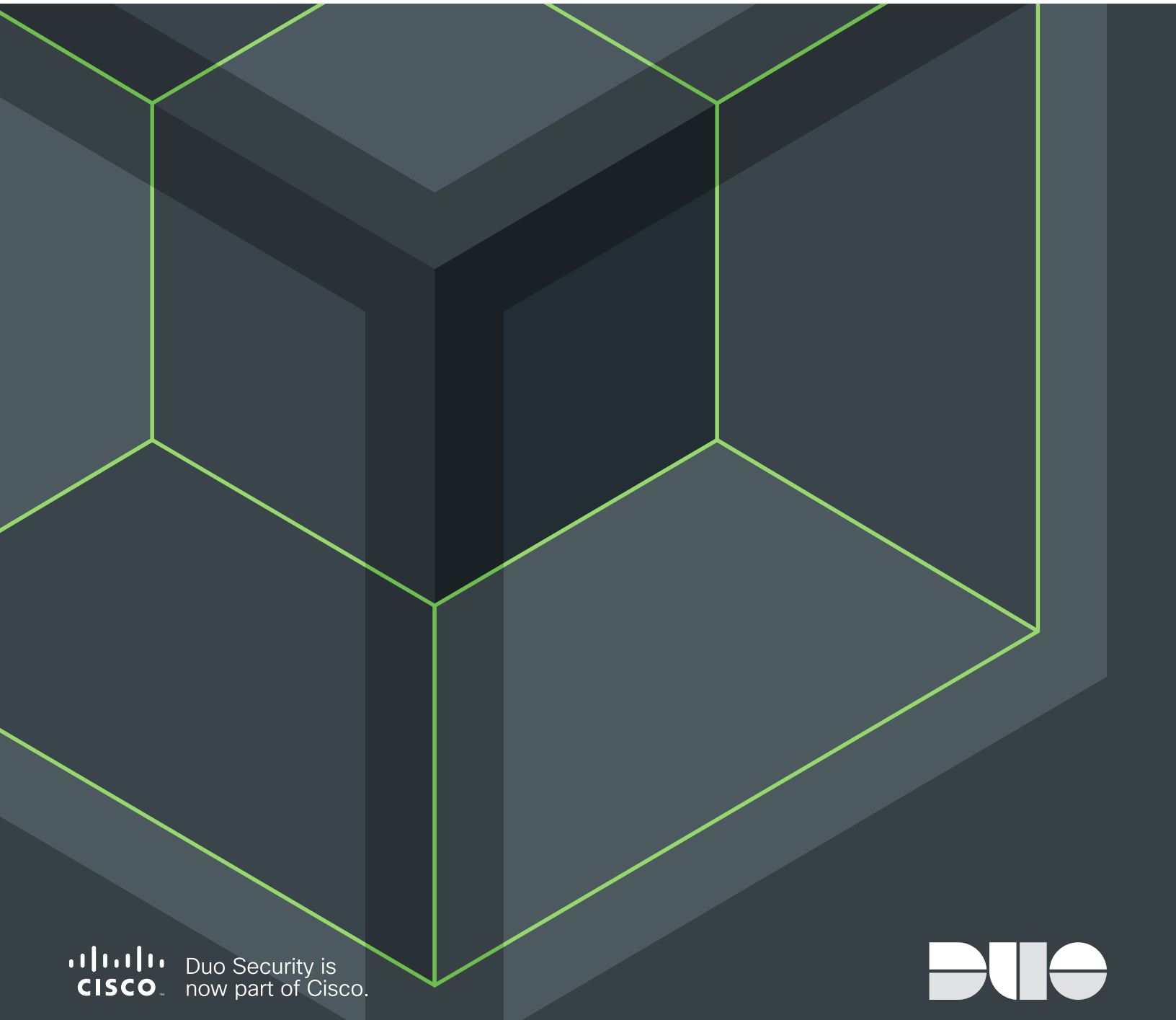
## The 2019 Duo

# Trusted Access Report

Expanding the Enterprise Perimeter with Zero-Trust Security for the Workforce



Duo Security is now part of Cisco.

# The 2019 Duo
# Trusted Access Report

Expanding the Enterprise Perimeter with Zero-Trust Security for the Workforce

# Enterprise Zero-Trust Security **Takes Hold**


## Here's the thing: the secure perimeter as you know it is evolving.

The explosion of cloud applications and mobility has expanded the concept of a perimeter security architecture, which assumes that every user and device inside company walls is secure and therefore trusted by default. Users, devices and applications are now everywhere, and they're more frequently outside of the traditional network. It's a transformation more than a decade in the making.

Organizations now must support different types of users, including contractors, third-party vendors and remote workers who connect to their corporate network. In a growing number of cases, these users are leveraging their own devices, such as smartphones and tablets, to connect to applications and networks. At the same time, apps, servers and other workloads are communicating with each other across cloud infrastructure and data centers. Smart Internet of Things (IoT) devices are another entry point.

**Long story short: today's workforce is always on and always connected.** Workers now use their personal mobile devices to access cloud applications and expect frictionless access regardless of time, device or location. It's the epitome of any time, anywhere and from any device.

This creates new opportunities for businesses to embrace the capabilities of an always-connected workforce. They can leverage new technologies while giving their users more choice and flexibility.

Those opportunities, however, can carry with them challenges. Now more than ever, admins and IT security staff need to know:

- If their users are who they say they are
- If their users' devices are secure and healthy
- What's connected across the network
- What kind of data is accessible via the cloud
- Who and what can access that data

Admins and IT security staff need insight into the security hygiene of user devices and have to be able to granularly set access permissions based on user and device trust. It's a balancing act between freedom and security.

To ease this transition and to embrace the evolving workforce, organizations are deploying the building blocks of a zero-trust security framework. The goal is to deliver secure access to applications for all users from all devices from anywhere. Security pros regain control, while users enjoy freedom, flexibility and ease of use.


2019 DUO TRUSTED ACCESS REPORT

# Where Did Zero Trust Come From?

The concept of zero-trust security was first discussed in 2004 when the Jericho Forum was created to tackle “de-perimeterization.” The philosophy was born from the need to think past the firewall and expand the secure perimeter. Forrester Analyst John Kindervag is credited with coining the term “zero trust” in 2010 in his description of a security model that assumes no traffic within an enterprise’s network is any more trustworthy by default than traffic coming in from the outside. Since then, the concept of zero trust has evolved.

Google brought zero-trust security back to the forefront with its BeyondCorp implementation: a zero-trust architecture that requires securely identifying users and their devices and removing trust from the network, externalizing apps and workflow and implementing inventory-based access control.

Meanwhile, Forrester’s Zero Trust eXtended (ZTX) discusses breaking down “monolithic perimeters” into a series of micro-perimeters or network segments and applying security controls around them, adding that zero trust is a holistic approach to securing data, network, device, workloads and workforces.

As access happens everywhere, ensuring visibility and secure, trusted access is imperative. A zero-trust model secures the new perimeter, which is built around identity. Cisco Zero Trust provides a comprehensive approach to securing all access across your applications and environment, from any user, device and location. It protects your **workforce**, **workloads** and **workplace**.

## Workforce

ENSURE ONLY THE RIGHT USERS AND SECURE DEVICES CAN ACCESS APPLICATIONS.

## Workload

SECURE ALL CONNECTIONS WITHIN YOUR APPS, ACROSS MULTI-CLOUD.

## Workplace

SECURE ALL USER AND DEVICE CONNECTIONS ACROSS YOUR NETWORK, INCLUDING IOT.

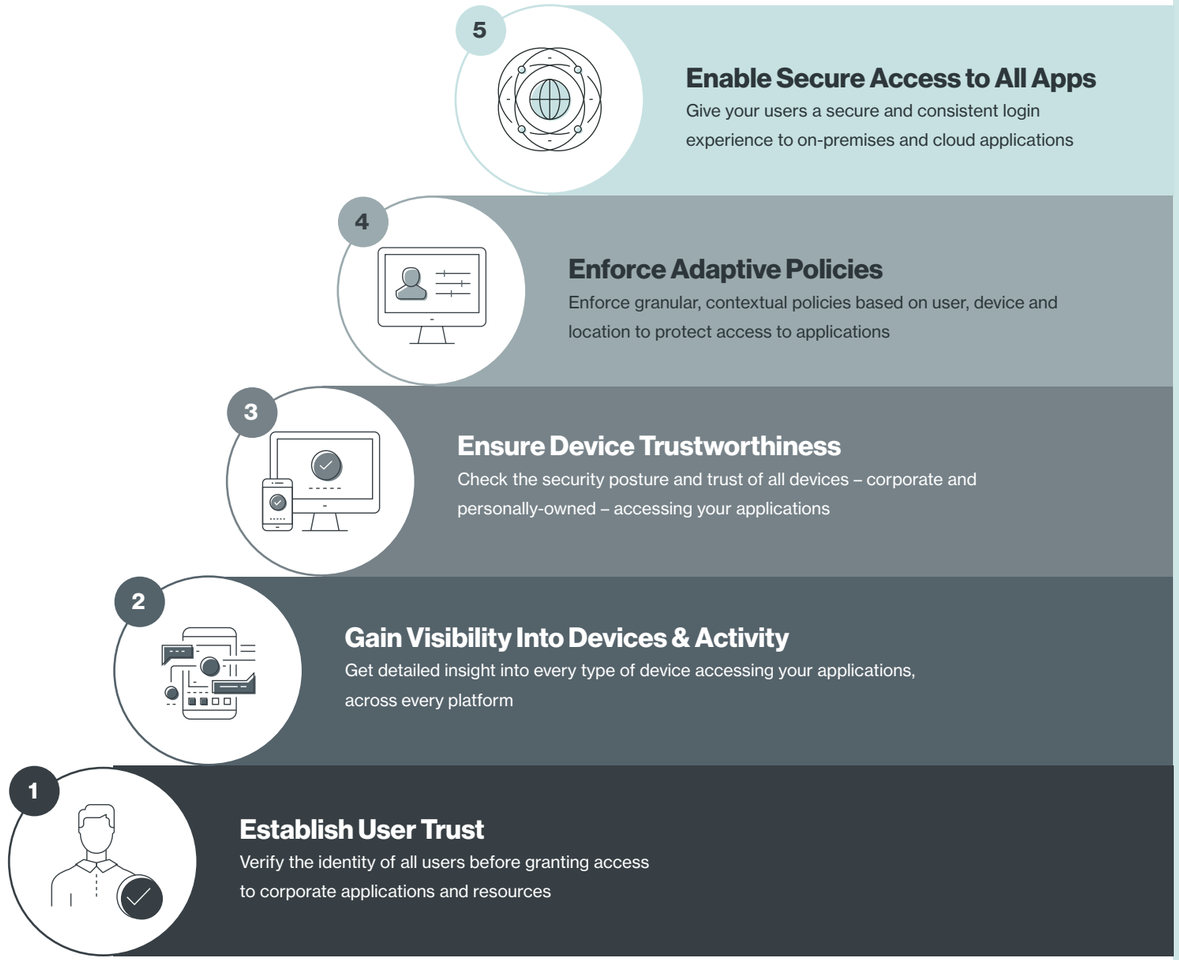
**Duo provides zero-trust security for the workforce,** meaning Duo ensures only the right users and secure user devices – your workforce – are accessing applications. This is the foundation of a zero-trust security model.

