THE 2021 DUO

Trusted Access Report

The Road to a Passwordless Future

DUO

cisco SECURE

THE 2021 DUO

Trusted Access Report

The Road to a Passwordless Future

AUTHOR
DAVE LEWIS

DATA SCIENCE
ROSE PUTLER

EDITORIAL
KATE BILLERBECK
CHRYSTA CHERRIE
J. WOLFGANG GOERLICH
TYRONE HARMON
WENDY NATHER
HELEN PATTON

DESIGN & DEV
CHELSEA LEWIS
SARAH OVRESAT
LAUREN FITZPATRICK
TRACY TOEPFER
HAFSAH MIJINYAWA
SUNNY BERRO
MARLA JONES
BEN ARMES
BEN COLMAN

PRODUCTION
EMILY GORDY

Version 1.0

1.0

The Logical Flow to a More Secure Future

For almost 58 years, we've used the venerable password as a security control. However, security practitioners worldwide know all too well that the level of security that passwords provide is the equivalent of the house key. The password has served its purpose, and now it's time for enterprises to move beyond passwords to a better method that ensures the security of their users, assets and applications.

Globally, we've spent more than a year and a half working in various versions of the remotely deployed enterprise. What was once seen as a matter of convenience had to be accommodated quickly as the de facto standard for getting business done.

As hybrid employees, or what we will refer to as hybrid workers, we've leveraged web conferencing technologies like Webex. We've learned that webcams are the new gold (and thanks to video conferencing really only dealing with our upper half, we've been able to save money on pants!). Employees have had the chance to build a strong work-life balance in the face of adversity.

Companies in every vertical have had to adjust their hybrid work policies and adapt in the face of the global health crisis. Fortunately, this worked very well for large portions of the workforce.

While hybrid work became the strategy to keep the economy moving, many organizations were able to make the shift in short order and do it at scale. Now, enterprises are moving toward new, more effective ways of handling access control and seeing in action how democratizing security can go a long way in enabling hybrid workers to focus on their core competencies without sacrificing security.

Multi-factor authentication (MFA) is the next logical step in the effort to shift to a better strategy for securing organizations, helping them better prepare for the pivot to passwordless authentication. With MFA, you can eliminate the risk of using passwords as the single form of user authentication and reduce the risk of credential theft by requiring a second method of identity verification that cannot be easily stolen remotely by an attacker. This sets the foundation for additional authentication methods, like biometrics, security keys and mobile devices, which can take daily use of passwords out of the equation, ultimately enabling security leaders to balance strong security and ease of use.

> "Passwordless provides the user benefit for initiatives strengthening authentication. Employees see faster authentication with fewer login prompts and less friction. Meanwhile, security teams are working to improve the overall trust in authentication.
>
> Trusted passwordless uses the login process as a policy decision and enforcement point, considering the context and conditions of the request including device health. Security teams establishing these controls are getting ahead of multi-factor phishing and biometric spoofing. Thus, passwordless both simplifies the experience for employees while increasing the difficulty on criminals."
>
> **J. Wolfgang Goerlich**
> Advisory CISO, Duo Security

Refining the User Experience

With employees worldwide now working in a non-standard manner, we have to account for the overarching requirement to democratize security. Applications must be able to support hybrid workers to focus on their key responsibilities without sacrificing the security of the user, device and applications. Just a couple of years ago, it was not uncommon for enterprises to utilize MFA only to protect key systems that had serious material impact to the business, in the event that they were compromised by a nefarious third party.

Now, there is a concerted effort to move all access to MFA to not only reduce the risk to the individual and organization, but also to streamline security operations.

Security workflows in the past were negatively impacted by using security controls that were ineffective and had outlived their useful life span. Driven by the requirement to accommodate a globally distributed workforce no longer tied to a physical office location, security is becoming much more streamlined.

The User Experience Matters

We've now reached the point where the user experience is a security control in and of itself. If security controls are cumbersome – or worse still, written by engineers for engineers – then the chance that the average employee will be able to efficiently utilize them is questionable. As Kevin Costner famously said in "Field of Dreams," "If you build it, they will come." People are more likely to adopt tools that are easy to use and effective.

From very small businesses, to enterprises, and all points in between, the rate at which remote access authentications are increasing is quite astounding. We've seen repeatedly where hybrid worker office productivity is in fact a viable model for many enterprises. Enterprises can keep their business running and protect logins by utilizing web conferencing, MFA, VPN and RDP technology.

A positive user experience plays a fundamental role in the security and success of the enterprise. If security is seen as a roadblock to progress with the organization, then employees may be inclined to find ways to work around the security controls, making security overall suffer.

Let's be real: Some authentication methods are simply more user-friendly than others. Remembering hundreds of passwords that are 20+ characters long can be daunting. A password manager application can go a long way in helping to simplify that process, but MFA or biometric security can help even more. Better yet, passwordless authentication utilizing a method such as Webauthn can enable users to complete their tasks without having to rely on carrying around a large cache of passwords, much in the same vein as a medieval dungeon master managing their access keys.

Leveraging more user-friendly authentication methods leads to greater security. If these methods are easy to use and still provide and surpass the expected benefits of older security controls, then we have a win. If security controls are difficult or cumbersome to use, then employees will be disinclined to use them correctly. Good design goes a long way to improve security.

Expanded usage of technologies such as single sign-on (SSO) can make it even easier for employees to get to work on what matters most to them. For example, we've observed a steady increase in the number of authentications using SSO. In 2020 we saw that 20.6% of all authentications were made to SSO applications, while in 2021 we saw an expansion of 20% to 24.8% of all authentications.

Expanding Security's Reach on the Global Stage

The global health crisis that has gripped the world since 2020 led to a rapid rise in hybrid work and presented businesses with new security challenges. This was not limited to a particular geographic locale. Enterprises and various organizations found themselves needing to ensure that their employees could securely access the applications and resources that keep the business running without introducing undue harm into the workflow. All the while, there's a real need to focus on reducing risk to the organization. Work had to continue on, and do so with a clear purpose, while ensuring that data, applications and intellectual property were not negatively impacted.

Seemingly overnight the focus shifted to a global workforce transition. As time has passed, we've observed, at least anecdotally, varying levels of success. Some companies have been able to pivot smoothly, while others were caught without the necessary resources in place to move from on premise. However, in general things have been trending positively for companies globally. There was a clear need to get organizations functioning and orchestrating systems so that they could enable and empower employees to function in this new global environment.

In the *2021 Duo Trusted Access Report*, we'll explore how companies are currently securing hybrid work and what makes a solid and secure remote access strategy. 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, and they're implementing the appropriate controls to ensure secure access to applications.

Leveraging more user-friendly authentication methods leads to greater security.

Methodology

A zero trust security strategy is based on 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 Data Science analyzed data from more than 36 million devices, more than 400 thousand unique applications and roughly 800 million monthly authentications from across our customer base, spanning North America, Latin America, Europe and the Middle East, and Asia-Pacific. We defined our 2021 annual time range as between June 1, 2020 and May 31, 2021, and examined authentications between those dates, inclusive. For non-authentication data, we counted metrics on May 31, 2021.

800 million

Authentications per Month

36 million+

Devices

400,000+

Unique Applications

An at-a-glance look at top trends.

RISING PASSWORDLESS ADOPTION

Users move toward lower-friction second factors. **Webauthn** shows a fivefold increase in usage since April 2019.

BIOMETRICS PRESS FORWARD

More than 71% of mobile phones have biometrics enabled, and total mobile phones with biometrics rose 12%.

IOS UPDATED MOST

On average, iOS devices were 40% more likely to be updated within 30 days of a security update or patch, compared to Android devices.

MFA CONTINUES TO STRENGTHEN PASSWORDS

Multi-factor authentication holds strong while adding to the security of only traditional password usage. Use of MFA with Duo rose by 39% in the past year.

CLOUD USAGE FLOATS ON

Authentications to cloud apps increased from 13% to 15% of authentications.

LOCATIONS BLOCKED

Roughly 74% of those who implement device-based policies restrict access from China and Russia.

PUSH PREFERRED

Duo Push is the most used auth method, accounting for 30% of all authentications, up from 23% the year before.

