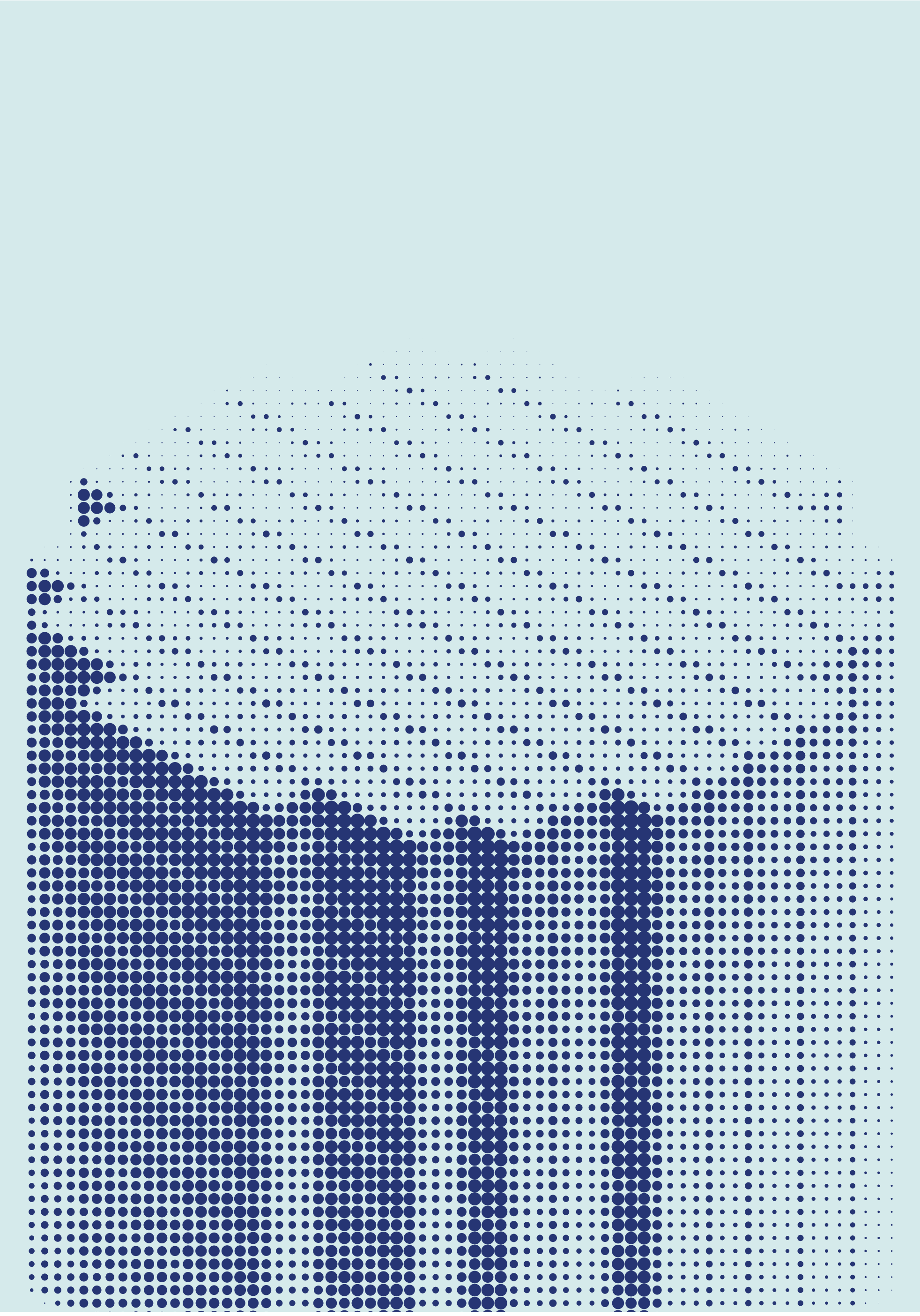
Whitepaper

Month Year

Identity Is Key to Stopping These 5 Cyber Security Attacks

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



A secure enterprise is a successful enterprise. Security threats are a massive burden for most organizations—but in spite of the fact that cyber attacks are continually becoming more sophisticated, many of them begin with the same weaknesses: user accounts. And that includes the credentials and login policies that are supposed to protect them.

Most enterprises understand that there's a link between identity and security, but few grasp how fundamental identity can be. Identity isn't just a first step, it's the foundation that modern security strategies should be built on.

What's at stake

Organizations that fail to provide adequate protection for personal and corporate information are likely to fall prey to cyber attacks. The financial losses from data theft and regulatory penalties are just the short-term consequences; the long-term damage to reputation and brand trust can be impossible to fully recover from.

It's a threat that remains persistent across sectors. In 2020, there was a **record amount of data stolen** through breaches as well as an unprecedented number of cyber attacks on enterprises, government bodies, and individuals. This is not entirely surprising, however. With the ongoing adoption of remote work practices where organizations have had to extend their security perimeter to their employees as well as their devices and home networks, cyber criminals are increasingly focused on obtaining workforce credentials.