# Zero Trust for the Workforce

A zero-trust architecture for the workforce ensures the trustworthiness of devices and users' identities wherever access is attempted and before granting access, whether users are on or off the network.

This security model verifies users and establishes trust in their devices (those users and devices comprise your workforce), no matter where they are located, what devices they use, and which applications they access.

ZERO TRUST FOR THE WORKFORCE IS BUILT ON **FIVE KEY PRINCIPLES:**




For *The 2019 Duo Trusted Access Report*, our data shows that Duo customers across all industries are starting to implement zero-trust security principles to secure their workforce. They're doing this in many ways, including:

- Laying the foundation for passwordless authentication
- Embracing biometrics
- Enforcing stricter policies to ensure only trusted users and devices are granted access
- Following security best practices that are tangential to zero trust, such as conducting internal phishing campaigns to educate and raise security awareness in their organizations.

This report shows how users are accessing apps and how that differs across key industry segments. It also looks at how access methods are changing to accommodate the shift to zero trust and the ongoing evolution of the traditional secure perimeter.

# Methodology

In this report, our security research team, **Duo Labs**, analyzed data from nearly 24 million devices, more than 1 million applications and services and more than half a billion authentications per month from across our customer-base, spanning North America and Western Europe.

**500+ million**
Authentications per Month

**24 million**
Devices

**1 million**
Applications and Services

**NOTE:** *Some data sets may differ when compared to previous reports depending on the timeframes analyzed. For this report, we're referring to data from Jan. 1, 2019 to May 13, 2019 (unless otherwise noted), and data from the full calendar years 2017 and 2018.*

1.0

# Key Findings

**A brief, at-a-glance look at 10 data points from our research.**

## Duo Push is Favored Auth Method

Across all industries examined, Duo Push is the authentication method Duo customers use most frequently. More than half of successful authentications in Healthcare, Financial Services, Higher Education and Federal Government use Duo Push.

## Biometrics Use is Climbing

Over the last four years, customers are more often using biometrics as a second authentication factor to access applications. This year, 77 percent of devices used by Duo customers have biometrics, such as Apple Touch ID and Face ID, Android fingerprint sensors and Windows Hello, configured.

## Fewer Fooled by Phishing

Data from our phishing simulator tool revealed that in 2019 internal phishing campaigns are capturing fewer credentials and finding fewer out-of-date devices. Users are also opening phishing emails less frequently.

## Windows 10 Use Rises, Windows 7 Use Down

Our data shows that Windows 10 usage continues to steadily climb while Windows 7 uses dwindles as the operating system nears end of life. Wholesale & Distribution, Business Services and Non-Profit are the industries adopting Windows 10 at the fastest rate.

## Use of Flash Fizzles

As Adobe Flash Player continues to crawl toward end of life, more Duo customers have Flash uninstalled from their devices. So far this year, 71 percent of Duo customers have removed Flash, which is up from previous years.

## Android Devices Still Most Out-of-Date

Android devices lead the pack of out-of-date devices at 58 percent. Meanwhile, as of May 31, 2019, only 9.7 percent of Android devices were on the latest patch, which had been released 26 days prior.

## Cloud App Use Skyrocketing

Cloud application integrations are steadily climbing - cloud integrations are up 56 percent year over year based on the number of customers authenticating to cloud apps, and up a whopping 189 percent year over year in terms of the number of customers using each cloud app.

## Chrome Vulnerability Sparks Policy Shift

A recent zero-day vulnerability found in Google Chrome resulted in a massive spike in the number of authentications denied due to out-of-date browsers, platforms or plugins, which was 30 times higher than the average from the week prior and represented a 79 percent increase in the use of the policy to not allow access from any out-of-date browser.

## Edge Leads Out-of-Date Browsers

At the time of our data collection, we found that Edge is the most frequently out-of-date browser (73 percent) on end user devices, while Internet Explorer was the most frequently up to date (2 percent out of date).

## Remote, Mobile Work Increasing

Our data shows 45 percent of requests to access protected applications came from outside the business walls, showing that users are truly mobile and the perimeter has expanded to where access occurs.

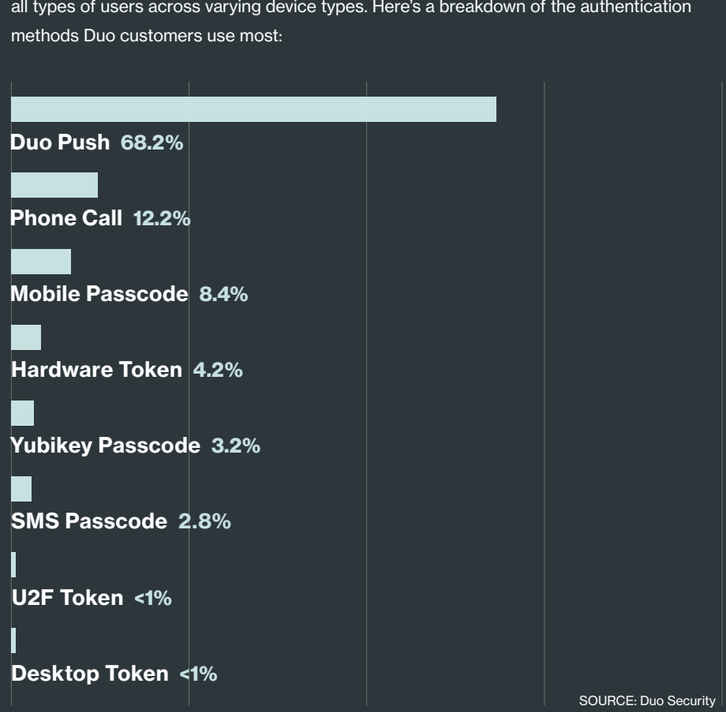
2.0

# User Trust

The first principle of a zero-trust security model for the workforce is establishing user trust, or verifying your users' identities when they attempt to access applications. Our research found that Duo customers establish user trust and verify their users are who they say they are through different authentication methods, and they're starting to leverage new ways to confirm those identities, such as biometrics.

## How Users Prove Who They Are

Duo offers various authentication methods to ensure establishing user trust is easy for all types of users across varying device types. Here's a breakdown of the authentication methods Duo customers use most:




SOURCE: Duo Security

### SMS-BASED AUTHENTICATION USE CONTINUES TO FALL

In 2016, the National Institute of Standards and Technology (NIST) changed its guidelines and declared that **SMS-based authentication methods were no longer secure**[1] because the phone may not always be in possession of the phone number and because SMS messages can be intercepted and not delivered to the phone.

Duo users have taken note, and the use of SMS as an authentication method has fallen over the years. **SMS-based authentication use hovered between 6 percent and 8 percent in 2016**[2], and today that number is down to less than 3 percent, a sign that Duo customers are opting for more secure authentication methods. While we believe SMS-based 2FA is better than no 2FA at all, we recommend users select the most secure methods available, such as Duo Push and U2F.