OUT-OF-DATE FAILURES

The number of authentication failures due to out-of-date devices increased 33% between 2020 and 2021.

ENTERPRISES EMBRACE A HYBRID APPROACH

While slightly below their peak from March through August 2020, enterprise remote access application usage continued to show 15% higher levels in the nine months after that time compared to the nine months before, based on average monthly authentications.

Policy Usage

An interesting factor with any security solution is the human element that needs to be taken into account. There is a fundamental mismatch between systems that are deployed and what was intended to be implemented. No plan survives first contact with the adversary. Policies need to be implemented to help unify the systems and applications necessary for users to accomplish their jobs and support their organization's aspirations and mission. Duo allows companies to reduce the overall risk by being able to enforce controls. Having the ability to define policies by user groups and on an application basis, with granularity, allows the security team to improve security without needing to compromise the user's ability to get their job done.

2.0

Democratizing Security

The demand for enterprises to strengthen their capabilities for employees to work safely and securely continues to rise. Security for enterprises must be made simpler and more automated. A zero trust strategy should be viewed as encompassing more than just access control. There is a clear need to safeguard workloads from on-premises systems, to the edge, to the cloud, and help enterprises navigate the complexity of disaggregation and virtualization.

> "Everyone should have the ability, and the right, to control the access to their resources and data. Trusted access blends the topics of security, compliance and privacy in a way that affects all of us on a daily basis. Evolving this trusted access is a top priority for our digital future."
>
> **Wendy Nather**
> Head of Advisory CISOs, Duo Security

Authentications are the first touchpoint for an enterprise employee to access the systems that help them get their jobs done. Multi-factor authentication is a great example of how that journey toward a zero trust strategy can begin to unfold.

Streamlining

Reducing security debt is a huge shift that we have seen underway across multiple industry verticals in the last year. As we saw in the Cisco ***Security Outcomes Study***, enterprise workforces deployed remotely in many parts of the world since March of 2020, organizations have had time to reflect on how to streamline operations and best enable their teams to work effectively.

We've seen enterprises improve their security agility and shore up their resilience to adapt to the rapidly changing IT landscape. Leveraging security strategies of continuous trusted access and zero trust, enterprises have taken the opportunity to improve on their visibility of user and device activity, application discovery and risk management.

Further streamlining opportunities have presented themselves under the guise of applying unified policies and enforcement. Implementing greater use of network zone segmentation and access management across the now-extended enterprise which comprises their secure edge has served to improve security and reduce risk.

Enterprises are also streamlining security by using automated detection and response mechanisms. By gathering more intelligence from devices and applications and making use of automation as well as further orchestration of security controls to compliment the already existing workforce, enterprises are improving their security's ability to enable the workforce, workplace and workload to operate efficiently and effectively in a safe and secure manner.

Taking the time to get a firm handle on security debt within an enterprise allows you to free up resources to focus on your organization's most important projects. Many organizations over the years have found themselves with systems deployed for a project specifically geared toward satisfying the aspirations of the business. However, many of these initiatives lacked a continuous maintenance work breakdown structure to ensure the systems' long-term sustainability. This has led to an accumulation of deprecated systems that may or may not have been patched to current standards or properly configured. As a result, this lack of attention to detail on older systems can inadvertently introduce vulnerabilities into the enterprise.

By streamlining the network architecture for an enterprise, security and IT personnel can reduce risk to the organization. This is where the concept of continuous trusted access comes into play. Having a coherent strategy to improve your organization's security will help with the transformation of IT systems to best support the business.

Enterprise use of cloud applications grew significantly in the last year to support the hybrid work model. According to our data, the period from June 2020 through May 2021 saw more than a 65% increase in average daily authentications to cloud applications over the average from that same period from June 2019 through May 2020.

We reviewed the data in relation to authentications for cloud-based applications and how the authentications changed in how enterprises handled their authentications for hybrid workers in North America, Europe and the Middle East, Asia Pacific and Latin America. Year over year from 2020 to 2021, there was an increase in the proportion of authentications to cloud applications across all regions. Europe and the Middle East demonstrated the largest spike, of 190%, and all other regions demonstrated relatively modest gains of 38%, 18% and 13% for Asia Pacific, Latin America and North America, respectively.

Industries Where Passwordless Access Increased

For this report, we examined the top industry verticals to see how authentications have evolved from more cumbersome second factors to more streamlined methods such as biometrics, which herald a low-friction, passwordless authentication future. We looked at the top five industries moving forward with the change in how we handle the modernization of authentication. Of these industries, Financial Services saw the largest increase in biometrics as second factors overall with an elevenfold uplift, while Technology saw the smallest change at an 11% increase from 2020.

INCREASE IN BIOMETRIC AUTHENTICATIONS FOR INDUSTRIES WITH TOP 2021 BIOMETRIC USAGE

FINANCIAL SERVICES:

↑1100%

Increase to 85,000 authentications

EDUCATION:

↑770%

Increase to 1.8 million authentications

HEALTHCARE:

↑580%

Increase to 13,000 authentications

IT & TELECOM:

↑160%

Increase to 200,000 authentications

TECHNOLOGY:

↑11%

Increase to 1.7 million authentications

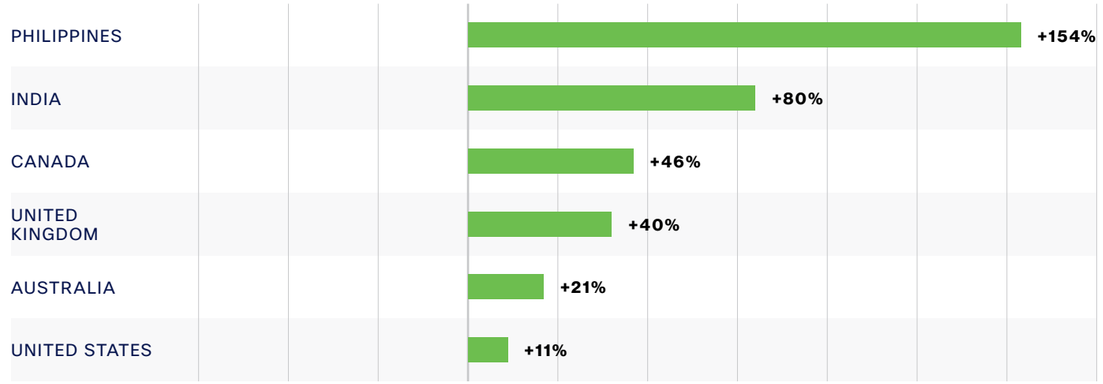
Global Increase in MFA

We also examined which geographic regions are experiencing the largest increases in MFA technology use. In North America, for example, average daily authentications utilizing MFA technology grew overall. In the US, authentication volume rose 11% while their neighbours to the north in Canada saw a 46% increase in the number of authentications.

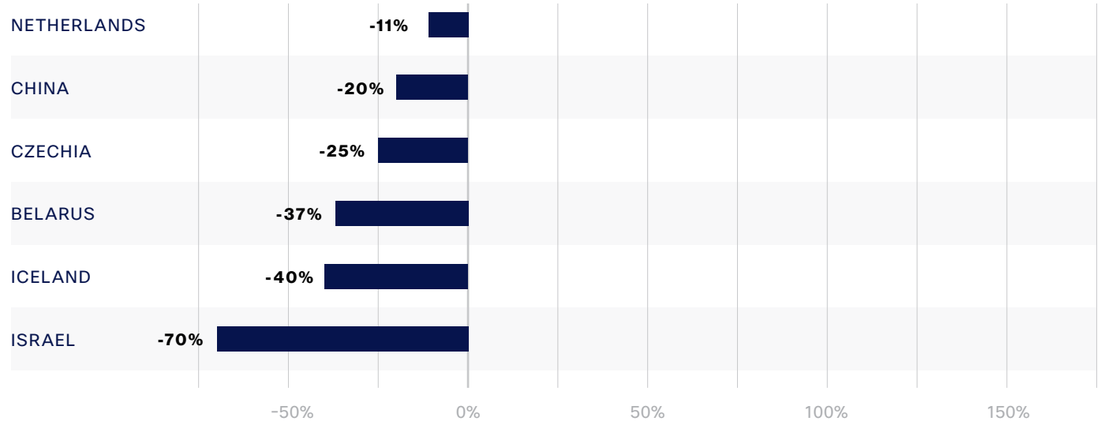
In the UK, the volume of authentications rose 40% over the same period.

