

The 2022 Duo

Trusted Access Report



LoginsInADangerousTime



.....|



SECURE



AUTHOR
DAVE LEWIS

DATA SCIENCE
BEN EDWARDS,
CYENTIA INSTITUTE

EDITORIAL
CHRYSTA CHERRIE

DESIGN & DEV
MARLA JONES
TRACY TOEPFER

The 2022 Duo

Trusted Access Report

Logins in a Dangerous Time


LOGINS IN A DANGEROUS TIME	1
KEY FINDINGS	11
THE TALOS PERSPECTIVE	15
DEVICES	21
APPLICATIONS	43
SUMMARY	47
REFERENCES	49

Logins in a Dangerous Time

The Trusted Access Report is an annual report analyzing Duo product data – and how our customers are using Duo. This year's report has taken a decidedly different tone from **last year's iteration**, in light of the world stage we find ourselves on.

This is not a chance to press upon fear, uncertainty and doubt. Rather, it's an opportunity to understand the gravity of where security stands today. As global conflicts spill over into the digital realm, the idea of protecting the individual through to the enterprise has taken on a greater sense of urgency.

In the report, we will explore data findings gleaned through review of more than 13 billion authentications from almost 50 million different devices across our customer base in North America, Latin America, Europe, Middle East, and the Asia Pacific, over the course of a year.



Some of the key findings were uplifting. We noted that the adoption of passwordless authentication continues to rise. The number of authentications using Duo increased 41%. Conversely, data showed that biometrics enabled on mobile phones stalled at 81% after a steady increase over the last several years. Most organizations do not make use of geographic-based blocking policies, interestingly enough. This is good to see as defenders need all the help they can get to counter cybersecurity-related threats.

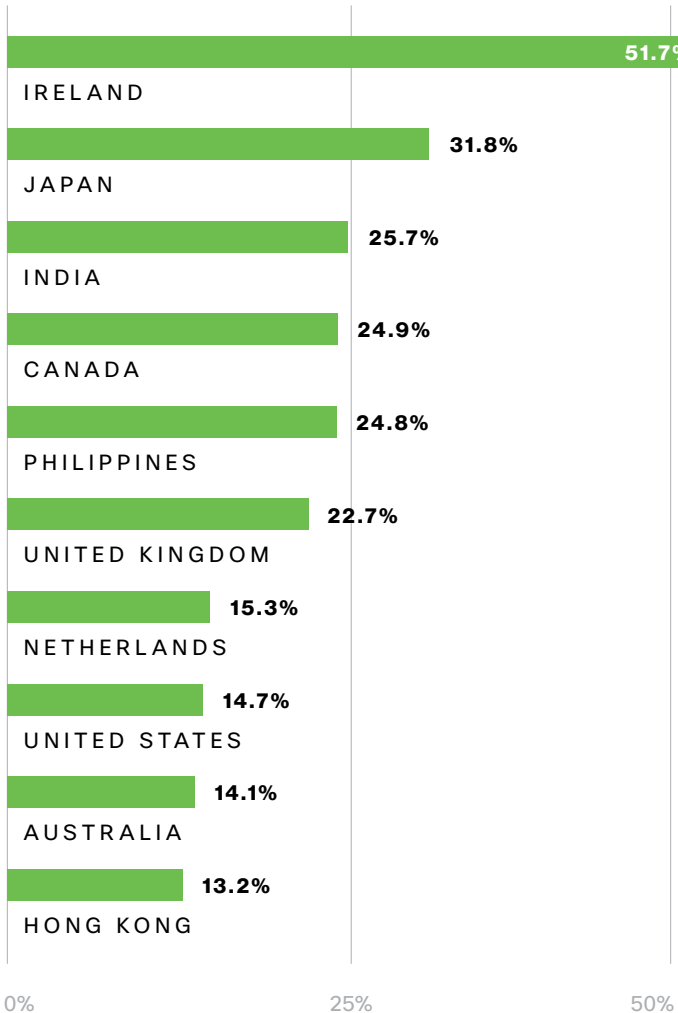
We have moved well beyond the discussions of password complexity to those where investing in multi-factor authentication (MFA) and passwordless technology are mandatory costs of doing business:

To help protect against the wide array of adversaries we face, these technologies go a very long way to helping to reduce risk for organizations.

Take, if you will, the plight of the warfighter – a long and storied legend from the world over, sent off to battle for vassal states through modern conflicts between the most economically developed countries. Technology was ever-present as a contributor to the success or failure of campaigns since the Greeks marched into battle in a phalanx formation. We’ve seen the advent of technology of catapults, muskets and Enigma machines. Cyberwar is not all that different on the face of it. We still have combatants on the field engaged in kinetic warfare. Technology has always helped us tip the scales in favor of one side versus another, and modern technology has offered the ability to compromise computers via malicious software. This allows for greater surveillance campaigns, and most importantly, greater intelligence gathering and processing capabilities. The information revolution has indeed impacted modern military engagements.

In the face of these and other threats, we’re seeing an increasingly global adoption of MFA authentications from Ireland, Japan, India, Canada and the Philippines. This demonstrates that a wider base of countries are rising to the challenge, defending their systems against the threats of today. We can see the impact of this global threat environment in usage data from Duo's products, which we will explore in this report.

FIGURE 1: YoY INCREASE IN MFA AMONG COUNTRIES WITH THE HIGHEST NUMBER OF AUTHENTICATIONS



It has been almost 30 years since the publication of the RAND Corporation [document](#) “Cyberwar is Coming.” While it spoke to the idea of cyberwar, it materialized partially along the lines that the authors envisioned – that knowledge must be shaped into capability to address the challenges that we face. If we utilize the current war in Ukraine as an example, we see both sides engaged in efforts to compromise each other's networks and systems in a bid to gather information or cause damage.

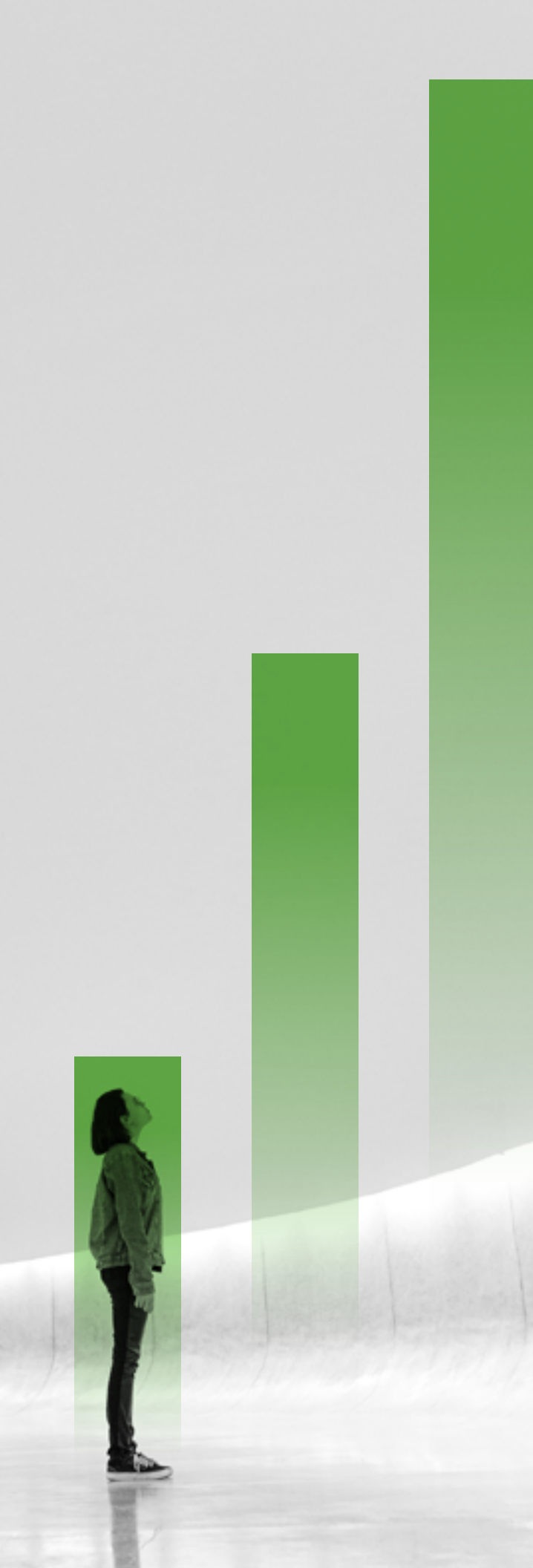
Aiming to augment their cyberwar capabilities, the Ukrainian government enlisted the help of hackers to attack Russian targets. In addition to more destructive functions, these parties also collect open-source intelligence (OSINT) data for Ukraine to better mount a defense of their country.

Surveillance is a key component of military engagements today. While we have deterrents such as mutual assured destruction (MAD) for nuclear war, there really is no such parallel for cyberwar. History has witnessed many iterations of surveillance, but never has it been so prevalent as in this current conflict in the guise of GPS, cellular providers and satellite feeds.

Intelligence gathering has been fundamental from a cyberwar perspective. When we review the war in Ukraine as an example, we see where information security has played a significant role, from targeting armor in the field to curtailing supply chains and destroying war ships. While all of these may appear to be solely kinetic in nature, they were assuredly aided by computer-based OSINT data. To counter this, defenders work to crush the ability of attackers to access systems and resources.

We see that organizations based in Ukraine and other places that have experienced significant political events – such as Hong Kong – attempt to authenticate from a wide variety of countries. Coupled with passwordless technologies such as WebAuthn, and having strong intelligence capabilities help to counter a large portion of the offensive attack surface, any nation with access to the internet will have some level of investment in cybersecurity from an offensive and defensive strategy perspective.

Cyberwar is a force multiplier, as opposed to a standalone theater. Much like the Greek introduction of the phalanx, cyberwar has fundamentally shifted how modern warfare is waged. The idea presented in the RAND document that cyberwar allows a reduction in overall force size has not borne fruit. That being said, cyberwar is not a panacea, and the crossover from cyber to kinetic was evident in regards to Stuxnet. This serves as evidence that cyberwar is yet another addition to the warfighter's toolkit to counter adversaries.



There are dangers in the world today. This should not come as a surprise to anyone, but it does bear repeating.

If we rely on tools of the past and hope to use them to defeat our adversaries, we are doing ourselves a disservice.

Bad actors will always find new and interesting ways to cause us undue harm. When we frame the discussion point of threats, not only as tools for illicit financial gain, but for augmenting lethal warfare capabilities, we realize that the importance required to address cyber security issues has never been more prescient.

But all is not lost. We see that the scales are tipping in favor of the defending organizations. Denials are dropping as we see adversaries often stymied when they encounter systems protected by multi-factor authentication (MFA). This can be explained. When an adversary encounters MFA they often move on to other targets rather than engage, as they can have better success with softer targets. In fact, the percentage of organizations who have any kind of policy denying specific geographic locations has dropped 20% since 2020.

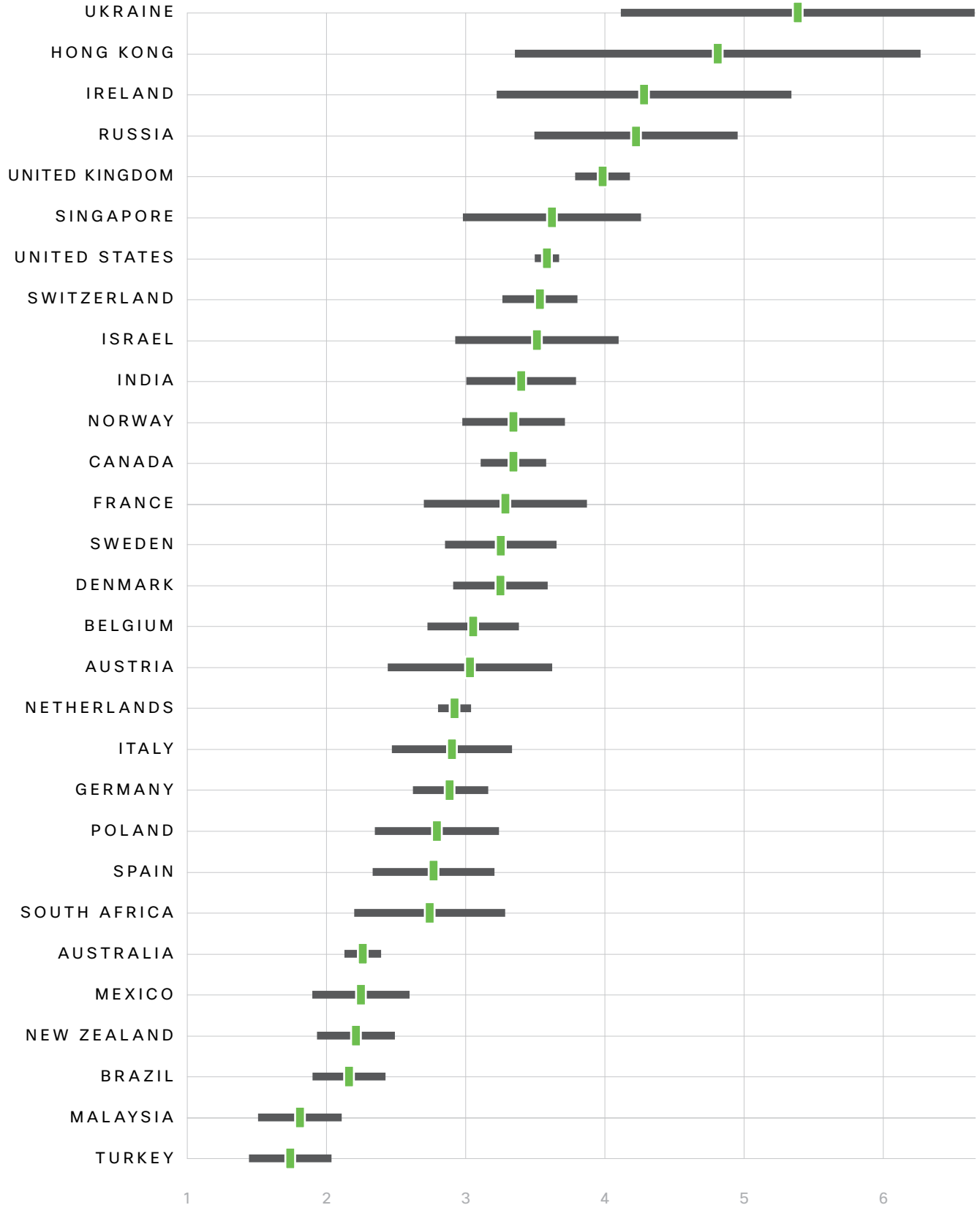
But which countries are organizations explicitly denying authentications from? Figure 3 shows the top 20 most denied countries. In 2022, for example, 82% of organizations that had specific denial policies denied authentications from Russia. What we note in this graph is that denial policies for the top 20 countries are in fact decreasing, while realizing that the top six countries have remained relatively consistent. The outlier here, Belarus, rocketed from the 20th position to 8th overall.

Looking back over the last few years, we saw a massive global push to hybrid work environments. Almost overnight we observed business move from the occasional work-from-home day to entire workforces working from home to ensure that business kept rolling on.

FIGURE 2: AVERAGE NUMBER OF COUNTRIES FROM WHICH ORGANIZATIONS BASED IN DIFFERENT LOCATIONS AUTHENTICATE

The vertical axis is an organization’s principal location. The central green rectangles represent the means, and the grey bars represent the 95% confidence

intervals for the estimate of the mean. For example, organizations based in Ukraine authenticated from nearly 5.5 different countries on average.



