]

Unfortunately, Windows XP has stayed the same at 1% year over year. While support for the ancient OS ended in 2014, thousands of endpoints used in the enterprise still run on the legacy system.

Regular, timely patching is key to protecting against known vulnerabilities.

SECURITY UPDATES **TO WINDOWS 10**

In the Windows 10 Anniversary Update released last August, Microsoft rolled out security improvements to its platform architecture that uses hardware-based isolation to protect sensitive Windows components and data from the rest of the OS.

Other feature improvements include one that automatically scans PCs to ensure they're safe and up to date; and one that alerts users on Edge or Internet Explorer of potentially malicious sites.

The company also improved its AppContainer sandbox to isolate the browser from the rest of the OS, apps and user data in efforts to further protect its system from external threats.[3]

MICROSOFT WARNS **AGAINST WINDOWS 7**

Mainstream support has ended for Windows 7, although extended support still exists, with the complete end of security and technical updates slated for Jan. 14, 2020.[6]

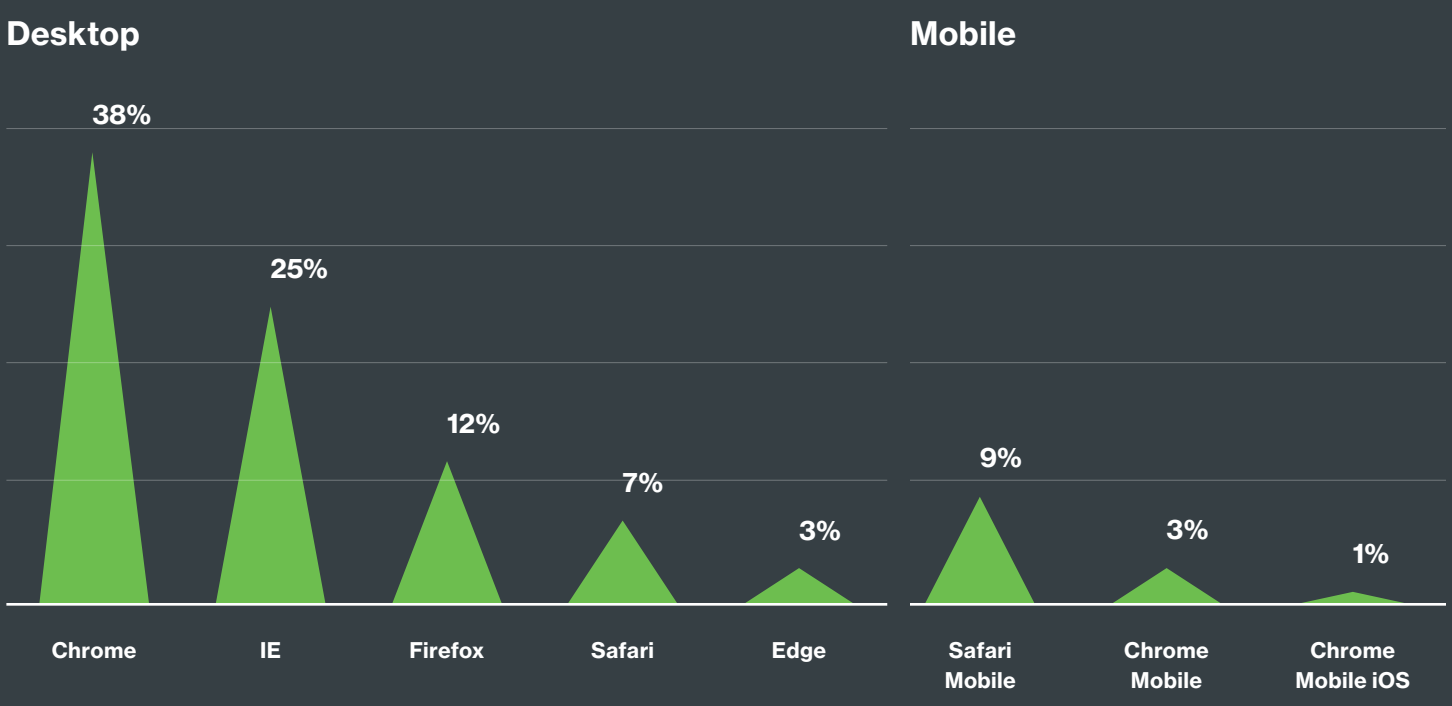
While in 2009, Windows 7 was the first step on the way to the cloud, it can no longer keep up with the increased security requirements of modern technology.

Microsoft Germany has warned against using Windows 7, as enterprises will face higher operating costs, increased maintenance and time lost due to attacks associated with its long-outdated security architecture.[7] Microsoft advises enterprises to start planning to migrate to Windows 10 as soon as possible.

Browsing Ever More Securely

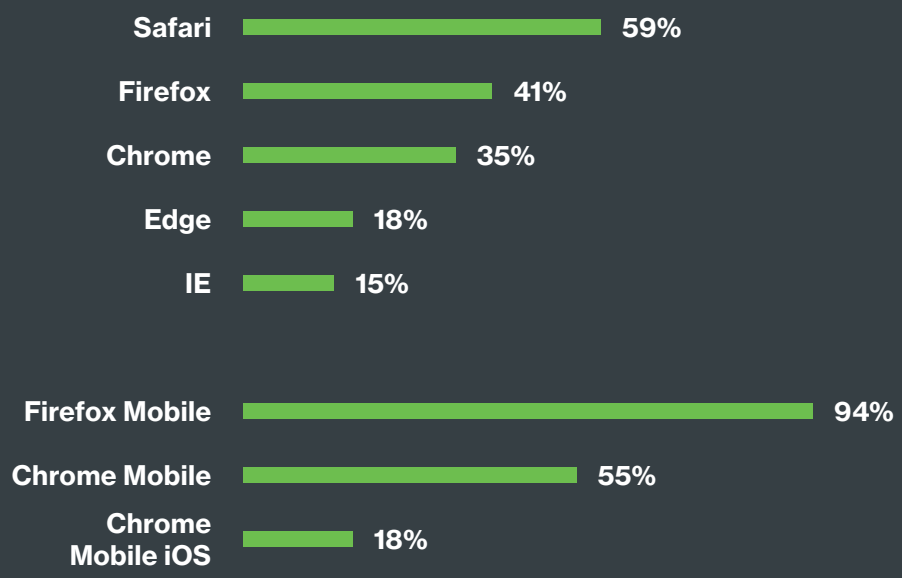
The majority of our users are browsing with Chrome (38%), followed by IE (25%) and Firefox (12%).

Overall Browser Distribution



While 75% of Chrome endpoints are running the latest version, and 85% of IE/Edge, only 59% of Firefox mobile endpoints are up to date. The Firefox mobile browser ranks first as the most out-of-date browser used by enterprise endpoints at 94%, and Chrome Mobile takes third at 55%.

Endpoints Running Out-of-Date Browsers



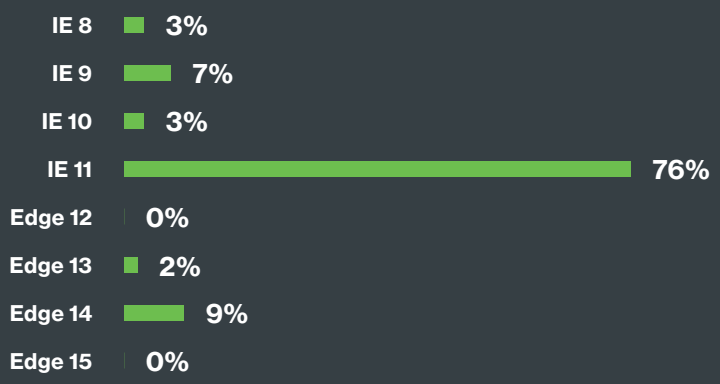
Endpoints on the latest version of Chrome 56 decreased last year from 82% to 64% in 2017. Firefox endpoints are increasingly more up to date, with 66% on Firefox 44 + 38 (the latest versions last year) compared to 76% this year on Firefox 51 + 45.

Internet Explorer: 2016 to 2017

Compared to last year, there has been a rise in endpoints running the latest versions of IE/Edge, from 58% in 2016 to 85% in 2017. This correlates with double the amount of endpoints running Windows 10.

Unsupported Internet Explorer

There's still 13% of endpoints running an unsupported version of IE (8, 9 & 10), compared to 19% last year. The majority of these endpoints are running Windows 7 (78%), and Windows 10 (12%).



