THE 2020 DUO

Trusted Access Report

Ensuring Secure Access Amid a Major Shift to Remote Work

Duo Security is now part of Cisco.

THE 2020 DUO

Trusted Access Report

Ensuring Secure Access Amid a Major Shift to Remote Work

Version 1.1

1.0

When Work From Home Becomes the Norm

Over the past few decades, modern computing has enabled organizations across all industries and sizes to accommodate remote work. Most people have worked from airports, coffee shops and hotels from time to time. Some companies have offered remote work options, either full time or a few days a week. Some startups even lack physical office space altogether, opting instead for a fully remote workforce that gets together in person at scheduled times for company all-hands events.

The benefits of enabling remote work are plentiful: it can lower capital costs associated with physical office space, reduce the environmental impact of commuting, and provide better work/life balance for employees.

But when the COVID-19 virus spiraled into a pandemic and global health crisis in early 2020, many companies were forced to quickly revamp or revise their remote work policies and for much of the workforce, work from home was deemed the new normal.

According to a survey conducted by **CSO Online**[1], as of March 23, 2020, 77.7% of survey respondents were working from home at least 60% of the time – that's a jump from 16.55% just three months prior. **Global Workplace Analytics**[2] estimates that 25% to 30% of the total workforce will continue working from home multiple days a week through the end of 2021.

While remote work had already been steadily climbing – largely driven by the boom of cloud and mobile technologies, along with security improvements that protect devices roaming outside of the office – many organizations weren't fully prepared to shift to remote work at such massive scale.

Securing Remote Access at Scale

The almost instantaneous spike in remote work presented businesses with new security challenges. Organizations must ensure their employees have secure access to the tools and resources they need to do their jobs, without introducing additional friction into their daily workflows. At the same time, these organizations must protect critical information and minimize risk, all while accommodating myriad types of users and devices using unsecured networks.

There's always been a delicate balance between security and convenience, and working to maintain that balance is paramount during major workplace transitions.

For *The 2020 Duo Trusted Access Report*, our data shows that more organizations across all industries are enabling their workforces to work from home now, and potentially for an extended period of time. They're also implementing the appropriate security controls to ensure secure access to applications. In this report, we'll look at how companies are currently securing remote work and what makes a solid and secure remote access strategy.

Methodology

A secure remote access strategy comprises three key pillars: users, devices and applications. It asks the questions:

Users

Who has permission to access your information?

Devices

Which devices are being used to access applications?

Applications

Which applications are users accessing?

For this report, Duo's Data Science team analyzed data from more than 26 million devices, more than 500,000 unique applications and roughly 700 million monthly authentications from across our customer base, spanning North America, Western Europe and Asia-Pacific.

700 million

Authentications per Month

26 million

Devices

500,000+

Unique Applications

Key Findings

An at-a-glance look at 10 top trends.

The Remote Reality

Our data shows a 60.1% swell in daily authentications from outside of physical offices, using VPN and RDP technology.

So Long, SMS

Policies to disallow SMS as an authentication method increased by 85%.

Cloud Skyrockets

The average number of daily authentications to cloud apps increased 40%.

Biometrics Booming

More than 80% of active customer devices have biometrics enabled, and total devices with biometrics rose 64%.

iOS Updated Most

iOS devices are nearly four times more likely to be updated within 30 days of a security update or patch, compared to Android devices.

Locations Blocked

Roughly 70% of Duo customers who implement location-based policies restrict access from China and Russia.

Push Preferred

Duo Push is the most used authentication method, accounting for 68.6% of all authentications.

Out-of-Date Failures

Authentication failures due to out-of-date devices increased 90.5% during the first three weeks of March.

Enterprises Go Remote

Enterprise remote access application usage surged by 32.2% based on monthly authentications per user.

Windows 7 Wanes

Windows 7 use dropped to its lowest level yet, with only 10% of Windows devices remaining on the outdated OS.

2.0

Going Remote

Remote Access Climbing

It's no surprise that authentications to remote access applications are up across businesses of all sizes. Organizations are accessing applications from outside of the office using VPN and RDP technology, and they're protecting those logins with two-factor authentication.

When comparing the time periods from June 2019 to February 2020 and March 2020 to June 2020, our data shows daily authentications to Duo increased by more than 5 million authentications per day, with 71.9% of the increase being due to remote access (VPN and RDP).

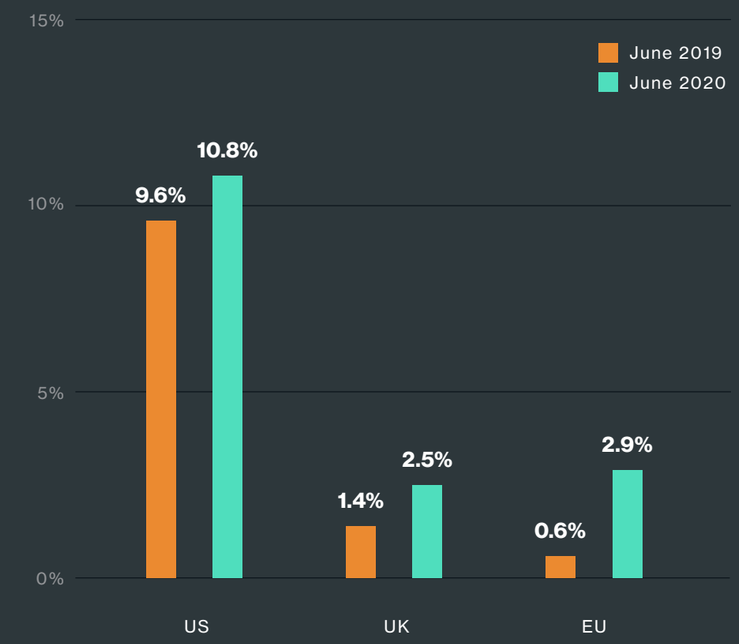
Overall, daily authentications to VPN and RDP technologies rose 60.1% year over year.

Cloud Use Surges

Access to cloud applications also surged starting in March 2020, when many organizations shifted to a remote work model. According to our data, the period from March to June 2020 saw a 40% rise in average daily authentications to cloud applications over the average from June 2019 to February 2020.

We also examined the change in authentications to cloud applications in the United States, the United Kingdom and the European Union. We looked at the percent of authentications to cloud applications as a fraction of the overall authentications from each region. When comparing June 2019 and June 2020, we found that each region saw an increase in authentications to cloud applications, with the European Union experiencing the largest spike, while the U.K. saw the smallest uptick.

AUTHENTICATIONS TO CLOUD APPS

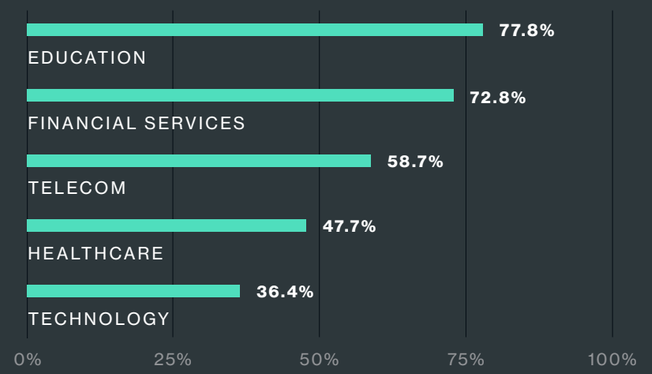


Industries Where Remote Access Rules

We looked at the top five industries leading the remote access charge with the highest rates of VPN and RDP authentications. Of these, Education saw the largest increase, while Technology saw the smallest bump.