## Authentication Method Usage By Industry

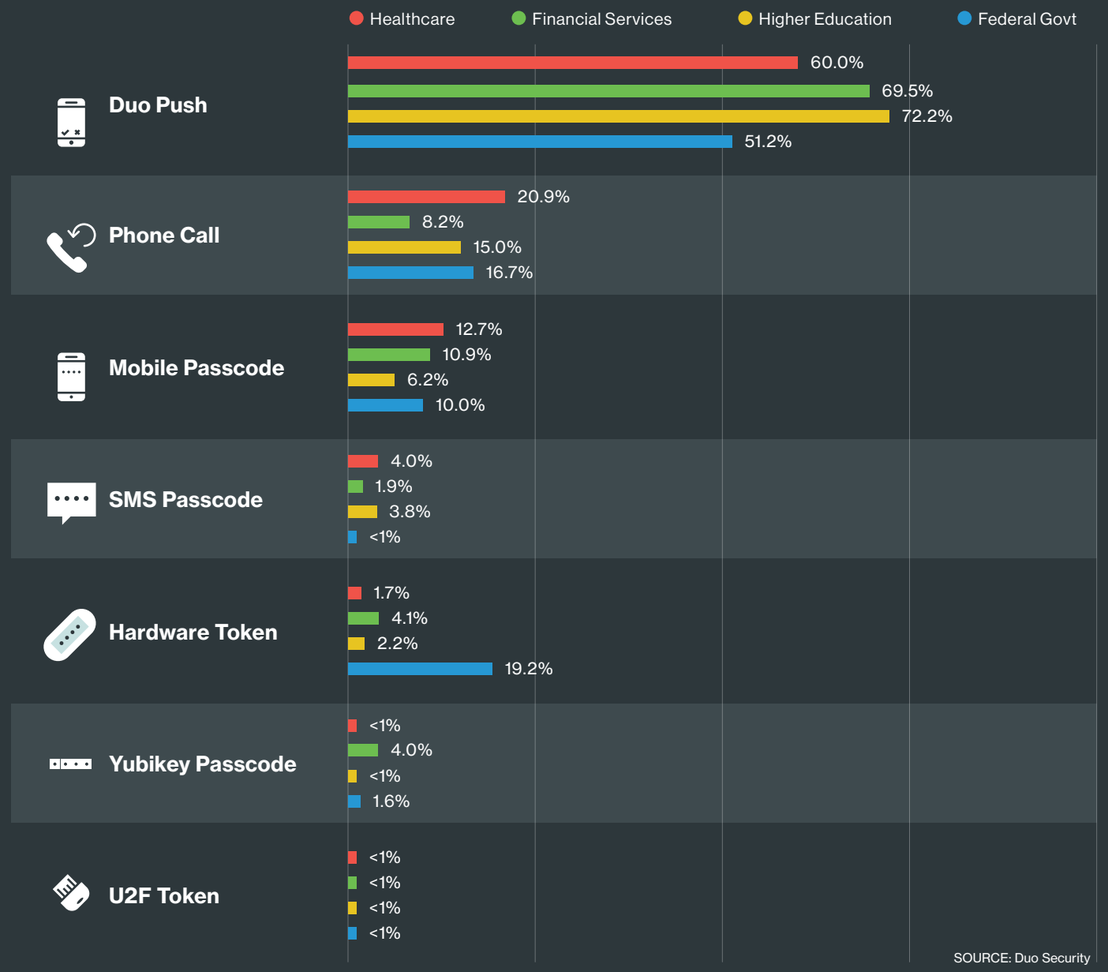
Our data found that different industries rely more heavily on different authentication methods. While Duo Push is the resounding leader across all industries, the second most frequent authentication method varies widely. For example, in Healthcare, 20.9 percent of users leverage phone calls as an authentication method, while 19.2 percent of Federal Government users leverage hardware tokens.

The data shows that more heavily-regulated industries, such as the Federal Government, are more likely to use hardware tokens to establish user trust. In the case of the Federal Government, hardware tokens directly correlate to their required use of Personal Identification Verification (PIV) and Common Access Cards (CAC) to sign into systems.

Phone callbacks are a common authentication method across Federal Government, Healthcare and Higher Education – industries where end users use landline phones or may not use a smartphone, yet still require a second authentication factor.

Meanwhile, the use of SMS passcodes is in single digits across all industries, a sign that as more convenient, more secure authentication methods, like Push, become available reliance on SMS passcodes dwindles.

**AUTHENTICATION METHODS BY INDUSTRY**



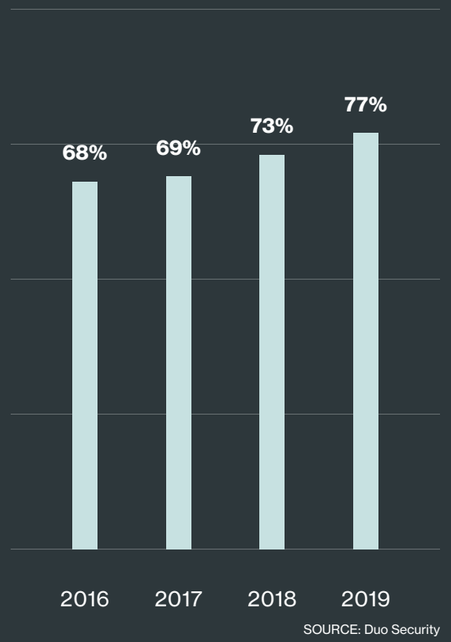

SOURCE: Duo Security

# Kissing Passwords G00d8y3!

Passwords are passe. Well, that may be a bit strong, but technologies like WebAuthn and biometrics are doing their part to put passwords where they belong: in the past. Our data shows that the use of mobile biometric sensors, such as Apple Touch ID and Face ID, Android fingerprint sensors and Windows Hello is steadily climbing as a method through which Duo customers are establishing user trust. The use of biometrics has risen consistently over a four-year stretch, heralding that people are relying less on passwords and the passwordless future may be closer than you think.

Biometrics usage will continue to increase as more device manufacturers support them, which is a giant leap toward a passwordless future. We'd like to see more sites support passwordless logins via tools like **WebAuthn**[3] and the FIDO2 standard, which will further reduce reliance on passwords as a login method.

MOBILE DEVICES WITH
**BIOMETRICS CONFIGURED**




SOURCE: Duo Security

## The passwordless future may be closer than you think.



### THE DEATH OF THE PASSWORD?

The information security industry has been sounding the death knell of passwords for years: they're hard to remember, hard to make complex and hard not to reuse.

## But what would a future without passwords look like?

Passwordless authentication means when a user authenticates to a remote server, that server does not require a password during the authentication process. This can be achieved securely in any number of different ways by leveraging public-key cryptography, which uses a public key that may be shared with anyone safely, and a private key that stays on the local device so that – unlike a password – it isn't susceptible to eavesdropping attacks. In the authentication standard WebAuthn, web application servers can integrate with strong authenticators already built into devices, such as Apple Touch ID and Face ID and Windows Hello, to generate a private-public keypair, called a credential, for that website. Then, the server can authenticate the user without receiving the private key or any shared secret directly.

Although biometric authentication isn't required for WebAuthn or passwordless authentication more broadly, fingerprint and facial authentication capabilities are increasingly prevalent on commercially available phones and computers. Many users are already unlocking their cell phone with the touch of a finger every day. For this reason, biometrics may be a natural choice for enabling strong local authentication, easing the transition to passwordless authentication with a device that's already in your pocket.

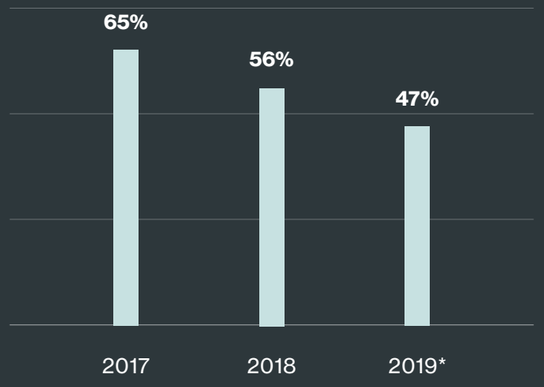
# Phishing:
# Fewer Users Getting Hooked

How will your users react when they receive a phishing email? Will they get hooked? That is, will they open it, click the link and enter their credentials (often a username and password)? Duo allows IT and security teams to launch phishing simulations to assess user awareness. These internal phishing simulations look and behave like a real phishing scam, but instead of actually stealing credentials, they alert admins to how users behave in the face of a phish.

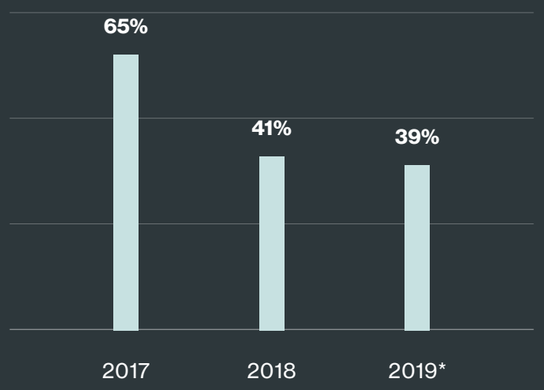
So far in 2019, Duo customers have used **Duo Insight** to launch 3,421 simulated phishing campaigns. Nearly half of those campaigns (47 percent) captured at least one set of credentials, and more than a third (39 percent) involved at least one out-of-date device. That's a slight improvement over the annual averages from the previous two years.

Out-of-date devices are more susceptible to vulnerabilities and attackers can exploit out-of-date devices to gain access to enterprise applications. The decline in out-of-date devices and captured credentials is indicative of a rising awareness in security and in the threat of phishing as more companies work to educate their users about security best practices. It could also be indicative of vendors making it easier for users to update their devices so they'll do it more frequently, ultimately reducing the number of out-of-date devices. For example, Duo's **Self-Remediation** lets admins notify and warn users of out-of-date software at login, enabling users to update their own devices immediately by providing a direct link to the update.