Microsoft announced they would no longer provide security updates or technical support for the browser versions last January, meaning endpoints running these browsers are exposed to many vulnerabilities and exploits, without the ability to patch for them.[11]

IE BROWSER **BUGS EXPLOITED**

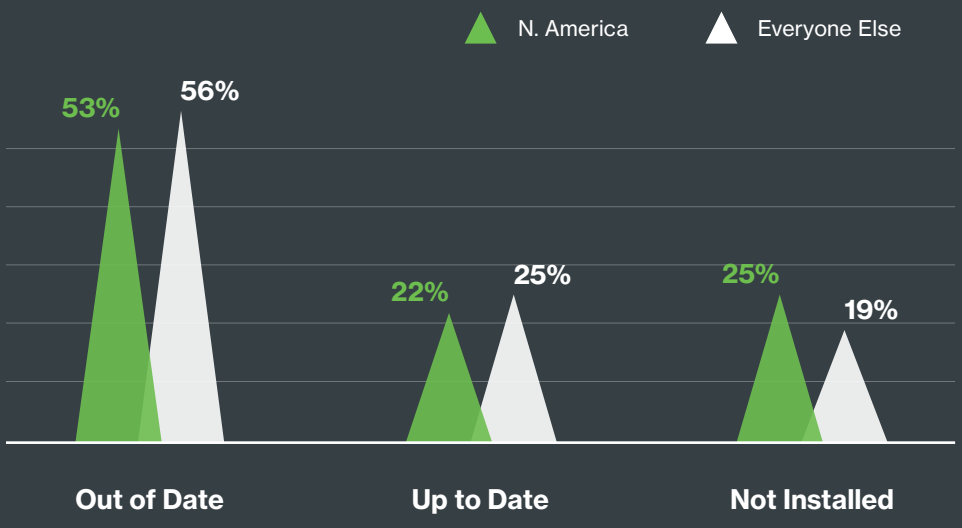
In late February, a high-severity bug affecting IE 11 and Edge browsers was found, CVE-2017-0037. This flaw gave malicious hackers the ability to create websites that cause IE and Edge to crash and potentially allow the sites to gain control over the browser, giving attackers complete control over your systems.

A patch for this vulnerability and many others was released in March's Patch Tuesday update that included updates for the past two months.[9] Ars Technica recommended Windows users should consider using a 64-bit version of Chrome instead of Edge or IE until they were patched.[10]

Flash: Increasingly Out of Date

Things are looking worse for Adobe's Flash plugin – the percentage of endpoints running an out-of-date version of Flash has increased from 42% in 2016 to 53% in 2017. Flash is the most out of date on IE (58%), while most up to date on the Chrome browser (65%).

Out-of-Date Flash



FLASH EXPLOITS **KNOW NO END**

There are over 1000 public Flash vulnerabilities – the majority of which were reported within the last two years. From 2015 to 2017 (so far), there have been 628 total recorded in the CVE database – 207 of them are of high-to-critical severity.[12]

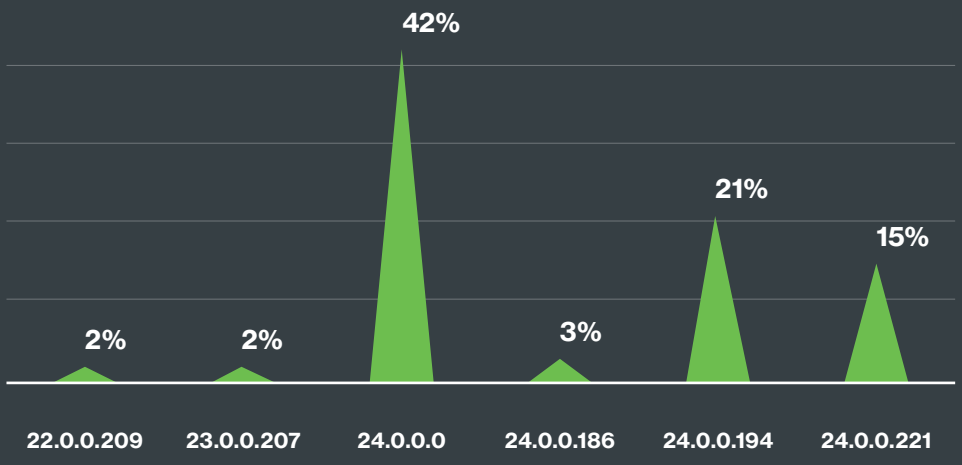
In 2016 alone, there are 266 reported vulnerabilities; 256 (96%!) of which were scored as high-to-critical severity, using the Common Vulnerability Scoring System (CVSS).[13]

Additionally, six of the top 10 vulnerabilities found in exploit kits in 2016 targeted Flash. One Flash vulnerability, CVE-2015-7645, was packaged into seven different exploit kits.[14]

In 2015, this bug was used in a number of phishing campaigns that targeted foreign affairs ministries.[15]

Flash will continue to be a highly effective and reliable target, spanning different platforms and different attack vectors, such as compromised websites and advertising networks. Uninstalling the plugin or enabling click-to-play can help reduce your attack surface.

Flash Versions

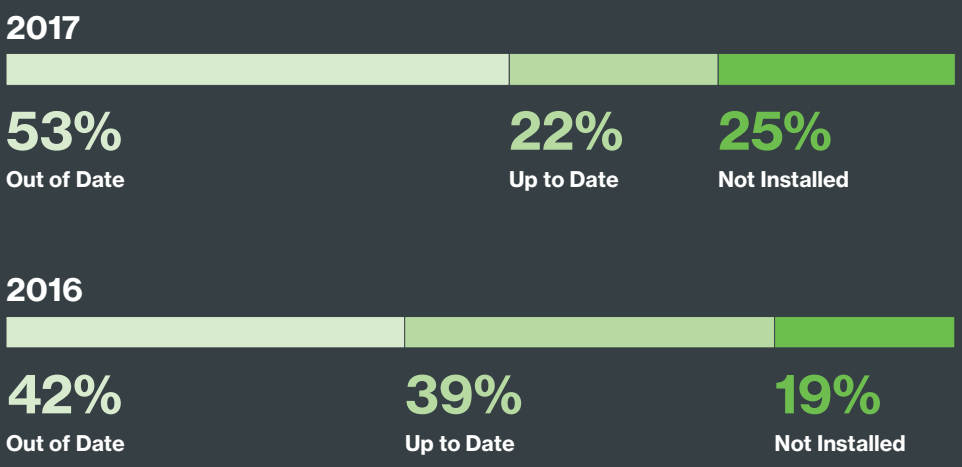


21%
of endpoints are running a version of Flash with 11 listed critical vulnerabilities.

According to the breakdown of endpoints on different Flash versions, we found that 21% are running version 24.0.0.194, which has 11 listed critical vulnerabilities published in February 2017.[16]

We also found that 15% of enterprise devices running version 24.0.0.221 are susceptible to at least 6 critical vulnerabilities again reported in 2017.

Flash Trends



This year, we see an increase in Flash uninstalls, from 20% in 2016 to 25%.

MOVING AWAY **FROM FLASH**

In January, Google disabled Flash Player by default in the Chrome browser, citing performance as a key factor – HTML5 is lighter and faster. According to Google, publishers are switching over to speed up page loading and save on device battery life.[18]

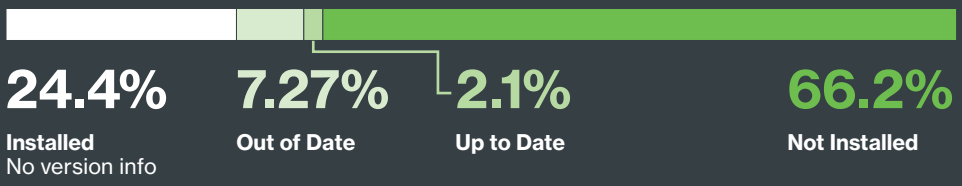
Similarly, Mozilla blocked the use of Flash in the Firefox browser in 2015, and now Microsoft is following suit, enabling click-to-play for Flash in an Edge browser update.[19]

Even Adobe has deprecated the use of Flash for its developers as they move to HTML5. While still technically supported, Adobe is encouraging developers to build with new web standards, renaming Flash Professional CC to Animate CC.[20]

Java Trends

Of all endpoints, 7.27% are running an out-of-date version of Java, and another 66.2% have Java uninstalled.

2017 Java Trends



Another 24.39% have Java enabled. Since last year, there has been an increase in uninstall rates, from 65% to 73% from 2016 to 2017.