Our data shows that all five of these key industries saw a major boost in remote work during March, and that they're taking the appropriate steps in securing remote access by coupling strong authentication with VPN and RDP solutions.

CHANGE IN DAILY AUTHENTICATIONS TO REMOTE TECH

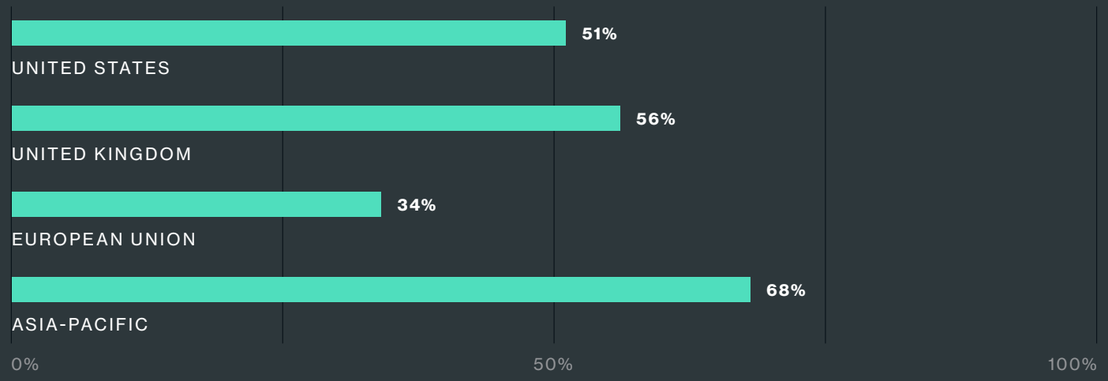


*This chart shows the percent change between average daily authentications computed from June 2019 to February 2020 and the average computed from March 2020 to June 2020.

Regional Remote Access

We also examined which geographies were seeing the largest increases in remote access technology use. In the U.S., for example, the average daily authentications to VPN or RDP technology grew 51% from February to June 2020.

REMOTE ACCESS TECHNOLOGY USE INCREASE BY REGION



While all regions saw an overall increase in remote access technology use from February to June 2020, our data shows that some regions, such as the U.S. and Asia-Pacific, relied more on remote access technologies for longer periods of time as work from home orders continued in those areas. The U.S. and Asia-Pacific saw remote access technology use increase from February to April 2020 and continue to increase from April to June 2020. Meanwhile, the United Kingdom and the European Union saw remote access technology use grow from February to April 2020, but the percentage change in average daily authentications started to decrease in the April to June timeframe.

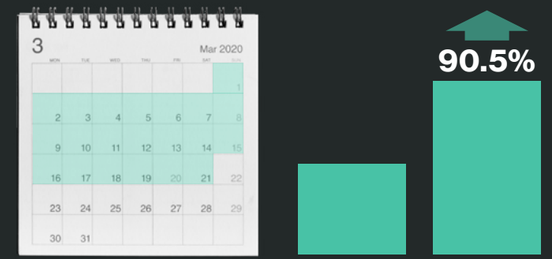
"If we look at the COVID-19 tracking data for cases in the European Union at that point in time, we see that there was a definite drop in the number of cases from a high water mark in March," said Dave Lewis, Global Advisory CISO, Duo Security at Cisco. "As the cases began to decline there was a fragmented return to normalcy. This presented itself when some people started to return to work in April. Conversely, workforces in the United States and Asia-Pacific continued to work remotely in an effort to stem the tide of new cases."

"The drop off in the use of remote access seems to reflect the back to work trends as well as the economic environment," said Richard Archdeacon, Advisory CISO for EMEA, Duo Security at Cisco. "**Research** in July showed different levels in the return to the workplace. In France, over 80% of office staff had returned to work. By contrast, in Spain, Italy and Germany around 75% were returning to work. The trend was much lower in the U.K., where just over 50% of workers had returned to work. In London, the figure of those still working remotely was as high as 69%. There may be other influencing factors. For example, service industries were 80% of economic output in the U.K. and this may have made it easier for parts of the economy to work remotely and stay that way. What will be watched closely is the trend towards the end of 2020 to see if the WFH trend remains solid or becomes more nuanced with workers still going to their place of work, just not so often."

How Remote Work Impacts Device Health

As work from home becomes a new reality for many, device health becomes even more important. Many users are accessing corporate applications from their own, unmanaged devices. Bring your own device (BYOD) has become more common. To understand the state of device health while working from home, we examined the number of authentications that failed due to out-of-date devices across the first three weeks of March 2020, when the majority of companies closed offices and implemented strict work from home policies.

> Our data shows a **90.5% increase** in out-of-date device authentication failures during the first three weeks of March.



This massive jump is likely related to the devices on which users are accessing data. They may be using different or additional personal devices for work, and if these devices haven't been updated recently, they're likely to fall outside of an organization's out-of-date device policy.

> "When companies around the globe found themselves in the unenviable position of having to transition to a fully remote workforce, this did not come easily," said Lewis.

"Many companies had to scramble to acquire the requisite assets they needed to be able to supply their employees with laptops for remote work. Some workarounds occurred where companies had to rely on the use of personal devices or BYOD in order to shore up for the near term. The priority for many organizations was in keeping the lights on and accepting risks in order to accomplish this end."

3.0

Users

Users are the cornerstone of a remote access strategy – they comprise the workforce and require access to corporate applications and assets. As the workforce becomes more distributed, verifying users' identities before granting access is imperative. Organizations must have security mechanisms in place that require users to prove who they are while also providing users frictionless, secure access to protect against credential theft and other potential threats. For many organizations, verifying user identities starts with strong authentication.

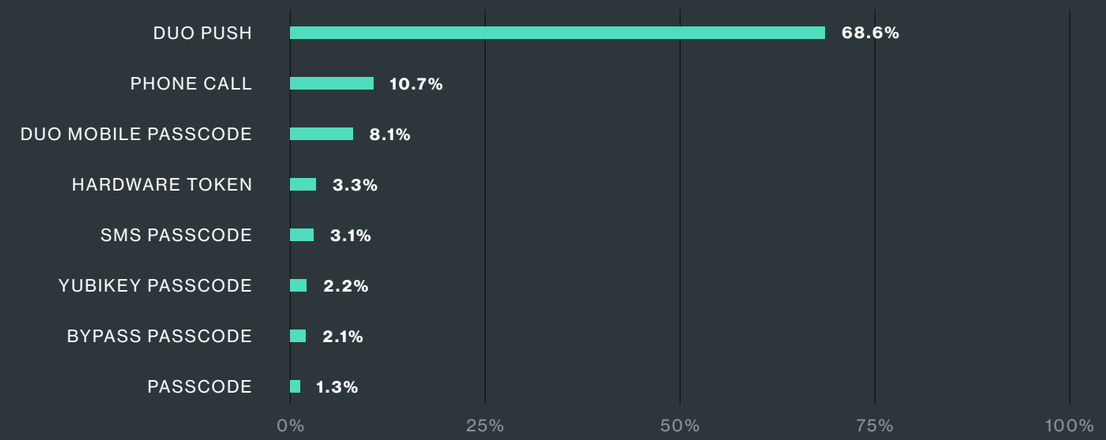
Users Opt for More Secure Auth Methods

While Duo has long said that any authentication is better than no authentication at all, not all authentication methods are created equal. That's why we recommend Duo Push or U2F as the most secure authentication methods.

