Whitepaper

September 2022

Anatomy of Identity-Based Attacks

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871

okta

Contents

Abstract

As a security practitioner, protecting your organization's data is your number one priority. With the explosion of the mobile and hybrid workforce, SaaS adoption, and application modernization, new attack methodologies are arising while existing ones are resurfacing.

Federal agencies such as the National Institute of Standards and Technology (NIST), and the Defense Information Systems Agency (DISA) as well as private entities like Google and Gartner all attest to identity being a pillar of modern security strategies such as a Zero Trust Architecture (ZTA). A Zero Trust Architecture represents a modern framework for securing the workforce enforcing principles of least privilege and not surprisingly, identity plays a significant role in the design and implementation. Despite the relative importance of identity, it has long been deprioritized and seen as an ideal attack surface by bad actors. Unsurprisingly, identity-based attacks have become more prominent and sophisticated. Security teams as a result have to ensure that proper identity and access management (IAM) solutions are incorporated into their security projects to thwart these attacks. Okta, the leading IAM solution, offers capabilities to help security teams mitigate many of these identity-based attacks.

Introduction

Identity has played a key role in organizations for many years, but historically has been regarded simply as an operational technology, without much consideration around security implications. As technology has evolved and users have become more dispersed and diverse, there has been a renewed focus around enabling users to not just be productive, but to do so securely.

Organizations are increasingly adding Identity and Access Management applications to their technology stack because they understand that identity will anchor their security strategy. Whether implementing an HRIS as the source of truth for users or a web gateway to enforce network policies, the identity accessing a resource is the common thread that ties the entire transaction from end to end. As a result, identity has come to the forefront for security leaders who have undertaken a Zero Trust journey to fortify their defenses. Both Gartner and Forrester explicitly call out identity as a core principle of a Zero Trust security strategy. According to Forrester, "We advise clients to start with identity/IAM, as it's foundational for identity-based access and one of the top vectors for external attacks."

Meanwhile Gartner believes that, "A Zero Trust architecture uses identity and context to manage adaptive trust decisions. Having a robust identity access foundation is a key prerequisite for success." In the public sector, M-22-09, the Office of Management and Budget (OMB) initiative aimed to move the US government towards Zero Trust cybersecurity principles explicitly calls out access controls in the Department of Defense's Zero Trust Reference Architecture. "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access."

While many organizations understand the foundational link between identity and security, there are still those who have yet to realize this truth. And as long as significant gaps exist in their identity security, the risk of a breach or compromise is ever present.

Identity-based attacks

As encouraging as the adoption of Identity as a Security Strategy (IDaaSS) is, it also puts the bullseye squarely on IAM solutions and on Identity as a threat vector. The proliferation of SaaS, the sudden explosion in a hybrid workforce and the digital transformation revolution businesses have gone through to replace their brick and mortar with web properties, all were aided by identity solutions that offer agility and modern capabilities. Yet these modern ways to operate a business and enable end users comes with its own share of challenges specifically around identity specific threats. Identity-based attacks have not only been highly prevalent in breaches (see Table 1) but are getting more sophisticated, forcing security teams to constantly be on the defensive and shore up the front door to their organization's data.

According to the 2022 Verizon Data Breach Investigations Report (DBIR), over 40% of all breaches involved stolen credentials and 80% of all web application breaches involved credential abuse. The presence of phishing attacks in breaches also rose from 25% in 2020 to 35% in 2021. Moreover, the attack surface continues to expand and

aside from the traditional enterprise and the digital consumer, third-party supplier risk has taken center stage. Even ransomware attacks have increased to now comprising 25% of all breaches; and while ransomware is not thought of in an identity centric lens, identity is often compromised in order for ransomware to be installed. It is abundantly clear to security practitioners that identity security is absolutely critical to protecting their data.