In a study of the most common vulnerabilities included in exploit kits, ones that targeted Flash were used most often, with Java and IE taking second and third place.[21]

U.K. and Europe, Mi East & Afri

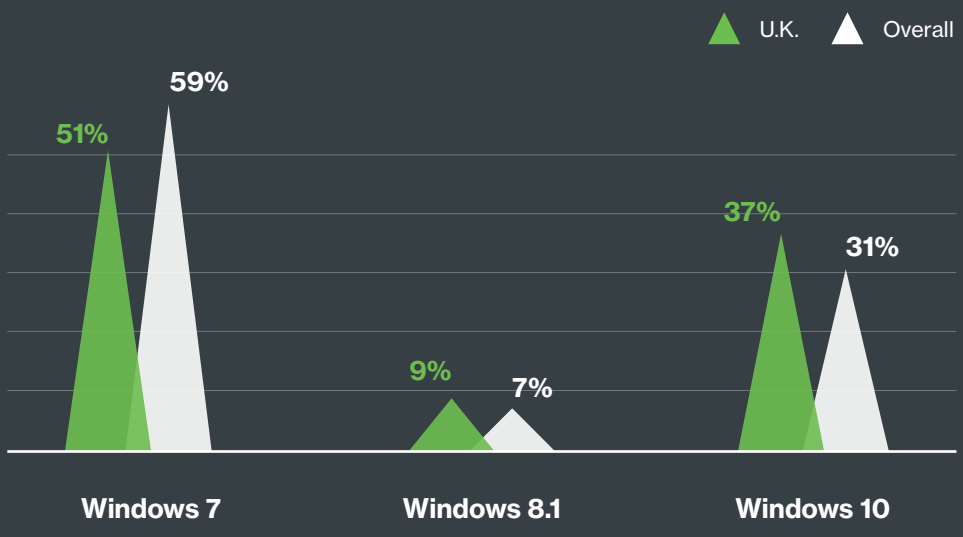
iddle
ca

How does the U.K. and EMEA stack up compared to overall enterprise endpoints and North America?

United Kingdom

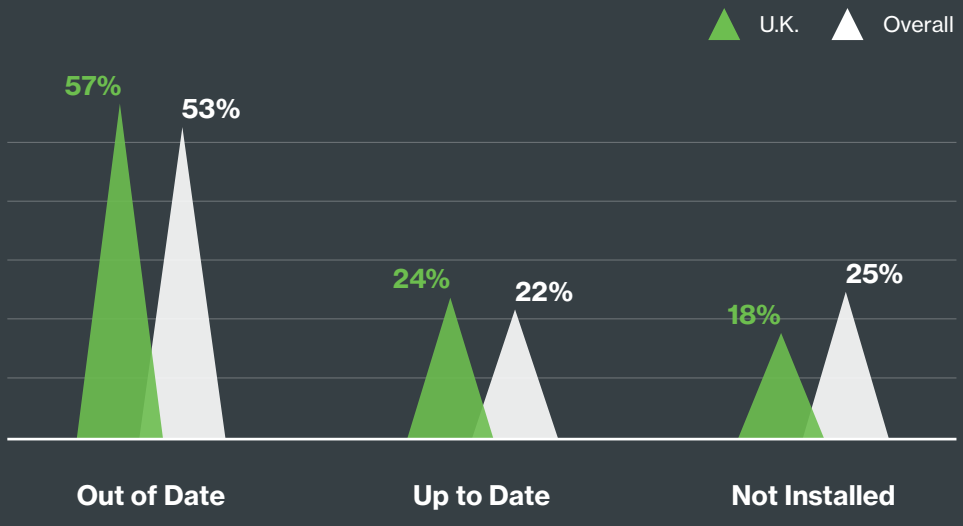
Taking a look at the U.K. alone, their endpoints running Windows OS appear to be slightly more up to date than the overall percentage.

Windows OS

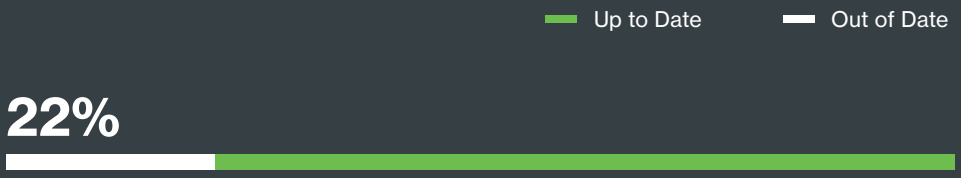


- 37% are running Windows 10 in the U.K., compared to 31% overall
- Another 51% are on Windows 7, compared to the 59% overall
- 9% are on Windows 8.1 compared to 7% overall

Flash

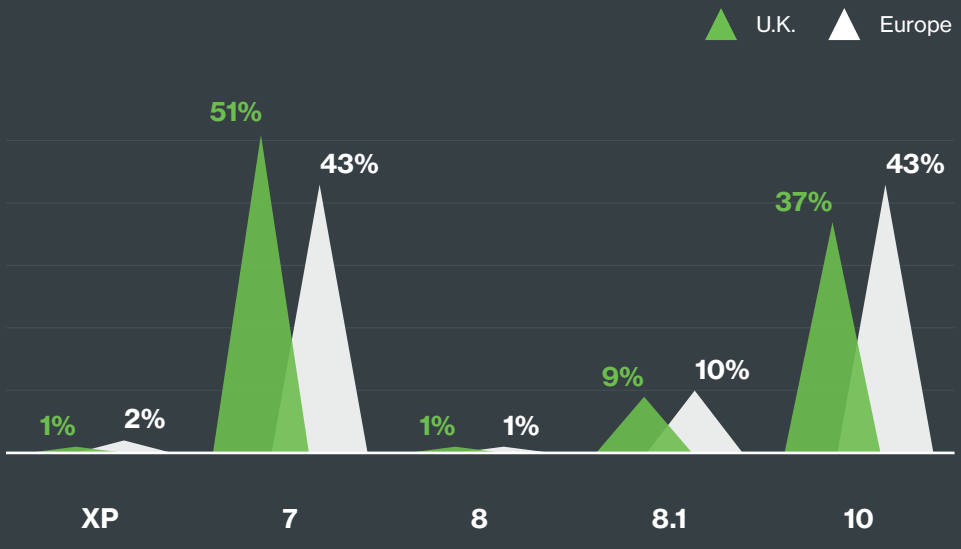


Browsers



The U.K. has a smaller percentage of endpoints running out-of-date browsers (22%) compared to other countries (32%).

U.K. Compared to Europe



But when comparing the U.K. to the rest of Europe, it appears they lag in upgrading from Windows 7 and 8.1 to the latest version, Windows 10. The U.K. has only 1% of endpoints running the unsupported Windows XP, while the rest of Europe is at 2%.

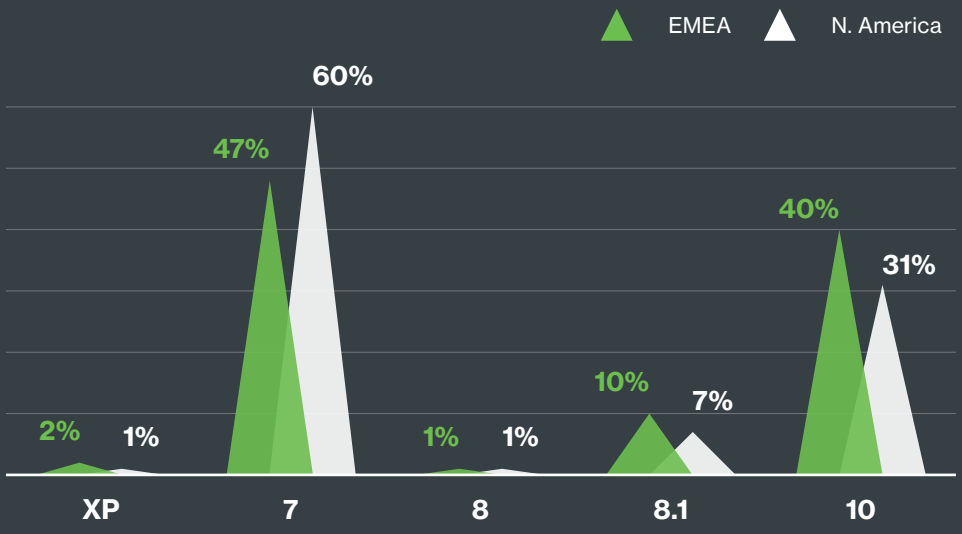
EMEA

Analyzing endpoints located in Europe, the Middle East and African countries, we found that they're generally more up to date than those located in North America.

