

 DORT

2023

STATE OF IDENTITY SECURITY

PROTECTING THE WORKFORCE



Table of Contents

Executive Summary	03
Identity Threat Landscape	04
2022 in Review	04
Brute-Forcing	05
Targeting Admins	07
Session Hijacking	08
Multi Factor Authentication: Adoption and Challenges	10
Types of MFA	12
Bypass Techniques	12
Organizations Lacking Strong Factors	14
Factor Enrollment Analysis	15
Identity and Access Management: Poor Hygiene Enabling Attackers	16
State of IAM Security	16
Dormant Accounts	17
Guest Accounts	17
Groups and Permissions	18
Unused Applications	16
User Inconsistencies	20
Summary	21
Recommendations	22
Relevant Compliance Frameworks	23

EXECUTIVE SUMMARY

Attackers no longer need zero days to get access to systems - they simply login. Whether through bypassing MFA, hijacking sessions, or simply brute-forcing passwords, almost every successful attack targets our identities.

These increased attacks are fueled by a massive expansion in identity attack surfaces, which have grown exponentially through the adoption of remote work, the shift to the cloud, and ongoing digital transformation efforts.

Unfortunately, IT and security leaders are largely unaware of the security risks that stem from this identity sprawl. This research paper analyzes the attackers targeting identities and current trends in identity posture. Through a comprehensive analysis of the latest research and real-world case studies, we aim to shed light on the challenges organizations face in securing their IAM systems and provide insights into best practices for mitigating these risks.

Some of our key findings include:

- **Enterprises lack strong MFA adoption.** The average company has **40.26%** of accounts with either no MFA or weak MFA. In contrast, phishing-resistant second factors account for only **1.82%** of all logins.
- **Dormant accounts are in the crosshairs but remain a security blind spot.** Dormant accounts represent **24.15%** of the average company's total accounts and are regularly targeted.
- **Attackers target administrators.** Admins are **three times** more likely to face account probing than regular users, owing to their elevated permissions. In some instances, these accounts were lacking—or excluded from—MFA controls.

Report Methodology

This report analyzed user data, login information, and information from identity providers including Okta, Azure Active Directory, Duo, and Auth0. In total, the analysis covers more than 500,000 identities from organizations with 1,000+ employees. The paper relies on a variety of threat detection rules, which have been created by the Oort Data Science team.

Organization Geography: North America

Sample Size: 500,000 identities

Date Range: 1 June 2022 to 31 December 2022

Sample Sources: Okta, Azure AD, Workday, Duo, Auth0, Slack, and Google.

40.26%

Of accounts have no strong forms of MFA

3X

Admins are three times more likely to encounter account probing than regular users.

24.15%

Of accounts are inactive, for the average company

Section 1

Identity Threat Landscape



2022 in Review

In 2022, several high-profile incidents thrust identity security into the spotlight. The most high-profile attacks were carried out by Lapsus\$ attackers and through campaigns like Oktapus.

According to research by the Identity Defined Security Alliance, 79% of organizations have had an identity-related breach in the last two years. In light of this, organizations are seeking new ways to detect and respond to identity threats.

To understand the most common identity threats, the following sections will focus on three types of threat activity that we saw most in 2022:

- Brute forcing
- Targeting of Admins
- Session hijacking

- JANUARY 2022.** Crypto.com loses \$30M after hackers managed to circumvent its two-factor authentication (2FA) protocols to carry out the attack
- January 2022.** Okta was breached by hacking group Lapsus\$, after the attackers targeted a customer support agent working for a third party. Via this identity, the attackers were able to access both internal company sites and customer service records
- JULY 2022.** Office365 users targeted across 10,000 organizations with session-hijacking
- August 2022.** Oktapus attackers targeted Twilio in order to access one-time passwords (OTPs) delivered over SMS
- August 2022.** APT29 launches brute-force password attacks on dormant accounts to enroll any compromised account in MFA with a device the group controls
- September 2022.** Games company Rockstar was breached caused by social engineering, with the hacker gaining access to an employee's Slack account
- September 2022.** 2K Games confirms a data breach after the hacker managed to get hold of system credentials belonging to a vendor they use to run their help desk platform
- November 2022.** GitHub repositories belonging to Dropbox copied after credentials were unwittingly handed over to the threat actor via a fake CircleCI login page
- November 2022.** Medibank breach announced, resulting from compromised login credentials
- DECEMBER 2022.** Okta's source code stolen after GitHub repositories hacked

\$4.5M

Average cost of a breach caused by stolen or compromised credentials

IBM's "Cost of a Data Breach Report 2022"

79%

Of companies have had an identity-related breach within the past two years.

ISDA "Identity Security: A Work in Progress"

82%

Of breaches involved the "human element" - stolen, credentials, phishing, or errors

Verizon DBIR 2022

Identity Threat Landscape

Brute-Forcing (T110)

Brute-forcing is a prevalent type of attack with several flavors, including password spraying and credential stuffing. In credential stuffing attacks, the hacker has access to a set of valid credentials which they use to attempt to log into additional accounts. In password-spraying attacks, the hacker does not have access to known credentials. Instead, they try to log into a user account with commonly used passwords.

While the technique may sound basic, some of the targets are not. In 2022, Oort observed attackers going beyond indiscriminate targets – going after key accounts: dormant accounts, executive accounts, and administrator accounts.