In the Asia-Pacific region, we saw an upward trend in Australia, registering a 21% increase in authentications, India jumped 80%, and we saw a whopping 154% increase in the Philippines.

TOP COUNTRIES WITH AN INCREASE IN AUTHENTICATION VOLUME



TOP COUNTRIES WITH A DECREASE IN AUTHENTICATION VOLUME



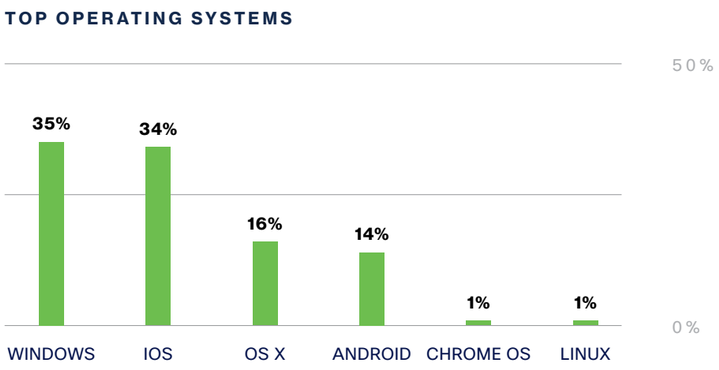
by 2021 Authentication Volume, Based on Access Device IP Address

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.

Windows Remains the Dominant OS

On the operating systems front, we find that Windows remains as the front-runner. According to our data, these are the top operating systems:



Toward a Passwordless Future

Enterprises are moving toward streamlining their systems to improve how they adapt their organizations to changing global headwinds. We see that the increase in biometrics utilization demonstrate that users are becoming more comfortable with non-traditional authentication methods, meaning users are open to leveraging similar methods, like passwordless authentication. Enterprises are taking steps to move away from passwords, which will significantly improve the login experience for the vast majority of users.

Passwords are a deprecated notion as a security control. Individuals continue to face a real and present risk from password reuse, not only because passwords are trivial to crack, but also because people tend to use the same passwords across multiple sites and applications, or create passwords that aren't long or complex enough.

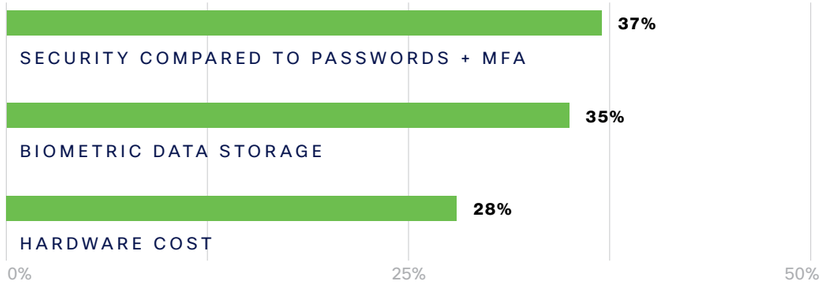
By moving toward passwordless authentication, your organization can gradually become less reliant on passwords, which in turn reduces the risks that passwords pose. The road to a passwordless future starts with strong authentication and reduced reliance on the antiquated password security control for access.

So what does it mean to be passwordless? Recently, Cisco conducted a survey with enterprises around the world to assess how they viewed the concept of passwordless in their environments. Across respondents from all countries surveyed, for a product to qualify as being passwordless, the most important condition is the technology itself incorporates some form of "passwordless" technology such as biometric authentication, PIN, key or smartcard. More than 36% of respondents found this to be the most important condition, with respondents from India feeling most strongly (49%).

There was a high level of frustration identified in the report when it comes to dealing with static passwords. Almost half of the respondents across all countries (46%) stated that security issues related to compromised credentials are the most frustrating or concerning aspect of dealing with passwords in their environment. That number jumped to 57% with respondents in India, but was only 36% among German respondents. This was the most common response in all countries.

Respondents who personally executed any type of security activity, no matter what those responsibilities were, found that the most frustrating or concerning aspect of dealing with passwords in their environment were issues related to compromised credentials, with those whose work entailed choosing security software showing the most concern (53%).

When the survey respondents were asked about their biggest concerns as it pertained to passwordless authentication methods their top three concerns were:

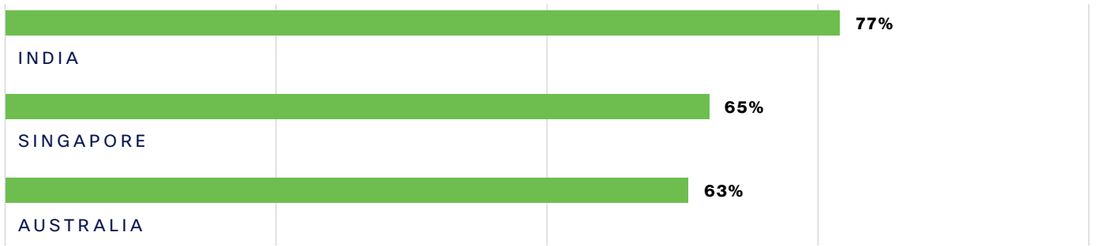


These concerns are completely understandable for any enterprise security team to have. Over 45% of the survey respondents who work in companies with revenue of $100 million – $499.99 million said that when thinking about passwordless authentication methods (such as biometric, PIN, or security keys), biometric data storage is one of their biggest concerns. In contrast, among companies with revenues under $100,000, 23% of respondents share this concern.

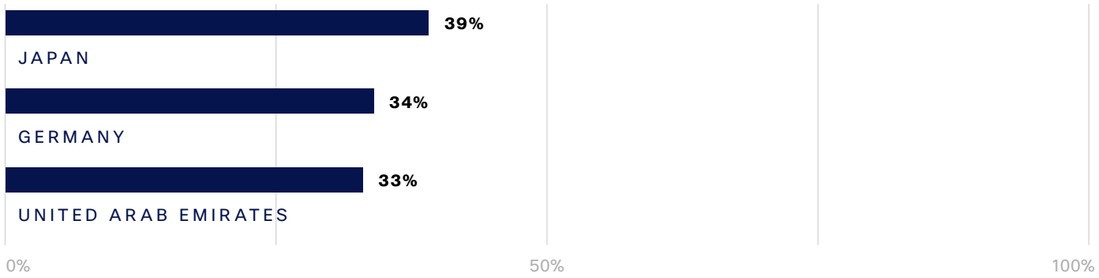
However, we also saw that almost 11% of respondents said that they have no major concerns when thinking about passwordless authentication methods.

The big question is, are companies currently considering implementing a passwordless strategy for their organizations? Interestingly enough, 52% of those surveyed are in fact planning to implement a passwordless strategy. Only in Japan were more respondents not currently considering a passwordless strategy than were considering a passwordless strategy, and even then the proportion of respondents was fairly evenly split (39% vs. 35%). However at this time, only 6% of those have already implemented a passwordless strategy at their organization.

Respondents in these countries said they are most likely to consider implementing a passwordless strategy in their organization:



By contrast, the survey found that respondents in these countries are least likely to be currently considering implementing a passwordless strategy:



Interestingly, some of the same countries where we found that respondents are least likely to be currently considering implementing a passwordless strategy are also those countries where the most respondents were implementing a passwordless strategy, with almost 10% of respondents in Japan and 9% in Germany saying they were currently or had already implemented a passwordless strategy at their organization.

For respondents from most countries, the most common reason for wanting to implement a passwordless solution was that it would improve the overall security of their company (44% on average), with improving user experience the 2nd or 3rd most common reason for wanting to implement a passwordless solution. In contrast, respondents in Singapore were most likely to say that improving the experience of the end users is a top reason for wanting to adopt a passwordless solution (53%).