Understanding the importance of an IAM solution is only the first step since not all solutions are equally effective. Selecting an IAM platform that can fortify your defenses against identity-based attacks is the next step. As a multi-tenant solution, each Okta customer environment (tenant) is a logically isolated environment, providing data separation and impact isolation. Also, being a cloud native solution has allowed Okta to maintain its agility in the face of ever changing security threats. Over the last decade, Okta has built capabilities into the products as well innovations into the platform to combat identity threats.

Let's take a look at how Okta can help security teams mitigate the threat of identity-based attacks.

Identity Protection at the Service Layer

An important preamble is that while numerous mitigation controls and capabilities are available for Okta customers to configure in their tenant, Okta has implemented numerous safeguards to the authentication flow well before any traffic reaches the specific customer's tenant. By scrubbing the traffic at our edge, we're able to block malicious traffic and reduce risk at the service layer, well before the tenant-level policies and controls are applied. Another significant offering is Okta's **ThreatInsights** capability powered by Okta's insights platform service. Because the Okta service is able to see hundreds of millions of authentications daily across our entire customer base, spread globally, it can interpret malicious authentication patterns and build a data lake of IPs that exhibit malicious behaviors. Okta customers can choose to leverage this capability to enforce IP restrictions based on those identified sources.

The anatomy of various identity-based attacks and possible mitigating solutions

The following section discusses prominent identity-based attacks and how they are carried out. We also look at how attackers are leveraging identity as a conduit for infiltration. Finally, we go on to suggest how security teams can leverage Okta to mitigate those attacks and reduce their organizational risk.

Password Spray

A password spray attack comes from the brute force family of attacks and played a role in the infamous **SolarWinds breach** as well as the 2019 **Citrix breach**. Password spraying is based on volume rather than targeting specific users or accounts. A threat actor attempts to use a few commonly known passwords across multiple accounts with the hope that even a single user has set that specific password for their login credential. By using a low number of qualified password guesses across many accounts, the attacker is able to stay under most account locking thresholds. Along with researching a company to pilfer possible password combinations, a threat actor may also do the same to determine if a system requires passwords to be a certain length, have special characters, include numbers and so on. This information is used to craft password guesses across the organization's systems.

Hacker gathers a list of commonly-used passwords

Hacker tries the same common password across multiple accounts

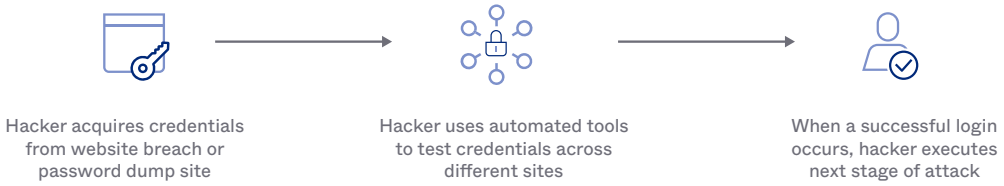
Once a login is successful, hacker harvests the sensitive data

Mitigation strategies

- The Okta sign-on policies can be set up to lock out the account after a low number of invalid attempts. If lockout creates too much friction, implementing a **CAPTCHA** can be a good alternative.
- The Okta tenant can help stay clear of common passwords all together by enforcing that specific password requirements during the initial account creation process. More information **here**
- Turn on Okta **ThreatInsights**, which can greatly reduce the impact of this type of attack
- Implement an alerting system that assesses failed attempts across multiple accounts. A review of logs for failed attempts or a high number of locked accounts is a good sign that an attack is taking place. The specific user identities should also be of interest to the security admin; as are the user accounts those of previous employees, or perhaps accounts that have never logged in but are suddenly displaying multiple unsuccessful attempts.

Credential Stuffing

Credential stuffing attack is another subset of the brute force attack category. The threat actor attempts to stuff different credentials (often username and password harvested from an online data dump) into as many different sites and portals as possible with the hopes of one of them being successful. This type of attack exploits people's tendency to reuse passwords across multiple sites. Because attackers are using lists of previously-used passwords, it is often successful as this type of attack does not exhaust one single system so any password lockout settings do not get triggered, and uses automated tooling to cover a vast number of systems in a short period of time.