There are also additional compliance considerations. The Sarbanes-Oxley Act (SOX) requires organizations to monitor and audit successful and failed login activity, account and user activity, and information access.

Targeting Dormant Accounts

In August 2022, APT29 launched brute-force password attacks on dormant accounts. According to [Mandiant](#), APT29 conducted a password-guessing attack against a list of mailboxes and successfully guessed the password to an account that had been set up but never used. The group knew that these inactive, dormant accounts did not have the same scrutiny as others. Furthermore, they could enroll any compromised account with their own MFA.

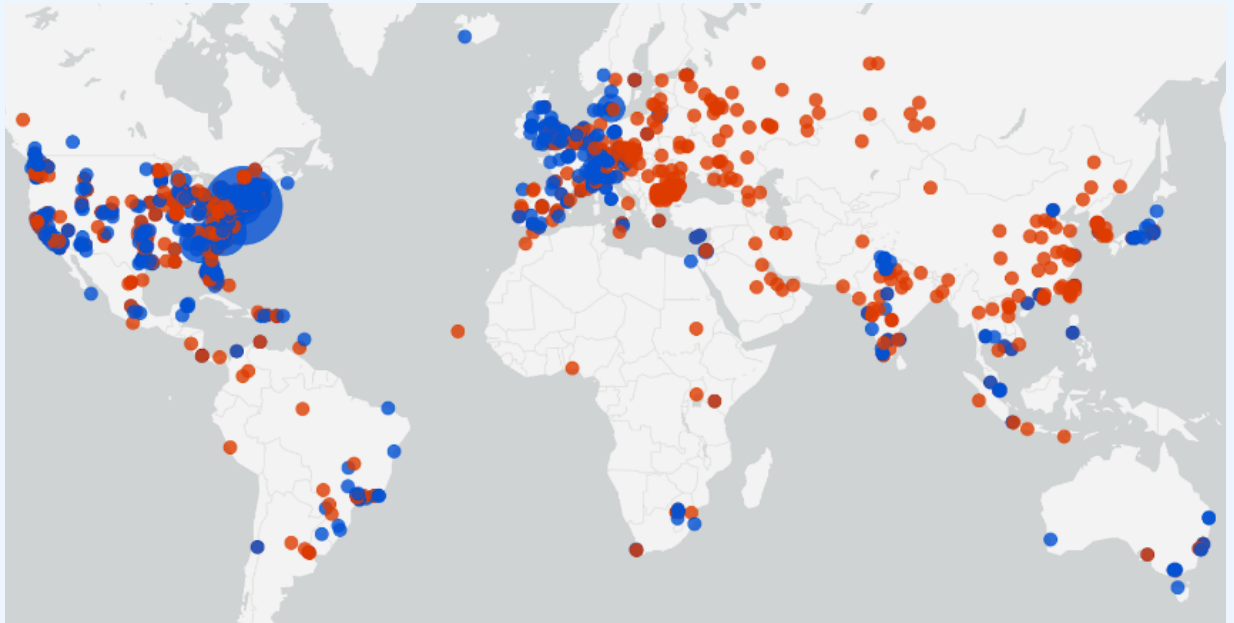
The targeting of dormant accounts was reflected in our analysis. Between November and December 2022, Oort detected an average of 501 attempts against inactive accounts per organization. Worse still, every day, we see a number of these accounts come back alive. We call these "zombie" accounts.

501 On average, organizations face 501 attacks against dormant accounts every month.

Targeting Executives

Another key target for attackers is executives, who often have access to some of the most sensitive applications and data. Executives are given more leeway and flexibility when it comes to security controls. For example, it's common for us to see executives bypassing MFA controls on the weekends.

Organizations should enforce MFA on executives, even if some of those members do not like the friction.



Failed and successful logins by executives in H2 2022

Identity Threat Landscape

Targeting of Administrators

Administrators are an appealing target for attackers. An attacker who has acquired domain admin rights essentially has the keys to the kingdom and can make changes that can help the attacker move laterally or maintain persistence.

Given the appeal to attackers, there are a number of actors that sell access to domain admin accounts. These actors, known as 'Initial Access Brokers', sell access to company domain admin accounts for an average price of \$8,187.

Selling Network Full Access (Domain Admin)
3lv4n · Jul 15, 2020

Jul 15, 2020

Electric Power Company - Amman - Employees: 8,150 Revenue: \$719 Million (Domain Admin + NTDS + Full internal network info) Price: 3200\$

Hospitals - Saudi Arabia - Employees: 7,400 Revenue: \$1 Billion (Domain Admin + NTDS + Full internal network info) Price: 3500\$

Insurance - Thailand - Employees: 520 Revenue: \$131 Million (Domain Admin + NTDS + Full internal network info) Price: 1000\$

Insurance - Saudi Arabic - Full Network Access (Domain Admin + NTDS + Full internal network info) Price: 3000\$

Government - Kuwait - Full Network Access (Domain Admin + NTDS + Full internal network info) Price: 3000\$

CyberPunk Hacker
Premium

Joined: Jul 15, 2020
Messages: 31
Reaction score: 12
Deposit: 0 \$

Initial Access Broker Listing. Source: <https://www.techrepublic.com/>

We often see failed logins from accounts with administrative privileges at a much higher rate than regular users. Admins have three times (300%) higher chances for probing than regular employees. Many of these administrators have weaknesses, too. We observed numerous administrators with no MFA, weak MFA, and sitting in MFA exclusion groups. Subsequent sections will explore these MFA and IAM hygiene trends in more detail.