This is a key point. A passwordless strategy done correctly will lead to a better user experience, and layering in effective policies will help to ensure the safety and security of the organization's workplace, workforce and workloads.

In reviewing our data, we discovered that the usage of biometric authentication increased by 48% year over year as more enterprises moved toward low-friction authentication methods. The proportion of authentications utilizing Duo Push also increased 30% year over year. These findings indicate a shift away from passwords, in favor of lower-friction authentication methods.

It's also notable that the proportion of overall applications using either WebAuthn or universal second factor (U2F) methods jumped 35% in the last year.

3.0

Devices

Enterprises have found themselves with dispersed hybrid workforces which have evolved from firefighting to the de facto standard. Controlling the security of variables can and will be a challenge for enterprises. Strong authentication helps verify identity, but it's almost impossible to ensure that employees are in fact using trusted networks and securing their data accordingly.

Devices like laptops and mobile phones are a key piece of the puzzle from a security perspective. Enterprises must be able to understand the posture and security of these devices. Ensuring that devices have good hygiene and are patched to current levels, or N minus 1, is paramount. Proper device health practices can help an enterprise control for location, operating system, encryption status, and more.

It's essential that enterprises address how to define the security posture of devices in your environment.

Putting a finer point on it, how do you gain visibility into devices on your network without violating your users' privacy? Many organizations have utilized employees' personal devices as part of their ability to further extend the remote workforce, so how do you protect them, too?

Whether devices are corporate-owned or personal, a strong zero trust strategy starts with establishing device trust.

Upon reviewing our data we found that device encryption had increased dramatically year over year! Last year we recorded that 74% of devices with the Duo Endpoint Health application had encryption enabled. However, in 2021 that number has jumped to 90%. A welcome increase in the battle to secure environments.

Another notable piece is that firewall usage on devices with the Duo Endpoint Health application installed saw an increase. The number of devices from 2020 which had a firewall enabled was 94% and this increased to 96% of devices in 2021.

Device-Based Policies

When enterprises are trying to reduce the risk and security debt, it's wise to ensure only secure and trusted devices can access applications and services through implementing and enforcing device-based policies.

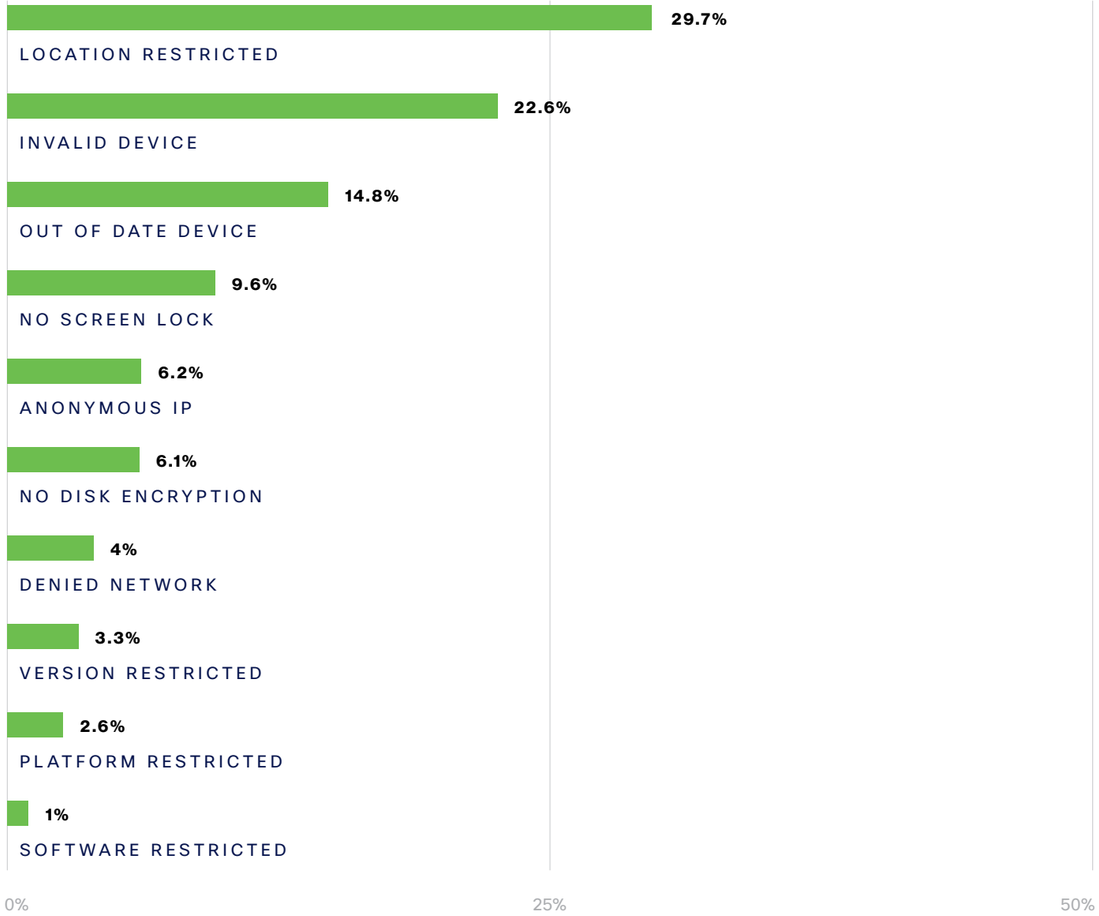
These device-based policies help your organization prevent potentially compromised or risky devices accessing data. As an enterprise administrator, you can apply security policies across every device, whether they're managed or unmanaged, to block or allow device access based on a specific device's security state.

> "Duo customers know that a secure authentication experience is a foundational security control for any organization. It is also the control that every employee, contractor and partner sees. Using continuous trusted access policies to manage authentication means their systems and data is protected. It also means their users can have a nuanced, appropriate security experience – requiring additional checks only when needed. This puts control of the user experience back in the hands of the users, addresses emerging compliance requirements, and makes the security administration function simple."
>
> **Helen Patton**
> Advisory CISO, Duo Security

Top 10 Policies

When an access device doesn't meet the terms of a security policy, the user's authentication fails or they're 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, or from an invalid or outdated device. A device is classified as "invalid" if a user attempts to authenticate but their device doesn't support the authentication method they've selected.

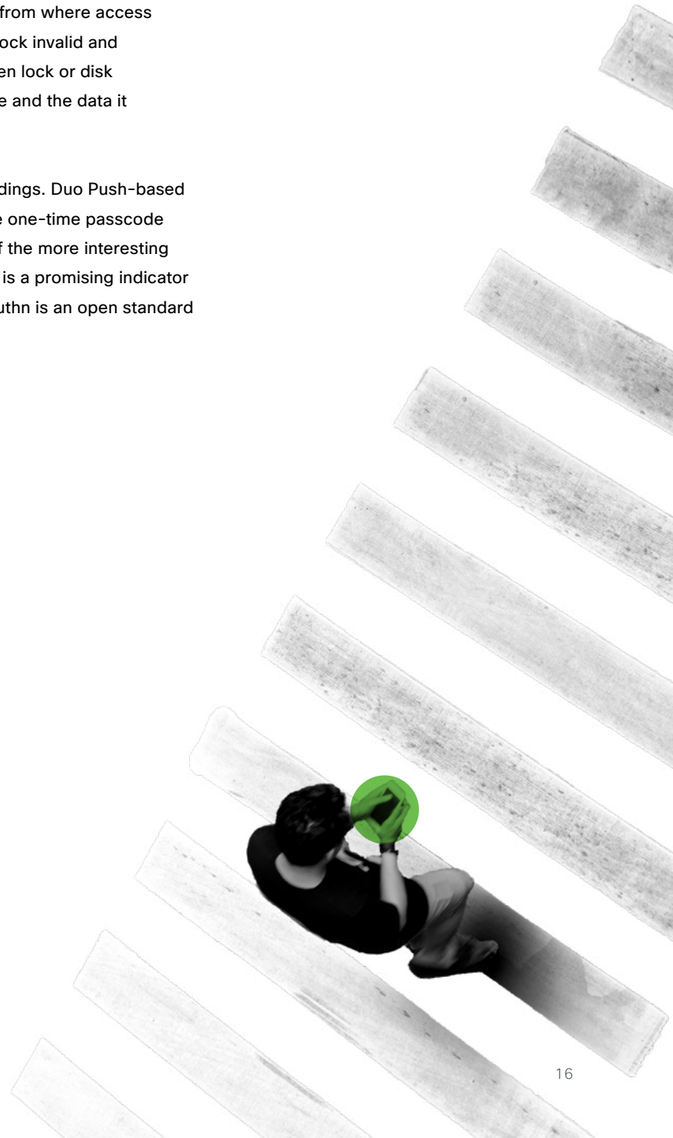
10 MOST COMMON POLICY-BLOCKED AUTHENTICATIONS



Overall we noted that an aggregate of 7.6% of all authentications had failed. When we dug into that 7.6%, we discovered that 40% of those failed authentications were due to the users not being enrolled in the system. By comparison, only 0.1% of failed attempts were due to the user attempting to connect from a restricted network or location.