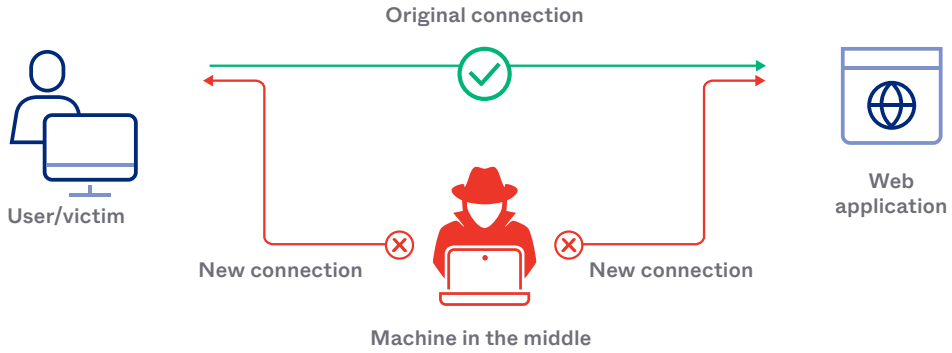


Mitigation strategies

- Okta's **Adaptive Multi-Factor Authentication** (AMFA) is a primary defense against credential stuffing attacks. By enforcing MFA, the threat actor is not able to complete the authentication flow even if they have a compromised credential. Leveraging additional data points such as location, IP, city, and state, can help to build a baseline profile and determine the risk level of the login attempt. In the event that MFA is not a control you can enforce for every user and every login, you can layer this control in conjunction with other checks such as device fingerprinting.
- Similar to Okta's MFA offering, security admins can set up **CAPTCHA** in the login flow in certain use cases to augment the security of the authentication request.
- Turn on Okta **ThreatInsights**, which can greatly reduce the impact of this type of attack
- Educating users to not reuse passwords, especially between sensitive and non-sensitive sites is another measure to reduce the likelihood of a credential stuff attack succeeding. For example, don't use the same password for your bank login and your local gym's class sign-up page. Okta's browser plugin can suggest unique passwords, and save them automatically when users are creating new accounts.

Machine In The Middle (MITM)

MITM attack is not new by any means - in fact it has been around for as long as computer networks have existed. With SaaS being so ubiquitous, and many business functions being moved to outside the network, it has found a worthwhile bounty. MITM occurs when a threat actor is able to sit in between the user and the resource they want to connect to. Then, the threat actor will broker traffic between the user and the destination site, unbeknownst to the user. In this manner, the application behavior appears normal, however everything the user is typing is going through the threat actor's system including passwords the user submits to login with.



Mitigation strategies

- Transport Layer Security (TLS) is the obvious mechanism that can thwart the majority of MITM attacks. Encrypted communication will deter the attacker from sniffing sensitive information between the client and server.
- Advanced attackers can issue their own certificate so communications are still encrypted as far as the end user and the destination is concerned. Using trusted networks to perform sensitive activities is the best defense against this threat.
- A strong phishing resistant MFA factor is the ONLY way to ensure the attacker is not able to obtain a logon session to the target server, while other methods can ultimately be phished. It does not however prevent the attacker from stealing credentials which may be used elsewhere.
- Man-In-The-Middle attacks almost always start with phishing, so user education and training end users to be critical of certificate warnings and urls that mimic legitimate sites also goes a long way.

Phishing

Phishing (and let's use it broadly to encompass all of the xxxx-ishing category) is a tried and true attack vector as old as the internet itself. Phishing is when a threat actor attempts to lure the end user into clicking, downloading, visiting, etc. a malicious endpoint by crafting communications that seem legitimate. Targeted individuals (spear phishing), targeting high ranking personnel (whaling), attempting to gain sensitive information over the phone (vishing), are all techniques with the aim to obtain sensitive credentials either by having the user download malware to steal the information, coercing the user to outright provide the information to an attacker, or having the user visit a site and enter their credentials.