CAMPAIGNS THAT CAPTURED AT LEAST ONE SET OF **USER CREDENTIALS**



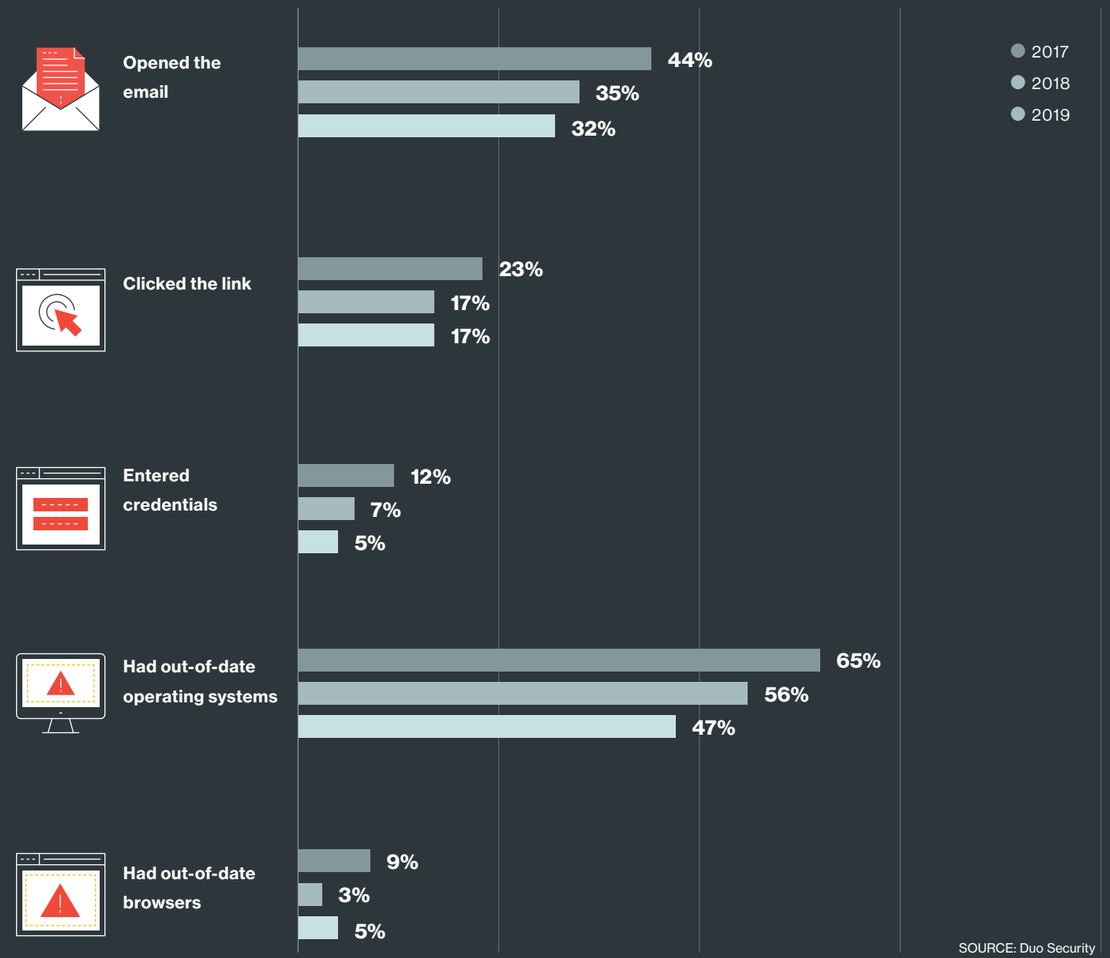

CAMPAIGNS THAT INVOLVED AT LEAST ONE **OUT-OF-DATE DEVICE**




*Based on phishing campaigns through May 13, 2019.
SOURCE: Duo Security



Elsewhere, our phishing simulation data so far in 2019 found that nearly one third of users opened the email, while 17 percent clicked on a link and 5 percent entered their credentials. Here's a detailed view:




SOURCE: Duo Security

Internal phishing campaigns still prove a viable, and valuable checkpoint to gauge the security awareness of users. The good news is, the percentage of users opening emails, clicking links and entering credentials has declined over the last two years. It's a sign that security awareness and education are taking a stronger hold within organizations and users are becoming more aware of what to look out for to avoid being victims of phishing attacks.

Two-factor authentication (2FA) continues to be a strong deterrent to phishers. Between October 2016 and January 2017, Emory University saw a 96 percent decrease in compromised accounts and a 92 percent decrease in the amount of phishing domains they had to block, which they credit to deploying Duo for 2FA. "These numbers prove that Duo has had the effect of both reducing not only the number of compromised accounts we have to respond to, but has also made us a much less attractive target for phishers," the university wrote in a blog post[4].

3.0

# Device Visibility

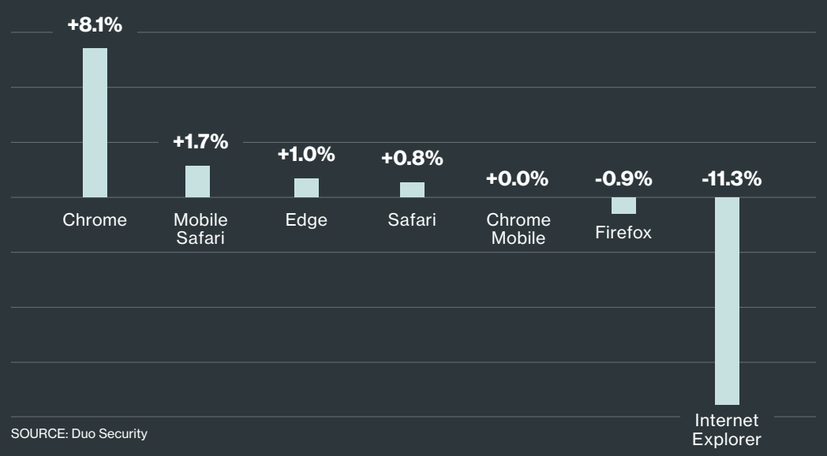
Gaining insight into the devices accessing your data and applications is the second principle of a zero-trust security framework for the workforce. This visibility includes detailed insight into what type of devices are accessing your applications (mobile, desktop or laptop); the browsers and operating systems those devices are running; and whether they're corporate-managed or personally-owned.

## Let's Talk About Browsers & Operating Systems

### Chrome is the Most Popular Browser for Business

Our data found that Chrome further extended its lead among browsers used by Duo customers, while Internet Explorer is seeing the most rapid decline.

**PERCENTAGE (YOY CHANGE)**




SOURCE: Duo Security



## Windows 10 Use Rising; Windows 7 Still a Thing

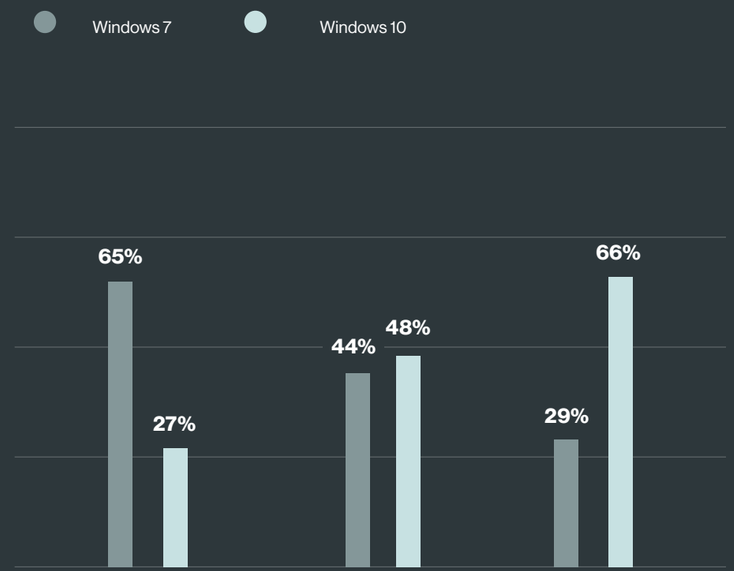
For the second straight year our data shows Windows 10 usage is on the rise, as more devices with Windows installed use the latest OS. Meanwhile, Windows 7 continues its steady decline, as **Microsoft plans to end security updates and support**[5] for PCs running Windows 7 on Jan. 14, 2020.

As Windows 7 use declines, it hasn't necessarily been cast off into the ether. Our data found that 62 percent of the Windows endpoints in Transportation & Storage still run on Windows 7, which is the highest rate by industry. Meanwhile, Healthcare is the most Windows-dominated industry, with nearly half a million endpoints (or 52 percent of Windows endpoints) still running the outdated operating system. Non-Profit, Business Services and Wholesale & Distribution have the smallest percentage of devices still running Windows 7.

Updating operating systems across enterprises with complex IT models and large fleets of devices is no easy feat. For example, Healthcare uses internet-connected devices and software that aren't always designed or updated by vendors to run the latest Windows OS. Some industries, such as Transportation & Storage, also depend on specialized or line-of-business software that may not be updated to run on Windows 10.

Running an older OS can increase an organization's vulnerability to attack. The 2017 WannaCry ransomware attack exploited a vulnerability designed to work against unpatched Windows 7 and Windows Server 2008 systems, **Microsoft said**[6]. Of the 400,000 devices worldwide infected by WannaCry, 98 percent were running some version of Windows 7, according to a **Kaspersky Lab report**[7].