Duo's 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, as well as 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.

When reviewing the policy data, we uncovered some notable findings. Duo Push-based authentication was present in 99.5% of all global policies. Mobile one-time passcode was in 98% of policies defined, and U2F ranked at 86.6%. One of the more interesting parts was that WebAuthn was in 55% of the global policies. This is a promising indicator of a welcome step toward passwordless implementation. WebAuthn is an open standard that was first published by the W3C in March 2019.

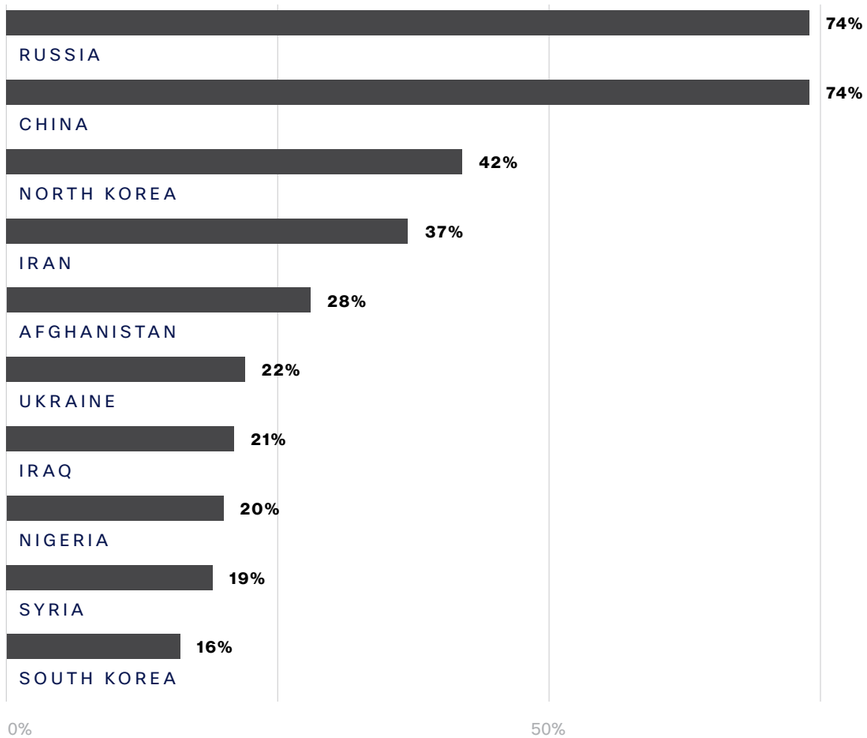


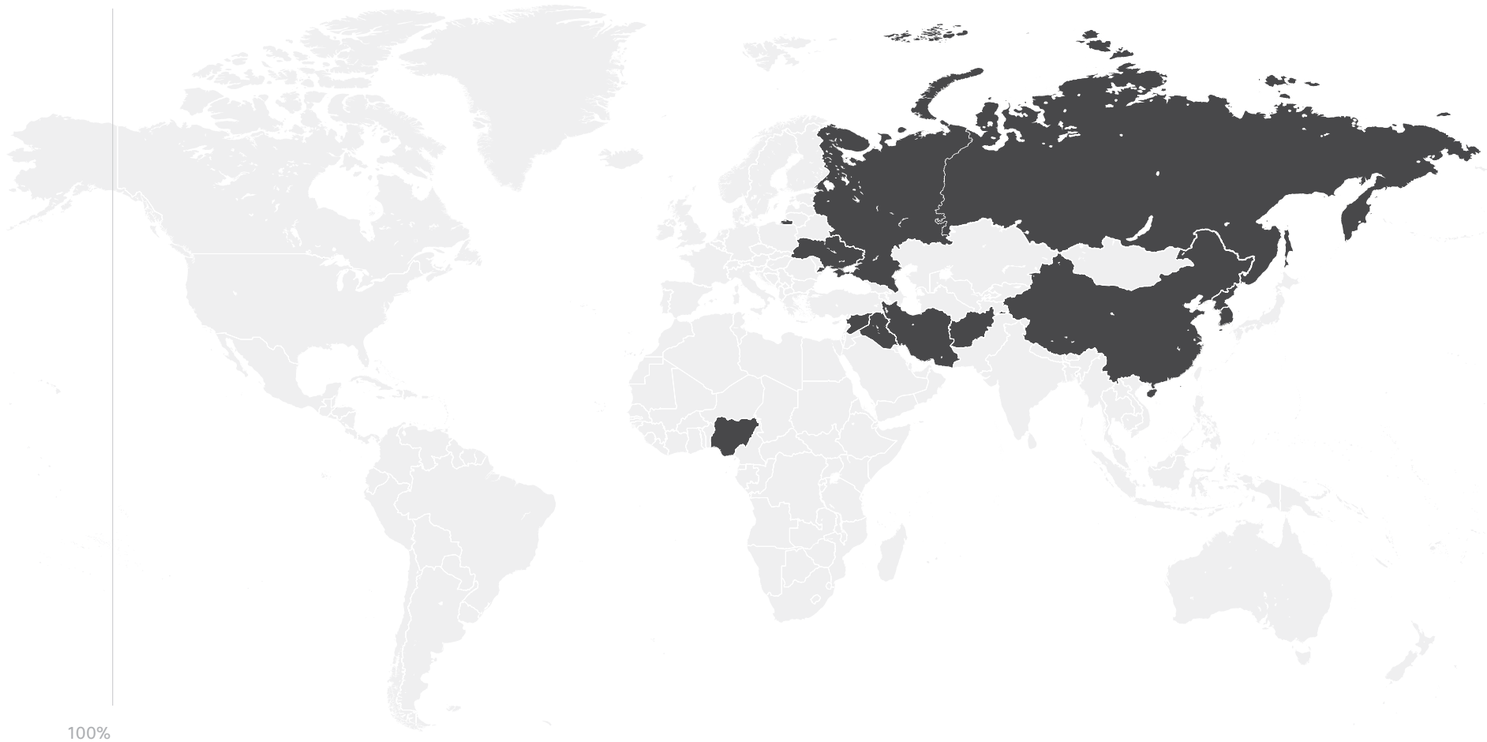
Top Restricted Countries

When we review the policies that Duo customers commonly use, disallowing access from restricted locations provides guidance with regard to which countries our customers deem risky from a security perspective. While rationale may vary, the primary reason is that blocked countries are often viewed as points of attack that should be protected. This differs from one customer to the next, as they will restrict access from almost 250 countries and territories. When reviewing our data, we found the following top 10 restricted locations based on the percentage of all policies with location restrictions to block those countries:

According to our findings, roughly 74% of organizations that implement location restrictions choose to restrict access from Russia and China. It should also be noted that Duo automatically denies authentications from locations on the Office of Foreign Assets Control (OFAC) sanctions list, including from IP addresses that geolocate to Crimea, Cuba, Iran, North Korea, Sudan, and Syria as of this writing.

TOP RESTRICTED COUNTRIES





Top Policy Enforcement by Industry

Our data also illustrates that different industries implement different policies to enforce device trust. For example, educational organizations block more authentications per month based on invalid devices than any other industry, while financial services institutions most frequently block authentications because a device does not have a screen lock.