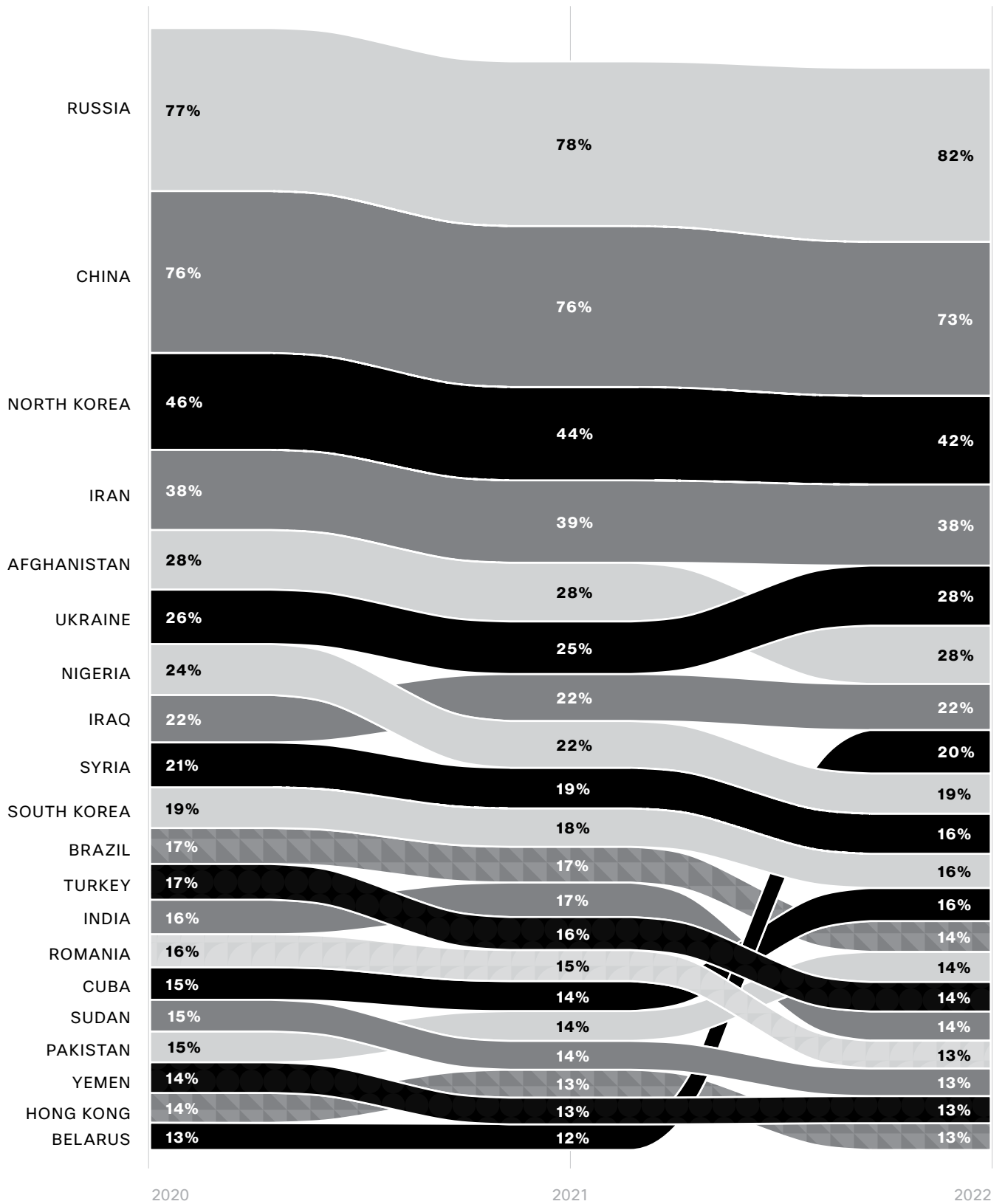


In last year's report, we made reference to the venerable security control, the password, as being the functional equivalent of a house key. Attackers who target corporations and individuals for access to resources they would not otherwise have are aware of this analogy. Countries engaged in kinetic warfare also make use of stolen passwords to obtain data and intellectual property to bolster their cause, surveil targets and even to destroy their adversaries.

MFA is one way that organizations can better protect themselves against intrusions. It removes or reduces one of the easiest avenues for adversaries to attack organizations and individuals. Imagine for a moment, how much damage could an adversary inflict with purloined access for just one day? Considering that data breaches are often undiscovered for weeks, it is troubling to think what could transpire.

We have now arrived at a turning point with respect to cybersecurity. It has become clear that MFA is basic "you must be this tall to ride the rollercoaster" for any organization. Companies around the world have historically made use of MFA to protect mission critical assets as opposed to protecting the entire enterprise. The COVID-19 pandemic taught the world some valuable lessons. Companies needed to find better ways to secure access with their workforces being moved to a hybrid model. Enterprise security teams took the step of adding MFA to all of their access as a way to reduce the risk exposure of so many moving parts due to staff working from home.

FIGURE 3: ACCOUNTS DENYING COUNTRY BY POLICY IN THE LAST THREE YEARS





Methodology

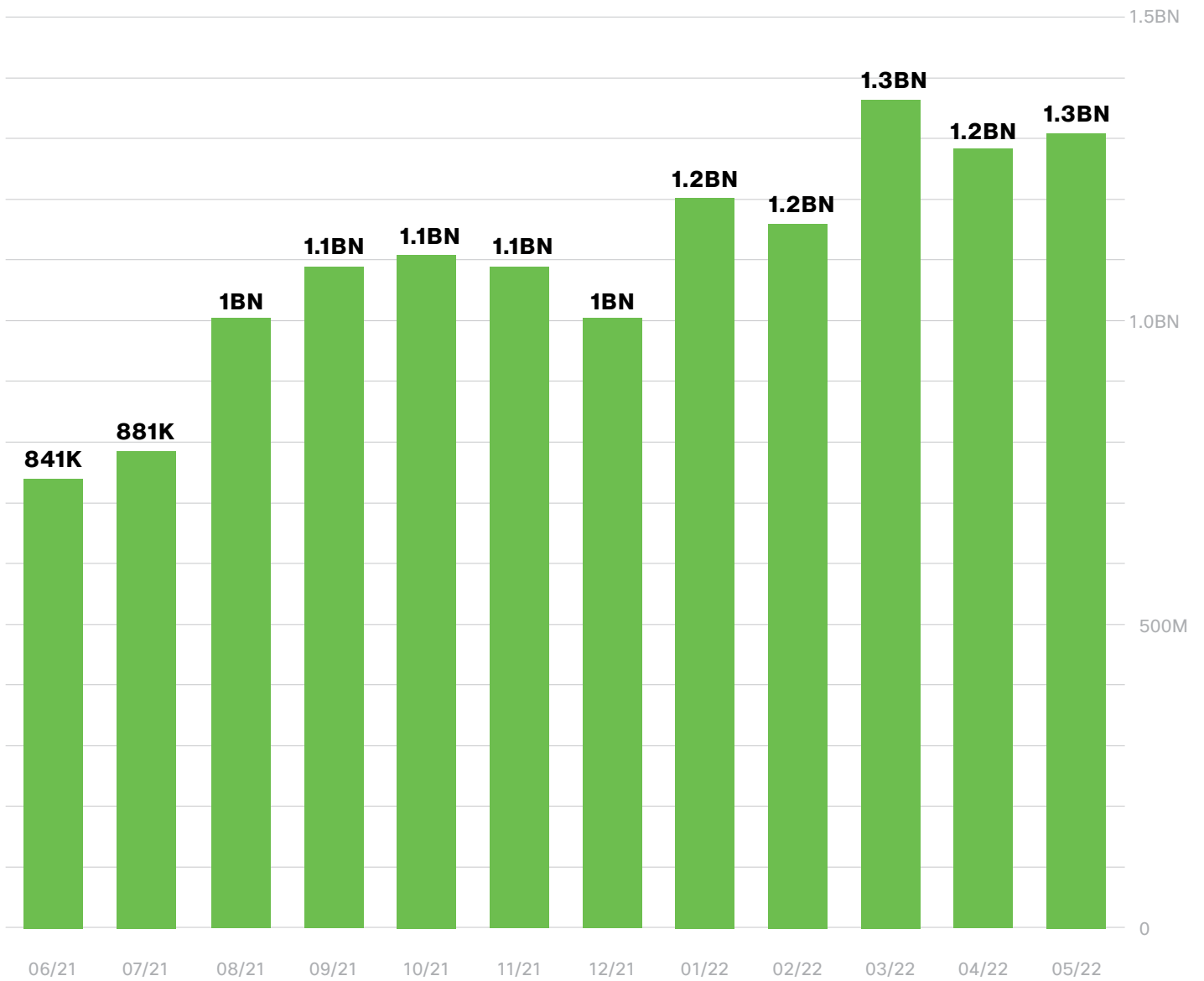
A zero-trust security strategy is based on three key pillars: users, devices and applications. It asks the questions:

- Who has permission to access your information?
- Which devices are being used to access applications?
- Which applications are users accessing?

For this report, we analyzed data from more than 13 billion authentications on 49+ million devices, more than 490 thousand unique applications and roughly 1.1 billion 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, 2021 and May 31, 2022, and examined authentications between those dates, inclusive. For non-authentication data, we counted metrics on May 31, 2022.

For year-over-year comparison, we defined our 2020 time range for authentications as between June 1, 2021 and May 31, 2022, inclusive. We counted metrics for non-authentication 2022 data on May 31, 2022.

FIGURE 4: MONTHLY TOTAL AUTHENTICATIONS



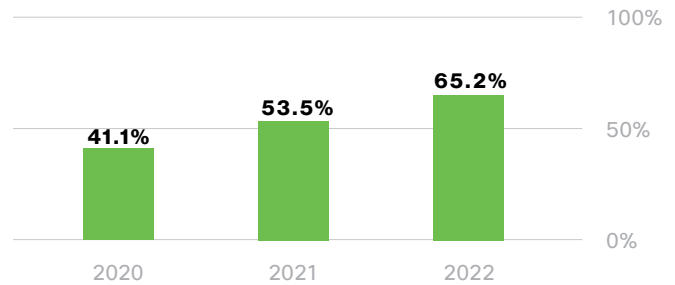
Key Findings

TOP 10 TRENDS AT A GLANCE

01 **PASSWORDLESS ADOPTION CONTINUES TO RISE**

Our data shows a 50% increase in the percentage of accounts allowing WebAuthn authentication and a fivefold increase in WebAuthn usage since April 2019.

FIGURE 5: PASSWORDLESS AUTHENTICATION STILL ON THE RISE



02 **BIOMETRICS HAVE STALLED**

The percentage of phones with biometrics enabled held steady at around 81% (a minor increase from 2021), indicating that progress towards biometrics across the board has stalled.

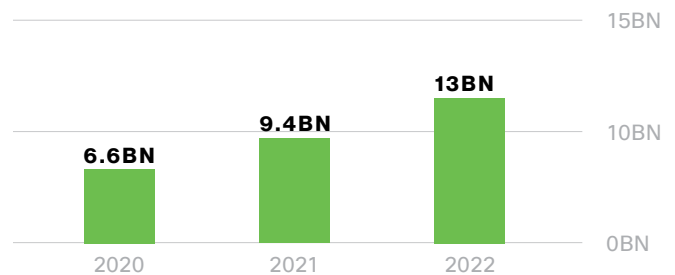
03 **PUSH PREFERRED**

Duo Push is the most used authentication method, accounting for 27.6% of all authentications.

04 **MFA CONTINUES TO STRENGTHEN PASSWORDS**

Multi-factor authentication holds strong while adding to the security of only traditional password usage. The number of MFA authentications using Duo rose by 38% in the past year.

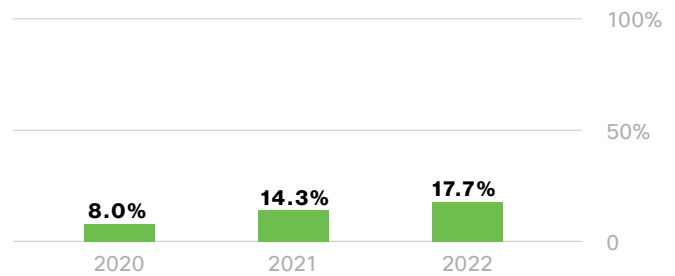
FIGURE 6: TOTAL MFA AUTHENTICATIONS



05 CLOUD USAGE CONTINUES TO RISE

An increasing number of authentications are attributed to cloud applications, with a 24% rise in the percentage of cloud applications in 2022.

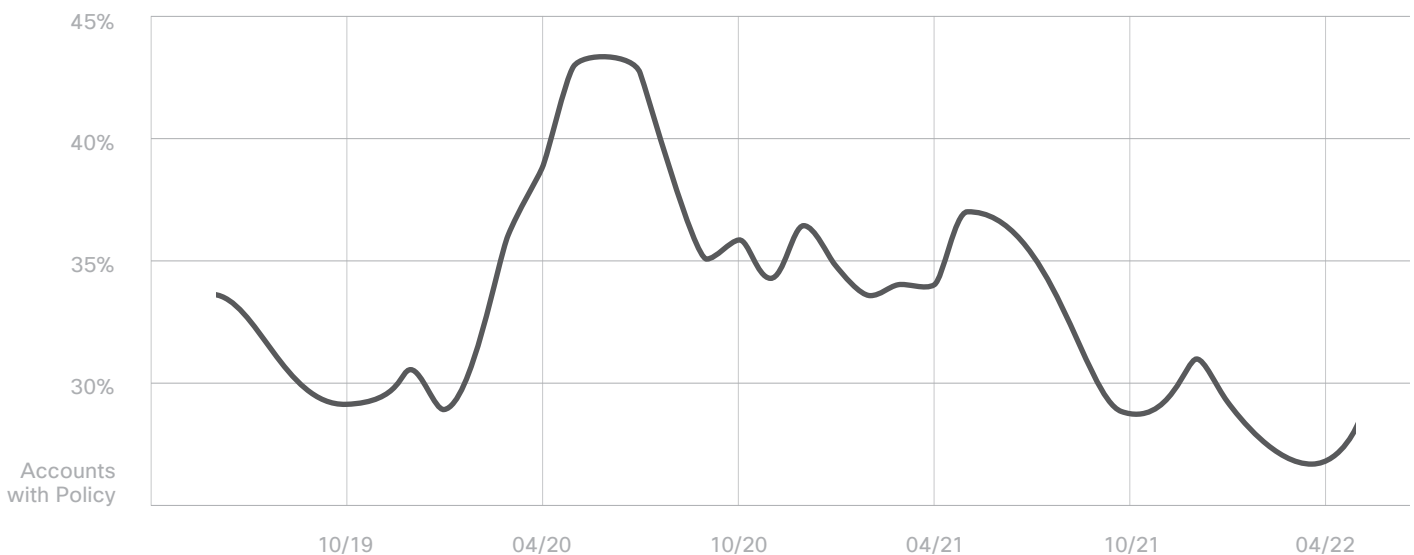
FIGURE 7: YoY INCREASE IN CLOUD APPLICATIONS



06 BACK TO THE OFFICE

Remote access authentications peaked in 2020 but have declined since then, reaching lower than pre-pandemic levels.

FIGURE 8: AUTHENTICATIONS FOR REMOTE ACCESS APPLICATIONS



07 LOCATIONS BLOCKED

Many organizations do not take the necessary step to implement geographic-based policies. Less than 1% of organizations implement explicit deny or allow policies. However, among those enterprises that do deny geographic locations, they block either Russia or China 91% of the time, and 63% of those organizations block both countries.

09 ENTERPRISES EVOLVE WITH THE TIMES

When Russia invaded Ukraine in February 2022, we noticed a significant drop in authentications from within the country. This was no surprise, as the daily lives of Ukrainian people were completely upended. The issue then transformed into one of a mobile populace: the need to safely authenticate from wherever they could get access – if and when they needed it. Being certain of the identity of the person logging into systems became even more pertinent.

Security controls need to be ramped up to address the needs of the day. Passwords have long been seen as a security control, but in this day and age we have come to the realization that they have limited utility. By updating to more modern security controls like MFA or passwordless authentication, we have far higher confidence that the person being authenticated is in fact who they should be. Conversely, when we rely on passwords as a control, we are hoping for the best.

In last year's report, we compared the password to a house key for security purposes. Sure, you can lock the door to protect yourself and your assets, but there is absolutely nothing to demonstrate that the person coming through the front door is in fact the person who is supposed to be. The venerable password has come to the end of its useful lifespan.

08 OUT-OF-DATE FAILURES

The percentage of failures due to out-of-date devices increased 51.8% between 2021 and 2022. This is despite the fact that the percentage of orgs with policies governing out-of-date devices decreased 7.1%.

We have moved as a society from contending with a global pandemic to dealing with global military conflicts that have spilled into the cyber realm with direct impact on individuals and organizations – all far removed from the theater of active warfare. The level of urgency to address deprecated security controls has never been so pressing as it is today.

Hybrid work environments have established themselves as a clear viable option for businesses to continue to function. The adversaries have adapted to this new reality as well. A strong work-life balance for hybrid workers needs to be clearly augmented with security that allows them to get their work done safely and securely.

Companies worldwide have found themselves having to adjust to this new paradigm. We have moved on from a firefighting mode to one of building out long-term strategies for dealing with how to best maintain and grow the capabilities for handling hybrid work.