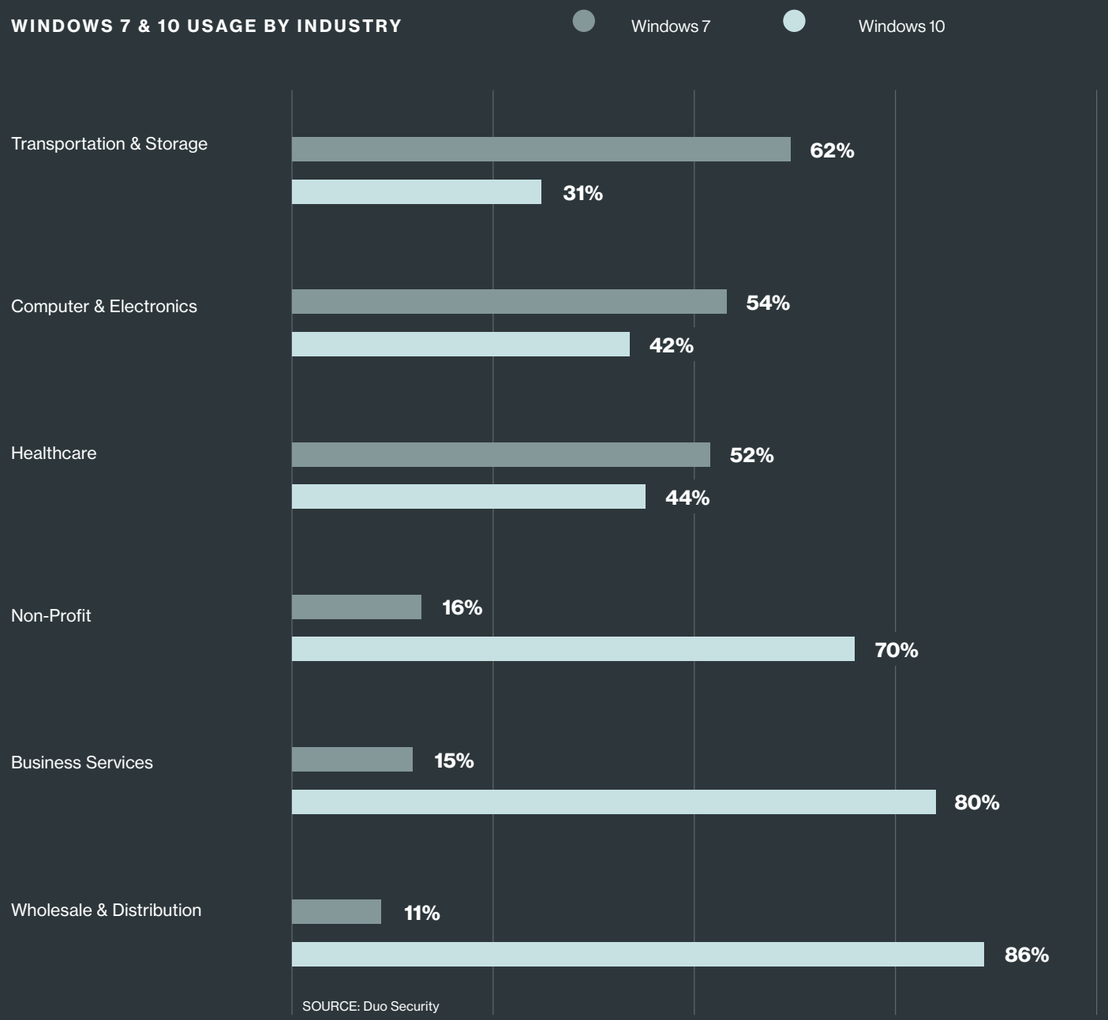
**WINDOWS 10 ADOPTION ACROSS ALL WINDOWS ENDPOINTS**




SOURCE: Duo Security

Meanwhile, the industries that are fastest to adopt Windows 10 are using Windows 7 the least (Wholesale & Distribution, Business Services and Non-Profit), while the top three industries using Windows 7 are the slowest to adopt Windows 10.

**WINDOWS 7 & 10 USAGE BY INDUSTRY**




SOURCE: Duo Security



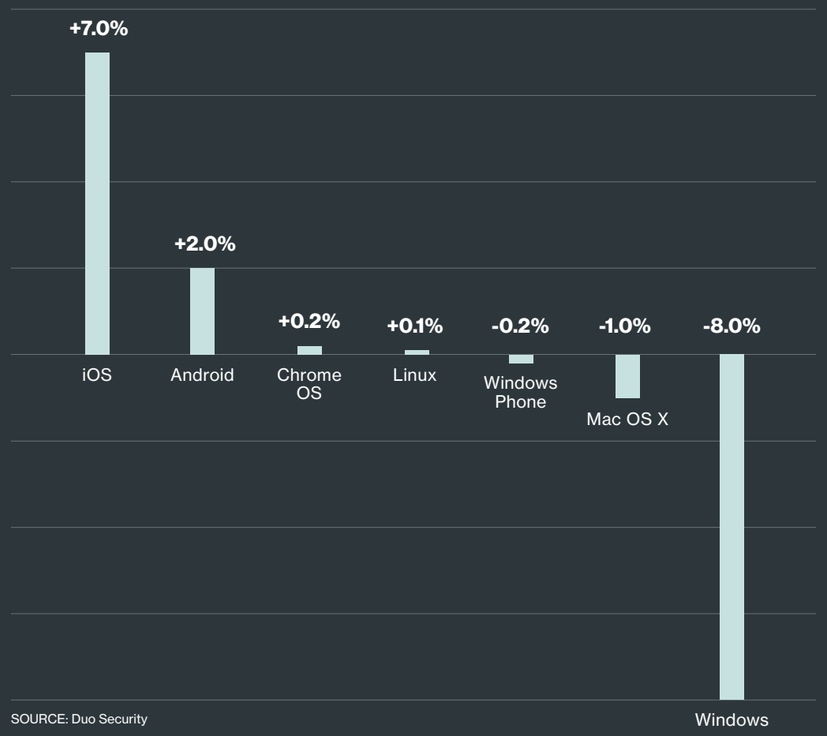
# The Rise of Mobile Work

Access from endpoint devices has grown rapidly over the last two years due to our customers accessing resources with more devices and from more locations. According to our authentication data, roughly a third of all work is done from a mobile device and mobile use for business is up about 10 percent. Without proper protections, such as strong user authentication and device hygiene checks, accessing business applications from mobile devices with out-of-date software and operating systems can introduce risk and increase exposure to threats that exploit user identities, such as social engineering and phishing, and device vulnerabilities.

Windows is still the most commonly used operating system, though its usage is down 8 percent year over year to 47 percent. While both iOS and Android saw upticks: iOS use is up 7 percent to 23 percent and Android is up to 10 percent, representing a 2 percent jump. Meanwhile, Mac OS X slipped 1 percent from last year to 17 percent.

The data suggests that while Windows is the dominant OS, iOS is starting to take a larger stake when it comes to corporate mobile devices.

**PERCENTAGE (YOY CHANGE)**



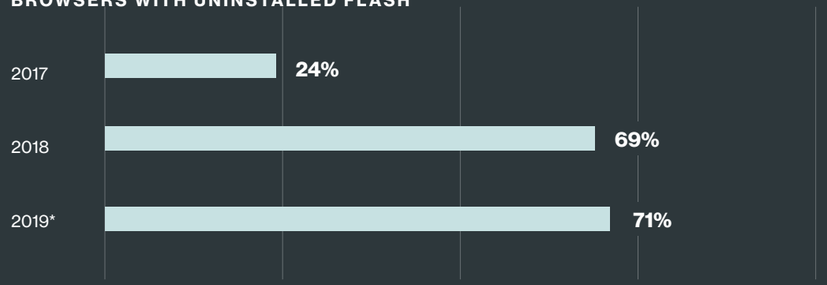

SOURCE: Duo Security

# Is Flash Fading Fast Enough?

Adobe Flash Player saw a major usage decrease from 2017 to 2018, but the mass Flash exodus has apparently slowed, according to this year's data, which shows Flash has been uninstalled on only 2 percent more devices than the previous year.

**Adobe will end of life Flash Player in late 2020**[8], meaning it will stop updating and distributing Flash Player. Many browsers, including **Firefox and Chrome have announced their intentions to disable Flash by default**[9]. For organizations that depend on Flash applications, it's time to start converting them to HTML5 or other standards ahead of Flash reaching end of life to avoid disruption.