3X

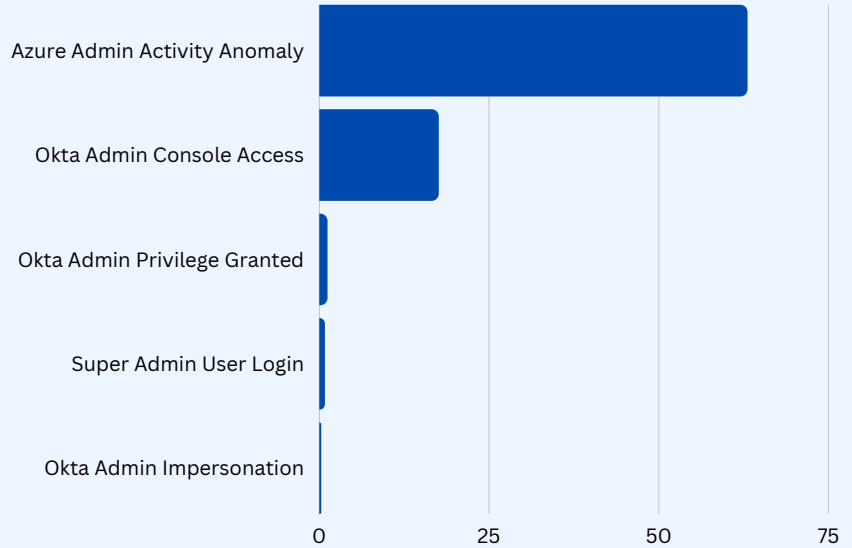
Admins are 3 times as likely to experience probing than regular employees

Monitoring Suspicious Administrator Behavior

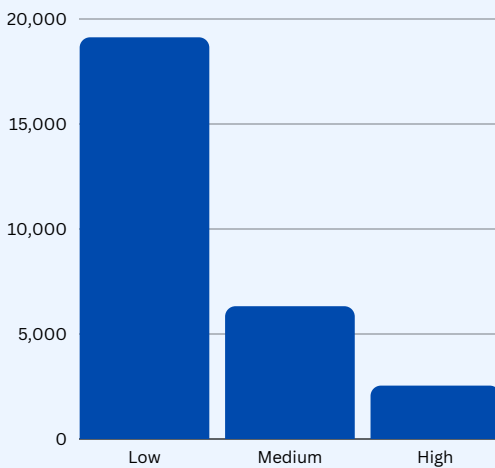
Once an attacker has gained access to an admin account, it's extremely difficult to monitor their activities.

For example, Oort recently detected one user that logged in from an entirely new location and started making administrative changes.

On the right hand side chart, you can see some of the most common high-risk actions that security teams should monitor for. When combined with other indications of risk, such as a new device or IP, these can indicate a malicious actor.



Admin risks associated with the average company per month



Severity levels of Microsoft Risk Attributes

Risk Indicators from Microsoft

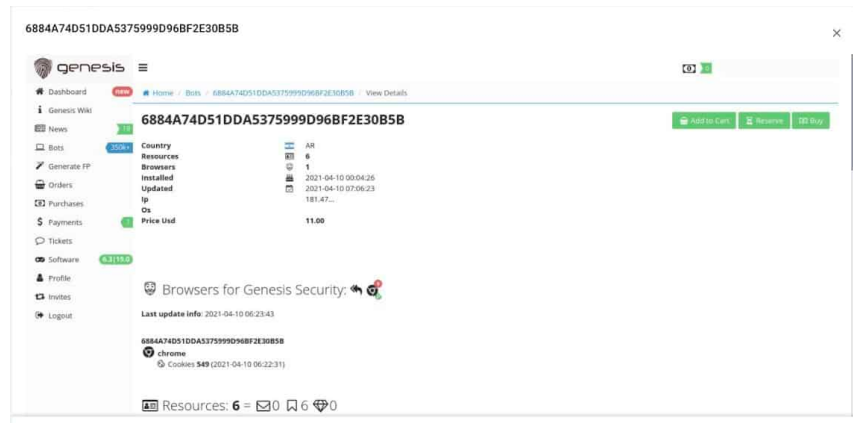
For organizations that subscribe to Microsoft's Identity Protection (Azure AD Premium P2), it's possible to get potential indications of risk. This includes suspicious admin behavior.

Unfortunately, the high false positive rate often results in them being ignored by security teams. As shown in the graph, the majority (68.2%) of Microsoft risk events are low-risk.

Identity Threat Landscape

Session Hijacking

Session hijacking is an attack where an attacker takes over an active session between a user and a website or application. The attacker can then use the session to access the user's sensitive information or perform unauthorized actions. Crucially, this is a way for attackers to bypass MFA.