Mitigation strategies

- User training is paramount; Okta **Workflows** can stage phishing campaigns by sending fake MFA prompts to train end users on **MFA Fatigue**
- Technical controls such as behavior detection and step up authentication can help to alarm the end user of abnormal activity on their part
- Okta's vendor neutrality allows security teams to **integrate** leading email providers and set up policies with the email solutions for enforcing MFA, killing sessions, and locking users accounts.

Machine-to-Machine communication

Often overlooked, service account security represents a growing attack surface for identity-based attacks. According to a recent CIO study, by the end of 2021 the average organization had a quarter million machine identities with the expectation that they will jump to half a million by 2024. Workloads are orchestrated to automatically authenticate to one another and proper security of service accounts, the security of API endpoints and best practices around use of credentials in programmatic access is vital. If credentials are hardcoded, referenced in an insecure manner or not protected with proper encryption, they can be accessed by threat actors without any knowledge of the compromise.

Mitigation strategies

- The **OWASP** offers guidance on best practices for application security
- Okta's **API Access Management (APIAM)** secures api endpoints so only authenticated clients can access the backend service and have only essential authorization scopes
- Perform penetration testing and static code analysis against non-prod instances of the application
- Create alerts to detect when machine credentials are being used in unexpected places or contexts

Third-Party Accounts

Identities under one organization's control are easier to manage and secure compared to those controlled by another organization such as a partner. Increasingly, third party service providers are standing up their own identity solutions and expect to leverage them for authenticating to resources in a customer's network; think consultants or temp agency workers logging in to a client's network to process payroll. Federation is a method of establishing a web of trust between identity providers (IDPs). When two or more IDPs federate, a user can authenticate to their own IDP and obtain a valid assertion that will allow them to seamlessly consume an application or resource hosted by the other identity provider. The nature of a federation is such that the service provider (the identity solution hosting the application) will trust the assertions that come from a partner's identity provider. While it may be certainly unintentional, the compromise and breach of a partner's IDP can allow attackers to hop to your Okta tenant and access applications as an authenticated user.

Mitigation strategies

- When partners are accessing resources on your IDP, they must accept that regardless of the security controls they've configured, security enforcement will still occur on your IDP
- Enforce step-up authentication at the application level
- Configure risk based authentication while enforcing phishing resistant factors for high risk logins
- Share login activity information with partners who can better assess anomalous behavior

Underground Markets

The adage *'Why break in when you can log in?'* certainly applies to security breaches. While sophisticated technical attacks and clever social engineering tactics are constantly employed, there is a huge market for purchasing harvested credentials. Whether they are usernames and passwords, or cookies and access tokens that will give the attacker a valid session, the data lake of compromised credentials is massive and publicly for sale on the darkweb. With rootkits and malware serving as the foundation of advanced persistent threats (APTs) to steal credentials, entire workstations can be purchased, offering unlimited potential for what the end user will access. While strong authentication is the first line of defense in this scenario, authorization is not far behind.

Mitigation strategies

- Okta's AMFA solution can enforce additional requirements to accessing a resource or application. Because the context of the request coming from the use of stolen credentials presents a high risk behavior, proper policies should be configured to block the request or ask for a phishing resistant second factor
- Access tokens should be scoped to have limited rights and further authorizations need to be request and approved via MFA
- Access token lifetimes should be configured to expire in a relatively short period. This will force re-authentication (coupled with MFA) in order to obtain a new access token.

Privileged User Accounts

While not a threat in accordance with the aforementioned attacks, privileged accounts account for valuable real estate in the attack surface territory. Privileged accounts carry higher levels of authorization and thus are the keys to an organization's crown jewels. If attackers can gain privilege credentials, all bets are off when it comes the to the havoc that can be wreaked. From reconfiguring systems and rootkit installations to silent persistence and data exfiltration, there is no limit to what an attacker can do. Many organizations have implemented credential vaulting solutions to store sensitive credentials that are checked out and rotated. While certainly an improvement, it still falls victim to a static value being made available to the privileged account which could be under the attacker's control. Not having passwords, especially for accessing sensitive workloads should be a best practice all organizations are exploring.