The European Union (EU) has strict privacy laws governing the collection of personal data, which may drive a stronger security culture and stricter regulatory environment.[22]

This can be seen most recently in the EU General Data Protection Regulation (GDPR) approved last April with rules around data portability, processing, breach notification and more. The GDPR also comes with strict noncompliance penalties for organizations processing personal data.[23]

EMEA vs. North America: Windows OS

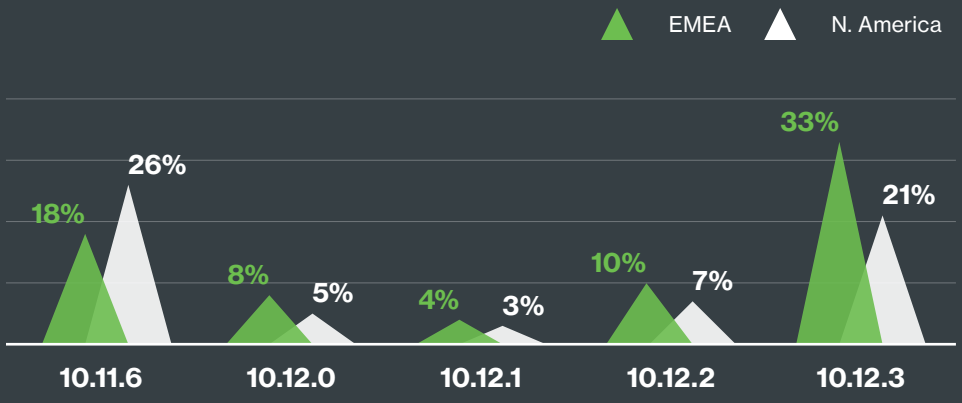


40% of EMEA Windows endpoints are running Windows 10, compared to 31% in N. America

47% of EMEA endpoints are running Windows 7, compared to 60% in N. America

2% of EMEA endpoints are running Windows XP, compared to 1% in N. America

EMEA vs. North America: macOS



33% were on 10.12.3 in EMEA (current as of our data collection), compared to 21% in North America

18% were on 10.11.6 in EMEA; 26% in North America

10% were on 10.12.2; 7% in North America

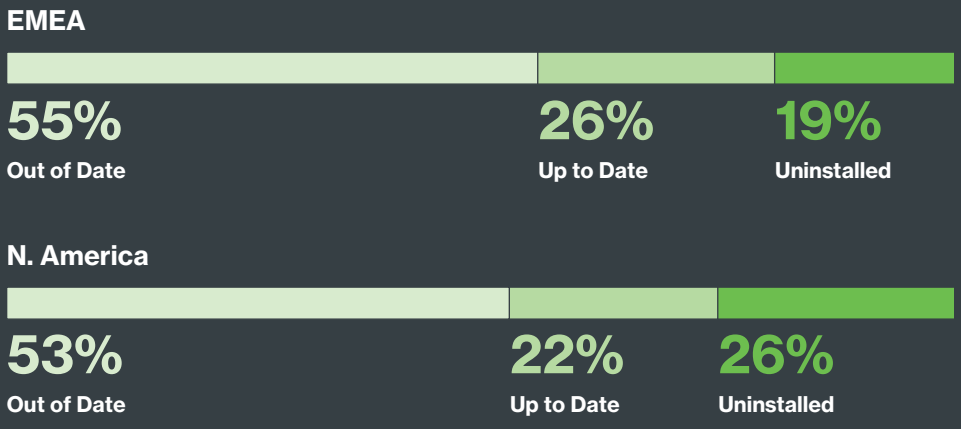
9% were on 10.10.5; 15% in North America

EMEA vs. North America: Browsers

EMEA endpoints are generally more up to date than North American endpoints.

EMEA was 79% up to date, compared to 69% in N. America.

EMEA vs. North America: Flash



19% of EMEA endpoints have Flash uninstalled, compared to 26% of endpoints in North America.

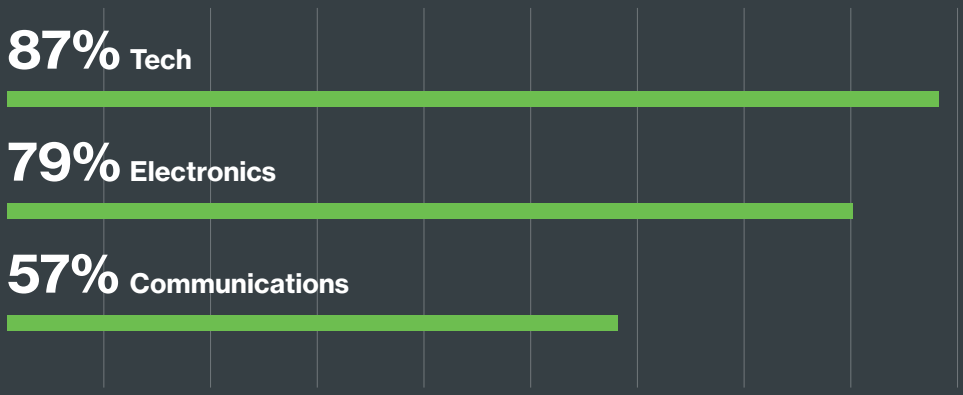
By Industry

See which industries are running the most up-to-date versions of operating systems and browsers, and discover which ones have mobile security features enabled – and which ones lag behind.

Windows & macOS

The tech industry has the highest percentage of endpoints running the latest Windows 10 operating system (87%). Machinery (6%) and Healthcare (16%) came in last for the percent of endpoints running Windows 10.

Windows 10: Top 3



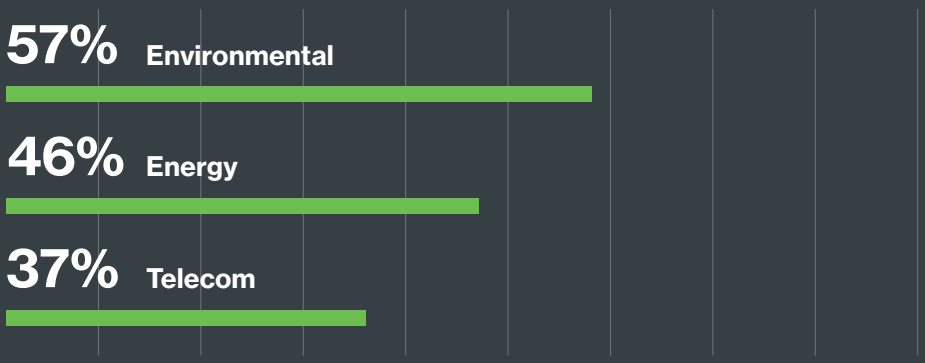
Windows 10: Bottom 3

The machinery (6%) and healthcare (16%) industries came in last for the percent of endpoints running Windows 10.

Environmental has the highest percentage of endpoints running the latest macOS version. However, 76% of state and local government's endpoints are running version 10.10.5, which may be due to old hardware that cannot run the latest macOS.

The latest version of macOS, 10.12.4, addresses 127 security issues, including a firmware patch that addresses potential firmware attacks for **some machines**.[24]

macOS



57% of environmental endpoints are running the latest macOS version 10.12.3, followed by 46% of energy, 37% of telecommunications.

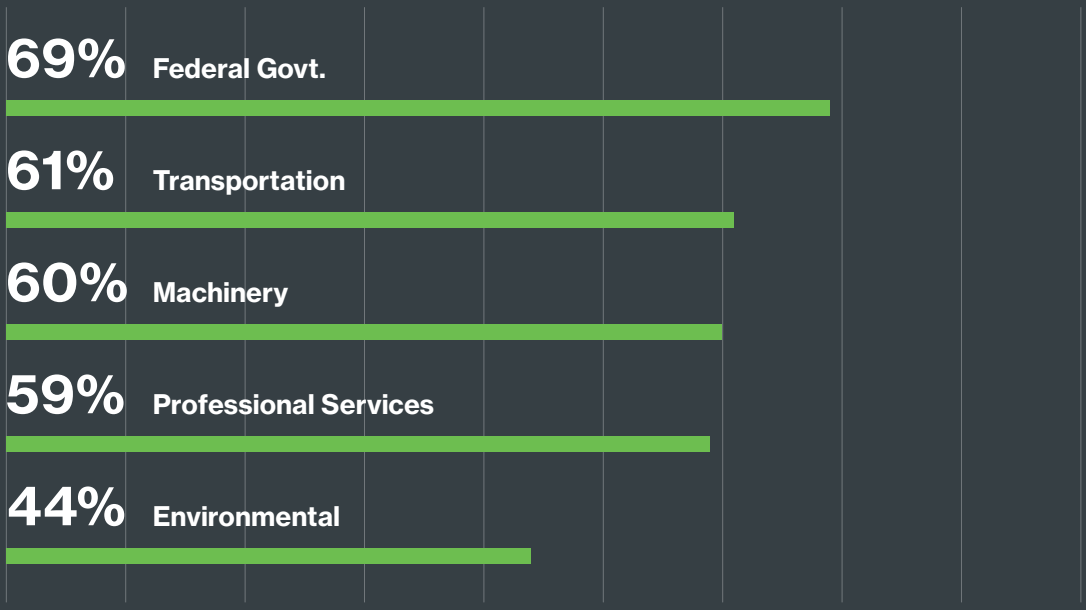
Out-of-Date macOS

As for out-of-date Apple endpoints, 76% of state and local government's endpoints are on 10.10.5, an old version of macOS that was released in August 2015.