**BROWSERS WITH UNINSTALLED FLASH**




SOURCE: Duo Security

*Through May 13, 2019

**Adobe will end of life Flash Player in late 2020.**

4.0

# Device Trust

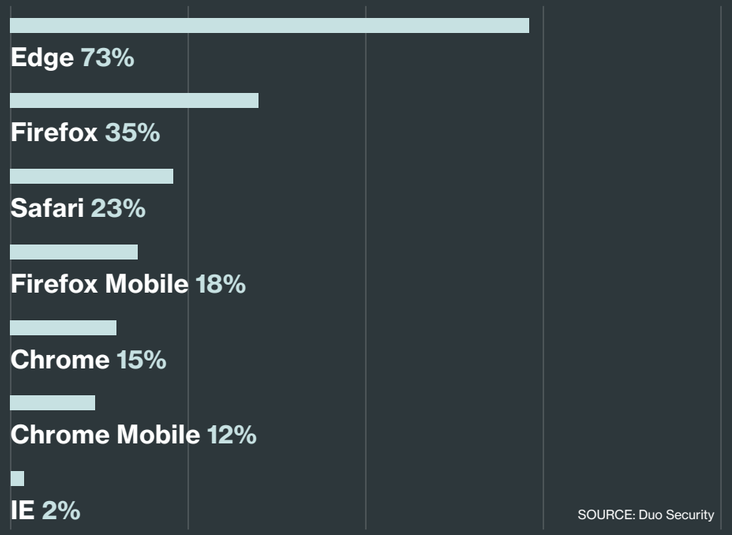
Trust. Trust in users and trust in devices. Establishing device trust is a critical step in the path toward zero-trust security for the workforce, and is one of its key principles. Ensuring device trust includes implementing controls and policies to keep risky endpoints from accessing applications – verifying the trustworthiness of all devices is imperative. Our data shows Duo customers are taking major steps toward establishing device trust to reduce their risk of a breach by flagging out-of-date browsers and operating systems.

## Which Browsers Are Most Frequently Out of Date?

Understanding the browsers user devices are running — and granting or denying access based on whether these browsers are current or out of date — is critical. At the time of data collection, we found that Edge is the most frequently out-of-date browser on end user devices, while Internet Explorer was the most frequently up to date.

When compared to 2018's data, Edge rose to the No. 1 most frequently out-of-date browser from fifth place. That is likely due to Edge being coupled with Windows 10 and enterprises struggling to run the latest and greatest version, according to Ars Technica[10]. Meanwhile, Firefox Mobile's frequency of being out of date dropped dramatically, falling from 2018's most frequently out-of-date browser with 93 percent to fourth place this year at 18 percent. Chrome also became less frequently out of date, shrinking from 53 percent in 2018 to 15 percent in 2019. These significant drops may be partly attributed to Firefox moving toward auto-updates[11] and Chrome encouraging users to turn on automatic updates[12] to always ensure they're running the latest version. IE is still the most frequently up to date, dropping from being out of date 5 percent of the time in 2018 to just 2 percent in 2019, which is likely due to IE not releasing a new version in 2013.

**OUT-OF-DATE BROWSERS**




SOURCE: Duo Security

## Chrome Vulnerability Drives Spike in Out-Of-Date Browser Policy Use

Google discovered a **zero-day vulnerability**[13] in Chrome in March 2019 that the Google Threat Analysis Group determined was being exploited in the wild. The vulnerability resided in the web browsing software and impacted all major operating systems, including Windows, Apple macOS and Linux. If a user opened a PDF in a compromised browser, an attacker could hijack the browser and use it to get into the system and execute arbitrary code. Google quickly released a patch, which required users to update Google Chrome to the latest version.

According to our data, news of the Chrome vulnerability was heard loud and clear by Duo customers. Our data shows a noticeable spike in the number of Duo customers enforcing a policy to only grant access to data and applications from the latest browser versions, which also prompts users to update to the latest browser at the time access is attempted.

**30x**

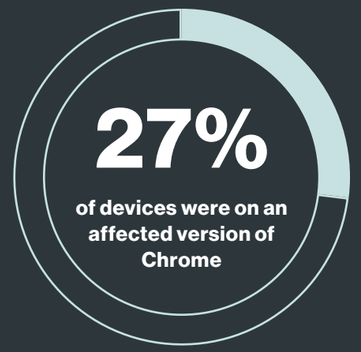
**Increase in Denied Authentications**

**79%**

**Increase in Out-of-Date Browser Policy Implementation**

The day the Chrome vulnerability was widely announced (March 7), the number of authentications denied due to out-of-date browsers, platforms or plug-ins was more than 30 times higher than the average from the prior week due to our customers implementing the browser out of date policy. The policy spike demonstrates a 79 percent increase in usage of the policy setting where no out-of-date browsers were allowed access. The increase in use of the out-of-date browser policy around the Chrome vulnerability shows that incident response teams are using and updating Duo policies to protect against zero-day vulnerabilities and exploits as they're discovered and announced to ensure potentially compromised devices can't access critical applications and data.

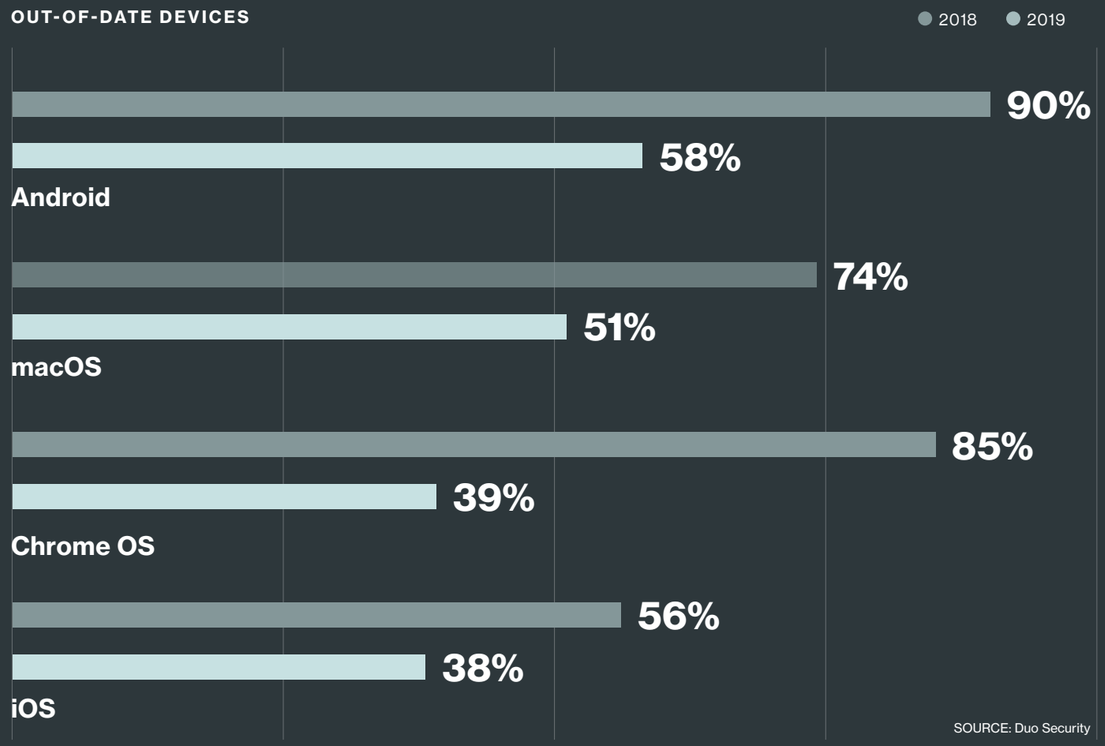
Duo customers also kept that policy active in the weeks following the announcement. Overall, 27 percent of authentications that used Chrome during the five weeks after the announcement of the zero-day vulnerability were on a version affected by the bug, meaning only accepting the latest browser version helped protect critical applications and improved security.



# Android Again Leads Out-of-Date Devices

For the second year running, iOS endpoints are most frequently running the most up-to-date version of their operating system, while Android is most frequently out of date, according to our data. Meanwhile, more than 90 percent of Android devices are not running the latest security patch – as of May 31, 2019 only 9.7 percent were on the latest patch, which had been released 26 days prior. NOTE: For this data, a device is considered "out of date" if it's not running the latest OS version.

**OUT-OF-DATE DEVICES**




SOURCE: Duo Security

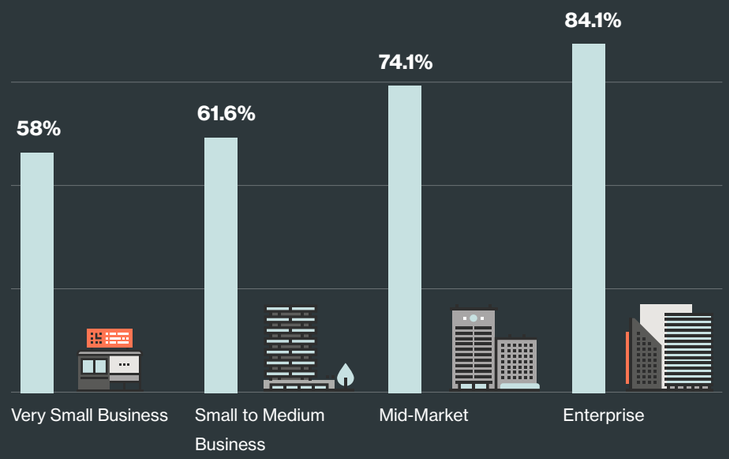
Out-of-date devices are more susceptible to vulnerability and can introduce risk to an organization. Improving visibility into the security health of devices accessing your network helps reduce risk.



# Big Business Locks Down BYOD

As more companies allow users' personal devices to access resources on their network, often known as bring your own device (BYOD), our data found smaller businesses are allowing untrusted devices, or endpoints without a device certificate installed, to access corporate data more than larger organizations, potentially leaving them at risk. Customers who use Duo's Trusted Endpoints typically have a certificate installed on all endpoints that authenticate through Duo. This is especially true for larger customers.

**TRUSTED ENDPOINT CUSTOMERS WITH NO UNTRUSTED ENDPOINTS**




While more customers are only granting access to trusted endpoints, some organizations are still granting access to untrusted endpoints, into which they have less visibility or insight. For example, 42 percent of very small businesses have one or more untrusted endpoints deployed. Identifying trusted endpoints gives organizations more control over which devices access which applications and allows organizations to reduce the potential risk of untrusted devices accessing applications. Duo allows its users to define which endpoints are trusted and grant secure access to applications with device certificate verification policies.