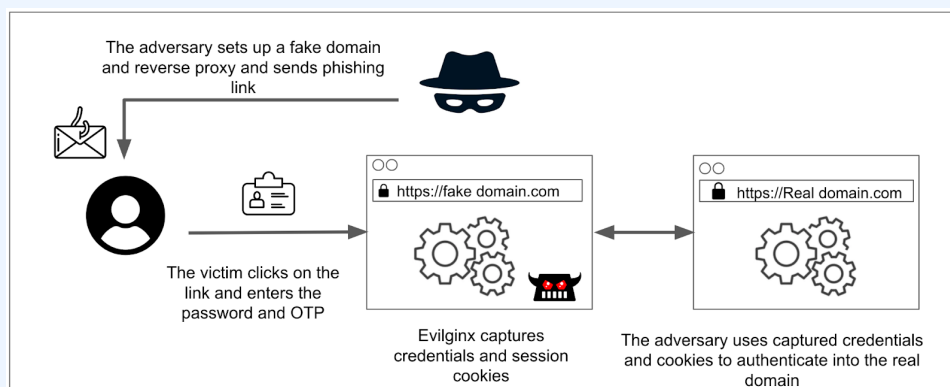
Genesis Market Listing. Source: Digital Shadows

These attacks have been increasing in popularity over the past two years, fueled by the rise of specialty markets like Genesis Market. [Genesis Market](#) pulls data from infected devices and sells full identities, including cookies and session ID information.

Case Study: Evilginx

Another approach to session hijacking is through a tool like Evilginx. This phishing tool acts like an Attacker in The Middle (AiTM), sitting between the real server and the client to steal session IDs. By doing so, Evilginx can bypass weak forms of two-factor authentication.

- The attacker sets up a convincing phishing site and sends it to target
- The victim clicks on the link and enters the password and one-time password (OTP)
- Evilginx captures credentials and session cookies
- The attacker uses credentials and cookies to authenticate into the real domain



How Evilginx works. Source: okta.com

Identity Threat Landscape

Detecting Session Hijacking

In order to understand the prevalence of session hijacking, we analyzed the number of suspicious Attacker in the Middle (AiTM) attacks.

AiTM attacks might look like when a user opens multiple sessions with the same website or application but come from different IP addresses or devices.

This can be an indicator of session hijacking because it can allow an attacker to take over one of the sessions while the user is still active on the other. The attacker can then use the hijacked session to access sensitive information or perform unauthorized actions.

- 8.38** # of AiTM attacks against the average organization in Q4 2022
- 46%** of orgs saw suspicious AiTM activity in 2022

Long Sessions Enabling Session Hijacking

Long sessions can enable terminated users to continue to have access to their inbox after termination or even for regular users to evade enforcement when you roll out new MFA policies until the next time they need to authenticate. They also help session hijacking: the longer a session, the less likely an attacker is to be kicked off.

Okta recommends total lifetime sessions do not exceed one working day. While there may be some instances to break that, any sessions that exceed 7 days (168 hours) can make it easier to hijack sessions. Our analysis shows that, while most sessions are limited to the working day, the average company has 16.83 sessions every month that exceed 7 days.

Organizations should ensure that they have robust session management practices in place to prevent parallel sessions and protect against session hijacking. This can include implementing timeout settings, invalidating sessions after a set period of inactivity, and using secure authentication methods, such as phishing-resistant multi-factor authentication. By taking these measures, organizations can reduce the risk of session hijacking and protect their sensitive information from being accessed by unauthorized parties.

16.83 The average number of monthly Okta sessions exceeding 7 days, per company

Multi Factor Authentication



Organizations use MFA to enhance the security of their systems and protect sensitive information from unauthorized access. MFA adds an extra layer of security beyond just a password, reducing the risk of data breaches and identity theft.

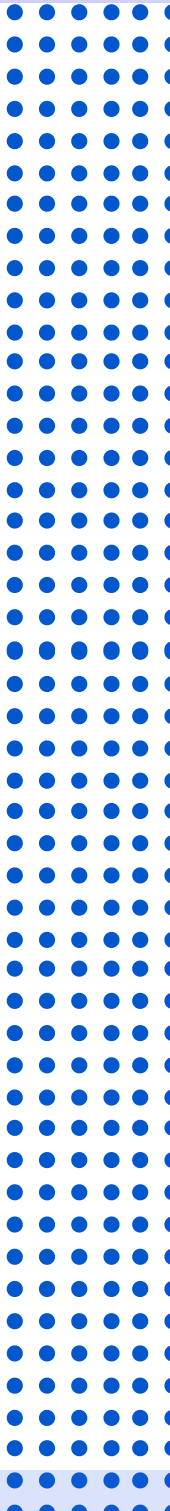
Examples of authentication factors include something a user knows (e.g., password), something a user has (e.g., a smart phone), or something a user is (e.g., biometric data). By requiring multiple factors, MFA helps ensure that only authorized users can access the system.

While any second factor is better than none, organizations are increasingly focusing on implementing phishing-resistant second factors. Examples of this include Touch ID, physical keys, and passwordless solutions.

There are several compliance frameworks that have requirements for Multi-Factor Authentication (MFA) to ensure the security of sensitive information:

- Cybersecurity Maturity Model Certification (CMMC)
- NIST 800-63-3
- SEC Cyber Risk Management Rules
- PCI DSS
- GDPR
- Gramm-Leach-Bliley Act

You can read more about the specific requirements of these frameworks in Appendix 1.



Multi Factor Authentication

MFA Bypass Techniques

The adoption of MFA has made accounts considerably more secure, but it's important to remember that this is not a silver bullet. There is no shortage of attackers looking to bypass MFA controls. In January 2022, Crypto.com announced losses of \$30M after hackers managed to circumvent its two-factor authentication (2FA) protocols to carry out the attack. Later, in August, Oktapus attackers targeted Twilio in order to access one-time passwords (OTPs) delivered over SMS.