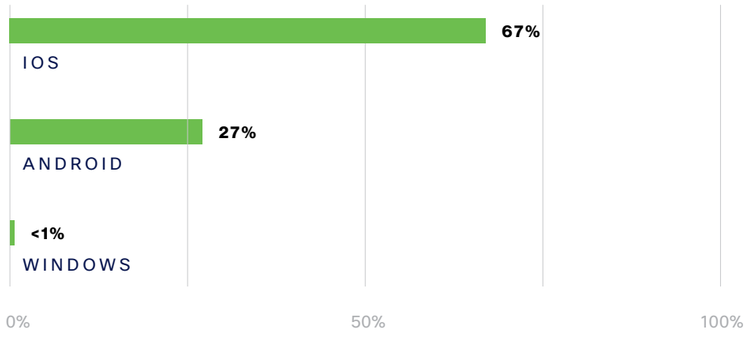
POLICY ENFORCEMENT BY INDUSTRY

POLICY	TOP INDUSTRY
BLOCK UNENROLLED USERS	TECHNOLOGY
USER NOT PERMITTED	FINANCE
LOCATION RESTRICTED	IT & TELECOMMUNICATIONS
INVALID DEVICE	EDUCATION
OUT-OF-DATE DEVICE	TECHNOLOGY
NO SCREEN LOCK	EDUCATION
NETWORK DENIED	IT & TELECOMMUNICATIONS
VERSION RESTRICTED	TECHNOLOGY
NO DISK ENCRYPTION	TECHNOLOGY
ANONYMOUS IP	EDUCATION

iOS Distribution

Apple's iOS remains the clear leader, with just shy of 67% of devices:

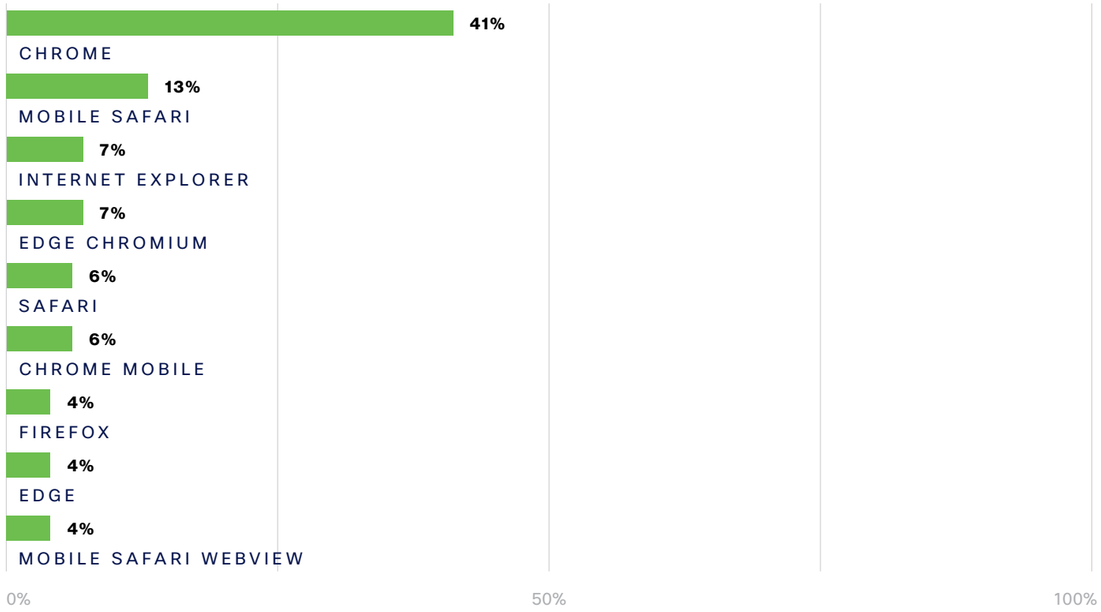
MOBILE OS USAGE



Chrome in Command

Google Chrome remains the browser of record for businesses. There are no other browsers that even come close to supplanting the leader.

TOP BROWSERS

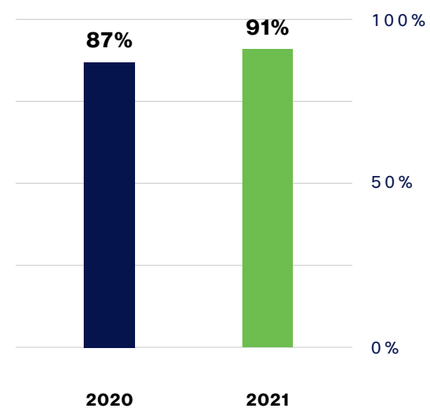


Browsers Improving Security Posture

Every year we take a moment to look at how web browsers are fairing from a security perspective and this year we noticed one piece of information that was heartening. In 2020 we noted that 81% of browsers had no Flash installed. To put a fine point on this factoid, Flash reached its **end of life** December 31, 2020. To ensure the safety of their users, Adobe took a step further and blocked Flash content from being able to run in Flash Player beginning January 12, 2021. As a result, the number of systems running Flash shifted dramatically downward in 2021, now with 95% of systems no longer having it installed.

What about Java, you may ask? According to our data, in 2020 87% of browsers had no Java installed. That number has increased to 91% of systems in 2021.

BROWSERS WITHOUT JAVA



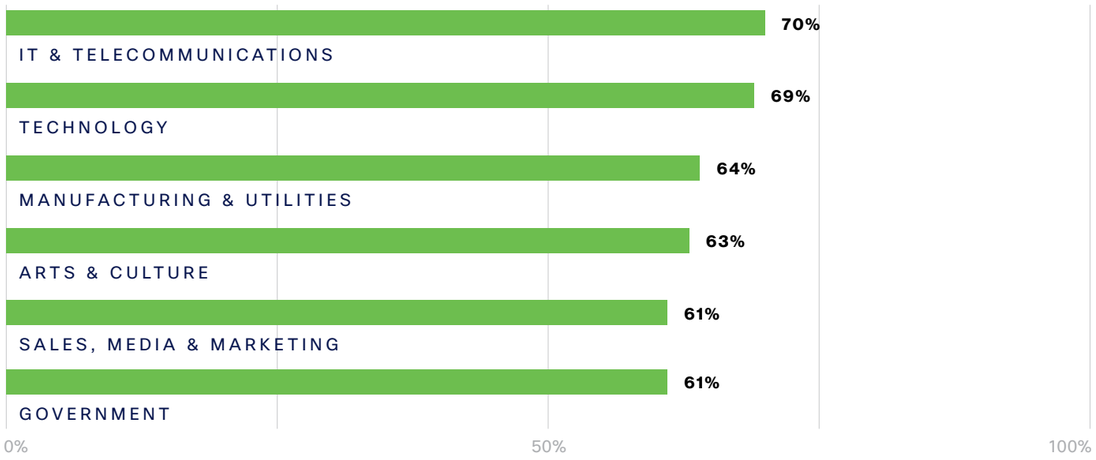
Cleaning Out the Outdated Device Detritus

As enterprises increasingly leverage collaborative technology, the ability to clearly identify trusted users is just one component of a security strategy. Device hygiene and security must be brought up to current standards, or at least to the latest available revision. Outdated devices can inadvertently expose the corporate environment to potential attacks due to unpatched vulnerabilities or misconfigured systems. This could leave an enterprise exposed to threats from malicious software, as well as ransomware and data breaches, to name a few.