With employees now working in a hybrid fashion globally, we have to continue to account for the overarching requirement to democratize security. We know that 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's a concerted effort to move all access to MFA, not only to 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. A prime example of this is the password. Driven by the requirement to accommodate a globally distributed workforce no longer tied to a physical office location, security is becoming much more streamlined.

For this report, Duo partnered with the Cyentia Institute to analyze data from more than 49 million devices, 490+ thousand unique applications and roughly 1.1 billion 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, 2021 and May 31, 2022, and examined authentications between those dates, inclusive. For non-authentication data, we counted metrics on May 31, 2022.

DEVICES: 49,000,000+

APPLICATIONS: 490,000+

**AVERAGE AUTHENTICATIONS
PER MONTH: 1,106,000,000+**



The Talos Perspective

One strength of the Cisco family is that in addition to the Duo team, we benefit from the invaluable contributions of the Talos Intelligence team. Talos has been actively engaged in **supporting the Ukraine government** by providing defensive guidance, forensic analysis and intelligence, as well as engaging in threat-hunting activities.

Analyzing the approach of Russia, Talos found that their cyber capabilities broke down into three core buckets. First and foremost were the cyberattacks which included, but were not limited to, distributed denial of service attacks and destructive attacks designed to disrupt operational technology. Second were concerted attacks against complex systems such as supply chains. Finally, disinformation campaigns were used to attempt to change the global view of the war, as well as attempting to exploit internal dissent or ethnic, religious and political divides.



There were also sharp divides emerging, as various cybercriminal groups chose their sides. For example, the Conti ransomware gang chose to support the Russian side of the war and announced that they would target western countries who support Ukraine.

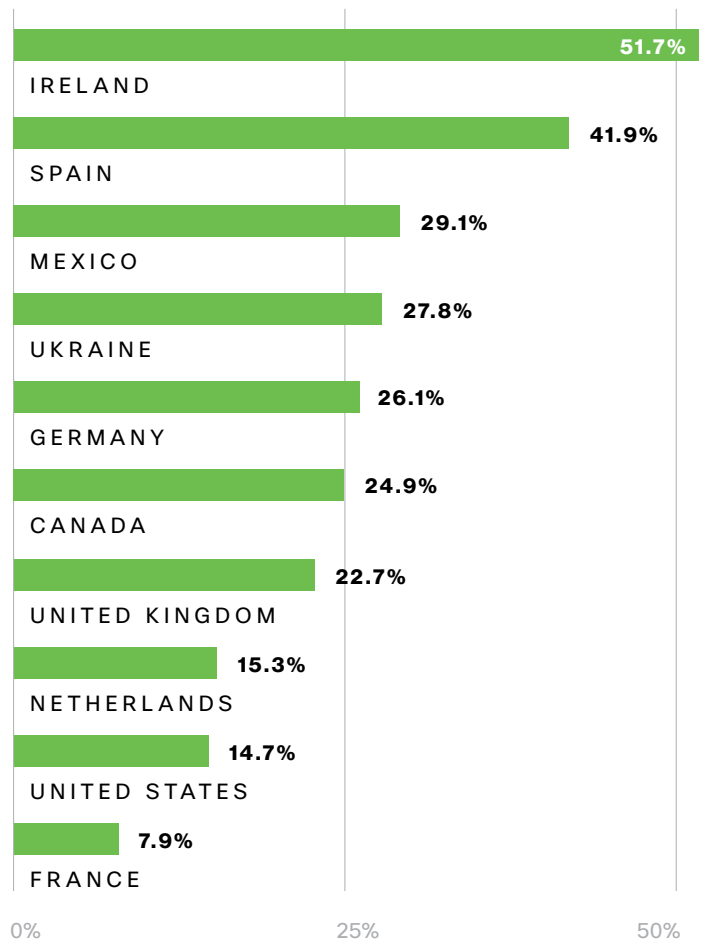
Anonymous launched a campaign to compromise systems in Russia in direct response to the war. The common thread that came to light was the constant attacks against systems utilizing misconfigurations, missing patches and purloined static passwords.

Global Rise in MFA Usage

We reviewed 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 U.S., authentication volume rose 15%, while neighbors to the north in Canada saw a 25% increase in the number of authentications. In Ireland, the volume of authentications rose 52% over the same period.

In the Asia-Pacific region, we saw an upward trend in Japan, registering a 32% increase in authentications. New Zealand increased by 30%, and we saw a significant 27% increase in Indonesia.

FIGURE 9: YoY INCREASE IN MFA AMONG COUNTRIES WITH THE HIGHEST NUMBER OF AUTHENTICATIONS IN THE AMERICAS AND EMEA REGIONS



But not all countries saw an increase in authentication volume.

Figure 11 details countries that saw significant declines in the percentage of MFA authentications.

While the bounce in authentication volume of 15% might seem curious when looking at it through the lens of 2022, it should be noted that there was a significant drop of 37% in the report last year. This may have merely been a correction.

The massive increase in authentication volume in Czechia, a NATO member state, can be attributed to the increase in cyberattacks targeting the country from cyberattackers who have allegiances to Russia. As an example Czech Television, CT24 and Czech Radio's news server **all came under distributed denial of service attacks in April, 2022.**

FIGURE 10: YEAR OVER YEAR INCREASE IN MFA AMONG COUNTRIES WITH THE HIGHEST NUMBER OF AUTHENTICATIONS IN THE APAC REGION

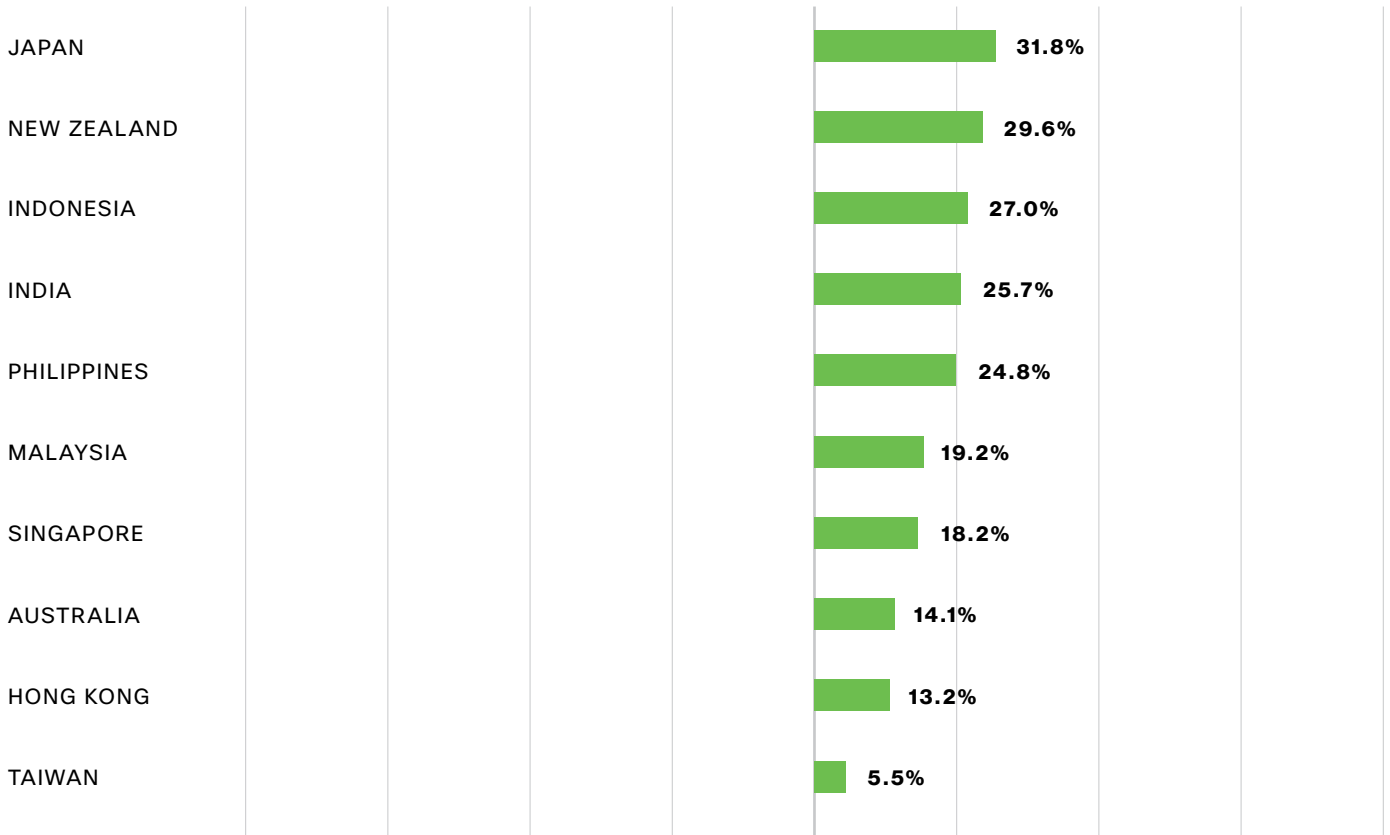
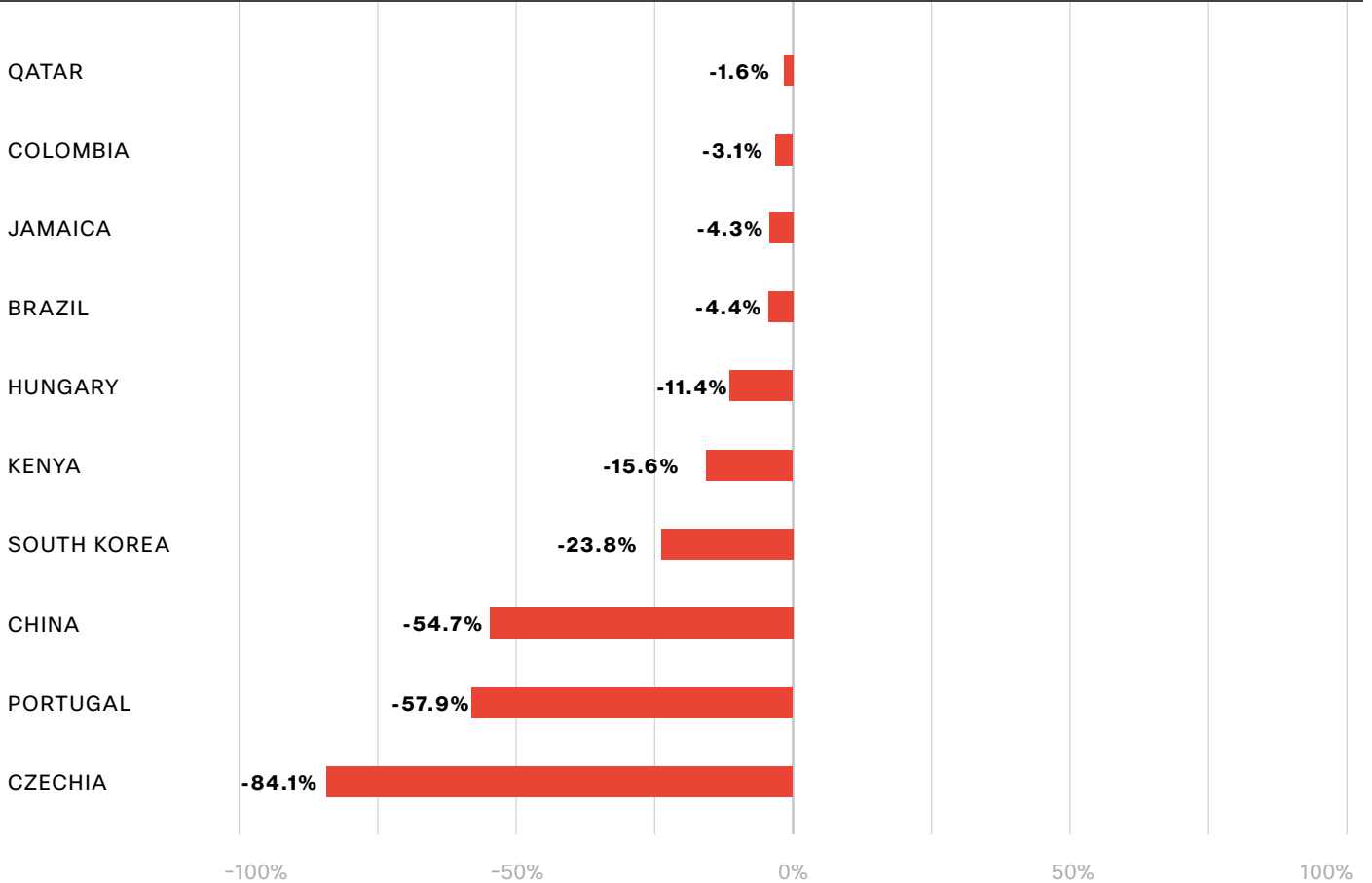


FIGURE 11: AUTHENTICATION DECLINES AMONG COUNTRIES WITH HIGH AUTHENTICATION VOLUME





Device Visibility

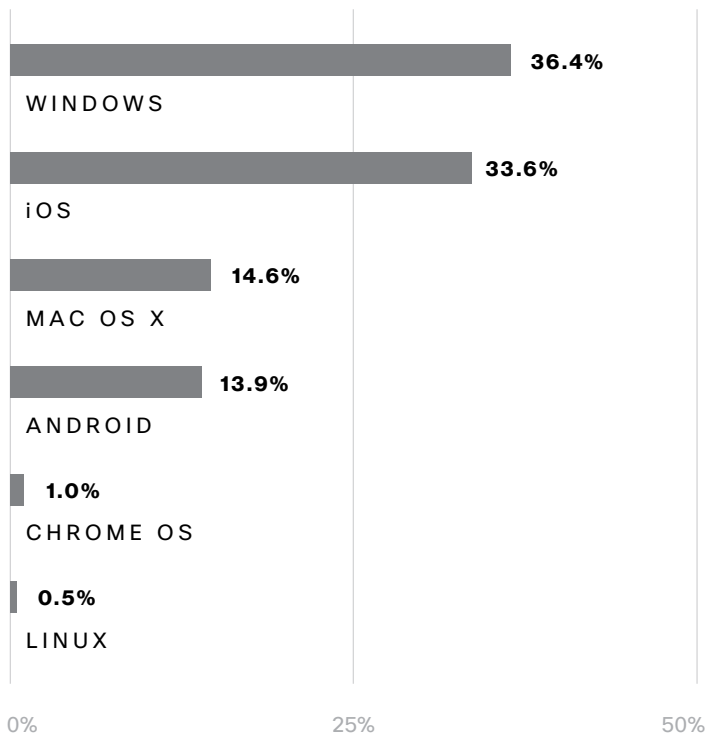
Establishing device trust requires visibility into the devices accessing applications and data. Understanding which operating systems and which browsers those devices are running, and whether those OSes and browsers are up to date (among other things), can determine whether they're considered trustworthy.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

Windows Continues as the Prevalent OS

On the operating systems front, we found that Windows remains the front-runner. According to our data, these are the top OSes Duo customers use.

While the Redmond stalwart continues to lead the pack, we note that iOS is a strong second at 27% in the overall listings. Now with more people working in a hybrid environment, we see that they're working in the way that suits them best. With more people making use of what would have historically been seen as a non-traditional operating system platform, a new paradigm is emerging. Linux still lags far behind, unfortunately.

FIGURE 12: PERCENTAGE OF ENDPOINTS BY OPERATING SYSTEM






Devices

Enterprises find they have to contend with attackers online who are financially and politically motivated, in addition to supporting their dispersed hybrid workforces which have evolved from firefighting to the de facto standard. While protecting enterprises once entailed simply keeping the lights on, it now requires defending against all manner of external attacks. Making sure that devices are both secure and have strong authentication continues to 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 such as laptops and mobile phones are indispensable tools for business. Protecting these assets is essential, and 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 also key that enterprises address how to define the security posture of devices in the surrounding 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 used 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 by establishing device trust.

We took a closer look at data collected by the Duo Device Health app this year and refined our analysis. In particular, we wanted to know if organizations were generally increasing or decreasing their use of various protections. This is important because as a total percentage of devices with encryption decreased from 90% to 87.2%, and firewall usage decreased from 96% to 88.4%. But this was largely due to a few accounts with a large number of devices.