Our data shows that while working remotely, organizations are opting for more secure authentication methods, getting the nudge they need to finally move away from methods that have long been deemed less secure. We're looking at *you*, SMS.

TOP AUTHENTICATION METHODS

Duo customers can choose from several authentication methods based on their specific use cases. Here's how Duo customers authenticate:



SMS Use Shrinking

The National Institute of Standards and Technology (NIST) updated its guidelines in 2016, declaring that SMS-based authentication methods were no longer secure because:

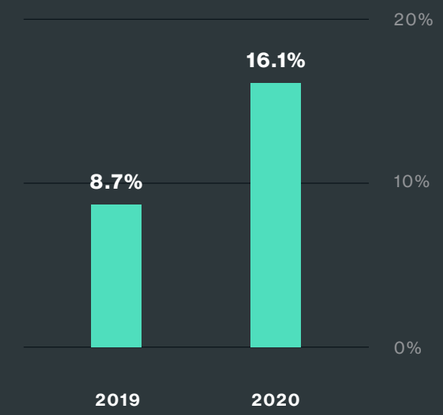
1. **The phone may not always be in possession of the phone number.**
2. **SMS messages can be intercepted and not delivered to the intended phone.**

Duo customers are taking notice of the change. Our data shows that only 3.1% of authentications are performed through SMS.

Duo customers are also using policies to disallow the use of SMS authentication, which helps them align with NIST recommendations. The percentage of customers with policies in place to disallow SMS-based authentication has increased by 7.4%—that's an 85% swell in the number of customers that ban SMS as an auth method—from 2019 to 2020.

"SMS is one of the more common methods for two-factor authentication. The problem here is that SMS is not a secure medium by definition," said Lewis. "Attackers have the capacity to intercept these messages using a wide variety of tools. Since the SMS is tied to the phone number of the individual, this is a target of opportunity for attackers to leverage attacks such as SIM swap attacks that will allow the attacker to clone the SIM card and thereby intercept 2FA messages and potentially take over the victim's accounts."

CUSTOMERS WITH SMS DISALLOWED



> "The problem here is that SMS is not a secure medium by definition. Attackers have the capacity to intercept these messages using a wide variety of tools."
>
> **–DAVE LEWIS**
> ADVISORY CISO, DUO SECURITY AT CISCO

Authentication Method Usage by Industry

Different use cases require different **authentication methods**.[4] We examined which authentication methods are used most frequently across various industries. While Duo Push is the No. 1 authentication method across all industries examined, the second most frequently used method varies widely based on industry. For several industries, mobile passcode, which lets users confirm their identity with a secure passcode generated by a physical token, a mobile device or a network administrator is the second most used authentication method. Phone callbacks are also in the top three across most industries, while in Healthcare, it's the No. 2 authentication method by a wide margin. Remembered device, which allows a device to be remembered upon an authentication and thus be deemed trustworthy, thereby requiring two-factor authentication less frequently, has also become one of the most used authentication methods, especially in Education, where it ranked a close No. 2.

"Industries will vary on the type and scope of their authentication methods for myriad reasons. The risk appetites will change from one organization and vertical to the next. As a result we see some industries leading the charge such as Media & Entertainment, Financial Services and Technology. They did so via the use of stronger authentication regimens such as Duo Push technology," Lewis said.

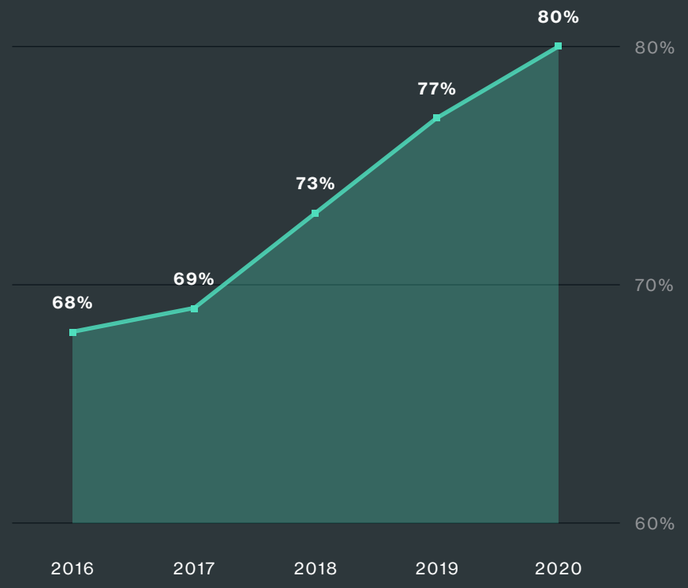
> "Industries will vary on the type and scope of their authentication methods for myriad reasons."

Are Passwords Passé?

As we approach a **passwordless future**[5]—yes, there is life after passwords—Duo customers are relying more and more on biometrics as a form of authentication. We've seen a steady uptick in the number of active customer phones with biometrics enabled, such as Apple Touch ID and Face ID, and Android fingerprint scanners.

"Passwords are akin to cuneiform in many ways," said Lewis. "They served their purpose at a point in time, and while we can understand the legacy that they have provided us, we need to evolve beyond the confines of what was once seen as the lingua franca for security. We have better ways to handle authentication now. There is multi-factor authentication, biometrics and even a future with passwordless. The days of the venerable password are coming to their end."

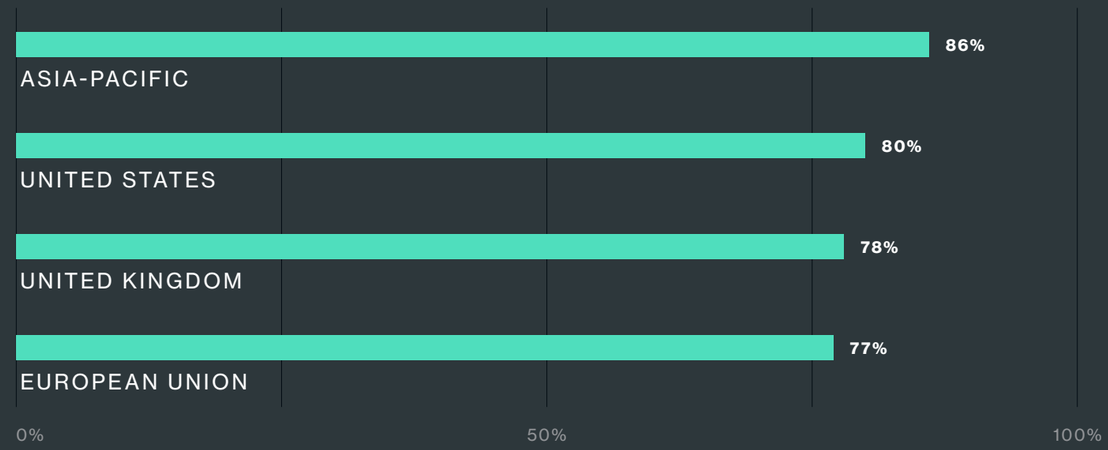
ACTIVE PHONES WITH BIOMETRICS ENABLED



Meanwhile, the total number of active Duo customer phones with biometrics enabled has increased 64%, rising from 5.4 million in 2019 to 8.9 million this year.