Android & iOS

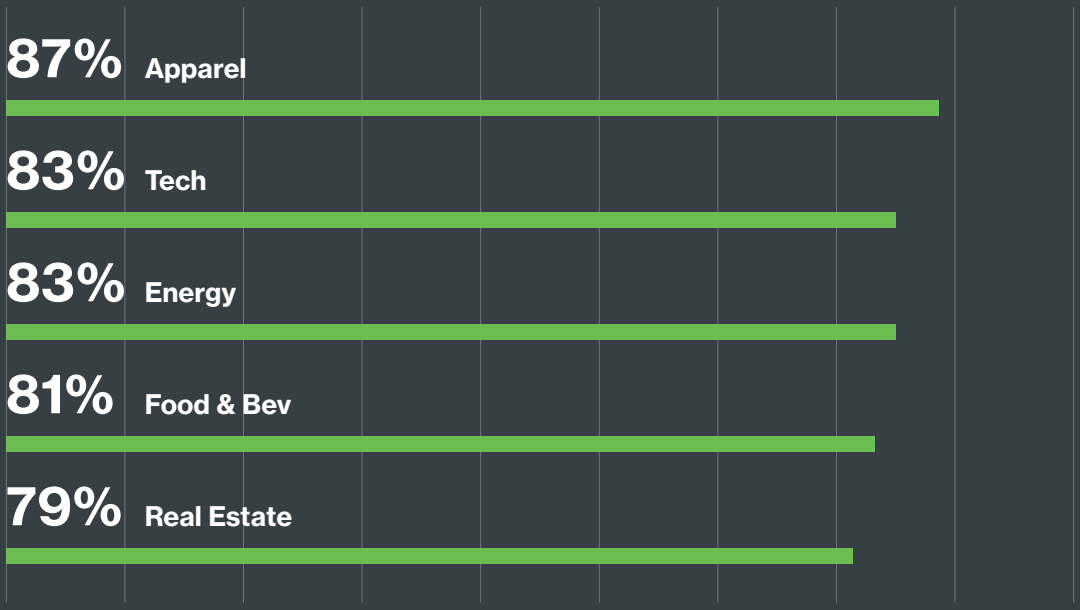
The top industries using Android include transportation, machinery and professional services. Meanwhile, the apparel and tech (consumer web) industries use mostly iOS devices to authenticate into their applications.

Android



The industries that are using mostly Android phones to authenticate into work applications include transportation machinery and professional services.

iOS



Those dominating with iOS devices include apparel (87%), tech (83%) and real estate (83%). Healthcare, education and legal all have more iOS endpoints than Android.

Mobile Security Features

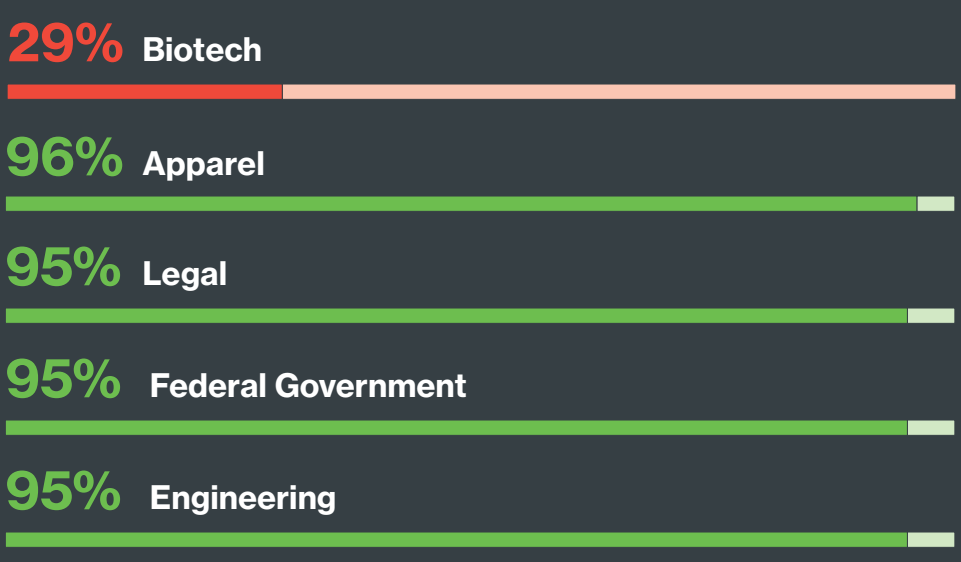
When it comes to mobile security features, biotech lags the most with the least percent of encrypted phones, and the highest percent of phones without a passcode/screen lock.

This is troubling as the biotech industry regularly works with highly confidential intellectual property, such as new drug development and testing.

Full Disk Encryption, By Industry

Biotech is the most at risk at 14% encrypted, while tech is the most secure at 41% encrypted.

Lock Screen/Passcode, By Industry



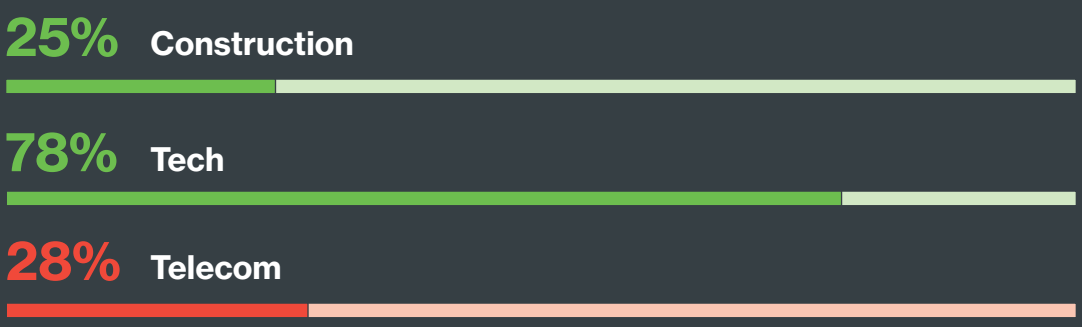
Biotech is the most at risk at 29% without passcode. Apparel is the most secure at 96% with passcodes. Legal, Federal Government, Engineering, Energy are also very secure at 95%.

The biotech industry comes in last for phone encryption and screen locks.

Tech companies have higher percentages of encrypted phones and Touch ID/fingerprint authentication enabled. Unsurprisingly, the tech industry is typically at the forefront of quickly adopting new technology, hardware and, in turn, security features, as a result of the nature of the industry and demographic of its users.

Apple also made Touch ID a key step in setting up new iPhones with iOS 10, which may have influenced more secure user behaviors and higher adoption of this particular mobile security feature.