### TRUSTED DEVICES VS. UNTRUSTED DEVICES

The Trusted Endpoints feature in Duo Beyond helps you define and distinguish between trusted endpoints and untrusted endpoints that access your applications.

Installing a Duo certificate marks a device as "trusted," which means it's either owned and/or managed by your organization, or it's known, as in it's been seen before and it is expected to be seen again, like with BYOD.

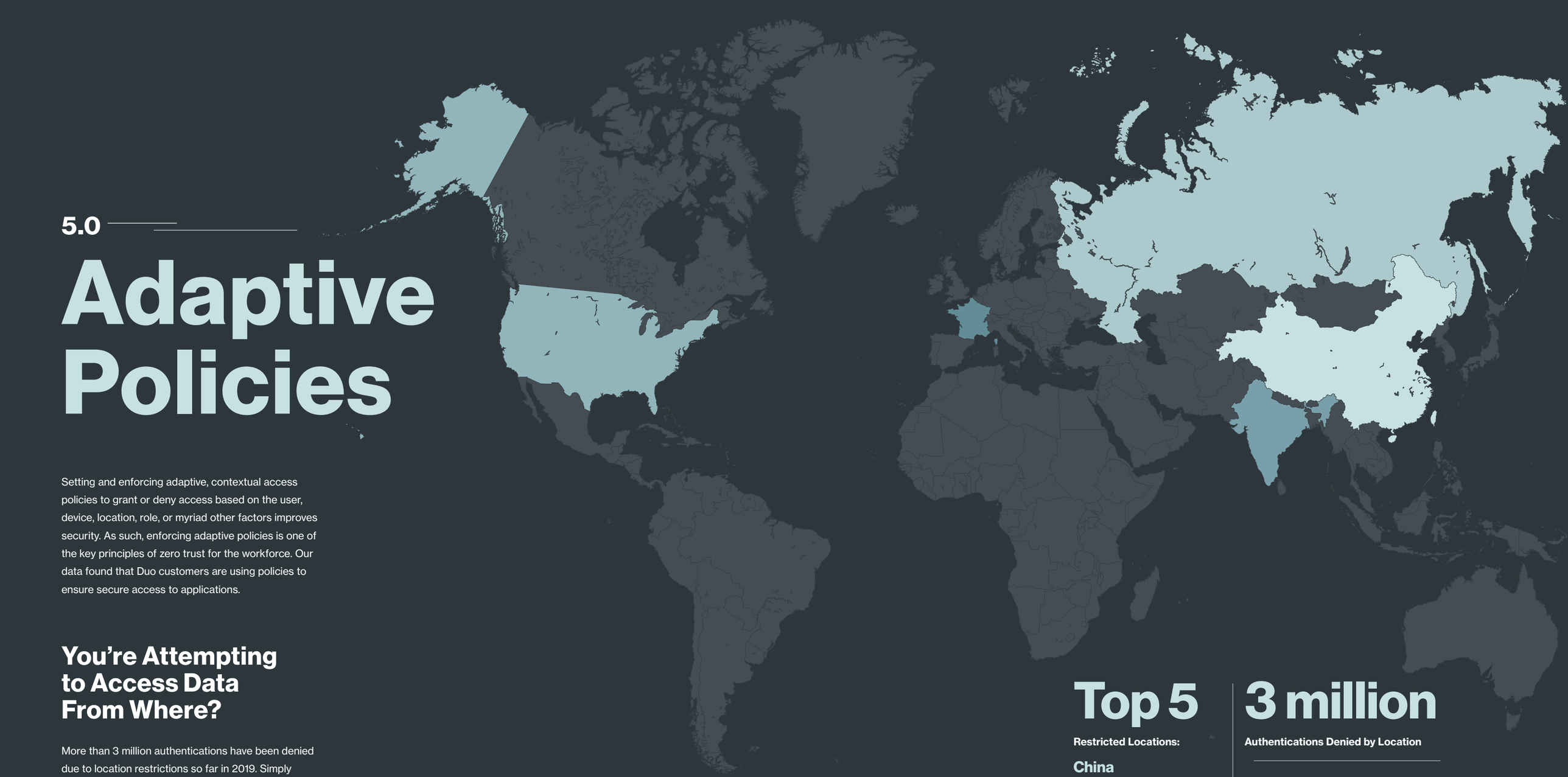
5.0

# Adaptive Policies

Setting and enforcing adaptive, contextual access policies to grant or deny access based on the user, device, location, role, or myriad other factors improves security. As such, enforcing adaptive policies is one of the key principles of zero trust for the workforce. Our data found that Duo customers are using policies to ensure secure access to applications.

## You're Attempting to Access Data From Where?

More than 3 million authentications have been denied due to location restrictions so far in 2019. Simply put, businesses have put rules in place that block attempts to access corporate data or applications from specific locations. Of these denied authentication attempts, about 10 percent originated in China, more than 100 times as many as Russia, which was the next-highest location. Overall, authentications denied by location restrictions so far in 2019 came from 178 different countries.



**Top 5**

**Restricted Locations:**

**China**
**Russia**
**United States***
**India**
**France**

**3 million**

**Authentications Denied by Location**

**178**

**Countries with Denied Authentications**

*The U.S. is the third restricted location due to companies based outside of the U.S. not allowing users to authenticate from outside of their home country.

# Frequently Used Policies

The most frequently used policies implemented and enforced by Duo customers run the gamut. From denying access from anonymous IP address to requiring encryption and screen locks on user devices. Here are the four most frequently used policies in the U.S. and Great Britain:

- Disallow Rooted Devices
- Require Device Lock On
- Require Encryption
- Disallow Anonymous IP Addresses

The list of most frequently used policies presents an interesting hierarchy regarding the level of difficulty in enforcing them. Disallowing rooted devices creates little friction among end users, making it easier to enforce, while admins may face resistance from end users who find requiring device locks and encryption and not allowing access from anonymous IP addresses disruptive.

The ability to set and enforce fine-grained access policies puts admins and IT security pros in control over what they'll allow. Our research found that businesses that protect sensitive or classified information, such as Financial Services and Business Services, tend to enforce security policies, such as requiring encryption and screen locks, more frequently than other sectors like Retail and Manufacturing.

Our research shows that customers who enforce security policies are successfully blocking authentication attempts from out-of-policy devices. For example:

### RESTRICTED LOCATIONS

**51%**

of customers who use the location restriction policy have blocked at least one authentication attempt a month from a restricted location

### SCREEN LOCK

**27%**

of customers who require devices to have a screen lock have blocked at least one authentication attempt a month from devices without a screen lock enabled

### DISK ENCRYPTION

**22%**

of customers who require disk encryption have blocked at least one authentication attempt a month from a device without encryption enabled

### ANONYMOUS IP

**20%**

of customers who disallow access from anonymous IPs have blocked at least one authentication attempt a month from an anonymous IP address

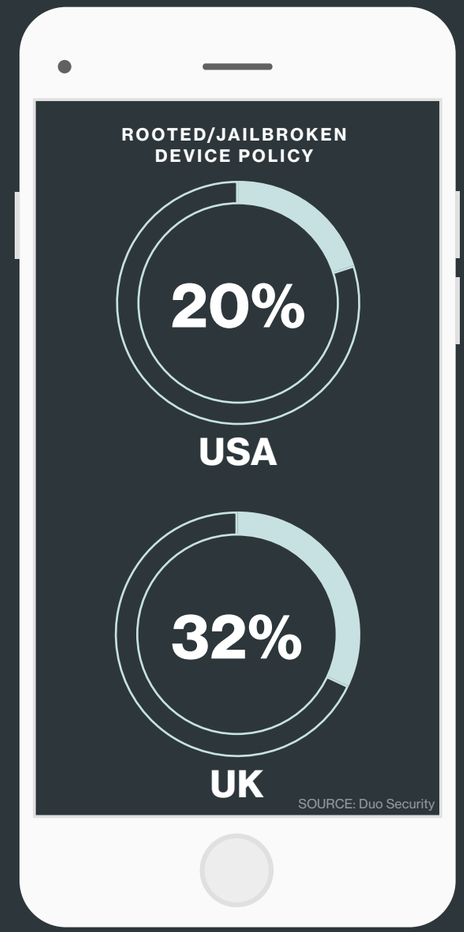


# Tonight There's Gonna Be a Jailbreak...

Early in the smartphone age, jailbroken/rooted phones were a big thing. You could take control of the device, install apps and make tweaks that weren't authorized by manufacturers and bypass security protections.

More than 20 percent of Duo customers in the United States set a policy to disallow rooted/jailbroken devices from accessing applications, while more than 32 percent of customers in Great Britain don't allow access from rooted or jailbroken devices.

Over the years, the total number of jailbroken/rooted devices used to attempt authentication has dropped to well below 1 percent to 0.3 percent. When looking at specific device types, Android leads the charge for jailbroken/rooted devices, with 0.8 percent jailbroken/rooted devices, while Apple is a mere 0.09 percent. Despite there being 2.4 times as many iOS phones than Android phones using Duo, we see roughly 3.6 times more jailbroken Android devices than iOS devices. Jailbreaking devices is slipping in popularity mainly due to jailbreaking only adding minor improvements. OS security has also improved, which makes it more difficult to jailbreak devices.