On a global scale, the Asia-Pacific region is the leader in biometrics adoption: 86% of customer devices in APAC have biometrics configured.

A GLOBAL LOOK AT BIOMETRICS



The Path to Passwordless

Growth in biometrics use indicates that users are starting to shy away from passwords as a form of authentication. Passwords have been proven ineffective as a security measure – they're relatively easy to crack because people tend to use the same password across multiple sites and applications or create passwords that are too short and too simple.

Moving toward passwordless authentication gradually reduces an organization's reliance on passwords, reducing the risk passwords pose. The path to passwordless starts with strong authentication and relying less on passwords for access.

> "Sixty years after adopting the password as the primary authentication factor, we're at a unique moment in history, where we can both improve the user experience and increase the security posture."
>
> **–J. WOLFGANG GOERLICH**
> ADVISORY CISO, DUO SECURITY AT CISCO

4.0

Devices

As the makeup of the remote workforce changes, so do the environments and circumstances in which people are working. Controlling these many variables can be a major challenge for companies. While strong authentication helps verify identity, it's almost impossible to ensure that people – even those deemed trustworthy – are using trusted networks and securing their data properly. Under these circumstances, devices become a key piece of the security puzzle. Good device health practices can help companies control for location, operating system, encryption status, and more. But how do you define a "healthy" device? And how do you gain visibility into user devices without violating their privacy – as a great deal of access now happens from personal devices?

Whether devices are corporate-managed or BYOD, a rock-solid secure remote access strategy starts with establishing device trust.

Device-Based Policies

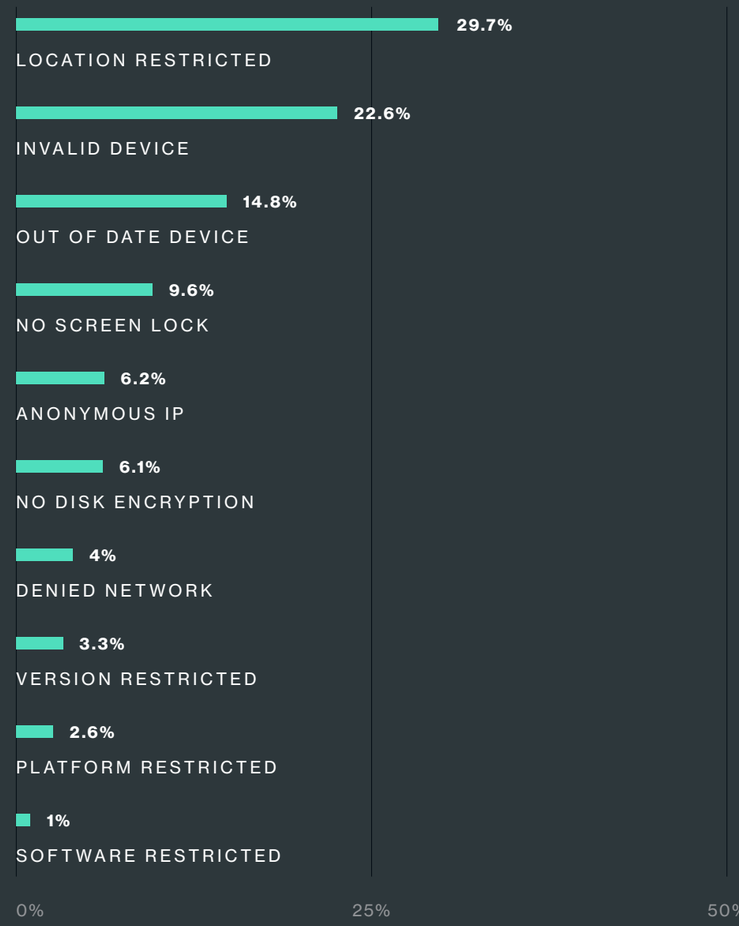
One way to ensure only secure and trusted devices can access applications and services is through implementing and enforcing **device-based policies**.[6]

Device-based policies help organizations prevent potentially compromised or risky devices from accessing data. You can apply security policies across every device – managed or unmanaged – to block or allow device access based on a specific device's security state.

Top 10 Policies

When a user's device doesn't meet the terms of a security policy, the user's authentication fails or they are prompted to update their device. Our data found the policies that result in the most failed authentications or blocked logins include access attempts by restricted locations, from an invalid device or from a device that's out of date. A device is classified as "invalid" if a user attempts to authenticate, but their device doesn't support the authentication method they've selected.

10 MOST COMMON POLICIES



Our data shows that organizations that implement device-based policies most commonly block access from locations they deem insecure and from where access should not originate. Organizations also tend to set policies to block invalid and out-of-date devices and devices that don't feature a screen lock or disk encryption, as those simple security steps can protect the device and the data it transmits from being viewed by others.

Top Policies by Industry

Our data also shows that different industries implement different policies to enforce device trust. For example, Education blocks more authentications per month based on invalid devices than any other industry, while Financial Services most frequently implements a policy to block devices without a screen lock.