These are just two real-world examples. We see seven main types of MFA bypass techniques.

1. MFA Fatigue

Consider how many one-time codes or push notifications a user receives in a week. From checking out from their favorite eCommerce brand to accessing their work email via the cloud, users have been conditioned to simply follow through with MFA instructions when they get an alert on their phone. Many cyber attackers now rely on the fatigue factor to ensure that when they attempt to log into a device illegally, the end user will simply press “allow” on their mobile device when the push notification comes up without questioning it.



Seven Types of MFA Bypass

2. MFA Flood

Similar to preying on victims' MFA fatigue, MFA flooding involves wearing them down through constant push notifications. Eventually, the victim may become so frustrated and tired of the constant alerts that they may finally relent, hitting the “allow” button to get some peace and quiet while the threat actor gets to work causing chaos.

3. Attacker in the Middle

An AiTM attack involves a cyber criminal intercepting communications between the victim and a legitimate organization. For instance, the attacker can create a login page that looks and operates like an online bank or brokerage's real single sign on (SSO), causing the victim to willingly enter not only their username and password but also their one-time code. Alternatively, they could simultaneously receive a push notification after they enter their credentials into the phishing site and, assuming the request originated from their own device, they press “allow.” In reality, the threat actor is simply working behind the scenes, leveraging automation to enter the stolen credentials obtained through the phishing site into the real login page at the same time.

Section 2

Multi Factor Authentication

MFA Bypass Techniques

4. MFA Reset

Attackers will often bypass MFA by bypassing the intended victim as well, choosing instead to contact their IT Helpdesk. By pretending to be the victim, they can ask a well-meaning IT Helpdesk technician to reset their account due to a lost device, allowing them to enroll a new factor upon sign-in or act during the generous reset grace period often offered by MFA policies.

5. SIM Swapping

Through this method, the attacker contacts the victim's mobile carrier to swap their phone number to a new SIM card in the attacker's possession. Any six-digit SMS codes will now be sent to the attacker's personal device, clearing the way for them to bypass MFA.

6. Oktapus Style

If cyber criminals are committed and patient enough, they could always "go big or go home" with an Oktapus-style approach. Named for its victim organization, the Oktapus phishing campaign that wreaked havoc in 2022 was unprecedented in its scale. Nearly 10,000 Okta login credentials belonging to users at Twilio, Cloudflare, Signal, and more were stolen through an elaborate, months-long phishing campaign. By infiltrating Twilio, attackers were able to intercept account enrollment SMS messages for the secure messaging app, Signal.

7. Ask Nicely

Sometimes, all it takes is a polite and authoritative tone. After spamming the victim with MFA push notifications, attackers will reach out to them by impersonating an IT Helpdesk representative and kindly suggest they either press the "allow" button or share the one-time password so the "IT employee" can resolve the MFA flooding issue for them.

1.24M MFA bypass attacks recorded in a single day (Auth0)

Multi Factor Authentication

Full Coverage Remains Elusive

Despite increased awareness of the importance of MFA controls, full coverage remains elusive to many organizations. Our analysis found that the average company has 40.26% of accounts with no strong MFA enabled. Some of these are service accounts, contractor, or dormant accounts – blindspots that we will dig into in the following section on IAM hygiene.

40.26%

Accounts with no strong MFA enabled

Attacks Target Weak Factors

Taking a sample of approximately 1.6 million logins, we learn that 20.28% of logins leverage SMS-based authentication. SMS is considered weaker than other forms of authentication as an attacker can intercept the codes sent to the end user, which are sent in clear text. This makes it easy for attackers to acquire and use these codes through phishing campaigns.

There were even a handful of bypass codes used (some of which were used multiple times). Phishing-resistant second factors (such as Touch ID, physical keys, or passwordless) only account for 1.82% of all logins.

This presents plenty of opportunities for attackers.

20.28% Logins leverage SMS-based authentication

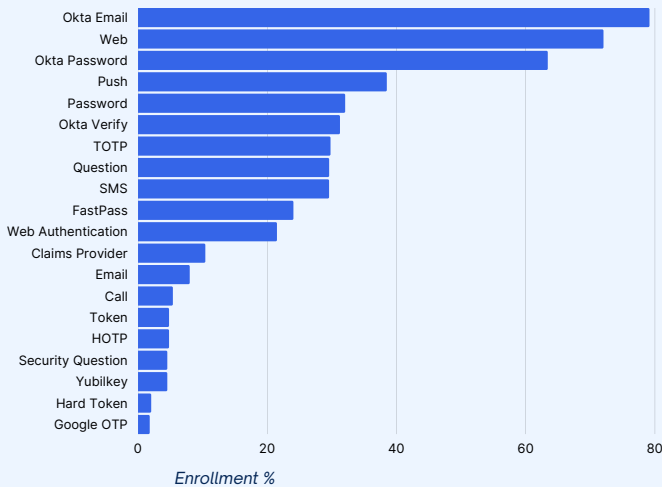
1.82% Logins leverage phishing-resistant authentication

While all employees should ideally have stronger forms enabled, special focus should be on those with administrative privileges in critical services like Okta and Workday, and providing them with physical authentication solutions like Yubikey.

Multi Factor Authentication

Factor Prevalence

As part of this analysis, we looked at the total prevalence of second factors across Okta, Azure AD, and Duo. We intend this to help administrators who may not be aware of prevalent factors. Less secure methods may have been enabled to support some of the population, but their ease of use makes their adoption more prevalent than admins might expect.