Phone Touch ID/Fingerprint Authentication, By Industry



Construction has the lowest adoption; 25% of phones support it but don't have it set up

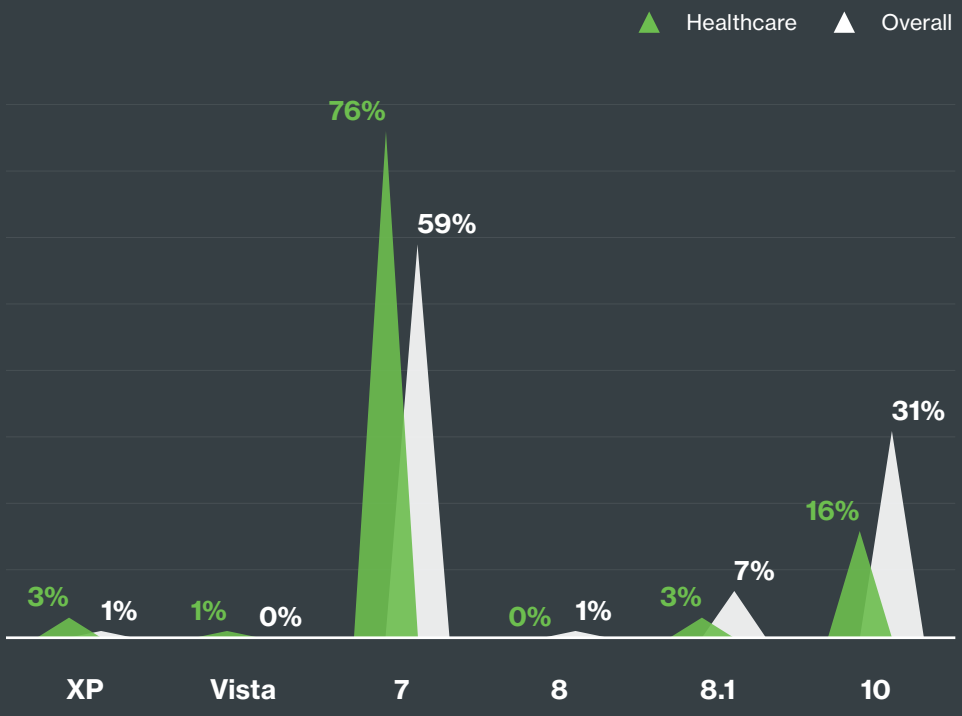
Tech has the highest adoption; 78% of phones support it and have it set up

Telecommunications has the highest percentage of phones that don't support it at 28%

Industry Highlights: Healthcare

A closer look at the healthcare industry shows that 76% of endpoints are running Windows 7, much higher than the 59% of overall endpoints.

Windows OS



Additionally, the percent of healthcare endpoints running Windows XP has increased from 2% to 3%, which is higher than the 1% of overall endpoints.

HEALTHCARE: **A PRIME TARGET**

Last year, the healthcare industry was hit hard by ransomware attacks, with 88% of attacks targeting hospitals.[25] Ransomware is malware that infects networked machines and systems, locking out users and encrypting data until victims pay attackers to decrypt their data.

There are many reported cases of ransomware halting hospital operations last year that shut down entire systems while declaring a state of internal emergency.[26] In one case, malicious hackers demanded bitcoin payment equivalent to millions of dollars; in other cases, they demanded more money and deleted patient records.

Across browsers, plugins and operating systems, healthcare is less up to date compared to the overall average.

Web Browsers

Healthcare

39%
Out of Date

Overall

31%
Out of Date

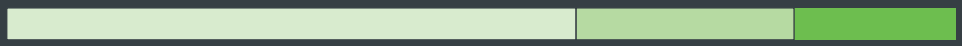
An alarming percentage of browsers used to log into work applications within the healthcare industry are out of date – 39%.

The healthcare industry is also slightly more out of date than overall when it comes to Flash – 60% of endpoints are running an older version, compared to 53% of all endpoints.

Another 17% of healthcare endpoints have uninstalled Flash, compared to the 25% of all endpoints.

Flash

Healthcare

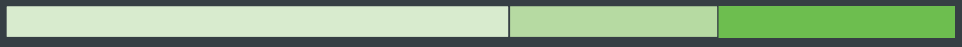


60%
Out of Date

23%
Up to Date

17%
Uninstalled

Overall



53%
Out of Date

22%
Up to Date

25%
Uninstalled

WINDOWS XP: **POTENTIAL COMPLIANCE ISSUES**

There are many reasons why the healthcare industry may still be running Windows XP, despite the OS's end of support.

The lack of budget for IT, hardware and software compatibility issues, legacy dependencies and more may keep hospitals on Windows XP – which could run afoul of The Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[27]

Of course, it's not only a compliance issue – an unsupported OS also leaves a hospital wide open to malware infection. Last year, three hospitals discovered malware infection via medical devices running on Windows XP.[28]

One of the hospitals had new enterprise-class firewalls, intrusion detection software and endpoint protection that failed to detect the old malware and established backdoors in the devices.

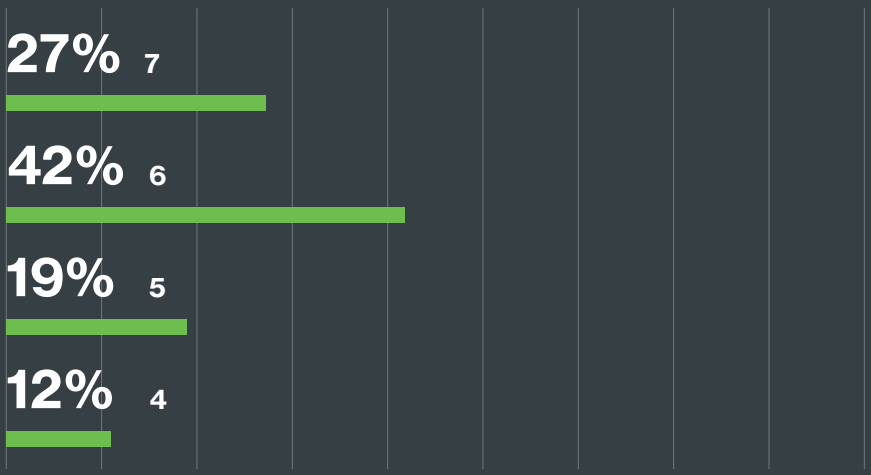
Mobile Security Health

A closer look at the security health of Android and iPhone devices, including security features like full disk encryption, lock screen, fingerprint authentication and more.

Android

We found that 27% of Android phones are running the latest major version 7, and 73% of iPhones were running iOS 10 or above. Monthly patches for Android devices do protect against known vulnerabilities, but each new major OS version also adds security features to proactively protect users. Both are important pieces that help complete the security puzzle.

Android Versions



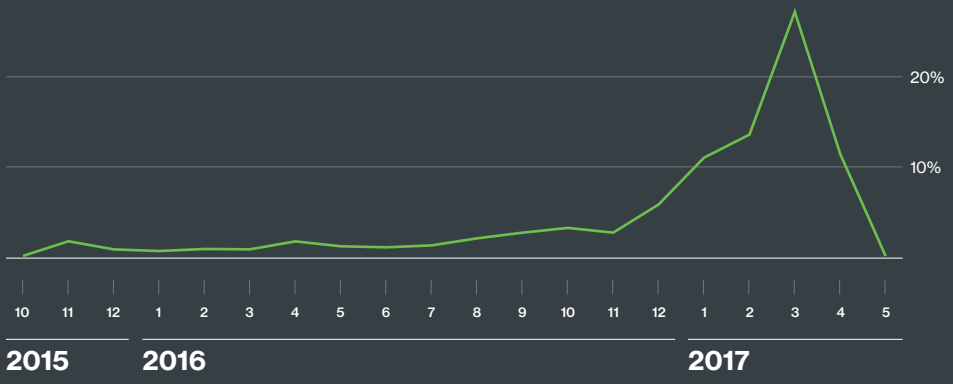
When it comes to running the latest version of OS, Android phones lag far behind iPhones.

MOBILE **UNCERTAINTY**

In a survey by Check Point and Dimensional Research, enterprise security professionals responded with low levels of certainty when it came to preparing for mobile security threats. While 20% have experienced a mobile breach, another 24% either didn't know or couldn't tell whether or not they've had one.

Two-thirds (64%) doubted that their organization could prevent a breach to employees' mobile devices. These numbers may indicate a lack of insight into mobile devices in the enterprise, and the inability to enforce policies or controls to secure their access to company networks.[29]

Android Patch Level



Based on data collected in February 2017, 18% of Android devices had January's patch, and 10% had patches released in February. Fourteen percent did not have any patches.

Within our Android devices, we found that 9% are running on an old OS version that cannot receive security updates. However, 59% of those devices would be capable of receiving updates if their carriers sent them a minor update that would allow them to run Android 4.4.4.

MANY ANDROID DEVICES, **LEFT BEHIND**

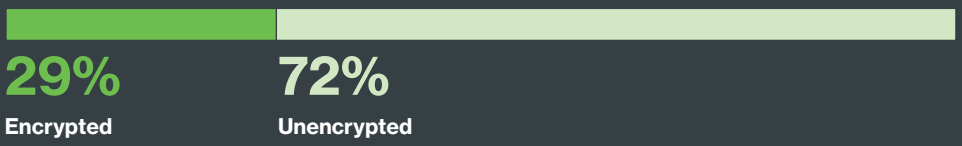
Part of the problem is, it can be difficult for Android users to update their mobile devices. Many Android devices that aren't part of the Nexus or Pixel family are at the mercy of their OEM or carrier for updates.