Mitigation strategies

- The primary control should be enforcing MFA on every login for a privileged account. As these accounts are highly sensitive, hardware/phishing resistant authenticators such as Yubikey and Webauthn are a must. With Okta, you can implement 14 different MFA solutions coupled with customized policies to remove user friction and enhance security.
- Okta's **Advanced Server Access** (ASA) product delivers ephemeral credentials by way of short lived certificates minted at time of request for accessing servers. Removing passwords in the authentication flow all together and relying on stronger assurance factors is a net positive in enhancing the security posture.
- ASA is able to stream events to a dedicated SIEM and should be configured to do so. Event logging and alerting are critical components of protecting against privilege account abuse. Any authentications should be alerted on; coupled with Okta's AMFA solution to enforce behavioral risk based policies. The ASA product provides verbose logging as well as session capture to assist audit and incident response requests.

Conclusion

The attack surface is rife with exploits when it comes to identity security. While these attacks are not necessarily new, and have plagued teams for decades now, we see more sophisticated threat actors leveraging the multiple tools at their disposal in order to carry out attacks that range from precise and direct campaigns to casting wide nets in the hopes of playing the economies of scale game. Motivations range from financial gain, disruption of business, and reputational damage. The reality is that a threat actor can be anyone from a nation state to a disgruntled employee. With this broad scope of threats, a comprehensive security strategy built on security best practices, combined with a layered defense model of people, processes and technology is most effective when it comes to identity security.

People: User Education

We need to stop thinking of our people as the weakest link and instead consider them the strongest asset for dealing with security threats, as a user's actions ultimately determine the fate of an organization's security posture. Equipping users with the appropriate tools, training and education is a must. Enforcing best practices around passwords is a good starting point and security teams can assist by coupling the education with Okta's granular password policy setup which will lead users in setting up secure passwords. If passwords are not reused, are not comprised of common dictionary words and users are mindful of separating sensitive logins from non-sensitive ones, then many of the techniques attackers deploy can be rendered ineffective.

Process: Log Correlation

Often overlooked but certainly critical is the logging and event correlation data. Okta's native syslog is extensive and detailed. Via Okta's **OIN** or new log streaming capabilities, this data can be fed to an organization's SIEM. SIEM logs should be reviewed and proper alerting based on events needs to be set up. For more information on how to query specific log events, see **here**.

Technology: Adaptive Multi-Factor Authentication and ThreatInsights

Defense in depth can be achieved by enforcing Adaptive MFA and turning on Okta's ThreatInsights. Traditional MFA solutions greatly reduce the success rate of identity-based attacks, and when phishing resistant factors are coupled with Okta's behavior detection, administrators are able to drive contextual risk based decisions that will thwart the efficacy of identity-based attacks while reducing user friction. ThreatInsights further harnesses the power of the Okta network and its over 16,400 global customers to proactively filter malicious threats and prevent attackers from reaching your Okta tenant.

In concert with the Zero Trust philosophy of continuous authentication and least privilege, anchoring the organization's security strategy to identity not only provides visibility across the technology stack to ascertain the validity of authentication requests but also will aid in mitigating risk.