Okta

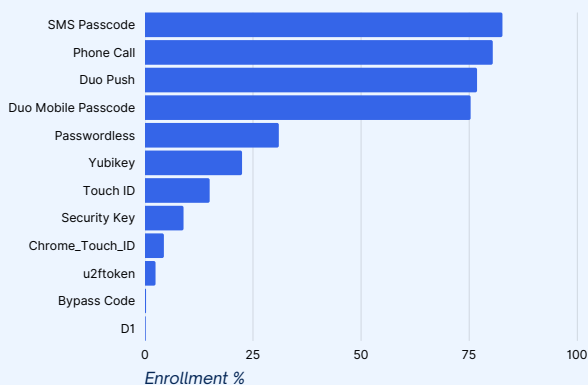
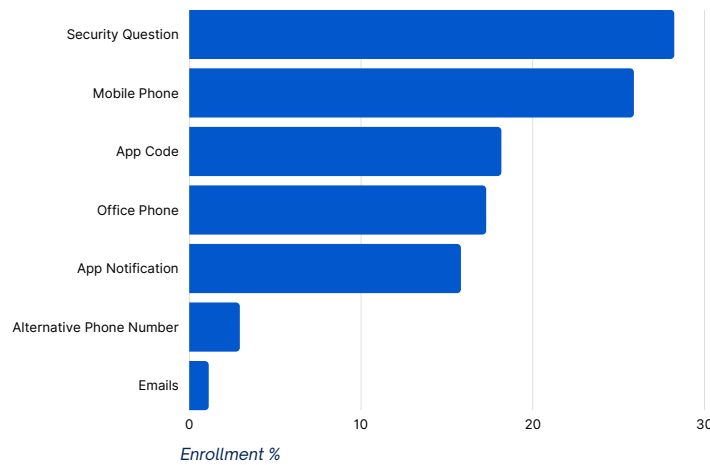
While SMS and Phone Calls are still used, there is a wider adoption of TOTP and Push. From this sample, hard tokens, such as Yubikey, have limited adoption.

We're hopeful of seeing an increased interest in Okta's phishing-resistant FastPass, and further adoption of this technology is something we will keep an eye on.

Azure AD

The most widespread second factors from our analysis were security questions and mobile phones. Some of these weaker factors are enabled by default, which security admins should be aware of.

As with Okta, there are still some users relying on email for a second factor, which should be avoided if possible.



Duo

SMS and Phonecalls are still popular methods for registering as second factors, with Duo Push close behind.

There is some promise in the adoption of phishing-resistant MFA, such as passwordless, Touch ID and Yubikey, but this still lags behind.

Identity and Access Management

Poor Hygiene Enabling Attackers



IAM Today: Complexity and Blindspots

IAM has become increasingly complex for IT and Security teams to manage. According to [One Identity](#), 41% of organizations use 25+ systems to manage identity and access rights. This identity sprawl has occurred for several reasons:

- **Microsoft Migration.** Companies that have historically had AD and are moving towards Azure AD but retain both.
- **Modern Tech Companies.** Since 2010, companies and startups have grown from G-Suite to Okta and other identity providers but have kept older IAM systems.
- **Large, Established Companies.** Similarly, more prominent and older companies tend to add trendier identity systems as they mature but fail to completely deprecate older IAM systems as they go.
- **Mergers and Acquisitions.** Companies that have acquired one or multiple companies now have to support numerous identity platforms.

This is further complicated by remote work, where employees and contractors log in from different locations and devices. Some employees even bring their personal email addresses to work, which causes duplication. On average, companies have 340.5 personal accounts (Gmail, Yahoo, Hotmail, iCloud, etc) with access to company data.

When IAM hygiene is poor, organizations' identity attack surfaces increase and provide additional opportunities to attackers. It makes it hard to investigate incidents as there is no single source of truth, and the critical chain of events is missing.

Finally, organizations must consider several compliance considerations, such as SOX. Regulations demand that organizations monitor and audit successful and failed login activity, account and user activity, and information access.

340.50 The average number of personal accounts, per company

Dormant Accounts

We outlined earlier how attackers target dormant accounts as they typically have fewer controls and monitoring in place.

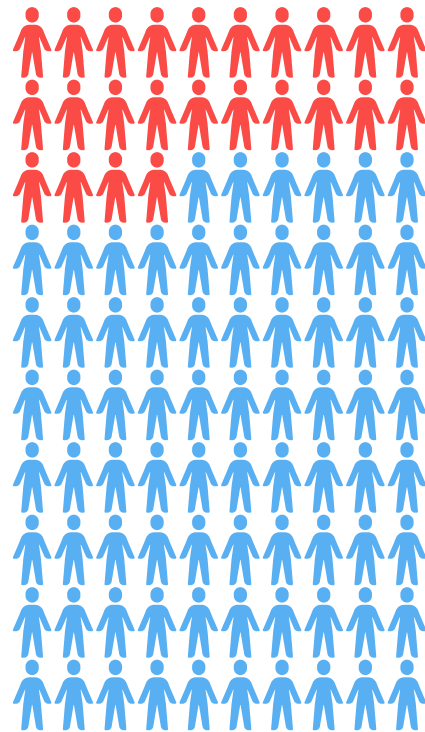
In this research, we analyzed accounts that had no activity in the last 30 days. The average organization has a large number of inactive accounts - more than 24% of its total identities. Many groups are dominated by inactive users. These groups have lots of inactive users, with an average of 196 groups with more than 75% inactive users.