On an organization-by-organization basis, we see that among those that had some kind of device encryption detectable, most (64%) increased the percentage of devices with encryption. In fact, on average, organizations increased the percentage of encryption usage by 43% and increased firewall usage 26%.¹

¹ These are geometric means as opposed to arithmetic means or medians. These are used because some orgs went from a tiny percentage of devices with these protections to nearly 100%, a many order of magnitude increase. We want to focus on "typical" so we use statistics robust to these types of measures.

Device-Based Policies

In prior reports, we discussed reducing the security debt that an organization has to contend with overall. The best way for an organization to tackle this is by way of reducing risk, for example by ensuring that uniform policies are applied to assets in the environment via device-based policies.

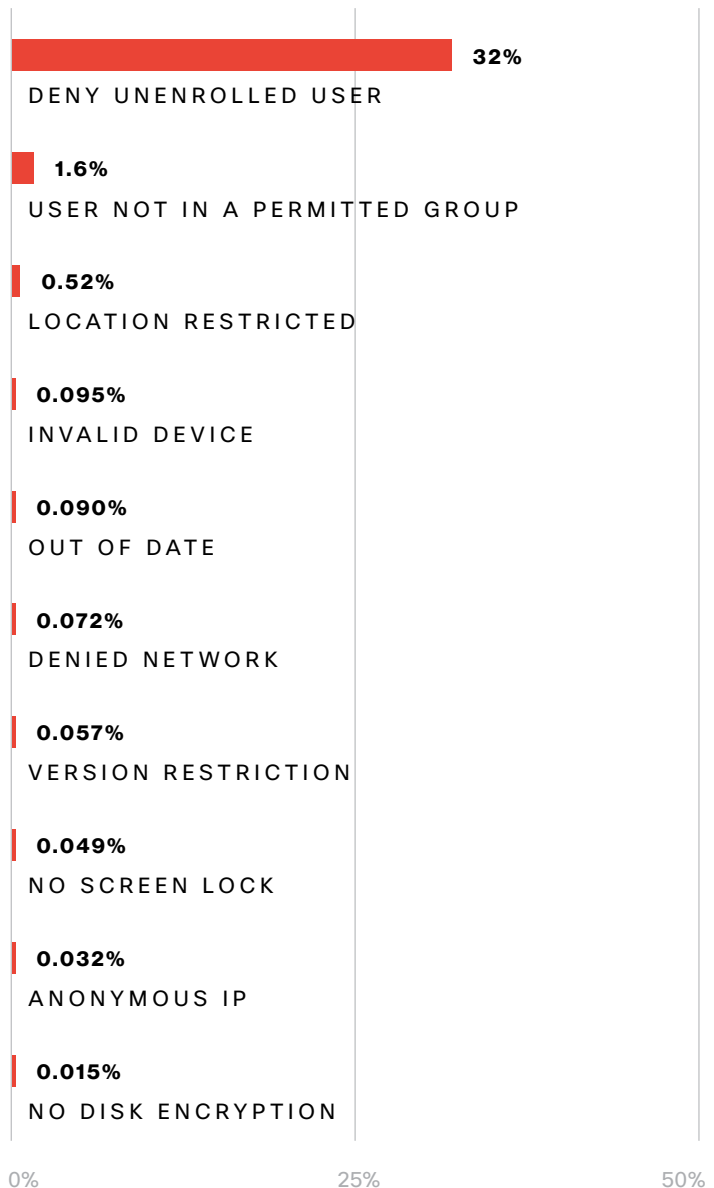
Device-based policies assist organizations by lowering the overall risk posture of corporate assets that could potentially lead to system and data compromise. The defenders of a digital enterprise must be able to apply security policies that cover every device managed within the domain. Even if a device is unmanaged, but granted access to the network, there needs to be an ability to control access based on the security posture of the device in question.

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.

It was noted that 5.5% of all authentications failed. When we further examined the data, we discovered that 32% of the failed authentications were due to the users not being enrolled in the system. By comparison, only 1.2% of failed attempts were due to the user attempting to connect from a restricted network or location. Perhaps more interesting is which policies have an outsized effect on authentication failures.

FIGURE 13: PERCENTAGE OF FAILURES DUE TO SPECIFIC POLICIES



Here we see that even though a little less than 1% of organizations have a policy concerning location, they account for a large (relative) proportion of failures.

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.

FIGURE 14: ACCOUNTS WITH POLICIES AND THEIR AUTHENTICATION DENIAL IMPACT

Note that "Unenrolled User" is excluded as an outlier here.

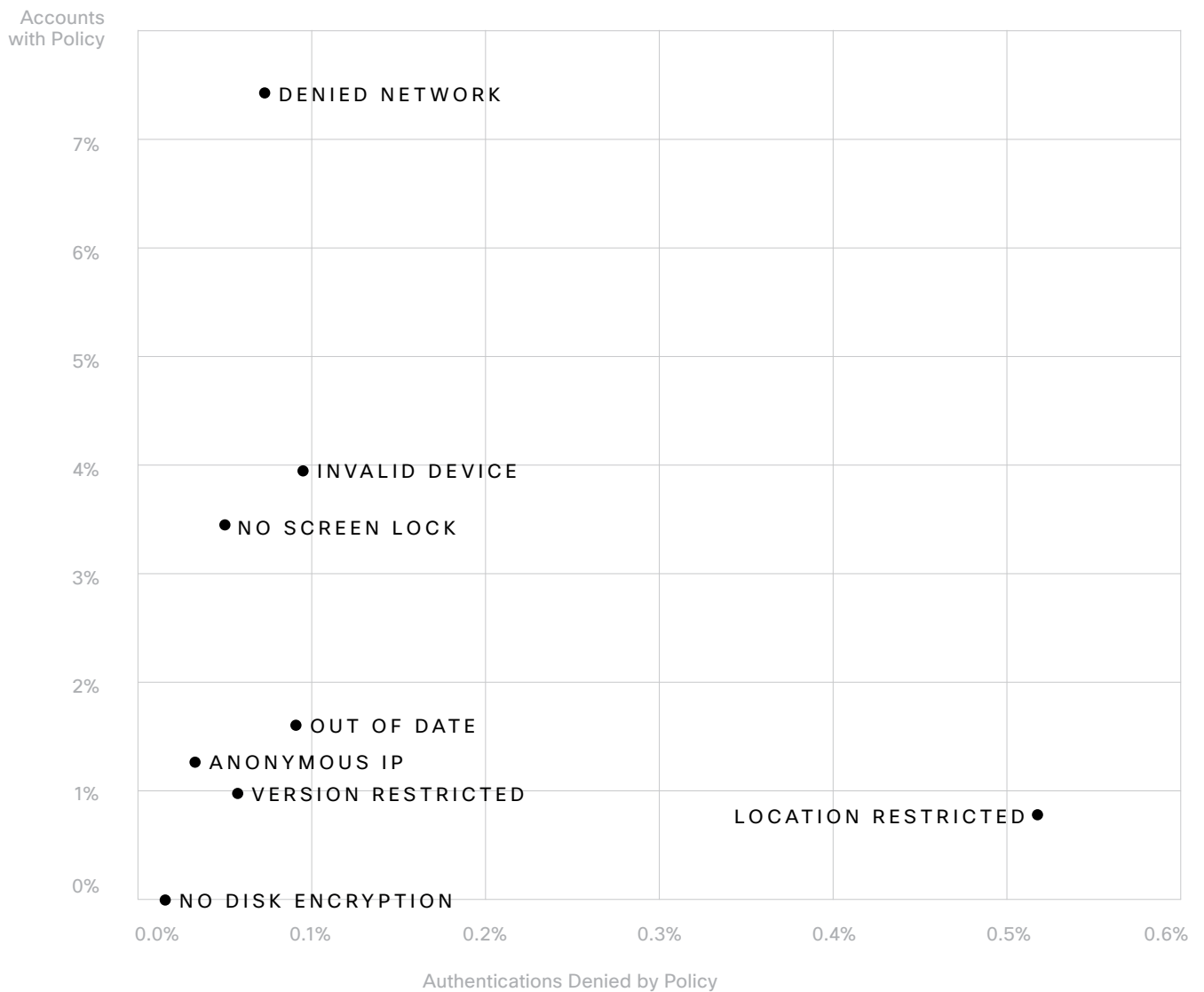
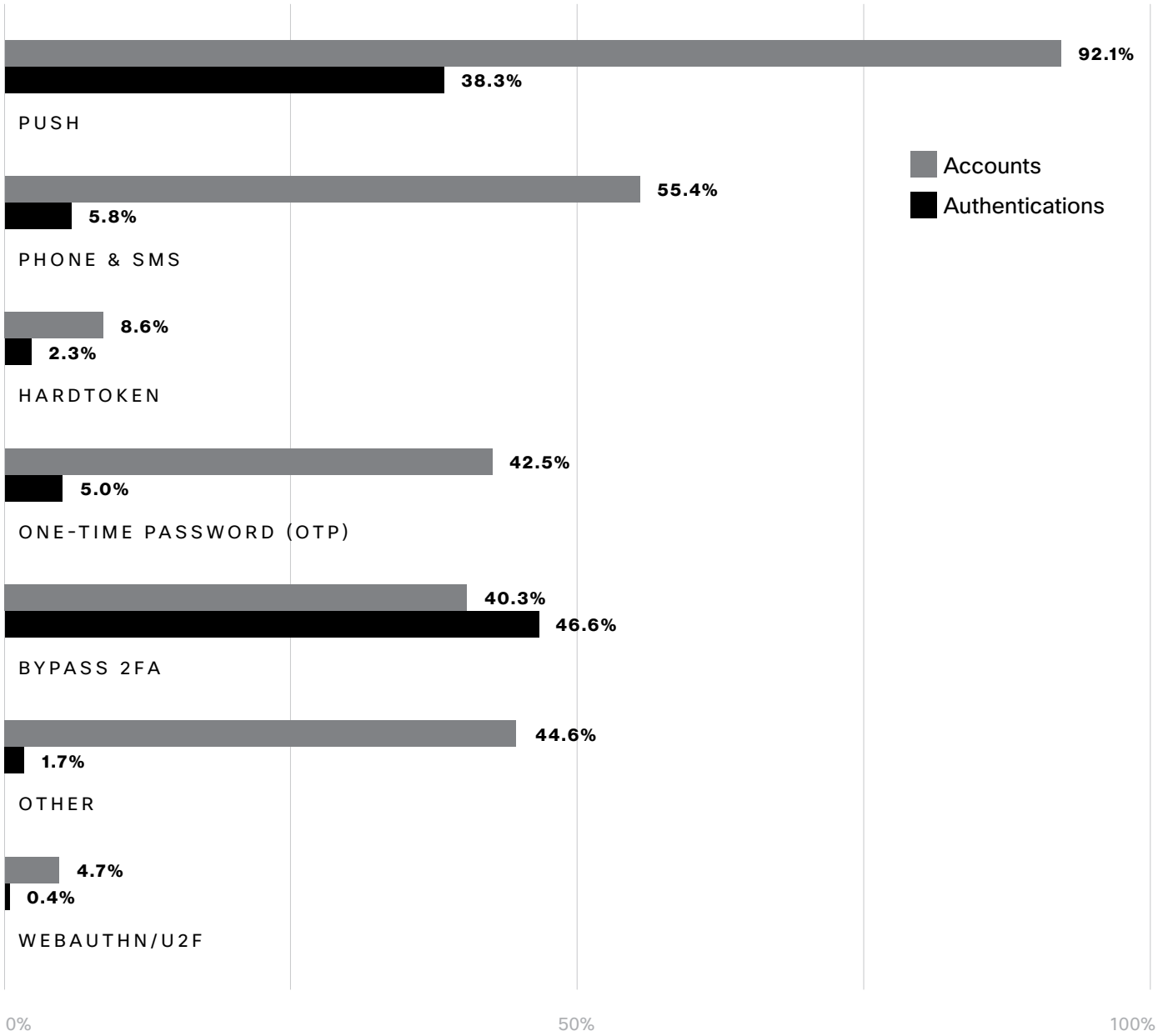


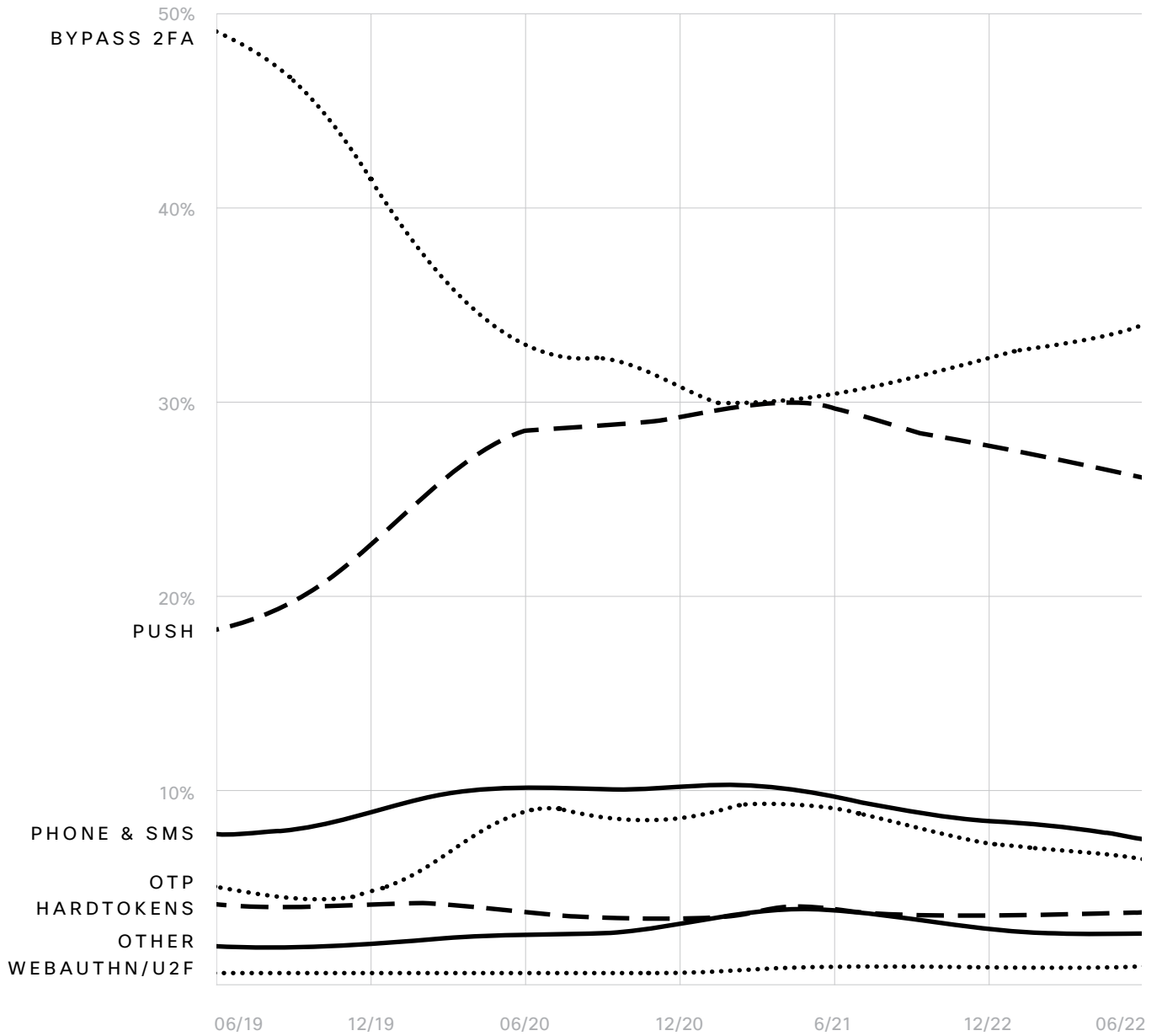
FIGURE 15: FACTOR USE BY ACCOUNTS AND AUTHENTICATIONS



When reviewing the policy data, we uncovered some notable findings. Duo Push-based authentication was used by 92% of all global accounts. This is unsurprising given that this is the main focus of the Duo product, as more than 99% have this factor enabled. Perhaps more interesting is where we see gaps. As we saw above, only 2.2% of

authentications relied on WebAuthn despite it being enabled on nearly 66% of accounts. One-time passcodes are enabled on 98% of policies, but only 55% of accounts availed themselves of this method, accounting for just 6% of authentications.