POLICY ENFORCEMENT BY INDUSTRY

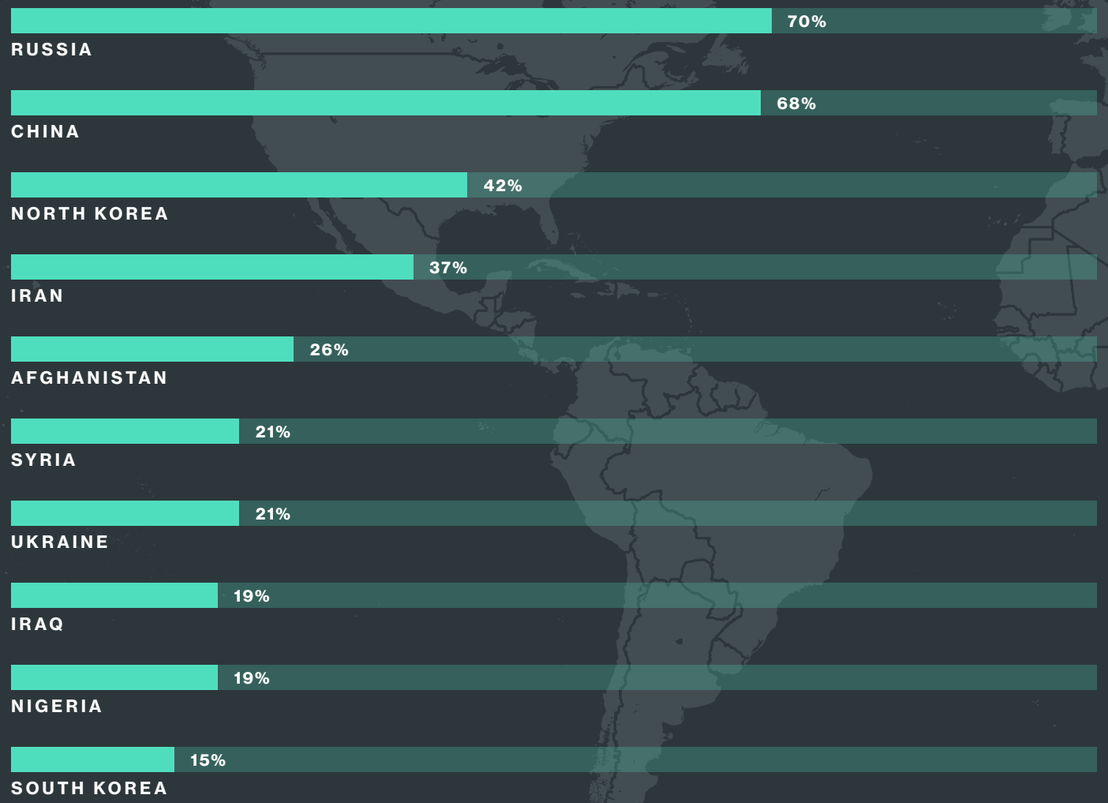
TECHNOLOGY:
LOCATION RESTRICTED

EDUCATION:
INVALID DEVICE

TECHNOLOGY:
OUT OF DATE DEVICE

FINANCIAL SERVICES:
NO SCREEN LOCK

Top Restricted Countries



Duo's most commonly used policy, disallowing access from restricted locations, gives us insight into which countries our customers deem risky from a security perspective. Typically, those restricted locations are seen as hotbeds for insecure activity or areas from where cyberattacks most often originate. Overall, Duo customers restrict access from more than 200 countries and territories. Above are the top 10 restricted locations based on the percentage of all policies with location restrictions to block those countries.

According to our findings, roughly 70% of organizations that implement location restrictions choose to restrict access from Russia and China.

> "The fact that such a high number of organizations implement location restrictions that include restricting access from Russia and China can be traced back to Export Administration Regulations, or EAR, which are regulations that control with which countries U.S.-based companies can conduct business,"

– DAVE LEWIS
ADVISORY CISO, DUO SECURITY AT CISCO

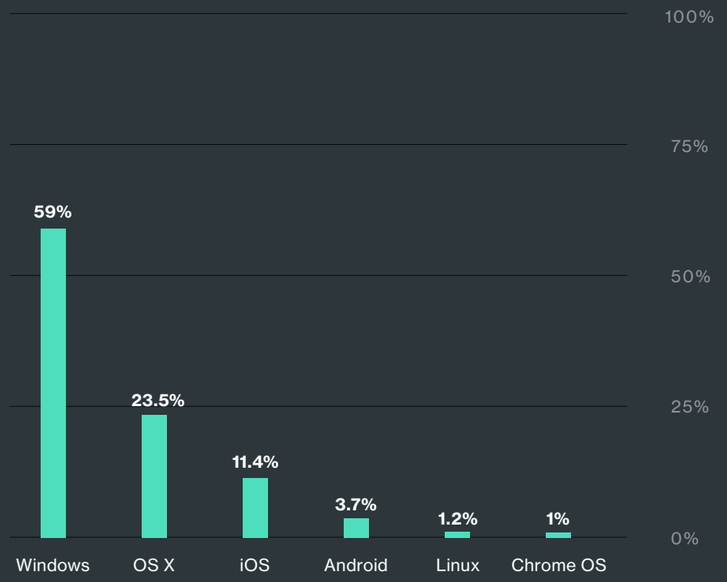
Device Visibility

Establishing device trust requires visibility into the devices accessing applications and data. Understanding which operating systems and which browsers those devices are running, and whether those OSes and browsers are up to date (among other things), can determine whether they're considered trustworthy. First, let's take a look at the browsers and OSes Duo customers use.

Windows Still Dominant OS

When it comes to operating systems, Windows is the clear leader by a wide margin. According to our data, which examined the percent of authentications from each operating system, these are the top operating systems Duo customers use:

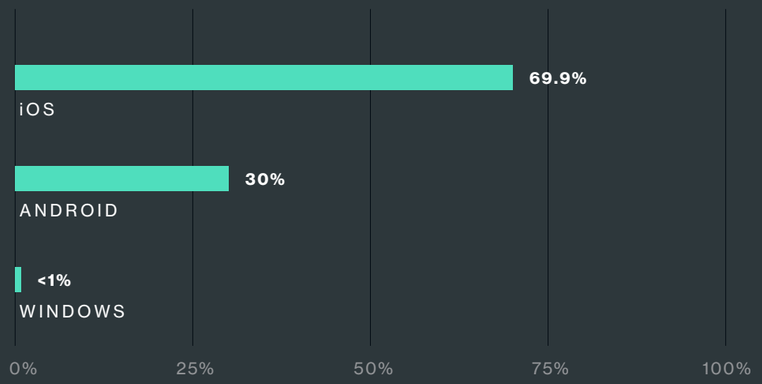
TOP OPERATING SYSTEMS



iOS's Incumbency

Meanwhile, on the mobile OS front, Apple's iOS is the clear victor, representing just shy of 70% of the phones Duo customers use to authenticate.

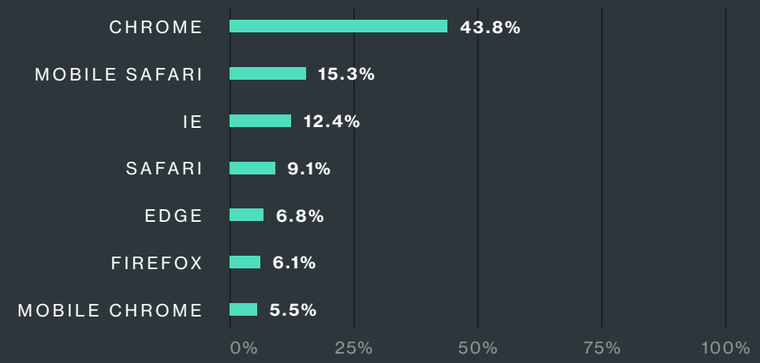
MOBILE OS USAGE



Chrome in Command

Google Chrome continued to trounce competing browsers to be the browser of record for businesses, with no other browsers coming close.