24.15% Average % of inactive accounts, per company


196.6 Average number of groups with >75% inactive users, per company

Organizations should clean up inactive accounts to prevent the risk of account takeover.

Inactive accounts in the average user population



 Inactive accounts

 Active accounts

Guest Accounts

To make it even more challenging, organizations need to manage the lifecycle and permissions of guest accounts.

Guest users can be invited to a directory, to a group, or to an application. This is often necessary for effective collaboration.

Some users may invite their personal IDs to create an alternative user that can be used to transfer data.

Given the challenges of managing guest accounts, it's no surprise that, for the average company, more than 3.24% of all identities are guest accounts.

3.24% Average % of inactive guest accounts

Groups

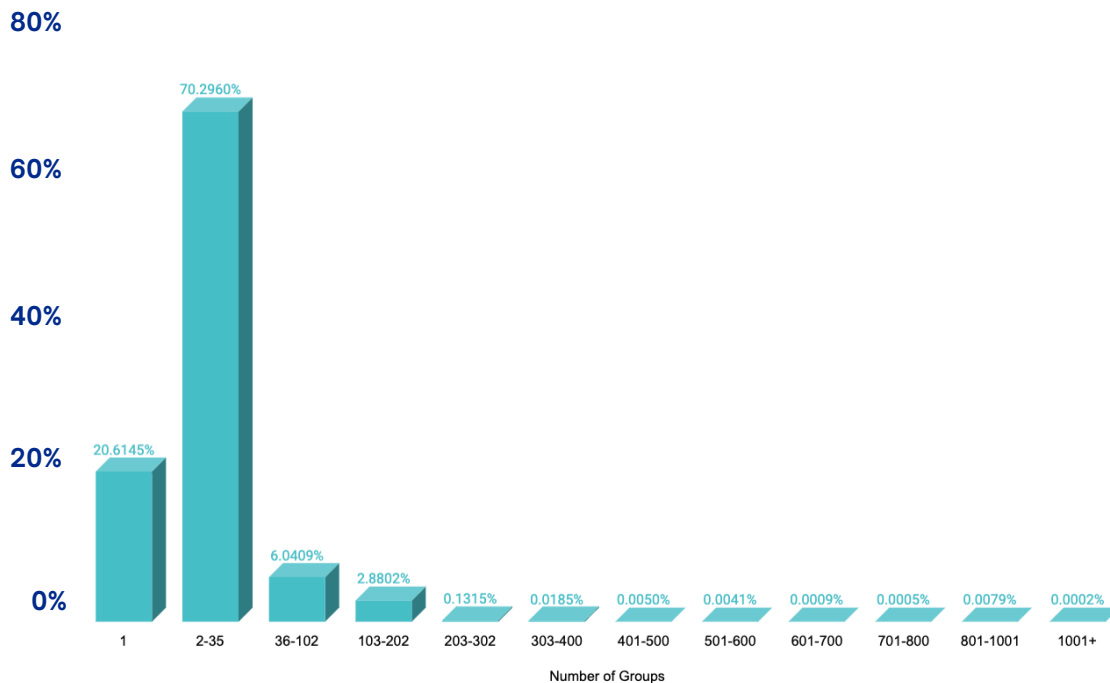
Over any employee's work history, it's easy to accumulate a myriad of permissions. Research by [Unit42](#) found that 99% of cloud users, roles, services, and resources are granted excessive permissions.

Permissions are typically granted by groups and we often see poor hygiene when it comes to group management. The average organization in this analysis had 7,740 different groups. Most users (70.30%) have between 2-35 groups, but individuals within organizations can have hundreds, and sometimes thousands, or groups. Given how closely groups are tied to permissions, this demonstrates how easy and pervasive it is for permission creep to exist.

There are also clear issues with many of these groups. For example, across numerous organizations, we see groups for users who are excluded from MFA - "MFA Exclude Groups". In many cases, accounts (including admins) remained in these groups for several months, and there were several different MFA Exclude Groups. The harder it is to understand who is excluded from MFA, the more likely it is these accounts will be successfully targeted.

7,740

The average number of groups, per company



Average number of groups per employee (as a percentage of the total population)

Poor IAM hygiene around groups and permissions creates opportunities for attackers by providing them with access to sensitive information and systems that they should not have. IAM hygiene refers to the process of ensuring that identity and access management systems are properly configured, up-to-date, and secure. This includes regularly reviewing and updating user accounts, groups, and permissions.

Unused Applications

In this research, we analyzed the average number of applications a user is assigned to. From this, we can understand the average number of apps the average company and user is assigned to, and how often those apps are actually used.

On average, companies have 302.88 apps in total. 147.50 (47%) of these were unused in the last 30 days. Users, on average, have 29.17 apps and 23.30 (79.87%) go unused.

In general, users have access to too many applications. This has an obvious cost to the business in terms of licenses, but there is also a security implication to having an excess of unnecessary access.

79.87%

Of applications go unused by users every month

User Inconsistencies

Orphaned Accounts

In September 2022, an attacker gained access to a Rockstar employee's Slack account – ultimately leading to a breach of the gaming company.