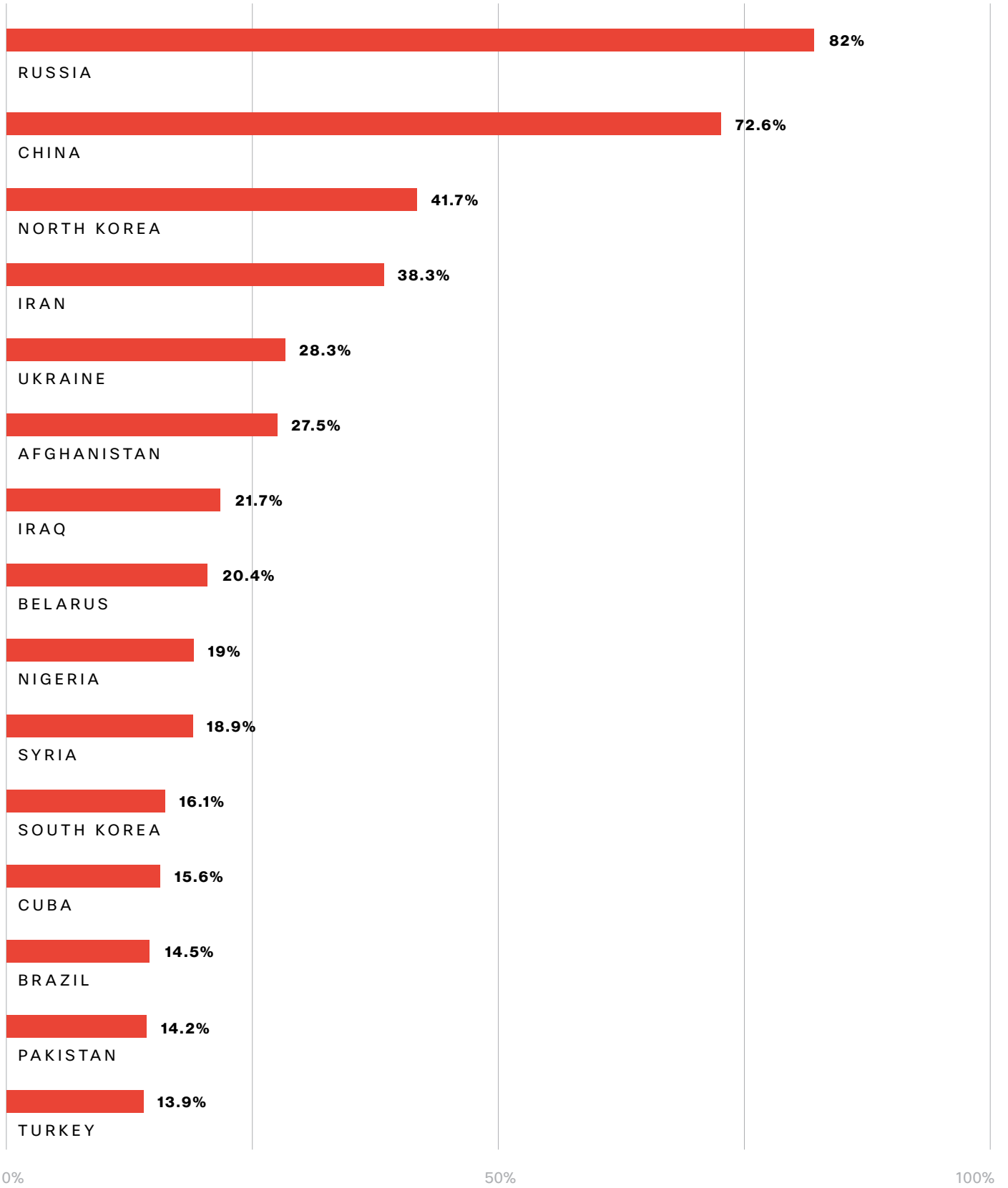
FIGURE 16: AUTHENTICATIONS BY FACTOR OVER TIME



It is also interesting to examine how the use of these factors has evolved over time, and we do just that in Figure 16. What we see is that the steady increase in Push, which one might have assumed was going to overtake fully Bypassing 2FA, with Push remaining

second. For less popular methods the ordering has remained relatively static, though in the last few years, we've seen an increase in OTP usage to become nearly as popular as phone and SMS.

FIGURE 17: PERCENTAGE OF ACCOUNTS DENYING AUTHENTICATIONS FROM A SPECIFIC COUNTRY



Top Restricted Countries

When we reviewed the policies that Duo customers commonly use, disallowing access from restricted locations gives insight in terms of 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. Reviewing our data, we found the following top restricted locations based on policies focused on this aspect.

According to our findings, roughly 91% of organizations that implement location restrictions choose to restrict access from Russia or China (60% block both). It should also be noted that Duo automatically denies authentications from locations on the Office of Foreign Assets Control sanctions list, including from IP addresses that geolocate to Crimea, Belarus, Cuba, Iran, North Korea, Sudan or Syria, as of this writing.

Another question we can ask is, “What percentage of authentications get blocked because they originate in restricted geographic areas, and how does that compare to what’s above?” Figure 18 takes a look at this. We see that China is not only blocked by policy a large percentage of the time, but also it accounts for the most authentication failures due to location.

The United States is an interesting case here. Less than 1% of organizations block authentications from the U.S., yet the high volume of authentications based in the U.S. means this accounts for the second highest number of total authentications failing based on location.

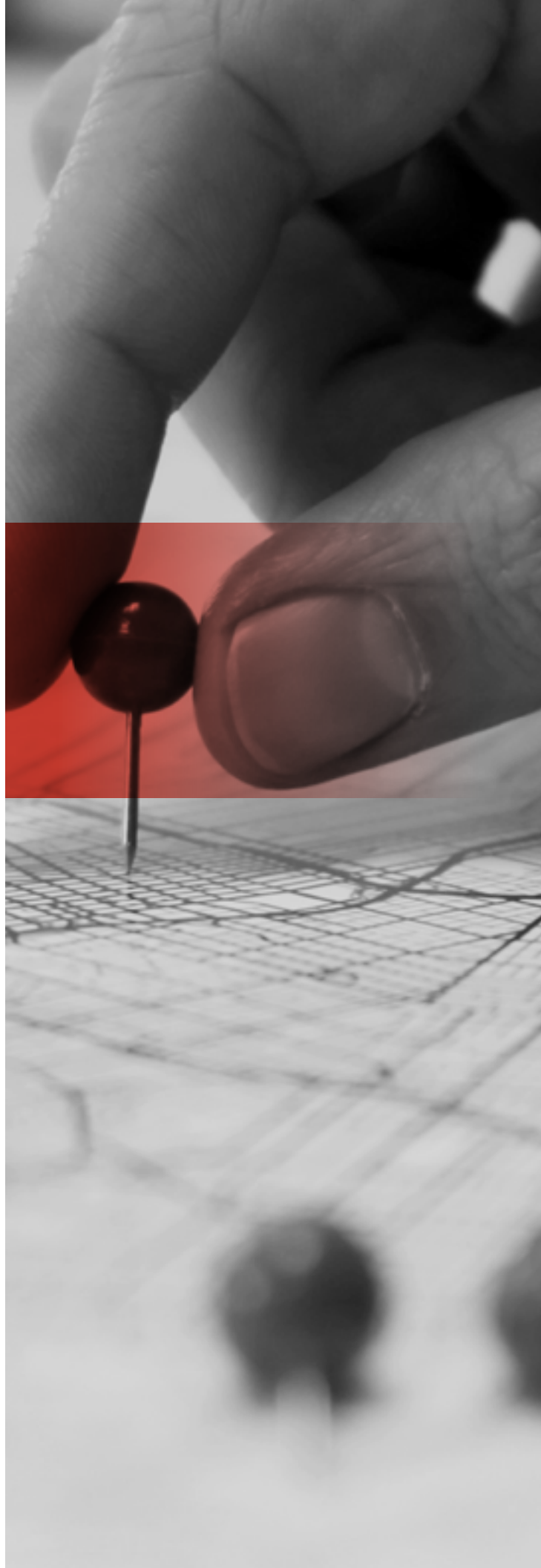
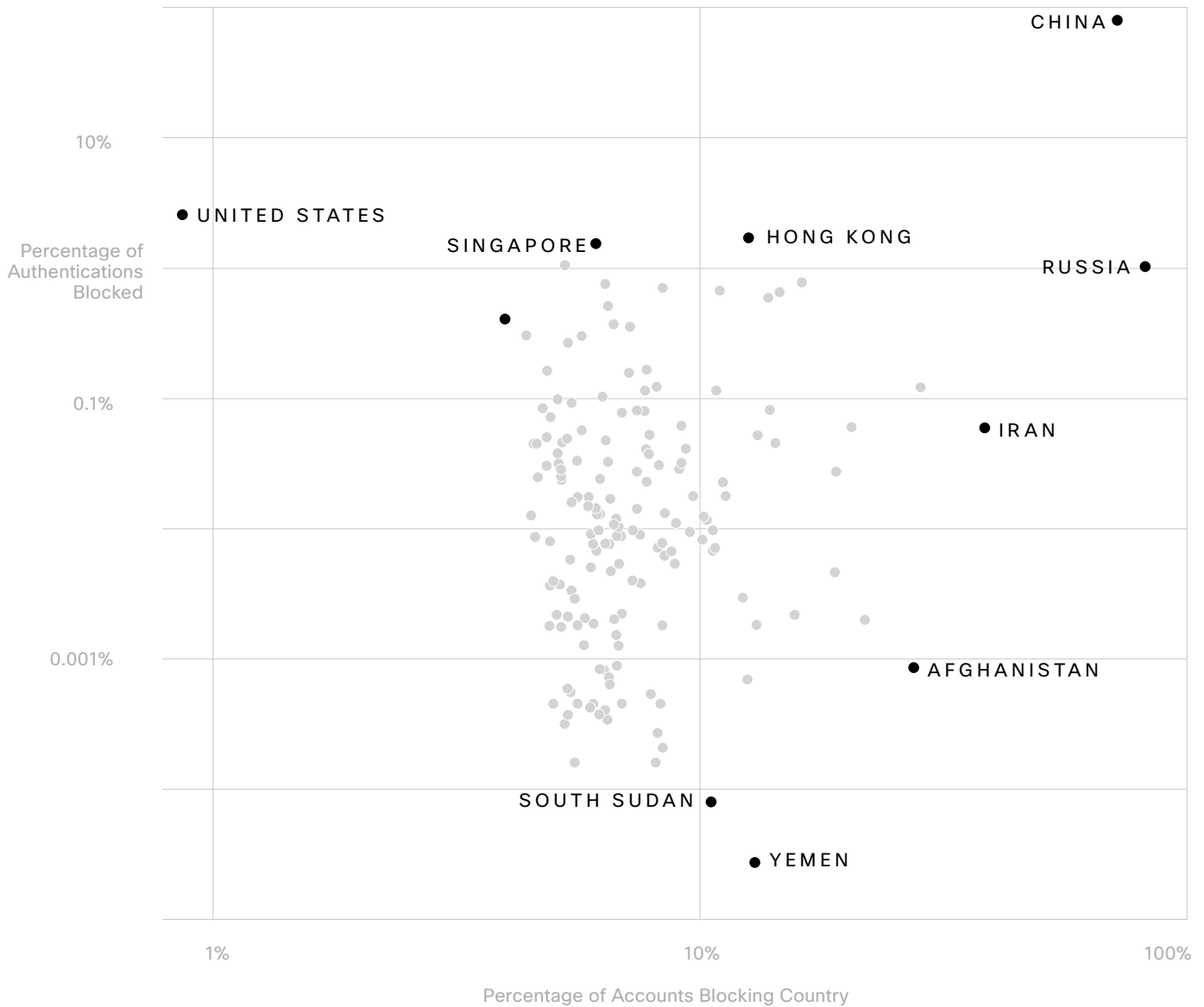


FIGURE 18: ACCOUNTS BLOCKING SPECIFIC COUNTRIES VS THE PERCENTAGE OF AUTHENTICATIONS BLOCKED

Note that the X and Y axes are labeled with log scales. Each point is a country, we have highlighted a few countries on the periphery in particular as

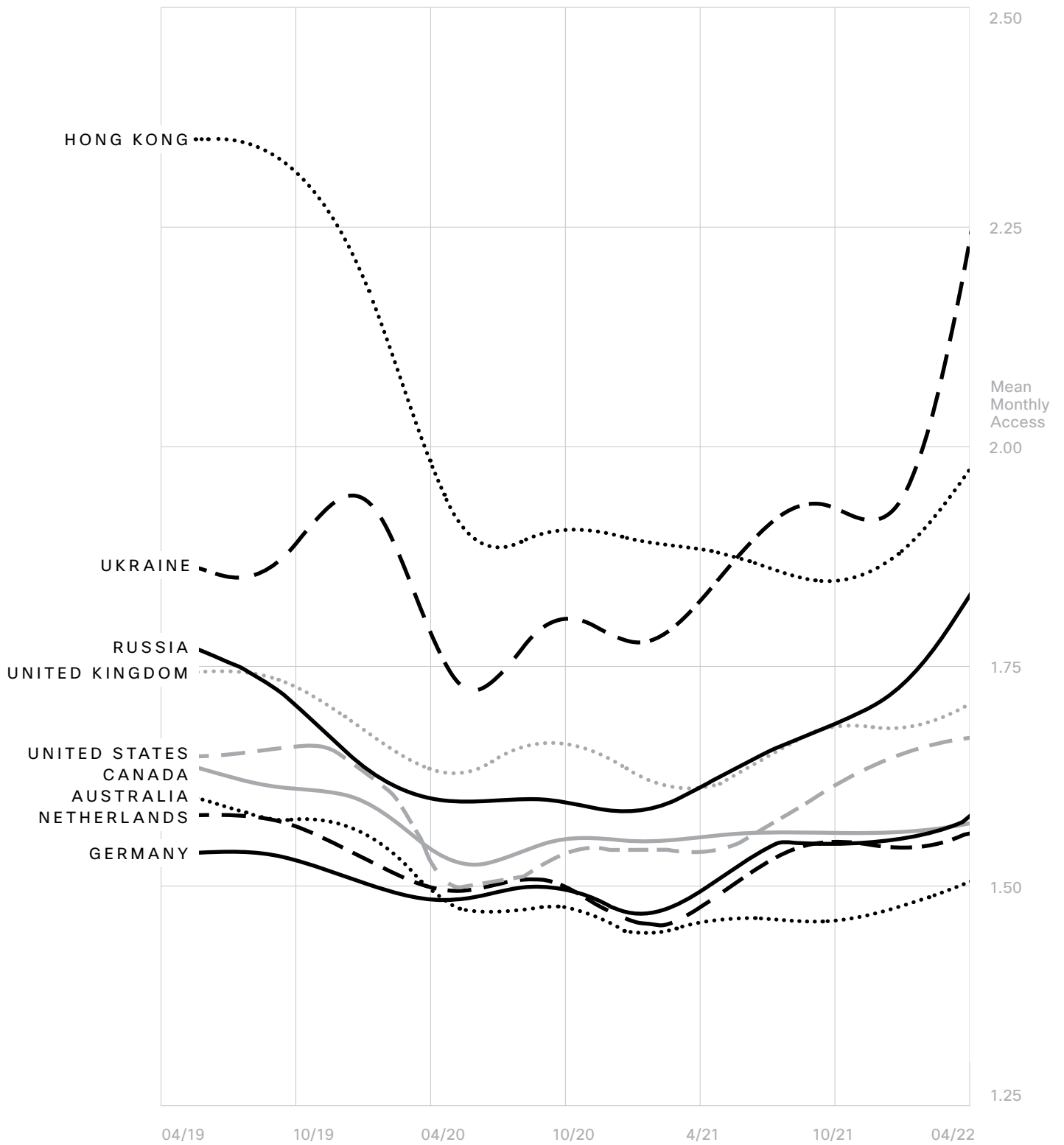
they exhibit interesting behavior, either high rates of blocked authentications or high rates of policies blocking that country.



This raises a slightly more interesting question: Are users attempting to authenticate, perhaps through the use of virtual private networks (VPNs), around some of these policy restrictions? We alluded to this fact way back in Figure 2, noting that organizations in regions that experience politically

significant events, namely Ukraine and Hong Kong, tend to authenticate from a wider variety of different countries than those in more stable regions. We can even see this evolve over time in the figure above, which tracks the average number of countries users are authenticating from over time.

FIGURE 19: CHANGE IN THE NUMBER OF COUNTRIES USERS AUTHENTICATE FROM FROM ORGANIZATIONS IN VARIOUS MARKETS AROUND THE WORLD



Early 2019 to early 2020, around the time of major pro-democracy demonstrations, saw Hong Kong with a high average until the COVID lockdowns

essentially sent everyone home. The Russian invasion of Ukraine in early 2022 has led to a quick spike for both Ukraine and Russia.