TOP BROWSERS



Winnowing Windows 7

For the third year straight, our data shows Windows 10 usage has supplanted Windows 7 usage, which continues to decline precipitously. While there are still some stragglers, our data found only 10% of Windows organizations still run Windows 7, which Microsoft stopped supporting as of Jan. 14, 2020.[7]

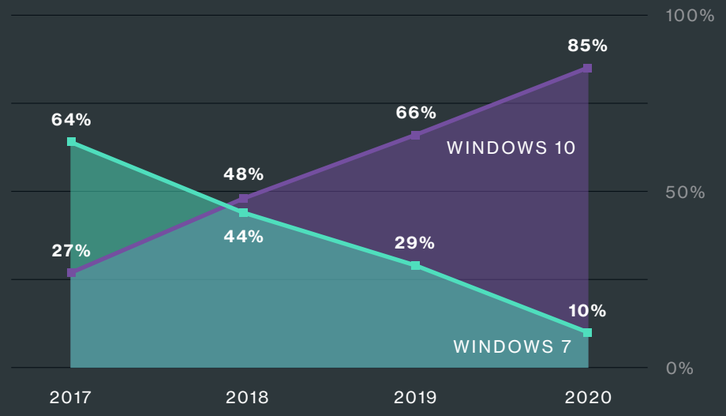
While Windows 7 is outdated and has been proven insecure, there are still some key industries lagging behind on the move to Windows 10. Healthcare, for example, still has more than 30% of its Windows devices running Windows 7, and Transportation still has 37% of devices running the now unsupported OS.

Meanwhile, industries such as Telecom, Business, Technology and Computers & Electronics have all seen more than 90% of their Windows fleets updated to Windows 10.

"Windows 7 reached its end of life support in January 2020 and still we see many organizations are making use of it. As a result, 'just patch it' is a common refrain we hear all too often. The problem here is that it is never that simple. Many organizations find they have to continue to make use of this deprecated operating system in order to keep in compliance with software terms and conditions of some third-party software companies. The rationale being that these software companies have not updated their code for a mission critical application." noted Lewis.

The slowness of some industries to upgrade to Windows 10 has prompted the FBI to issue a warning to organizations still using Windows 7. In August 2020, the FBI wrote in an alert: "As time passes, Windows 7 becomes more vulnerable to exploitation due to lack of security updates and new vulnerabilities discovered. Microsoft and other industry professionals strongly recommend upgrading computer systems to actively supported operating systems," according to an article in **Health IT Security**.[8]

WINDOWS 10 AND WINDOWS 7 USE



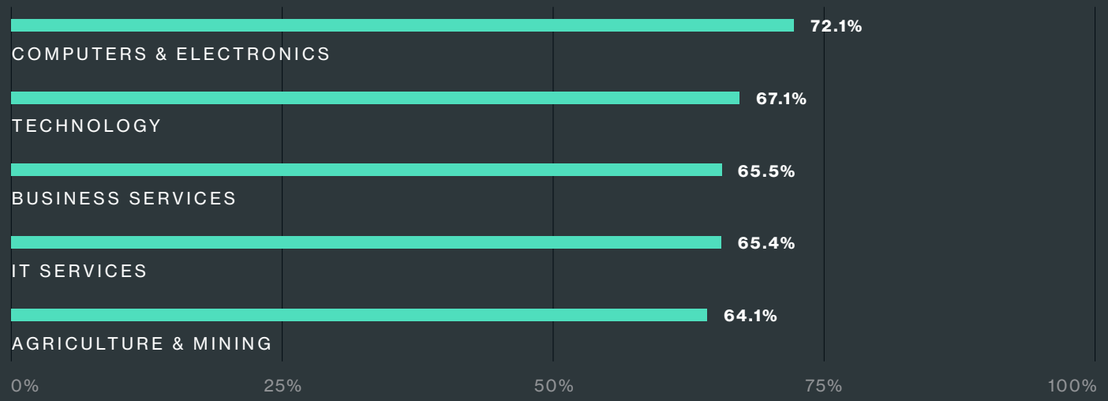
Out-of-Date Devices

Identifying trusted users is just one part of the secure access puzzle. Even a trusted user may be using a mobile device or computer that's running out-of-date software, and out-of-date software leaves devices susceptible to vulnerabilities and open to threats like malware, ransomware and more.

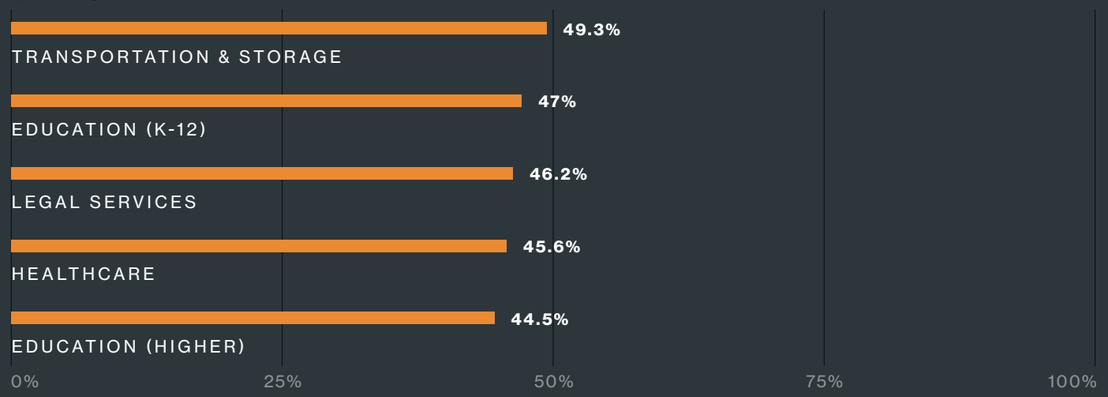
The percentage of endpoints that are up to date varies widely across industries. For our research, we consider a device up to date if it's running the latest version of the operating system.

For example, Transportation & Storage, Education (K-12) and Legal Services are most likely to have out-of-date devices with 49%, 47% and 46% out of date, respectively. Meanwhile, Computers & Electronics, Technology and Business Services are most likely to have devices that are up to date, with 72%, 67% and 66% of devices up to date, respectively.

INDUSTRIES WITH MOST UP-TO-DATE DEVICES
(percentage of devices that are up to date)



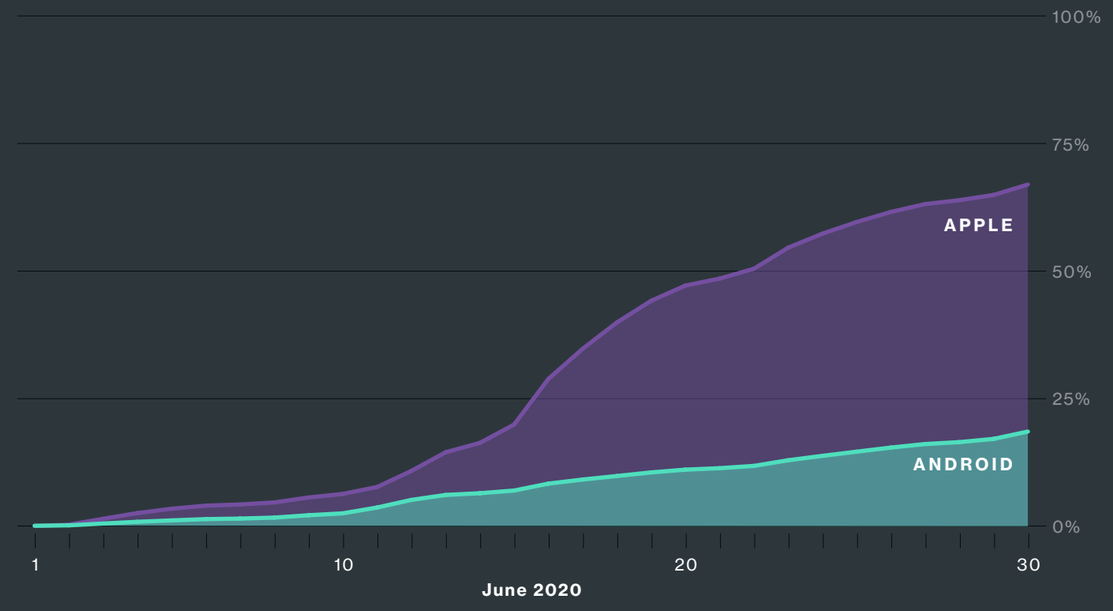
INDUSTRIES WITH MOST OUT-OF-DATE DEVICES
(percentage of devices that are out of date)