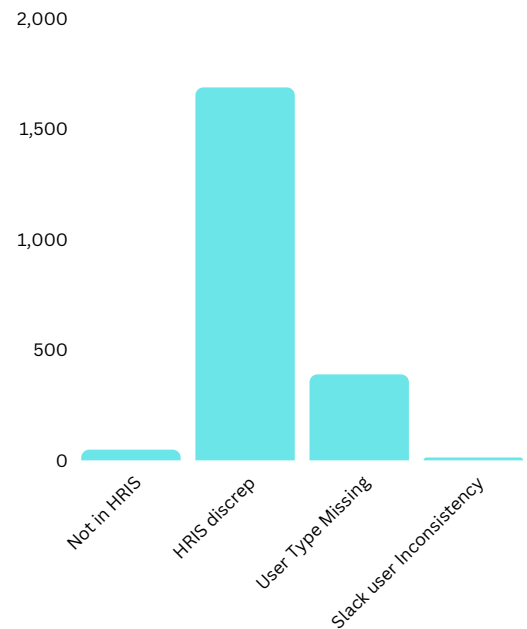
Slack is one example of a platform that might be out of sync with centralized IAM controls. We also see inconsistencies between human resource information systems (HRIS). This can lead to orphaned accounts that become difficult to manage.

Missing User Types

Another common type of inconsistency is missing user types. If accounts have a missing user type, you can't even begin the job of making sure that your accounts are configured properly and with the right policies.

The security policies that are applied to each account vary wildly depending on the classification (user type) of the account. Policies will differ depending on if the account is an employee, contractor, guest, or service account.

Average number of user inconsistencies



IAM Hygiene: In Summary

By addressing all of these IAM hygiene issues, organizations can reduce their attack surface and minimize the risk of data breaches and other malicious activities. This includes regularly reviewing and updating user accounts, groups, and permissions, as well as implementing access controls and monitoring systems to detect and respond to any suspicious activity.

Summary

Against a backdrop of rising identity threats, organizations are providing unintended opportunities to attackers. MFA is not comprehensive, and a number of authentications still rely on weak factors.

Worse still, there are entire areas of basic IAM hygiene that are being ignored—at the expense of organizations' identity posture. As the paper has demonstrated, this includes large numbers of dormant accounts, permissions creep, and poor MFA practices.

Looking forward, it's likely that increased scrutiny from regulatory bodies will continue to make identity security a board issue. Increasing implementation of Zero Trust strategies will see the importance of identity security grow. For better or for worse, high-profile identity attacks will generate board-level interest.

The increased emphasis on Identity Threat Detection and Response will help to shed light on these new techniques, but organizations should not lose sight of the identity attack surface.

"By 2026, 90% of organizations will use embedded identity threat detection and response function from access management tools as their primary way to mitigate identity attacks."

Gartner

Top 5 Recommendations

- **Get on top of your identity mess.** Build an identity inventory.
- **Tidy up.** Make sure accounts of users that are no longer employed with the organization are de-provisioned/deleted.
- **Shore up MFA.** For your internal workforce make sure your key employees use strong MFA. For your external workforce, make sure they use SSO or have MFA.
- **Ongoing monitoring.** This is not a one-time activity. Continually monitor for behavioral anomalies and threats.
- **Investigate user incidents.** Respond to suspicious activity by understanding the who, what, where, when, how, and why of every situation.

Additional Identity Threat Detection and Response Resources

- Okta [Leveraging Identity Data in Cyber Attack Detection and Response](#)
- Gartner, [Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response](#)
- [Mandiant Azure AD Investigator](#)
- [Hawk](#)
- [Azure AD Incident Response PowerShell Module](#)
- [Microsoft Azure AD Assessment](#)
- [HavelBeenPwned.com](#)

Appendix 1

Compliance Related to Identity

Compliance regulations, including SOX, CPRA, NIST, CMMC and PCI all require organizations to establish security and audit controls to ensure that business and customer data is protected. The table below displays the compliance frameworks most relevant for identity security.

Many of these frameworks are closely tied to information that sits across various identity platforms, which is often hard and time-consuming to access. Understanding if your are compliant can be arduous to do once, nevermind on a reoccurring basis.

	CMMC	PCI DSS	NYCR	NIST 800-63-3	GDPR	SEC	GRAMM-LEACH-BLILEY ACT	SOX	CCPA
Ensure MFA is used by all users for network/remote access	✓		✓						
Ensure MFA is used for privileged users for local access	✓								
Ensure MFA is enabled by accounts with access to any personal/customer information				✓			✓		
MFA must have two of three of something you know, you have, or you are		✓							
User access privileges to nonpublic information must be limited.			✓						
MFA to support verifier impersonation (phishing) resistance required				✓					
Protect and Secure User Data					✓				
Ensure users present a combination of two or more credentials for access verification						✓			
Monitor and audit successful and failed login activity, account and user activity, and info access								✓	
Ensure employee account information is removed					✓				✓

About Oort

Oort is an identity-centric enterprise security platform. As a turnkey solution for Identity Threat Detection and Response (ITDR), Oort is providing immediate value to security teams by working with existing sources of identity to enable comprehensive identity attack surface management in minutes.

Led by a team with decades of domain expertise across identity, networking, and security, Oort is backed by venture capital investors including Energy Impact Partners, .406 Ventures, Bain Capital Ventures, Cisco Investments and others. Market-leading technology companies, like Collibra and Avid Technology, rely on Oort to provide full visibility into their identity populations.

To learn more, please visit oort.io.