Top Policy Enforcement by Industry

Our data also illustrates that different industries implement different policies to enforce device trust. This results in different failure rates among authentications. If we turn our attention to the major industries that always garner attention, Education, Finance, and Information Technology (IT) & Telecommunications, we see some striking differences. In Education and Finance, the biggest reason for a policy failure is “User not permitted in group,” while location restriction is top for Telecommunications. Among these three, Finance accounts for the most blocks due to invalid devices, indicating that these orgs are likely stricter with what they let their users actually use.

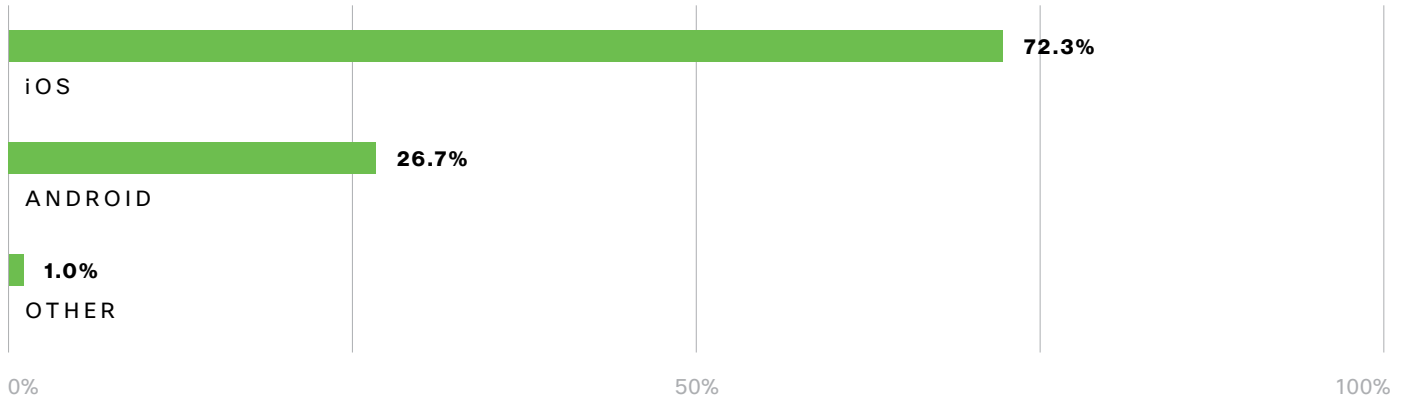
One caveat here is that we aren’t showing all the reasons for failure, in particular the most common reasons tend to be, “Whoops, didn’t mean to do that,” and a failure of a user to be enrolled in the first place. These are common across industries and we want to focus on noticeable differences, not things that are the same.

FIGURE 20: FAILURES DUE TO SPECIFIC POLICIES ACROSS TOP INDUSTRIES

Percentages are % of all authentications.

	EDUCATION	FINANCE	IT & TELECOMS
VERSION RESTRICTED	0.0002%	0.004%	0.009%
USER NOT IN PERMITTED GROUP	0.01%	0.04%	0.02%
OUT OF DATE	0.001%	0.005%	0.01%
NO SCREEN LOCK	0.002%	0.004%	0.003%
NO DISK ENCRYPTION	0.00002%	0.001%	0.003%
LOCATION RESTRICTED	0.003%	0.004%	0.1%
INVALID DEVICE	0.004%	0.01%	0.006%
DENIED NETWORK	0.000009%	0.002%	0.0004%
ANONYMOUS IP	0.001%	0.002%	0.003%

FIGURE 21: PERCENTAGE OF PHONE PLATFORMS



iOS's Distribution

Apple's iOS remains the the clear leader, with just under 72.3% of devices. The foothold that iOS has is rather remarkable. It continues to rule the roost in this category with the nearest contender being Android – and that has a far lower adoption rate at 26.7%. From a policy perspective, this is good news for organizations that are looking to better secure their environments. iOS is built with security as being top-of-mind and with the most recent iteration of the operating system, we see that patching is now enabled by default. Having increased from 67% in last year's report to 72.3%, it shows that within the Duo customer base iOS adoption continues to grow.

Chrome Continues to Dominate

Google Chrome continues to retain control as the top browser of record for businesses. No other browser even comes close to supplanting the leader. Breaking this out by mobile platform, Mobile Safari leads the way, with Chrome Mobile in second place.

FIGURE 22: DESKTOP BROWSERS BY TYPE

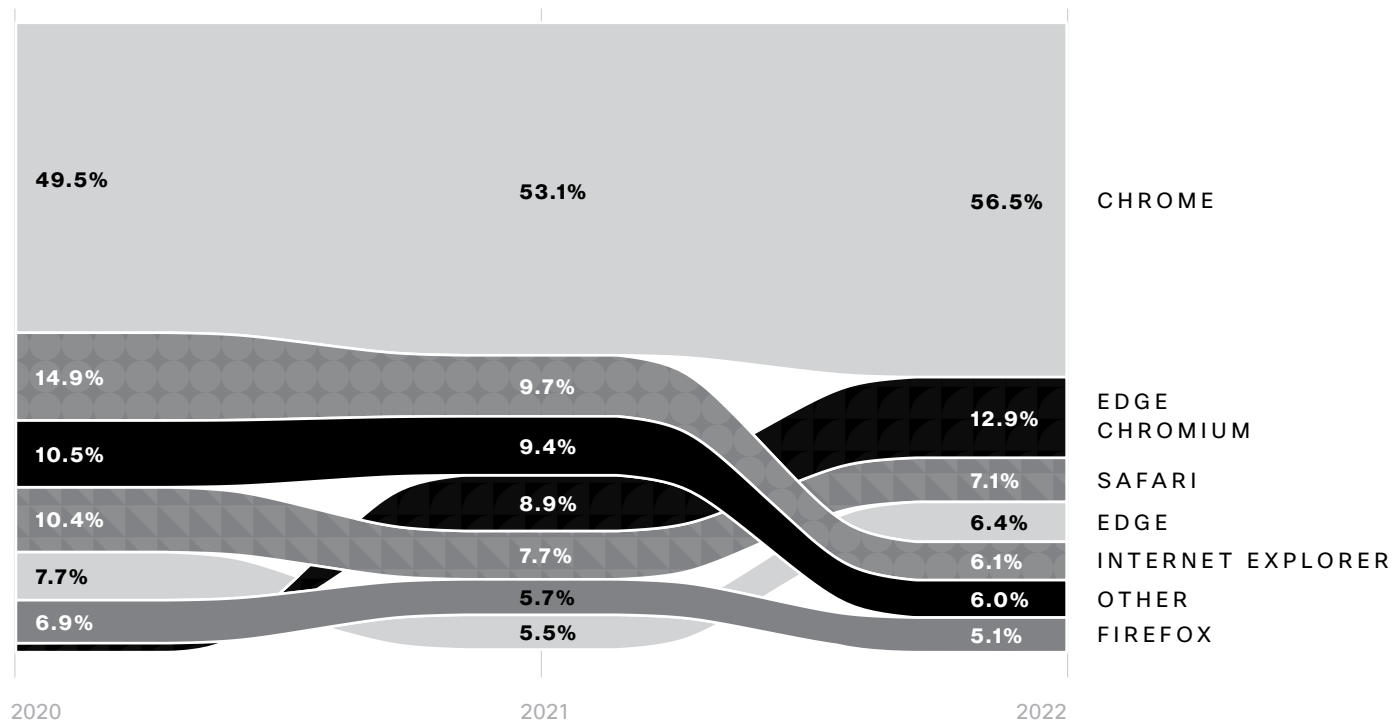
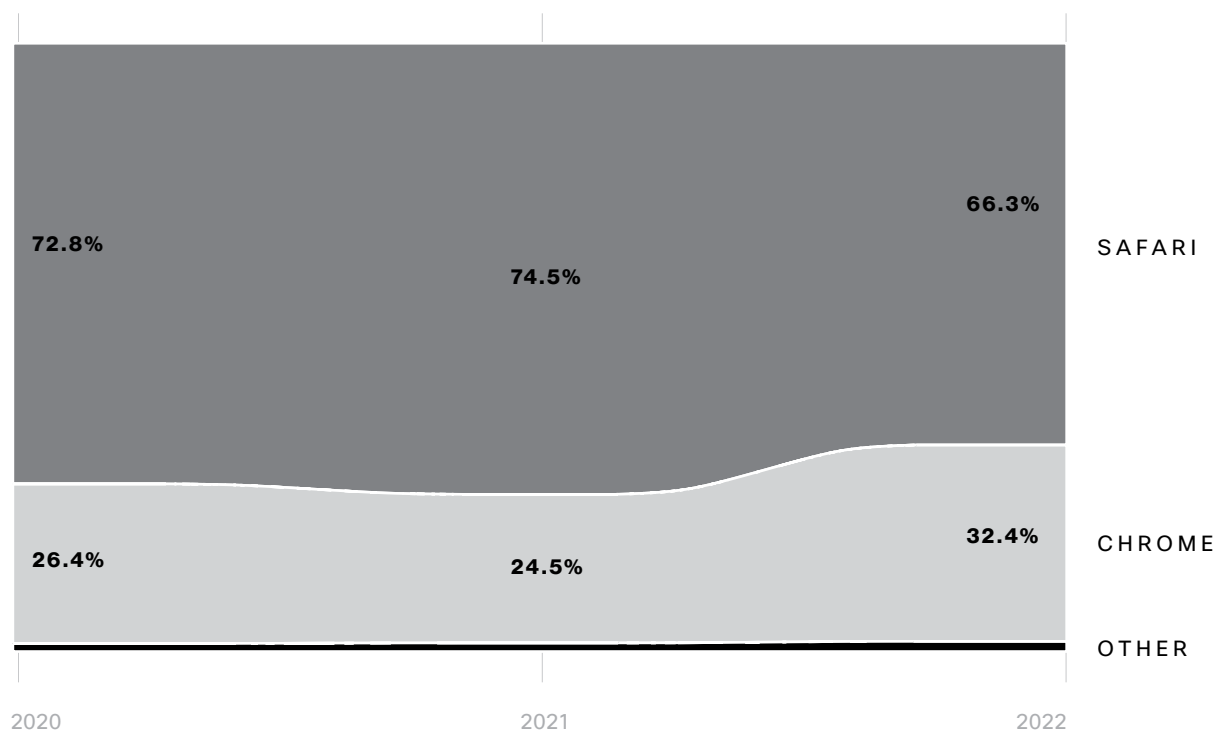


FIGURE 22: MOBILE BROWSERS BY TYPE





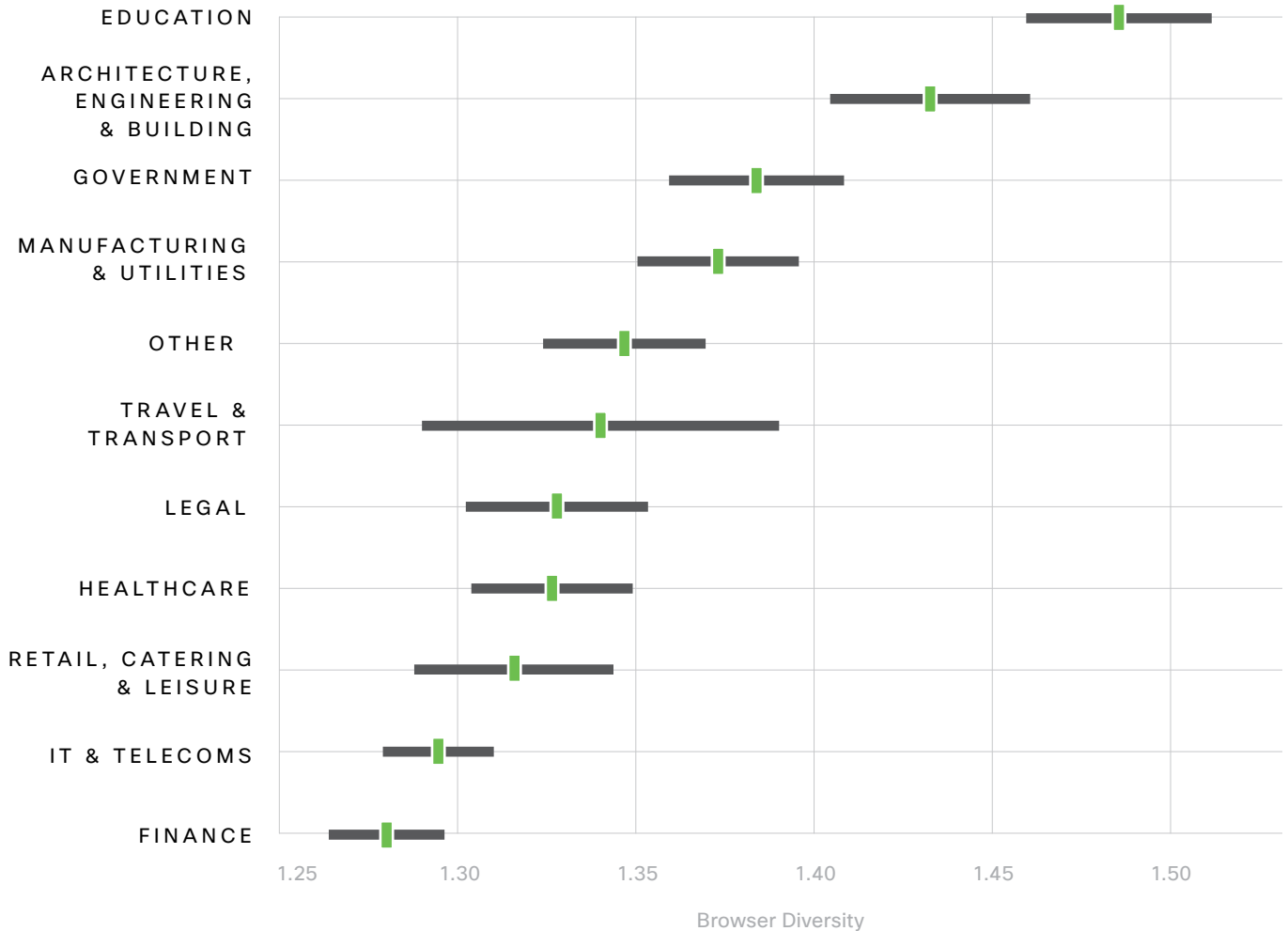
Reviewing the accounts being accessed via MFA, we find an interesting breakout as shown in the graphic below as it pertains to browsers being utilized. In particular, most organizations have a pretty even spread across the “big” mobile browsers, Safari (iOS) and Chrome (Android). It’s likely that some organizations have both and some have the majority in a single OS, with a smattering of the “non-traditional” browsers. However, the Education industry stands out here with a cornucopia of browser types. Forty-five percent of Education organizations have at least one user using mobile Firefox, compared to the next highest being Healthcare. When reviewing the data, we find that 23% of all Education organizations have someone running a mobile version of the Opera browser. In contrast, no other industry vertical has more than 3% of people using that browser.

This is just one more example of how IT and security in Education is much more dynamic than what is typically found in other industry verticals. This dynamism is likely the simple result of how many and how diverse the actual users are at academic institutions. Combine that with the fact that many have a wide geographic presence, and it’s a recipe for seeing the most obscure of devices and software. The chart above discusses only what percentage of organizations see any browsers of a particular type, but does that mean there really is a sort of “diversity” of browsers in Education? Well, read on.

FIGURE 23: PERCENTAGE OF ACCOUNTS WITH MOBILE BROWSER BY INDUSTRY

	SAFARI	CHROME	FIREFOX	EDGE CHROMIUM	OPERA
TRAVEL & TRANSPORTATION	61.4%	53.3%	10.0%	7.2%	1.7%
RETAIL, CATERING & LEISURE	58.4%	50.5%	9.6%	7.6%	2.3%
OTHER	52.2%	41.4%	4.0%	3.0%	0.3%
MANUFACTURING & UTILITIES	58.7%	50.7%	6.9%	6.5%	1.5%
LEGAL	63.7%	44.2%	4.6%	4.1%	0.5%
IT & TELECOMS	47.3%	44.4%	10.8%	7.5%	1.9%
HEALTHCARE	65.4%	58.1%	13.2%	12.0%	2.9%
GOVERNMENT	63.8%	55.3%	10.7%	7.7%	1.8%
FINANCE	56.5%	45.5%	6.0%	5.9%	0.9%
EDUCATION	73.8%	70.0%	44.7%	36.7%	23.0%
ARCHITECTURE, ENGINEERING & BUILDING	65.0%	51.5%	5.6%	6.1%	1.0%

FIGURE 24: BROWSER DIVERSITY BY INDUSTRY



What do we mean by diversity? Though the word may seem unusual in this context, it helps us communicate a particular scientific concept related to our research. From ecology, we are borrowing a calculation called the Shannon Diversity Index. This was developed as a method of understanding just how much species diversity existed in specific ecosystems. It attempts to distill two ways we might think of diversity into a single number: the number of different species and their relative prevalence.