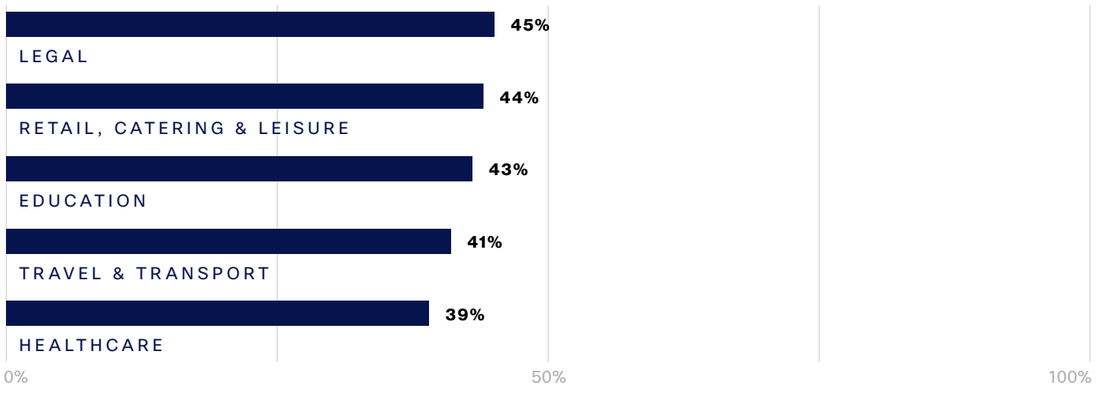
Across industry verticals, we find the percentage of endpoints that are patched and up-to-date varies widely.

Our research reveals that tech-savvy industries are more likely to have users with up-to-date devices, whereas industries slower to adopt new technologies or burdened by cumbersome, antiquated systems typically have more out-of-date devices in their fleets.

INDUSTRIES WITH MOST UP-TO-DATE DEVICES



INDUSTRIES WITH MOST OUT-OF-DATE DEVICES



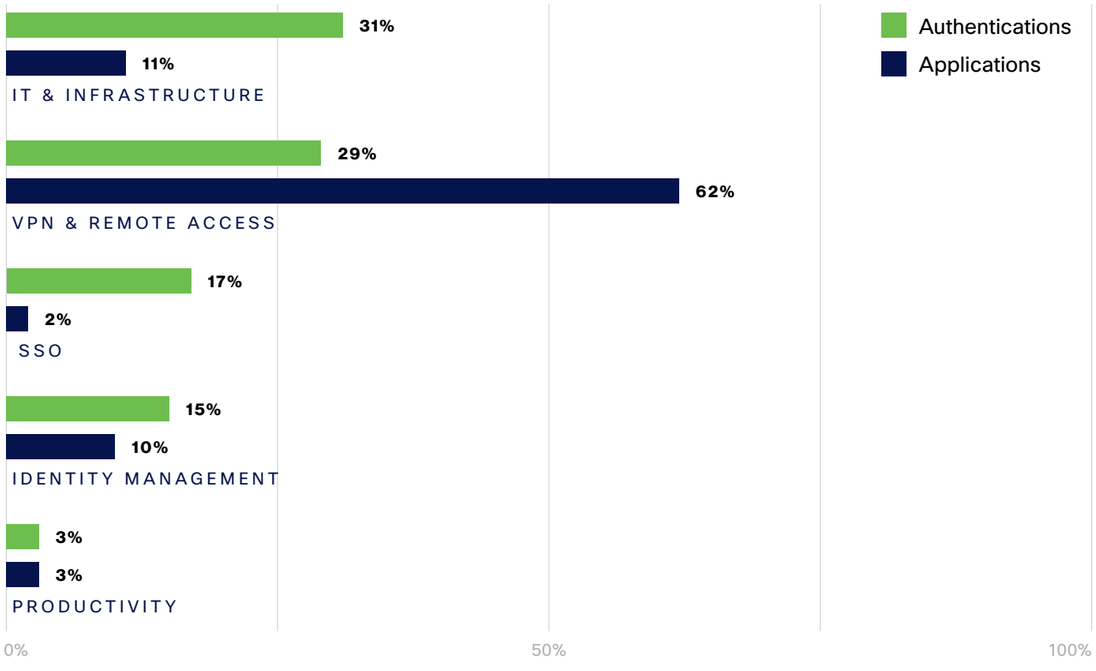
4.0

Applications

Enterprises have learned that secure access is necessary to ensure that users and devices can securely reach applications and data. The need to be able to secure devices, users and data has never been more important than what we've seen in the hybrid workforce landscape. Historically, many organizations viewed hybrid work as a perk, but we've learned it's far more than that: Working remotely is a clear path to keeping businesses operating.

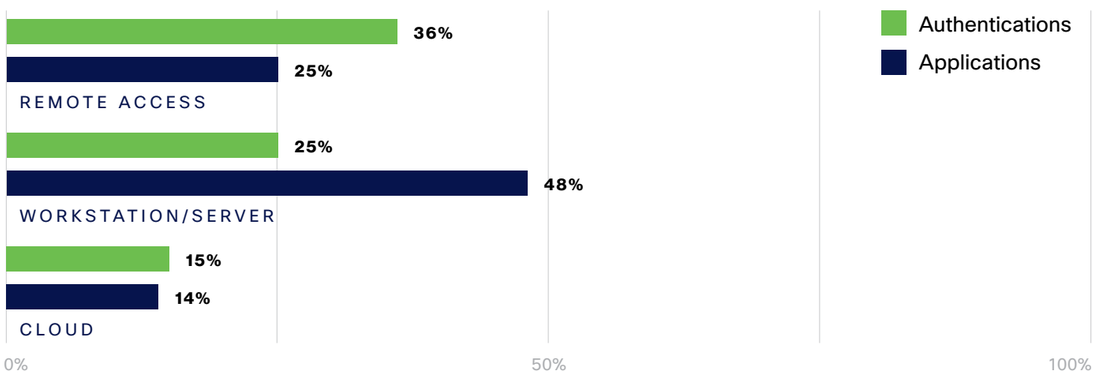
As part of our research, we examined the most common categories of applications that Duo customers access.

TOP APPLICATION CATEGORIES ACCESSED



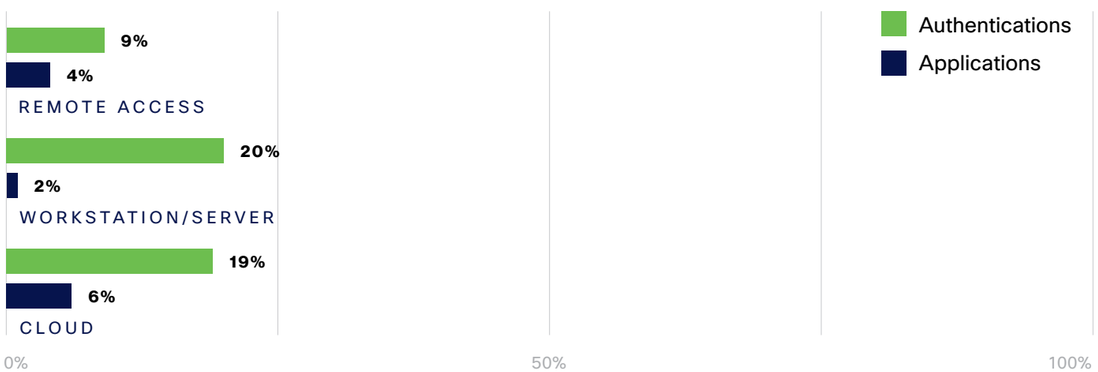
We also looked at application access in a different way: not just the category of resource they allow access to, but the type of resource.