Our data shows that more tech savvy industries are most likely to have users whose devices are up to date, while industries that are slow to adopt new technologies or are potentially finding themselves encumbered by bulky, outdated systems tend to have more out-of-date devices in their fleets.

"Device management is no small undertaking," Lewis noted. "Companies that have been slow to adopt new technologies more often than not see new tech as orthogonal to their historical business modus operandi. We as humans are resistant to change and as a result organizations become imprinted with this corporate cultural nuisance if it is not driven from the top as a priority for an organization."

UP-TO-DATE DEVICES: APPLE VS. ANDROID



Apple vs. Android: The Battle Rages On

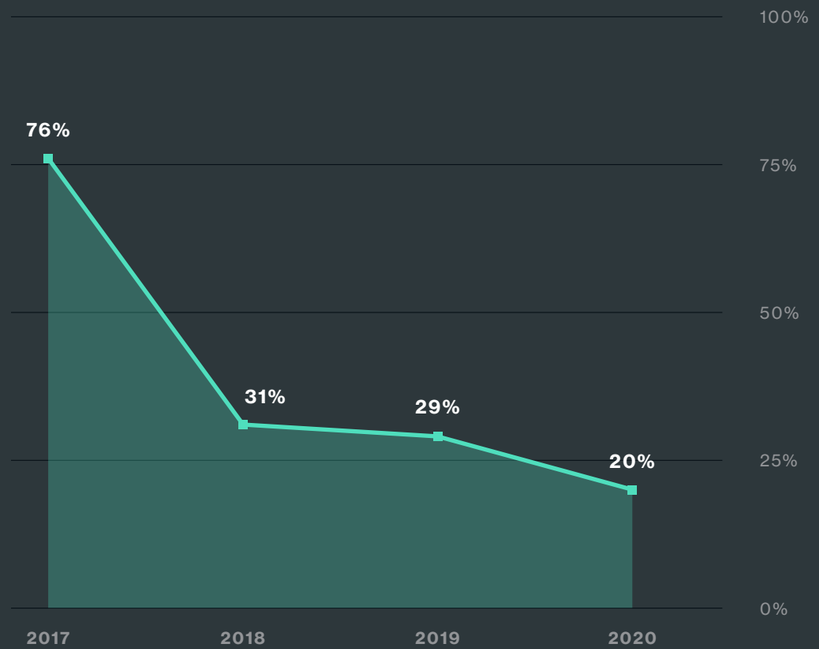
When we drill into specific types of devices, iOS endpoints are most frequently running the latest version of their operating system, while Android is most frequently out of date, according to our findings.

In the *2019 Duo Trusted Access Report*, our data showed Android devices were most frequently running out-of-date operating system versions, with 58% of devices being considered out of date.* iOS endpoints, on the other hand, were more likely to be up to date, with 62% of devices running the latest OS version in 2019.

For 2020, we took a different approach, examining how likely Android and iOS devices are to be updated following a security update, patch or new OS release. On June 1, 2020, Android released a **patch**[9] that fixed several high severity security vulnerabilities. On the same day, Apple released **iOS 13.5.1**[10] which also fixed a severe security vulnerability. This provided a unique opportunity to examine what percentage of devices from each OS would have the latest version/patch installed within a month's time.

According to our data, iOS devices were roughly 3.5 times, or 350%, more likely to be updated to the latest security release within 30 days.

*A device is considered "out of date" if it's not running the most recently released OS version.



Flash Still Fading

Speaking of out of date, let's look at Adobe Flash Player. For the fourth straight year, Flash experienced a decrease in usage. Adobe plans to officially kiss Flash **goodbye by the end of this year**.[11] Ditching Flash is no easy feat. It's estimated that **99% of all web users had Flash installed**[12] just 10 years ago. A slew of vulnerabilities and critical flaws, however, plague Flash to this day. Adobe disclosed the latest **critical Flash vulnerability in June 2020**[13].

As Flash fizzles, many browsers have already disabled Flash, including **Chrome**[14], **Firefox**[15] and **Safari**[16]. **Microsoft**[17], meanwhile, has announced it will end Flash support on Microsoft Edge and Internet Explorer 11 at the end of 2020. Flash's demise means developers must move toward alternative standards such as HTML5, WebGL and others.

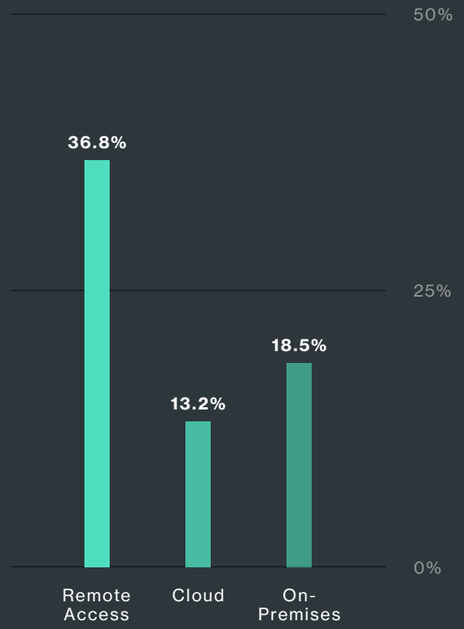
5.0

Applications

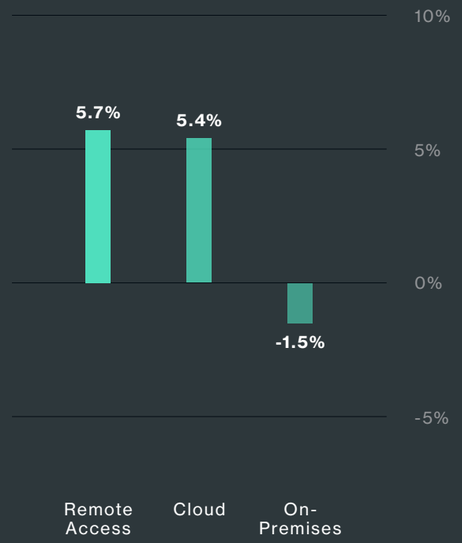
Ultimately, secure access comes down to ensuring users and devices can securely reach applications and data (and that those applications and data can't be compromised). We've said for years that mobility and the cloud will change access, and the uptick in remote work has proven that.