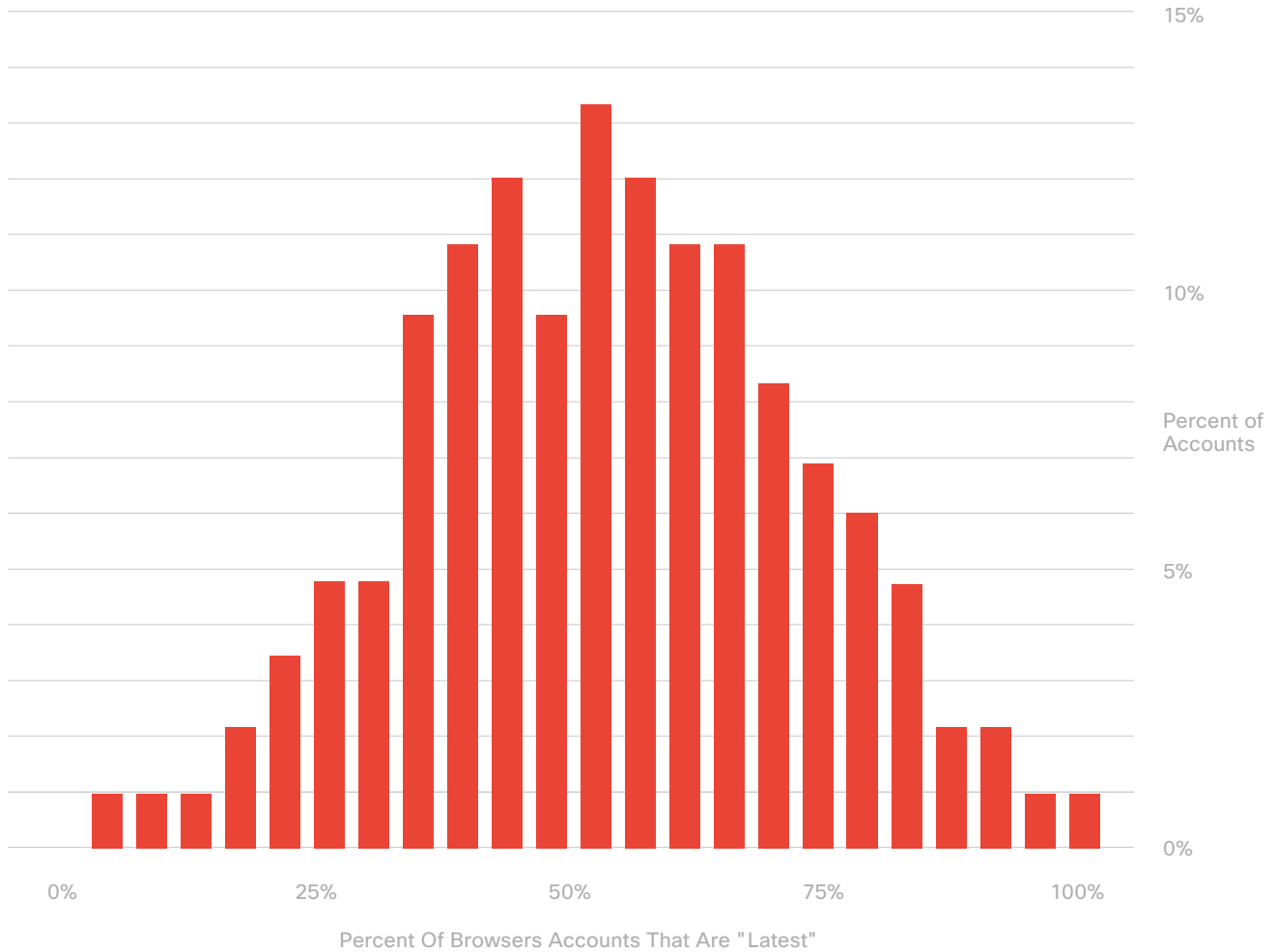
For example, we might consider an ecosystem with 100 types of insects diverse, but if 99.9% of them are mosquitos, maybe not so much. Shannon Diversity Index looks at the percentage of all individuals each species accounts for and calculates the following:

$$\text{Diversity} = -\sum p \log(p)$$

For us, each "species" is a browser and Figure 24 shows this browser diversity.

A notable data point that came up this year is the diversity of web browsers used among academic institutions compared to financial institutions. In particular, we found that there aren't just a few stray, weird browsers used at most educational institutions, but mostly large pockets of different "species" of browsers at most organizations.

FIGURE 25: DISTRIBUTION OF OUT-OF-DATE BROWSERS WITHIN AN ORGANIZATION

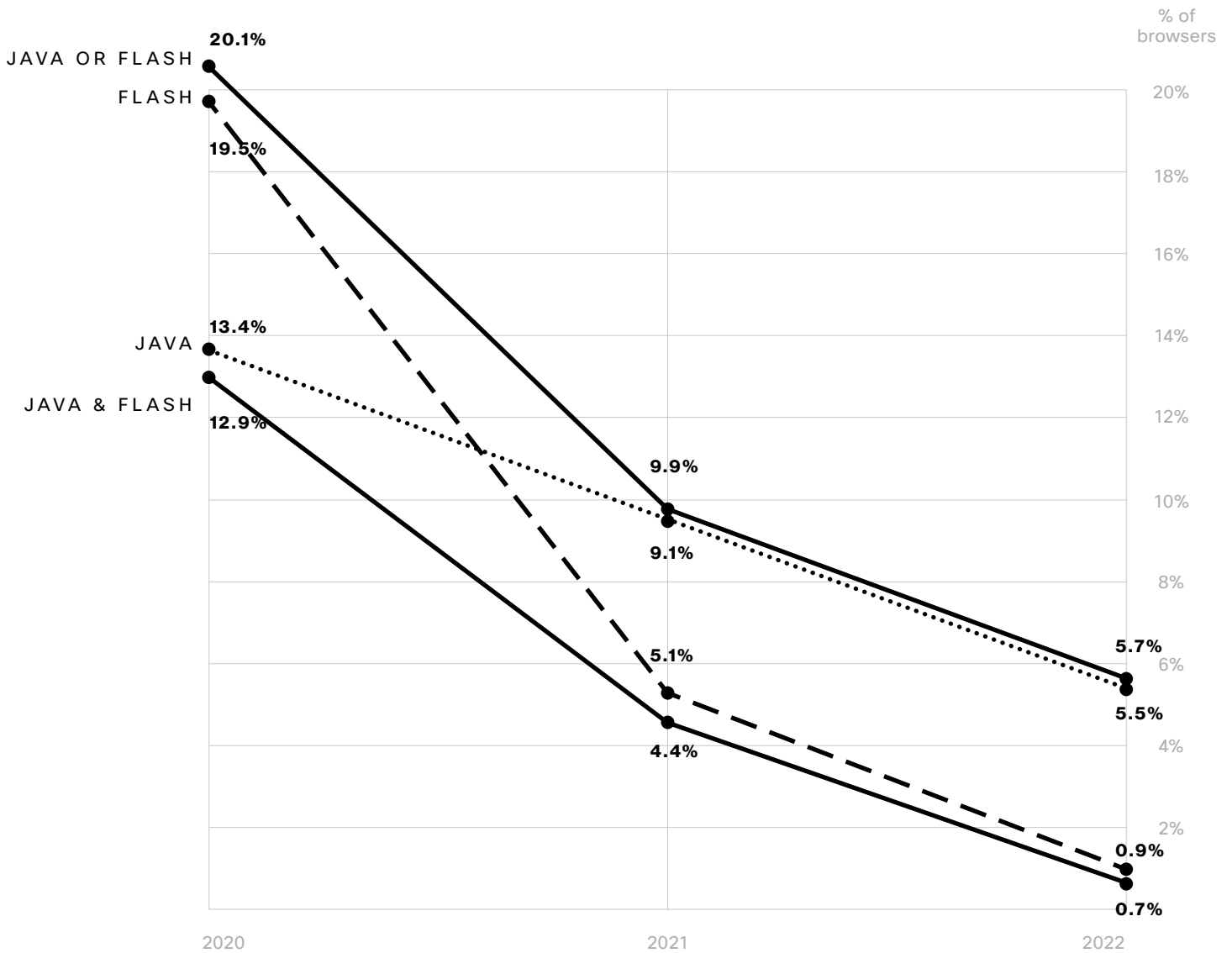


While it's good to see that 42% of all browsers were patched to current, it's troubling that 50.3% of browsers were identified as out of date. Of the remaining 8%, a small (but nonetheless terrifying) 2% are "end of life," and the remaining 6% are "unknown," meaning the version of the browser could not be assessed.

FIGURE 26: FLASH AND JAVA OVER TIME

Note: The lines here for “Flash” and “Java” indicate the percentage of browsers with that software installed, but not necessarily *just* that software

alone. If you're interested in understanding Java, for example, you can subtract the “Java and Flash” number from the “Java” number for a particular year.



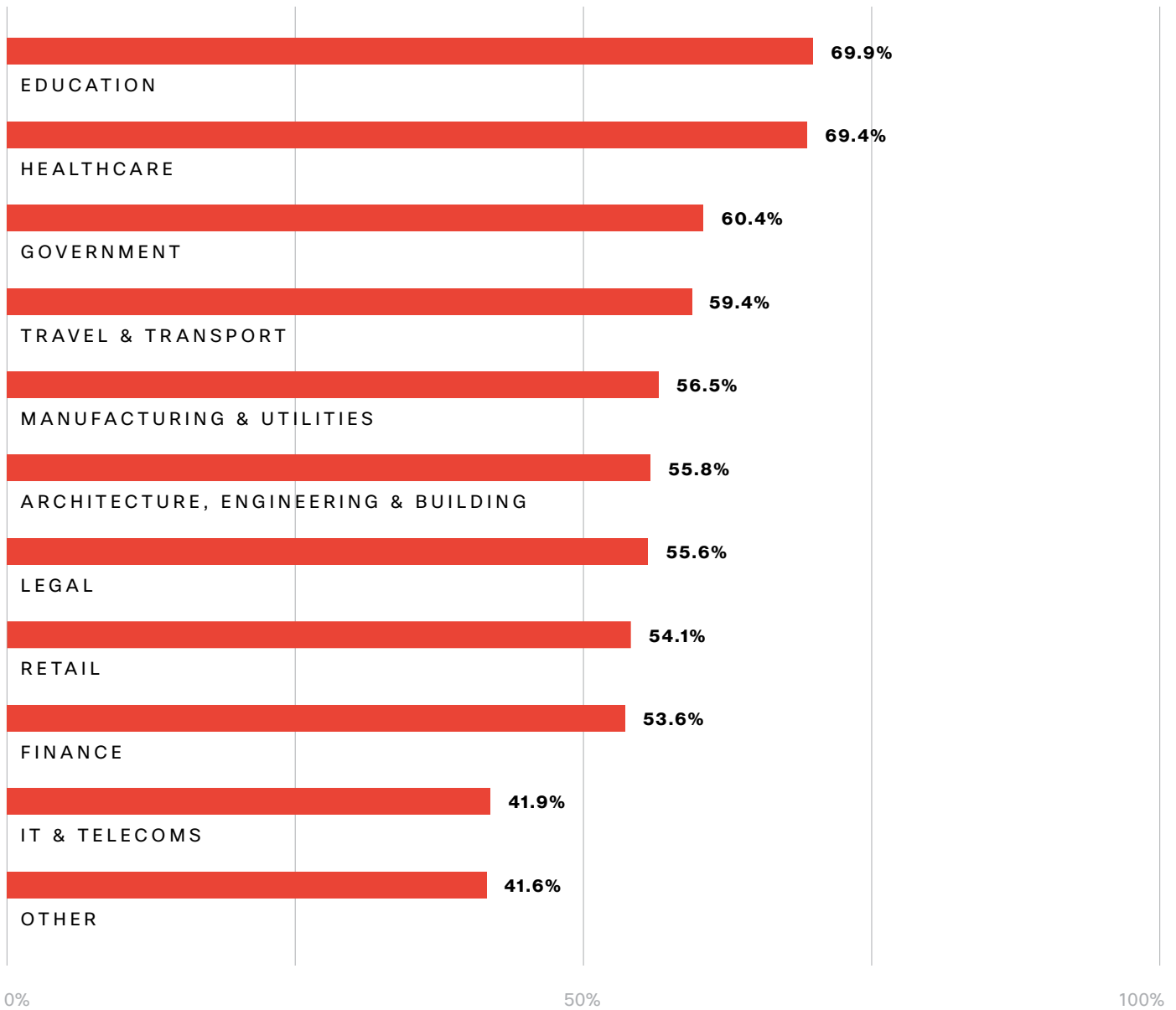
Browsers Improving Security Posture

Each year we review the security posture of web browsers, and last year we noticed a promising piece of information. 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

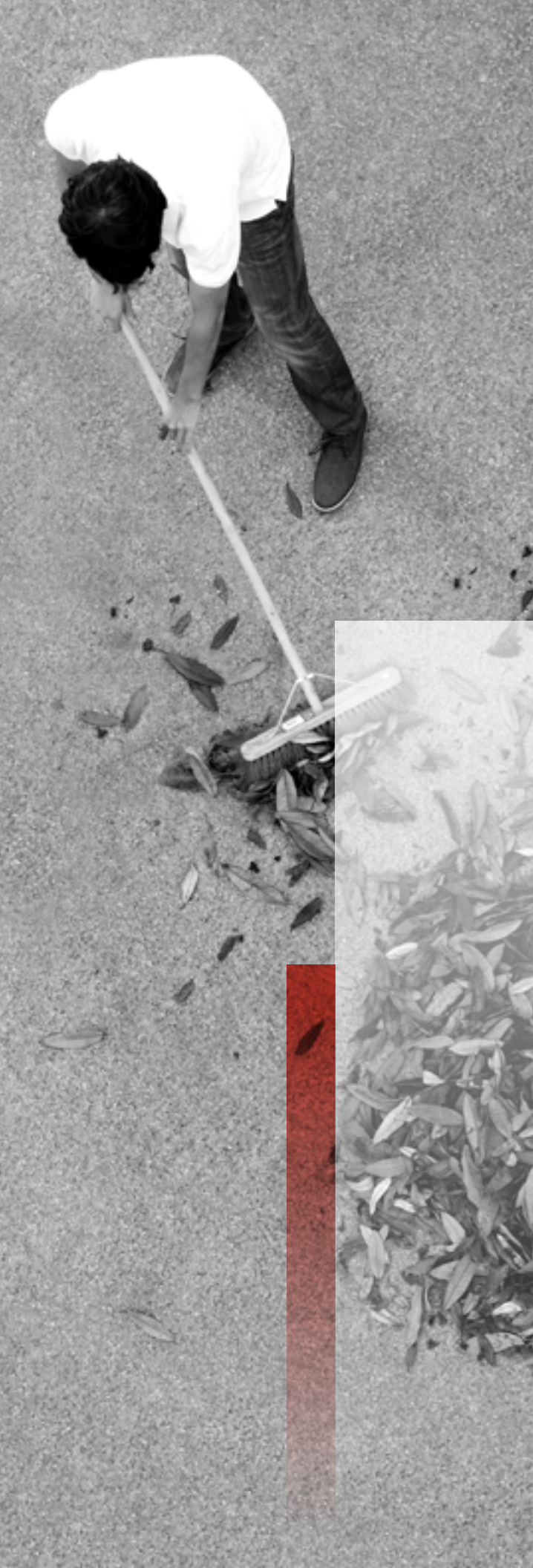
downward in 2021, now with 95% of systems no longer having it installed. In 2022, that number increased to 99.1%. A question remains: Is Java still hanging around?

According to our data, in 2020, 87% of browsers had no Java installed. The following year, that number increased to 91% of systems that don't have Java installed. In 2022, that number grew to 97%.