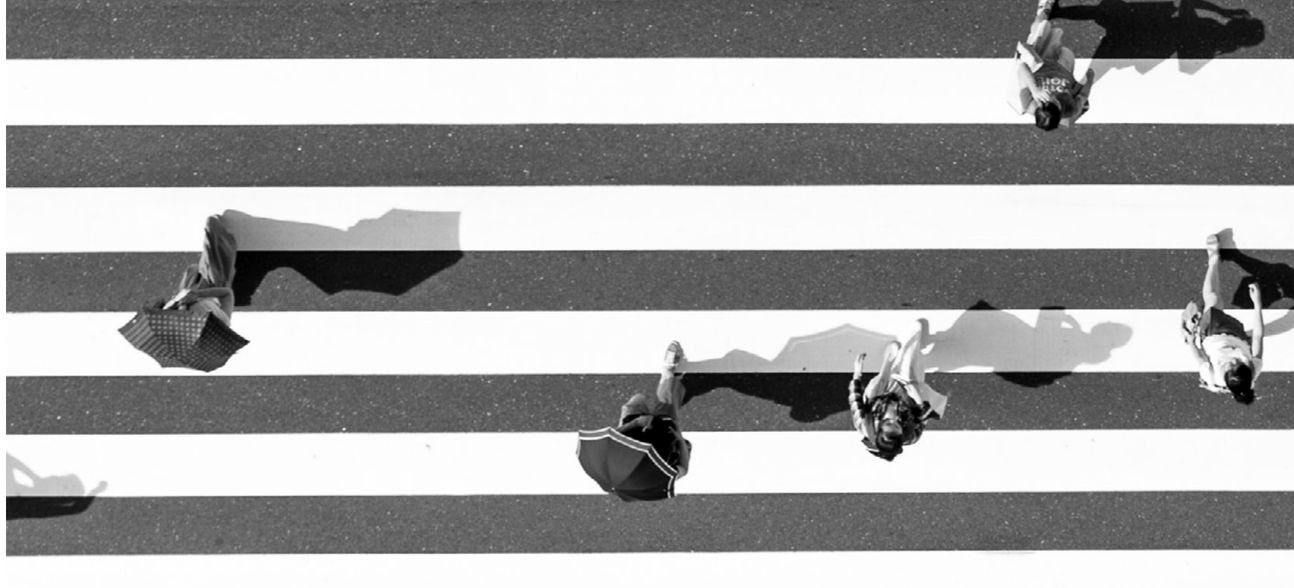
TOP APPLICATION TYPES ACCESSED



The year-over-year change between 2020 and 2021 indicates that remote access and cloud application use has continued its upward trajectory and will continue to do so for quite some time to come. Our data captures how the usage of these categories changed relative to overall usage.

APPLICATION USAGE PERCENT CHANGE





5.0

Summary

Collectively, the past year has taught us many lessons. Enterprises must streamline core IT security functions, enable hybrid workers to be able to focus on their core competencies, and address lingering security debt issues within the enterprise.

Hybrid work and hybrid business models are now the standard operating procedure for getting our jobs done. This will remain front and center in workplace culture among many industries for years, as organizations in 2020 had to quickly accommodate hybrid work at massive scale. Those accommodations were met and the corporate world grew with enterprises realizing that productivity could in fact happen in this environment. Many organizations have indicated that they will continue to utilize a hybrid model for employees for the foreseeable future.

This rapid expansion presented new security challenges, not least of which is ensuring that employees can work securely and without introducing new risk to the business. As businesses implemented their remote access strategies, some key themes emerged: the need to secure users and devices and their access to applications.

"Taking a zero trust approach helps address the issue of security debt. This debt can build over time and be reflected in many ways. Poor visibility over devices and assets, systems that need updating or simple misconfigurations. The debt builds up and needs at some stage to be paid back.

By applying an approach such as zero trust, which requires specific policy requirements are met before access is allowed, this level of debt can be identified and reduced. A simple example is the status of devices where access can be limited until an update is run. This is paying off debt by a standard constant process and is preventing the principal from increasing. It reduces the risk of this credit card getting out of control.

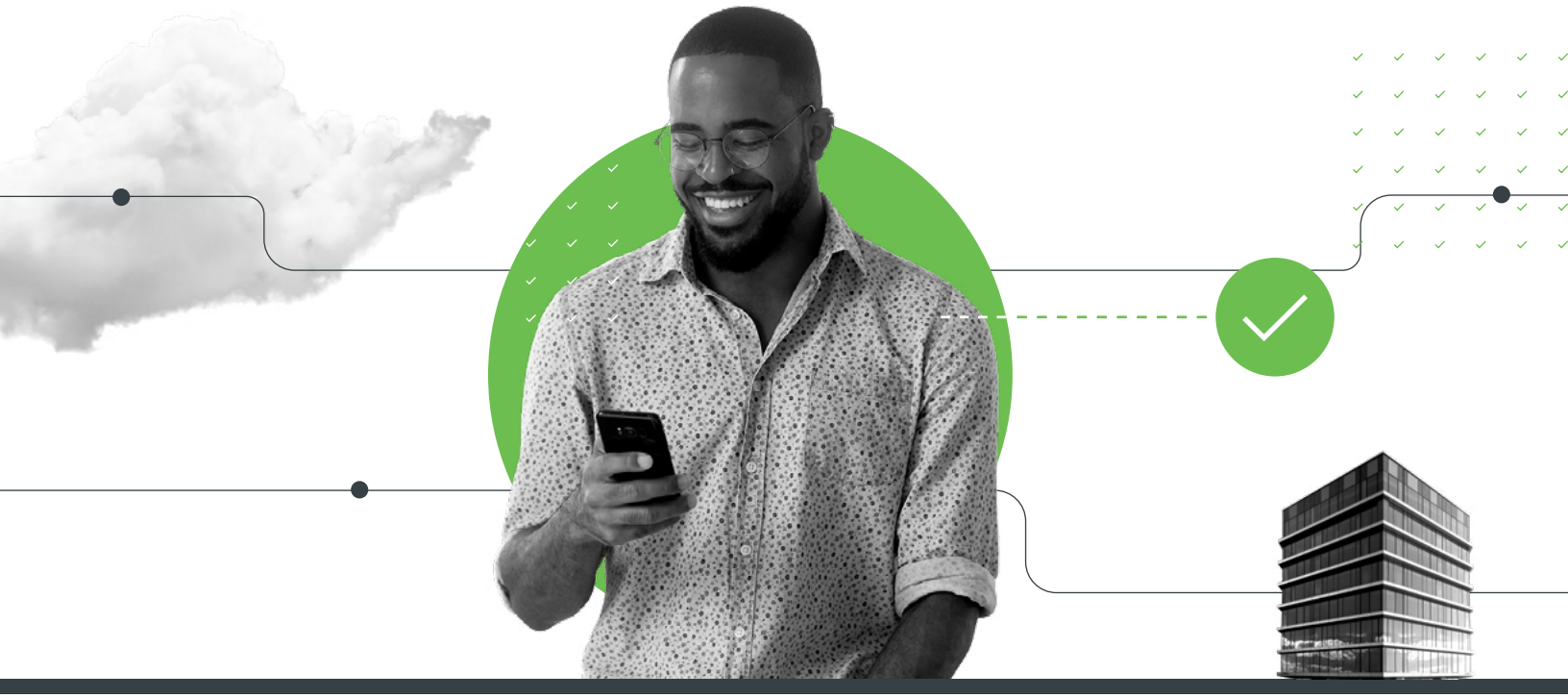
Of particular interest is compliance with privacy requirements which call for limitations on access to specific personal data. Often excessive privileges result from internal changes in staff and roles. These may not be readily managed at the time of change through the JLM process. This results in too many users having too many privileges over too much data.

By applying zero trust principles and reducing excessive permissions, organizations have managed to assure that they are compliant and pay off this element of debt. The same principle has been seen to help reduce the number of inactive accounts. This is another form of debt that may have been created over time, but which can be readily identified and paid back."

Richard Archdeacon
Advisory CISO, Duo Security

In order to help enterprises and organizations the world over, we need to provide support for businesses to improve their visibility, get a better understanding of policy management, and place a greater emphasis on automation to help security teams do more with the resources they have available. Strategies such as zero trust and a passwordless approach will improve security while reducing risk to the organization. With a stronger focus on user experience – which in turn allows for greater democratization of security. Lastly, a sensible approach to policy application and enforcement will accelerate a security team's ability to enable the business to operate safely and securely.

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



“The hybrid workplace demands the workforce to be secure, connected and productive from anywhere. For us, this means acceleration of cloud adoption, solid remote connectivity strategy as well as adoption of secure access service edge (SASE).”

Binaya Sharma
Director, IT Infrastructure
TechnoPro

Start your free 30-day trial and quickly protect all users, devices and applications at **duo.com**.

cisco The bridge to possible

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of the Cisco Zero Trust offering, the most comprehensive approach to securing access across IT applications and environments, from any user, device, and location. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Founded in Ann Arbor, Michigan, Duo also has offices in Austin, Texas; San Francisco, California; and London.