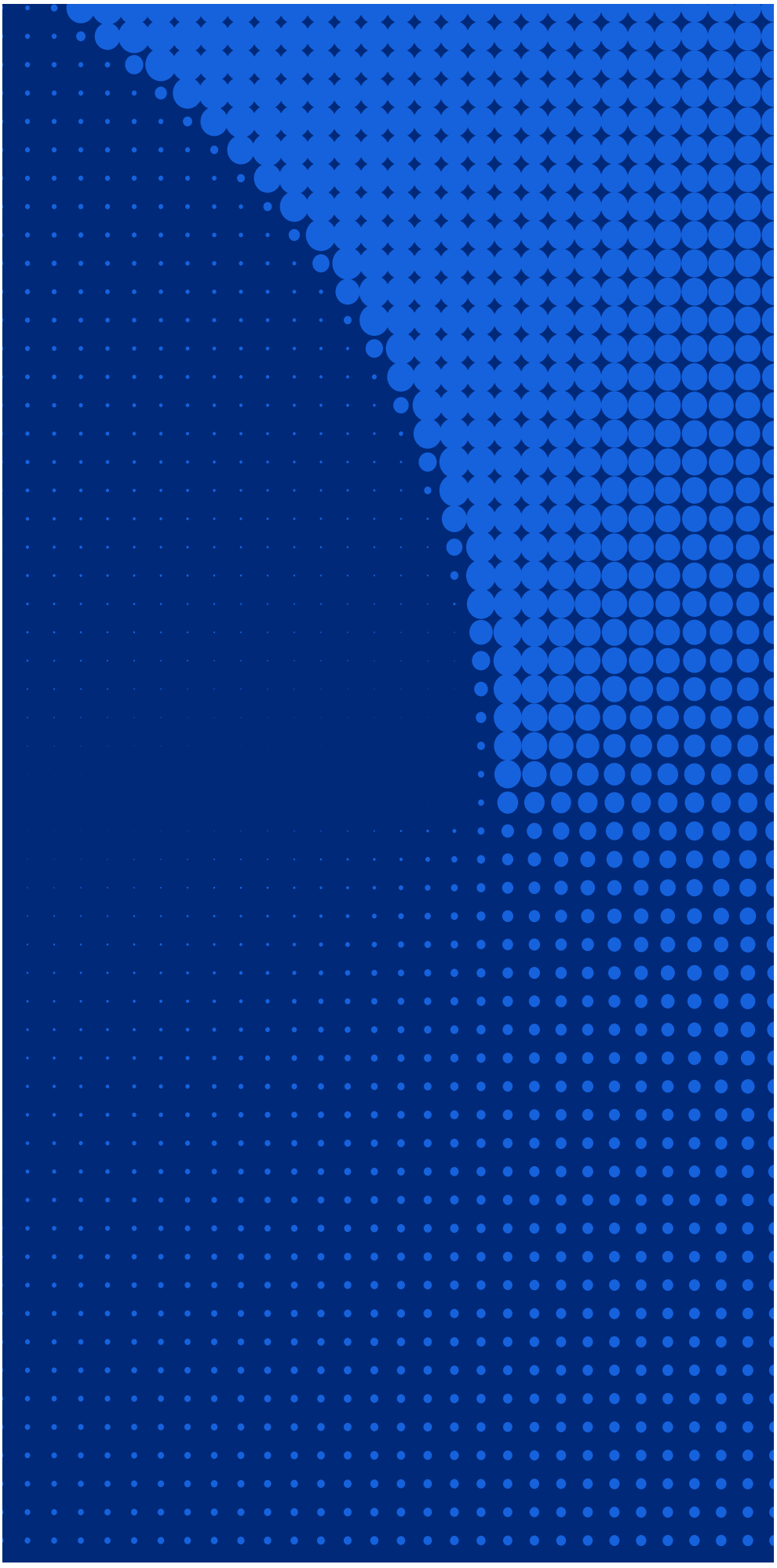
Table 1
Additional metrics on Identity-based attacks.

Attack	Metrics	Source
Brute Force Attacks	• 70% increase in reported RDP attacks from Q2-Q4 2020 vs 2019 • 94% of 1000+ employee orgs experienced identity related breaches • 24% of US security professionals say that their organization has experienced a brute force attack, including password spraying or credential stuffing, in the last two years.	**Identity Defined Security Alliance**
Credential Theft	• 60% of mid-sized businesses (250-5,000 employees) that have asked their employees to work remotely experienced a cyberattack; 56% of those experienced credential theft	2020 Ponemon Institute

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com**.

Whitepaper



okta