FIGURE 27: ORGANIZATIONS WITH AT LEAST ONE BROWSER RUNNING JAVA



Now when we look at the progress of removing Flash and Java from systems based on industry verticals, we notice a measurable difference. It would be lovely to say that Flash has finally passed off this mortal coil, but even the roughly 1% of remaining organizations still having it installed amounts to approximately 340,000 systems with some version of it existing – even now.



Cleaning Up the Device Cruff

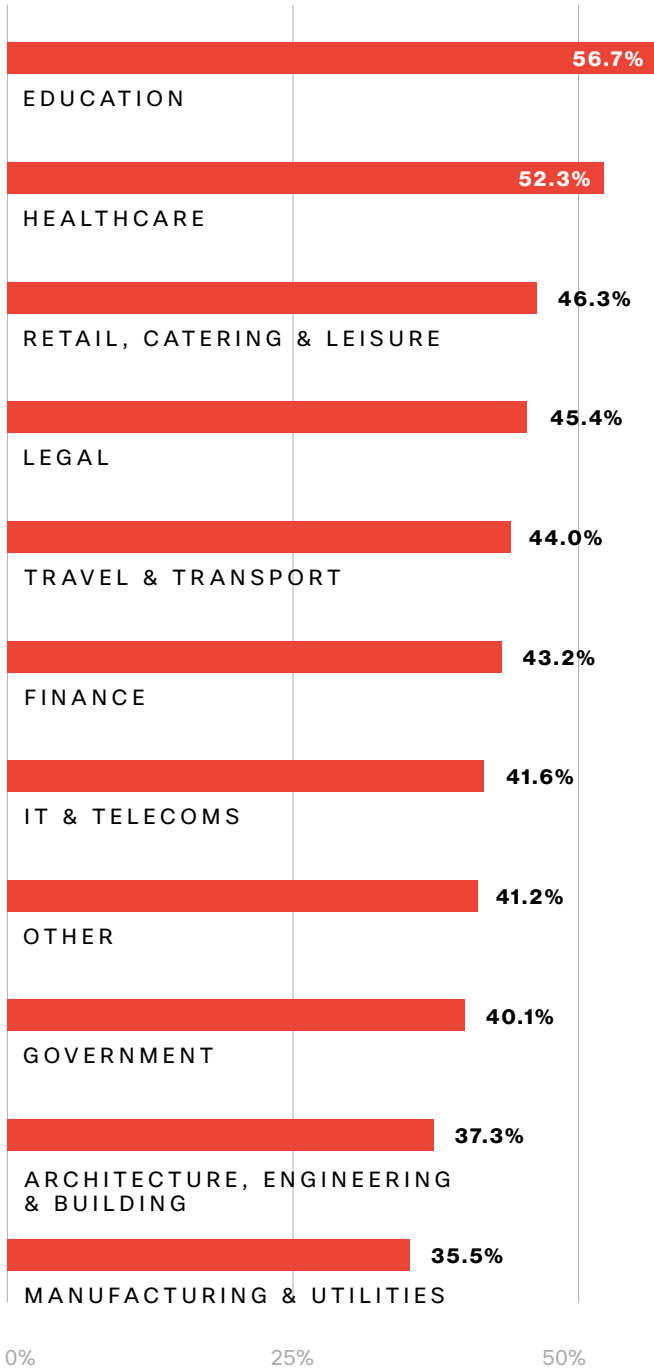
Device hygiene for the enterprise is an ongoing requirement. With the hybrid work environment present in so many organizations, we need to take into account the posture of the devices that employees use to do their jobs. When systems are not patched, current organizations are exposing themselves to potential and avoidable harm.

As an example, your intrepid scribe once worked at a company many years ago where we scanned all the laptops and desktops, searching for vulnerabilities. We discovered that the most secure device at that company was my own laptop, and it only had 267 high risk vulnerabilities. This was a clear danger for my organization when we took into account the vast numbers of staff who traveled for work. The risk for the organization was one that it simply did not have to take.

When we review industry verticals, we find the percentage of endpoints that have been patched and up to date varies widely. For the purpose of this research, we consider a device to be “up to date” if it’s running the latest version of the operating system.

Unsurprisingly, Education tops the list here again. Given the high diversity of browsers and operating systems we see there, it's no wonder they have a tough time keeping everything up to date. Another perennial industry that tends to be below the "Security Poverty Line" is Healthcare. Some surprises exist at the bottom, namely Government, clocking in at only 40% of browsers being out of date. Tight directives and control of endpoints likely keep their percentage down.

FIGURE 28: OUT-OF-DATE BROWSERS BY INDUSTRY



Application

Enterprises understand that it is necessary to have secure access to ensure that users, devices and data are protected. This is essential for any environment today. We have moved away from the historical view of working from home as a luxury to it now being part of the normal business model.

As part of our research, we examined the most common categories of applications Duo customers access. While IT and infrastructure are the most common, narrowly topping VPNs, they come in only third in the percentage of applications.

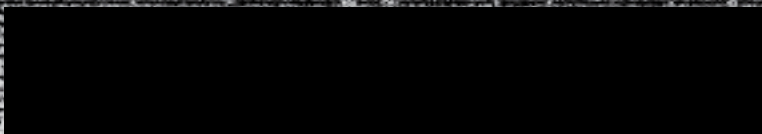
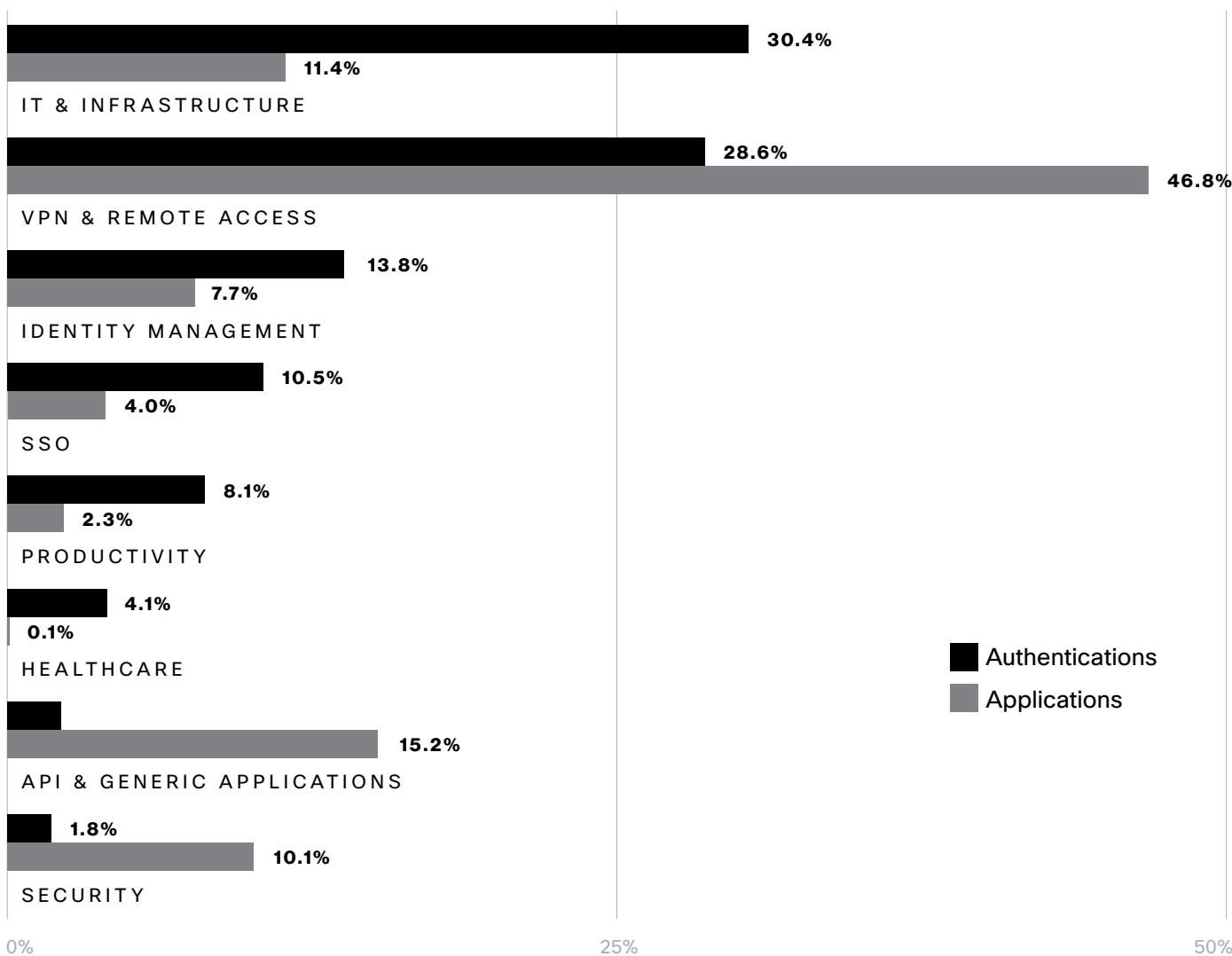


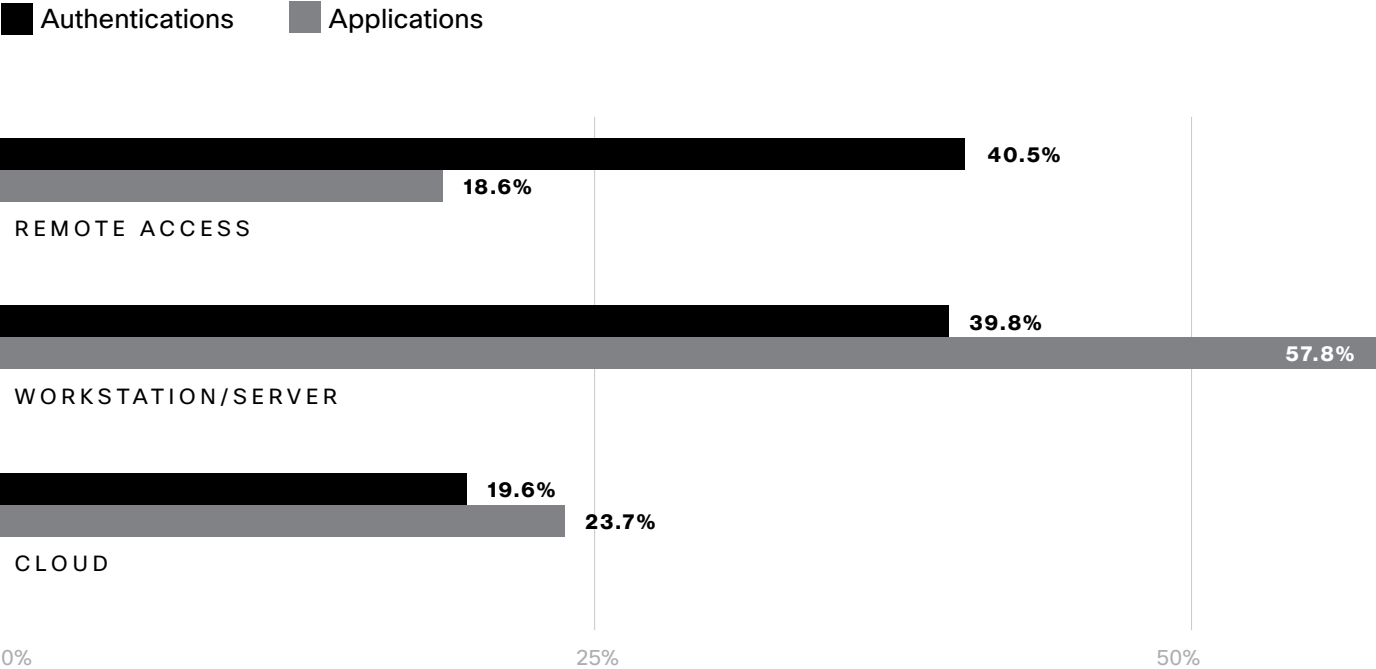
FIGURE 29: TOP APPLICATION CATEGORIES BY AUTHENTICATIONS AND TOTAL APPLICATIONS



We can also look at applications in a different way – not just what the application does, but what it provides access to. While remote access and workstation/server applications are neck and neck in the number of authentications, remote access is third in the percent of applications. This is likely due to the fact that most organizations have a single VPN or some other remote access product while they have multiple productivity applications that need to be authenticated. Most people are going to use that remote access application every day, resulting in many authentications, but for just a handful of applications.

The year-over-year change between 2021 and 2022 indicates that remote access and cloud application use has continued its upward trajectory and will continue to do so for quite some time. Our data captures how the usage of these categories changed relative to overall usage.

FIGURE 30: APPLICATIONS AND AUTHENTICATIONS BY APPLICATION ACCESS TYPE



Application Usage Percent Change

REMOTE ACCESS:

- -18% contraction in the proportion of authentications
- 17.4% expansion in the proportion of applications

WORKSTATION/SERVER:

- -20% contraction in the proportion of applications
- 24% expansion in the proportion of authentications

CLOUD APPS:

- -6.6% contraction in the proportion of authentications
- 23% expansion in the proportion of applications

The expansion in the proportion of applications that are being protected is a hat tip to all of the organizations moving beyond their original MFA deployments to cover more applications than ever before. This, coupled with the use of single sign-on (SSO), helps to improve the overall security posture of the enterprises that implemented these levels of protection.



Summary

The last year – even the last several months – have really rewritten the narrative for defenders around the globe. Organizations have spent considerable time and effort designing their hybrid work functions, and now they must be doubly certain that they have security resilience built into their deployments to contend with the current threat landscape as outlined by the Talos Intelligence team here at Cisco.

Lingering security debt that remains in organizations will continue to provide adversaries with targets of opportunity. Companies need to hone their craft and better focus on access control and dealing with deprecated systems that may continue to operate in their environments long past their life expectancy. Patching has been much maligned by

security practitioners over the years – not because it shouldn't be done, but rather because no one ever wants to do it. As a result, issues crop up with long-published vulnerabilities being made into exploits that realistically should not hold any sway in modern enterprises. Yet, they wait on the wire.

Making use of multi-factor authentication and / or passwordless authentication models are essential for the modern business enterprise. When we consider the tremendous amount of threat intelligence available to us as defenders, from sources such as Talos, we must take advantage of this knowledge and translate it into capability to protect our environments as effectively as possible.



The hybrid work model is now firmly established, and we need to be certain that we have the security resilience necessary to empower our enterprises and enable the democratization of security.

We need to allow people to focus on their job's primary duties with the confidence that they are secure wherever they are working.

Military adversaries today have learned the advantages of utilizing the internet to affect change of their respective fortunes. Cyber warfare is not a tenet of kinetic conflict as once predicted. Rather, much like the advent of the phalanx formation that the Greeks mastered centuries ago, cyber warfare has become an indispensable element of conflict. As defenders, it is our responsibility to ensure that, in the face of these new challenging times, we are able to have a clear strategy to safeguard our people, data and information.

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 in conjunction with passwordless solutions will make great strides to improve overall security, reducing risk by way of democratization of security with a stronger focus on the user experience. Lastly, a sensible approach to policy application and enforcement will accelerate a security team's ability to empower 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. By making use of multi-factor authentication, passwordless technologies such as Webauthn, and utilizing strong security intelligence inputs, we can lower the risk to our enterprises. Our hybrid work model access security is designed to safeguard all users, devices and applications. Everywhere.

References

1. “The 2021 Duo Trusted Access Report: The Road to a Passwordless Future,” Duo Security, October 14, 2021
2. “Cyberwar is Coming!” RAND Corporation, 1993
3. “Attackers Target Ukraine using GoMet Backdoor,” Cisco Talos, July 21, 2022
4. “Cyber Attacks Hit Romanian Government Websites,” BalkanInsight, April 29, 2022
5. Adaptive Authentication Policies for Applications, Duo Security
6. Adobe Flash Player EOL Enterprise Information Page, Adobe, January 13, 2021



The world is continuing to evolve, and we’re seeing a need for companies to provide employees with a way to work securely from basically anywhere in the world.”

Josephina Fernandez, Director of Security Architecture & Research, Cisco

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

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of Cisco Secure’s Zero Trust offering, the most comprehensive approach to securing access for any user, from any device, to any IT application or environment. Duo is a trusted partner to more than 40,000 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. Try it for free at:

duo.com.

Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it’s easy to deploy, manage, and use – and that it all works together. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform. Learn more about how we simplify experiences, accelerate success, and protect futures at:

cisco.com/go/secure.