While 2016 was the first full year that Google released monthly security updates, we found that only 36% of devices were on a patch released in 2017. That means 64% of Android devices used to log into enterprise applications may be vulnerable to 38 critical CVEs patched this year.[30]

Mobile Security Features

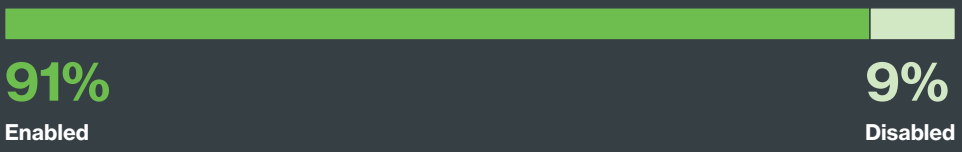
We also looked at the number of security features enabled on endpoints used to access work applications.

Full Disk Encryption



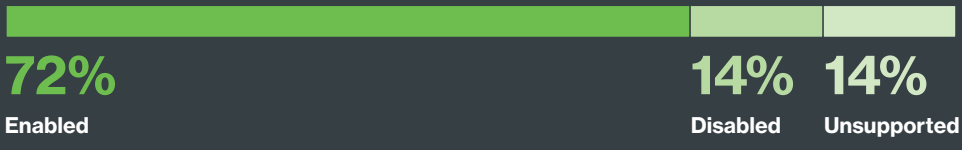
29% of mobile endpoints were encrypted, while 72% were unencrypted

Lock Screen



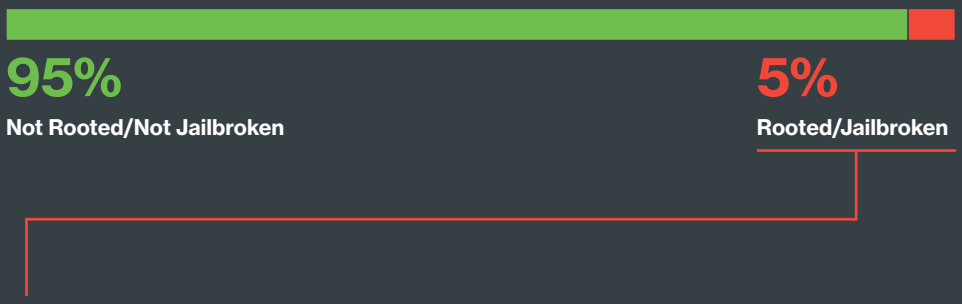
91% of mobile endpoints were locked with a passcode, only 9% were unlocked

Touch ID (iPhone)/Fingerprint Authentication (Android)



72% of mobile endpoints were configured to use Touch ID or fingerprint authentication
14% had it disabled on their phones
Another 14% of mobile endpoints did not support it

Jailbroken/Rooted



Jailbroken/Rooted OS Distribution

Our data found that 5% of phones using Duo's two-factor authentication for personal use, or for a small number of users (less than 10) are jailbroken/rooted. Of those devices, 96% are Android, another 4% are running iOS.

It would appear most of these phones are personally owned – and personal owners may be more likely to jailbreak or root their phones to add unauthorized apps and modifications, especially since these devices aren't managed or limited by any work-related security policies or mobile device management (MDM) solutions.

SECURITY RISKS OF **JAILBROKEN/ROOTED DEVICES**

Jailbreaking or rooting iOS/Android devices can potentially lead to a few risks:

Apps run outside of the iOS sandbox, which can allow them to access sensitive data

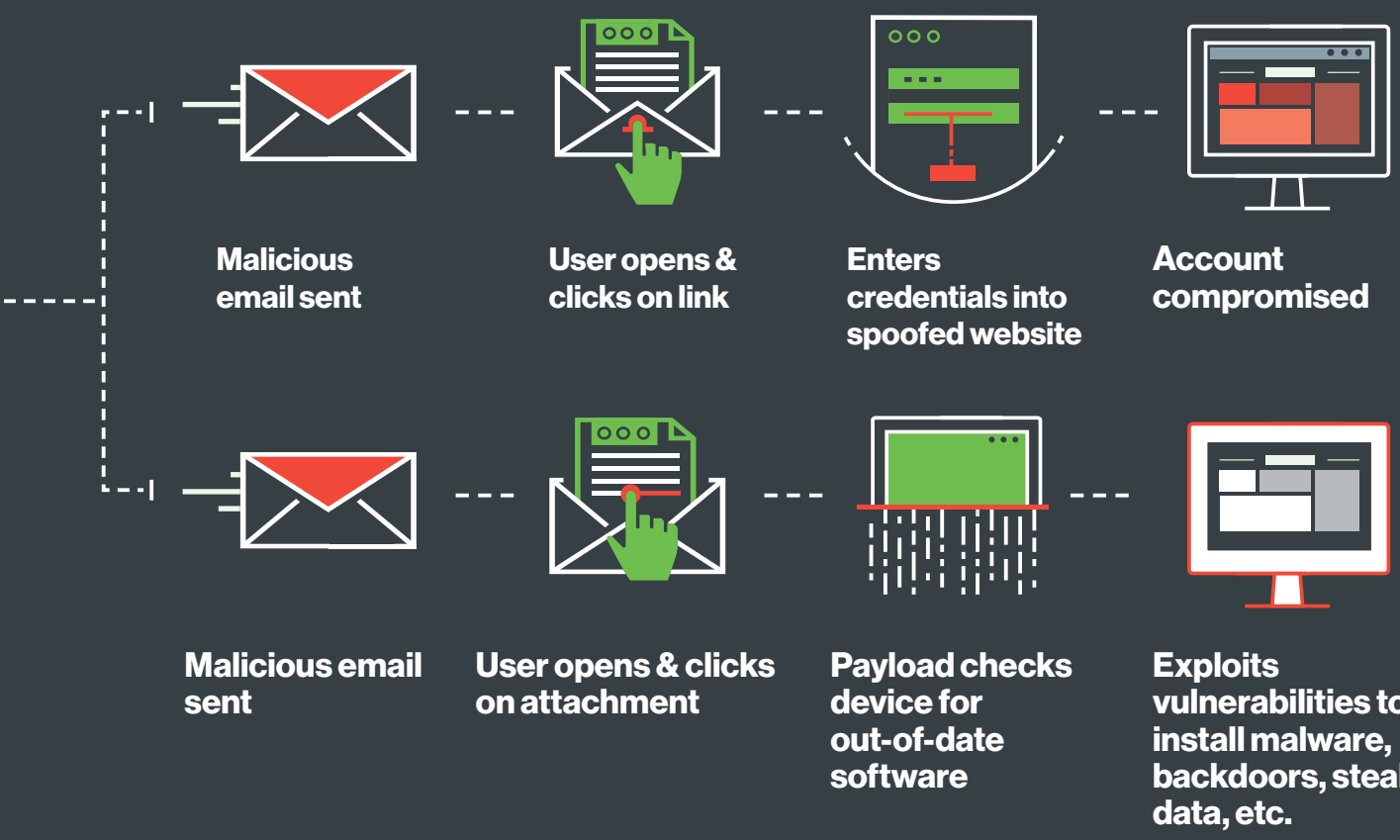
Apps can be installed from third-party sources, which may introduce malware to personal phones – passing along risk to enterprise apps the device logs into

Android devices that grant root access to apps may increase exposure to malicious apps

Many third-party Android apps have demonstrated malicious remote administrative capabilities[31]

Phishing

An analysis of the user behavior and device data collected from Duo's free phishing simulation tool, Duo Insight.



"The majority of phishing cases feature phishing as a means to install persistent malware."

—Verizon's 2016 Data Breach Investigations Report

25%
Clicked the link

44%
Opened the email

13%
Entered credentials

17%
Out-of-date Operating Systems

13%
Out-of-date Browsers

62%

of phishing campaigns captured at least one credential

68%

had at least one out-of-date device

62% of phishing campaigns captured at least one credential and 68% had at least one out-of-date device.

Phishing is a low-tech, fast and highly effective way for malicious hackers to steal user credentials, exploit out-of-date software, and gain access to enterprise applications and systems to steal, destroy or hold data for ransom.

By sending an email pretending to be from a credible source, the attacker attempts to obtain sensitive data (like passwords) from unsuspecting users. Attackers may also send malware email attachments to check users' devices for software vulnerabilities, then infect them.