As part of our research, we examined the most common application types Duo customers access. Not surprisingly, remote access applications (VPN and RDP) saw a significant jump from 2019 to 2020. Interestingly, access to on-premises applications still outweighs access to cloud apps, though the cloud is starting to catch up as on-premises declines.

TOP APPLICATION TYPES ACCESSED



APP USAGE PERCENT CHANGE

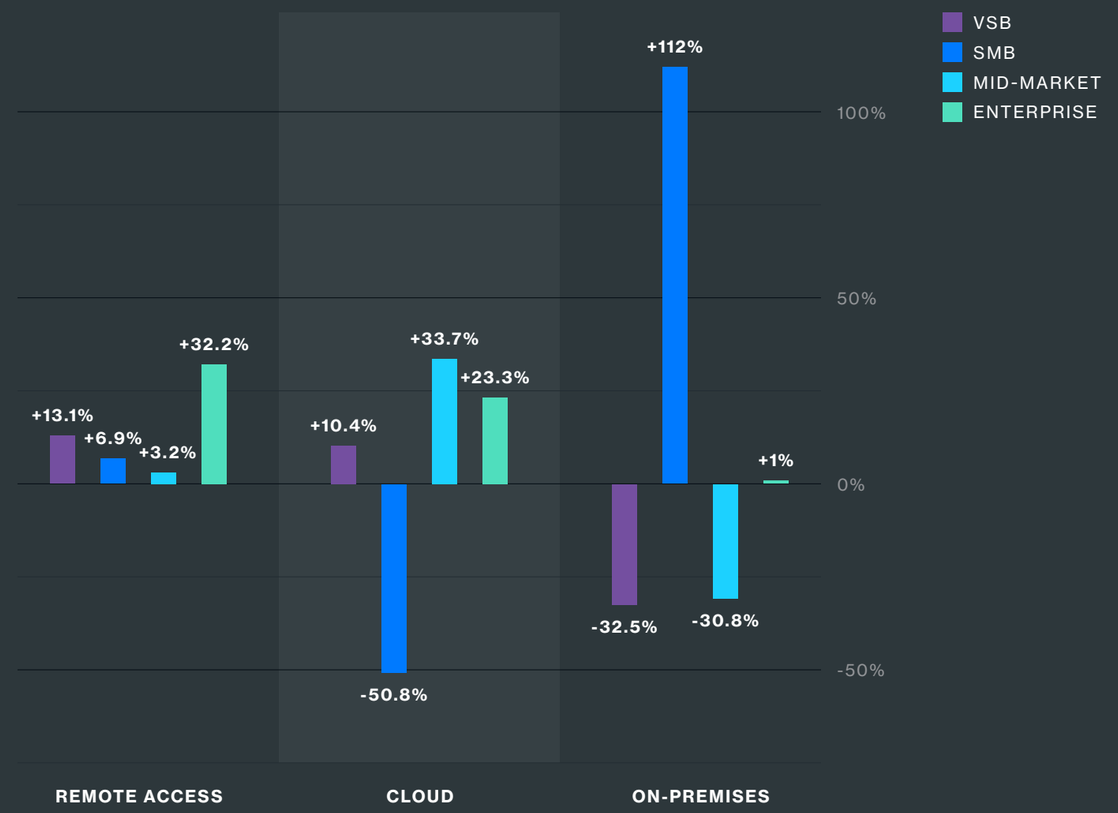


The year-over-year change between 2019 and 2020 shows that remote access and cloud app use is on the upswing and that they make up a larger share of the application types customers access. The percentages show how the usage of these categories changed relative to overall usage.

Enterprise Leads Remote Access Charge

The majority of the uptick in remote access application usage is coming from the enterprise, which saw monthly authentications per user jump 32.2% from June 2019 to June 2020. Meanwhile, the mid-market saw a massive swell in authentications to cloud apps, growing 33.7% year over year.

APPLICATION ACCESS BY MARKET SEGMENT



"Small and medium-sized companies tend to leverage on-premises solutions to run the day-to-day operations of their business. The reason is that these companies often do not have the bench strength internal to their organization to move towards a cloud-first strategy. As a result, they may rely on older, tried and true ways of deploying technology. This isn't a bad thing, but it does present itself as a limiting factor for future growth," Lewis said.

7.0

Summary

While remote work has been a part of workplace culture in many industries for years, organizations in 2020 had to quickly accommodate extreme remote work at massive scale. And the work from home trend is poised to continue in some capacity, as many large companies have announced they'll **extend remote work until at least mid-2021**.[18]

This rapid expansion presented new security challenges, one of which is ensuring that users can securely do their jobs without introducing new risk to the business. As businesses built out their remote access strategies, some key themes emerged: the need to secure users and devices and their access to applications.

> "The method in which we used to conduct business less than a year ago has been irrevocably changed,"

Lewis concluded. "When we look back at the massive global shift to a remote workforce it comes into sharp focus that this will be a way the workforce will be doing business for years to come. The need to dispense with old security thinking is apparent. Zero trust, multi-factor authentication, biometrics and passwordless are components of the path to a new bliss. It is of paramount importance to address the security of the workload in data centers and in the cloud as well. We are resilient and security can act as an enabler for the way forward."

> At Duo, it's our job to make application access more secure for organizations of all sizes – whether work happens at home, in an office or somewhere else entirely.
> Our modern access security is designed to safeguard all users, devices and applications. **Everywhere**.

References

[1] **Pandemic impact report: Security leaders weigh in**; CSO; April 1, 2020

[2] **Work-At-Home After Covid-19 – Our Forecast**; Global Workplace Analytics; 2020

[3] **UK lags behind Europe on returning to office**; Personnel Today; Aug. 6, 2020

[4] **Two-Factor Authentication Methods**; Duo Security; 2020

[5] **Passwordless: The Future of Authentication**; Duo Security; 2020

[6] **Adaptive Authentication Policies**; Duo Security; 2020

[7] **Windows 7 support ended on January 14; 2020**; Microsoft; 2020

[8] **FBI: Operating Windows 7 Increases Cyber Risk to Network Infrastructure**; Health IT Security; Aug. 5, 2020

[9] **Android Security Bulletin – June 2020**; Android Source; June 1, 2020

[10] **About the security content of iOS 13.5.1 and iPadOS 13.5.1**; Apple Support; June 1, 2020

[11] **Adobe Flash Player EOL General Information Page**; Adobe; 2020

[12] **What is Flash?**; BBC; Sept. 9, 2010

[13] **Security Bulletin for Adobe Flash Player | APSB20-30**; Adobe; June 9, 2020

[14] **Saying goodbye to Flash in Chrome**; Google: The Keyword; July 25, 2017

[15] **Mozilla: Firefox 69 will disable Adobe Flash plugin by default**; ZDnet; Jan. 14, 2019

[16] **Safari 14 Release Notes**; Apple Developer; September 2020

[17] **Update on Adobe Flash Player End of Support**; Microsoft Windows Blogs; Sept. 4, 2020

[18] **17 Major Companies That Have Announced Employees Can Work Remotely Long Term**; Entrepreneur; Aug. 17, 2020