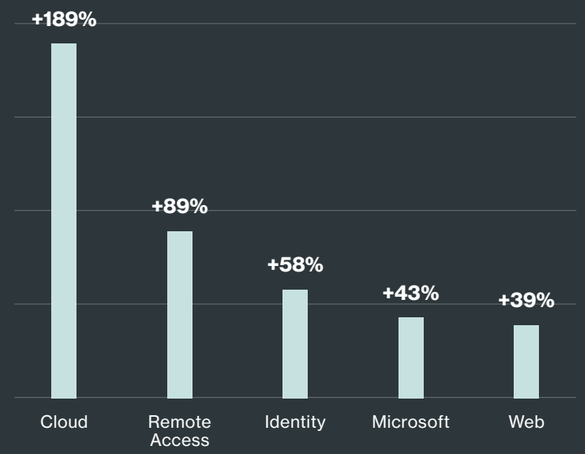
6.0

# Application Access

At the end of the day, zero-trust security for the workforce is all about ensuring only trusted users and devices have access to business-critical applications and data. The name of the game is secure access. Much of the push toward zero-trust architectures is precipitated by the prevalence of cloud and mobility. Our data shows that the use of cloud applications is on the rise and more customers are moving applications to the cloud as they embark upon their zero-trust journeys.

While integrations are up across most key categories, cloud application integrations are skyrocketing with the number of customers per application up nearly 200 percent (189 percent, to be exact) and the number of authentications per customer per app rising sharply by 56 percent. Remote access usage is also experiencing growth (customers per app is up 89 percent), as users work outside of offices yet still require access to applications.

**APPLICATION INTEGRATION GROWTH**
(Number of Customers Using Each Cloud App)

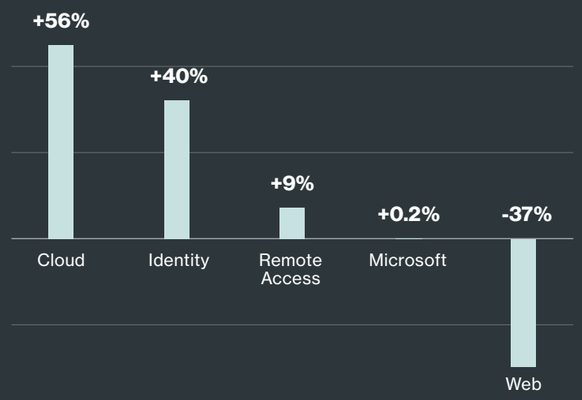



SOURCE: Duo Security

## Rocketing Into the Cloud

As more businesses adopt a cloud-first approach to application procurement and deployment, our data shows cloud application use has grown dramatically from 2018 to 2019 across Duo's customer base (both in the number of cloud applications customers are accessing and the number of customers accessing each cloud app).

**YEAR-OVER-YEAR APPLICATION INTEGRATION GROWTH**



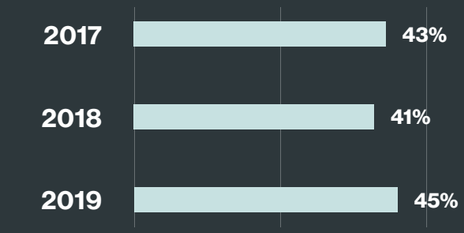

SOURCE: Duo Security

## App Access: Anywhere, Any Time

Mobility and cloud computing empower users to work from anywhere, on any device at any time. Our data shows nearly half of all requests to access protected applications and data come from outside the corporate office and network, which is a slight increase over the previous two years.

In 2019, 45 percent of requests to access protected apps came from outside the business walls, showing that users are truly mobile.

REQUESTS TO ACCESS PROTECTED APPS
**FROM OUTSIDE THE OFFICE**




SOURCE: Duo Security

7.0

# Summary

In summary, analyzing data on more than half a billion authentications per month, nearly 24 million devices, and more than 1 million applications and services reveals that Duo customers are diving head-first into zero-trust security and are adopting the principles of zero trust to protect their workforces, the users and the devices that access their critical business applications. Our data found that our customers are:

## Establishing user trust

## Gaining visibility into devices

## Establishing device trust

## Enforcing adaptive policies

## Enabling secure access to all apps



## Several of our key findings point to the adoption of these principles, including:

- The continuous rise of biometrics and passwordless authentication to verify user identities
- The decrease in the volume of credentials captured and out-of-date devices discovered through internal phishing campaigns
- The rise in Windows 10 use and the decline in Windows 7 use as users transition to more secure OS versions
- The flagging of out-of-date browsers and operating systems
- The spike of out-of-date browser policy used to block access from Chrome versions affected by the recent zero-day vulnerability
- The ongoing decrease of authentication attempts from jailbroken/rooted devices
- The enforcement of adaptive and contextual access policies
- The increased usage of cloud, remote access and identity applications

A zero-trust architecture for the workforce is a paradigm shift. It grants or denies access based on the trustworthiness of users and their devices, which comprise your workforce, and does so wherever access happens, instead of relying on a traditional perimeter security model.

As cloud and mobility continue to become must-haves, the enterprise must be able to give users access no matter where they are, regardless of which type of device they use or which applications they need to access. Implementing and adhering to the principles of zero-trust security for the workforce can make that happen.

# References


[1] ***Duo Aligns With NIST on New Authentication Guidelines***; Duo Blog; July 28, 2016

[2] ***NIST Shouted, Who LIstened? Analyzing User Response to NIST's Guidance on SMS 2FA Security***; Duo Blog; December 1, 2016

[3] ***WebAuthn Guide***; Duo Security; 2019

[4] ***Duo Two-Factor Authentication a Major Increase In IT Security***; Emory University, March 10, 2017

[5] ***Support for Windows 7 is Ending***; Microsoft; 2017

[6] ***Ransom:Win32/WannaCrypt***; Microsoft; January 10, 2018

[7] ***43% of Businesses Are Still Running Windows 7, Security Threats Remain***; Help Net Security; January 15, 2019

[8] ***Flash & The Future of Interactive Content***; Adobe Blog; July 27, 2017

[9] ***Mozilla: Firefox 69 Will Disable Adobe Flash Plugin by Default***; ZDNet; January 14, 2019

[10] ***Edge Dies a Death of a Thousand Cuts as Microsoft Switches to Chromium***; Ars Technica; December 6, 2018

[11] ***Mozilla Makes It More Difficult to Block Firefox Updates***; ghacks.net; July 28, 2018

[12] ***Update Google Chrome***; Google Chrome Help; 2018

[13] ***Minimizing Your Exposure to Chrome's Zero-Day Exploit***; Duo Blog; March 7, 2019



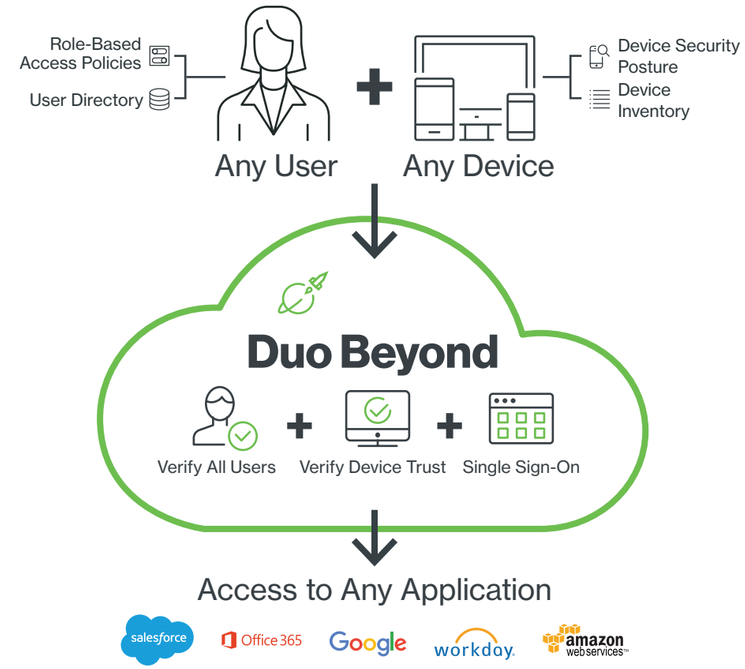

# Duo Beyond

## Zero Trust for the Workforce

With **Duo Beyond**, you'll receive:

**Full-featured two-factor authentication for every organization:**

- Protect logins with **Duo's MFA**
- Insight into an overview of **device security hygiene**
- Manage Duo's solution with **Admin APIs**
- Duo's secure **single sign-on (SSO)** provides a consistent user login workflow across all applications
- Protect access to both **on-premises and cloud applications**




**Essential access security suite to address cloud, BYOD and mobile risks:**

- Complete visibility into both mobile and desktops, including **corporate-managed and unmanaged** (personally-owned) devices to support BYOD policies
- Mobile device breakdown with visibility into enabled **security features and tampered or unencrypted devices**
- Enforce rules on who can **access which applications, under what conditions** (adaptive authentication)
- Enforce a policy to **allow only managed devices** access to sensitive applications
- Provide modern **remote access to multi-cloud environments** (on-premises, Azure, AWS, Google Cloud Platform) while enforcing zero-trust security principles
- **Notify users** to update their devices based on device access policies
- Identify users vulnerable to phishing through **phishing campaigns**
- Full-featured dashboards and custom reports for **compliance audits** and ease of administrative management

Learn more about Duo Beyond in our **documentation**.