The phishing data we analyzed was collected via **Duo Insight**, a free phishing simulation tool that allows companies to run an internal, targeted campaign to assess their risk. Our sample size was 3,575 campaigns and over 80,000 recipients.

A quarter of all phishing recipients clicked on the (potentially malicious) link in the email. The significance here is, if the user's device is running out-of-date software, they could be compromised by an exploit kit hosted on the website the user visited via the email link.

ONE CLICK TO **COMPROMISE IT ALL**

While phishing can lead to stolen passwords, it can also lead to compromised devices, particularly if those devices are running old, unpatched software that is susceptible to known vulnerabilities. This can expose risks to enterprise applications that the devices log into.

That's why a holistic security solution that combines strong user authentication, insight into device security hygiene and device access policies protects against several different attack vectors targeted in a phishing attack.

Implementing two-factor authentication can protect against the threat of compromise via a stolen password, while an endpoint security solution can detect and allow you to block any risky devices running out-of-date software.

Security Tips

Here's a few tips for what you can do to mitigate and reduce risks associated with the new enterprise IT model:

Use two-factor authentication.

Mitigate the risk of a breach of access via phished credentials by adding another way to verify your users' identities. Choose a solution that offers advanced user access policies, detailed authentication data, as well as easy deployment, management and usability.

Use a secure factor – U2F.

Universal 2nd Factor uses a physical USB device that users can quickly tap to log into accounts securely. The device protects private keys with a tamper-proof component, a secure element (SE), and can help protect against phishing attempts.

Patch and update regularly.

Keep an eye out for emergency patches that may happen out of the normal patch release schedule to keep your systems protected against critical and new vulnerabilities.

Enable mobile security features.

Turn on device encryption, screen lock and Touch ID/fingerprint authentication to keep your devices protected against unauthorized access. Also, don't jailbreak or root devices used to log into enterprise applications to reduce your risk of exposure to malicious apps.

Uninstall Flash and Java.

Avoid widening your potential attack surface by removing plugins you're not using. Or, disable the plugins from automatically running, and enable click-to-play.

Switch to Google Chrome.

The browser offers a few key security features, including Safe Browsing to notify users of sites suspected of malware or phishing, and automatic updates that regularly check browsers and roll out updates without any user action required.[32]

Duo's Trusted

Protecting against phishing attacks and other access-related threats requires a more comprehensive approach to enterprise security.

Duo's Trusted Access platform verifies your users' identities and the security health of their devices before granting them access to specific applications.

Consolidate your solutions into one effective and holistic platform to gain visibility, control and secure access to your applications.

Trusted Users

Verify the identities of your users.

Two-Factor Authentication

Let your users log into your applications remotely with confidence and ease – add a strong second factor of authentication that requires them to prove their identity via their **phone** or **USB device**. It's easy to deploy, manage, maintain and use – meaning, less headaches for administrators and users alike.

Phishing Simulator

Assess your risk of getting phished and identify vulnerable users in your organization by launching targeted phishing campaigns.

User Access Policies

With our detailed authentication request data, you can create data-driven policies and controls. Limit access by user groups, block login attempts from countries you don't do business in, or block users on anonymous networks to reduce the risk of unauthorized access.

Access

Trusted Devices

Check the security health of every device.

Device Insight

Get complete visibility into every device authenticating into your applications, including corporate-owned and personal phones, laptops, tablets, etc. Duo's administrative dashboard provides insight into out-of-date software and mobile security features, letting you drill down into specific devices, users and user groups.

Endpoint Remediation

Device access policies let you block risky devices from accessing your apps. Plus, you can notify users to update their devices before logging in, letting you quickly improve your company's security posture.

Trusted Endpoints

Only allow trusted, corporate-owned devices to access your sensitive applications by marking them with a device certificate, with easy public key infrastructure (PKI) setup – no agents required.

Every Application

Protect both on-premises and cloud applications.

Easy Application Integration

Secure your VPNs, cloud apps, on-premises and web apps, and use Duo's APIs and client libraries for everything else, including custom and proprietary software.

Secure Single Sign-On (SSO)

Let users log in just once to access work applications. Behind the scenes, Duo checks users' identities and device health every time they access your applications.

Application Access Policies

Limit remote access to only the applications each user needs – give your users easy, secure remote access to company cloud and internal web applications. No VPN required.

References

[1] **Should Your Business Upgrade to Windows 10?**; TechRadar; March 13, 2016

[2] **New Processors Are Now Blocked From Receiving Updates on Old Windows**; Ars Technica; April 13, 2017

[3] **Advancing Security for Consumers and Enterprises at Every Layer of the Windows 10 Stack**; Windows Business Blog; June 29, 2016

[4] **Microsoft Fixes Windows and Office 45 Flaws, Including Three Actively Exploited Vulnerabilities**; PCWorld; April 12, 2017

[5] **Mysterious Microsoft Patch Killed 0-Days Released by NSA-Leaking Shadow Brokers**; Ars Technica; April 15, 2017

[6] **Windows 10 Security Tackles Exploits, While Windows 7 Gets a Warning**; SearchSecurity; January 19, 2017

[7] **Windows 7 Support Endet in Drei Jahren**; Microsoft; January 16, 2017

[8] **Windows 10 Gets Major Update as Windows Vista Reaches Its End of Life**; April 11, 2017; Ars Technica

[9] **Microsoft Security Bulletin Summary for March 2017**; Microsoft; March 14, 2017

[10] **Google Reports "High-Severity" Bug in Edge/IE, No Patch Available**; Ars Technica; Feb. 27, 2017

[11] **Support for Older Versions of Internet Explorer Ended**; Microsoft; January 12, 2016

[12] **Adobe Flash Player Vulnerability Statistics**; CVE Details; April 13, 2017

[13] **Adobe Flash Player Security Vulnerabilities Published in 2016**; CVE Details; April 19, 2017

[14] **Adobe Flash Flaws Dominate Exploit Kits In 2016**; Dark Reading; Dec. 6, 2016

[15] **New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries**; Trend Micro; Oct. 13, 2015

[16] **Adobe Flash Player 24.0.0.194 Security Vulnerabilities**; CVE Details; April 19, 2017

[17] **Adobe Flash Player 24.0.0.221 Security Vulnerabilities**; CVE Details; April 19,2017

[18] **Flash and Chrome**; Google Blog; August 9, 2016

[19] **Microsoft Makes Flash Click-to-Play in Edge Browser Update**; eWeek; April 9, 2016

[20] **Adobe Finally Tells Developers to Stop Using Flash**; Wired; Dec. 2, 2015

[21] **In the Business of Exploitation**; Digital Shadows; April 18, 2017

[22] **Protection of Personal Data**; European Commission; April 26, 2017

[23] **The General Data Protection Regulation**; Deloitte; April 26, 2017

[24] **Apple Patches Hundreds of Vulnerabilities Across Product Lines**; Security Week; March 28, 2017

[25] **SERT Quarterly Threat Report Q2 2016**; Solutionary; April 24, 2017

[26] **12 Healthcare Ransomware Attacks of 2016**; Beckers Hospital Review; Dec. 29, 2016

[27] **Windows XP No Longer HIPAA Compliant**; The HIPAA Journal; Jan. 15, 2014

[28] **Windows XP 'Still Widespread' Among Healthcare Providers**; Naked Security by Sophos; Dec. 9, 2016

[29] **Survey: Enterprise Security Pros Doubtful They Can Prevent Mobile Breaches**; Check Point; April 12, 2017

[30] **Looking Back at Android Security in 2016**; Duo Blog; March 22, 2017

[31] **Projects/OWASP Mobile Security Project - Dangers of Jailbreaking and Rooting Mobile Devices**; OWASP; April 18, 2017

[32] **Explore the Chrome Browser**: Security; Google; April 13, 2017

Our mission is to protect your mission.

Experience advanced two-factor authentication, endpoint visibility, user policies and more with your free 30 day trial.

Try it today at **duo.com**.

Duo Security makes security painless, so you can focus on what's important. Our scalable, cloud-based **Trusted Access** platform addresses security threats before they become a problem, by verifying the identity of your users and the health of their devices before they connect to the applications you want them to access.

Thousands of organizations worldwide use Duo, including Facebook, Toyota, Panasonic and MIT. Duo is backed by Google Ventures, True Ventures, Radar Partners, Redpoint Ventures and Benchmark. We're located from coast to coast and across the sea.

Follow @duosec and @duo_labs on Twitter.

The Trusted Access Company