This is a trend they've been developing for years, taking advantage of the level of access they can gain by seizing employee accounts. In fact, according to Verizon, 81% of data breaches involve stolen or weak credentials, and 91% of phishing attacks are after the same information. This is just one of the reasons that identity is crucial to driving security.

Another key consideration is that modern attacks make all enterprise applications critical from a vulnerability standpoint. With access to applications being requested from both inside and outside the enterprise network, all business apps become subject to cyber threats. Bad actors are capitalizing on this vulnerability through phishing and social engineering attacks, and internal users with malicious intent have the opportunity to misuse their privileges and compromise corporate data. This becomes an authorization issue, where users aren't necessarily being given the right level of access. To get ahead of this issue, enterprises need a robust identity solution that can help manage authentication and authorization in a seamless and secure way.

With these and other security concerns on the horizon—and the need to protect all networks, cloud applications, and devices—identity is a much-needed source of strength. And as credentials continue to be a focus point for cyber criminals, identity has to become foundational to modern security.

Five leading security attacks—and the impact of a strong identity solution

A survey by IDG commissioned by Okta indicates that four out of ten senior technology and security leaders are aware that weak passwords, phishing attempts, and credential sharing are having a significant impact on their security posture. Here's a closer look at the leading attack vectors and how starting with identity can help mitigate them.

1. Broad-based phishing campaigns

Rising levels of remote work have been accompanied by skyrocketing rates of broad-based phishing attacks. Even in a well-trained organization, this type of phishing campaign can successfully compromise **one out of 20 employees**. This not only poses a serious security risk for your organization, but puts valued team members in the unenviable position of being responsible for a potentially catastrophic breach.

But how do these attacks work? The attacker compiles a list of emails, and then designs a generic message that will be believable for the intended group—for example, a fake Google login page. The phishing message is sent to as many potential victims as possible.

A threat agent only needs to gain access to a few accounts—or a single admin account—to compromise an entire organization, and credential theft from phishing is often the first stage of the **cyber kill chain**. Attackers can use stolen credentials to access data, or once they control certain accounts, they can assume those identities to launch more concerted attacks on higher-value targets.

2. Spear phishing campaigns

Another common type of phishing campaign is referred to as "spear phishing". Whereas broad-based campaigns rely on probability—the more people they reach, the more likely they are to succeed—spear phishing campaigns are highly targeted and predatory.

The level of social engineering behind these attacks tends to be more sophisticated, and they often feature messaging that plays on emotional triggers such as curiosity, fear, or rewards. It can also be very personalized, with threat actors conducting extensive research across sources such as social media and web presence to single out potential victims. By focusing on a small handful of employees, spear phishing also evades automated filters.

Messages may come from someone impersonating a manager, referencing a topical situation, or requesting an urgent favor or a time-sensitive task. This creates a reactionary response; the employee may be eager to respond to their supervisor and enter credentials to perform the requested action—equipping the attacker with everything necessary to access sensitive data or execute the next stage of the attack.

3. Credential stuffing

There are several types of brute force attacks that take advantage of weak login factors, but credential stuffing is among the most problematic. In these cases, the hacker acquires a large list of credentials from a password dump site, a website breach, or the dark web. These are then tested on several other websites—including yours—since people tend to re-use passwords across platforms. The average American internet user has approximately **150 online accounts**, and selecting unique passwords for all of them is almost unfathomable. As a result, most passwords are duplicates, and this is a major security risk.

What's worse, these attacks can be automated and carried out at scale. Credential stuffing incidences originating from bots are a top concern for account security professionals, and research from Akamai shows that bot-driven credential stuffing attacks are responsible for more than 40% of all user login attempts (criminal and legitimate) worldwide.

4. Password spraying

There's another type of brute force attack that's become increasingly prevalent: password spraying. In these instances, the attacker chooses a single common password that matches the complexity policy of the domain, and tries it alongside the usernames of many account holders on a particular site. By trying to log into accounts just once instead of making multiple attempts, password spraying attacks are often able to avoid detection. And, in many cases, the odds favor the attacker: users can be dangerously uncreative with their passwords—"password1" has appeared in data breaches more than 2.3 million times, **according to Pwned Passwords.**

5. Man-in-the-middle attacks

The final type of attack is neither a phishing campaign nor a brute force attack—and if criminals can pull it off, it can be one of the most devastating threats an organization may face. This is the man-in-the-middle attack (MitM), in which a network connection is intercepted and the perpetrator is in a position to monitor all user inputs and access all data in transit.

These attacks are highly sophisticated. The threat agent typically starts by leveraging tools that mimic a legitimate wifi access point—for example, a coffee shop's public wifi network. Users that connect to the MitM have unwittingly surrendered credentials, and even if they're working with encrypted data, the perpetrator can trick them into installing a malicious certificate or a different program as a way to decrypt it.

Once the MitM attack is executed, it enables illicit activities, including stealing credentials as users log on. "Session hijacking" also allows the attacker to compromise web sessions by stealing session tokens. Identity is the key to solving these five security challenges. Why? Because it's intrinsic to increasing visibility and control around which users have access to which resources—and to what extent. As such, identity goes a long way towards addressing potential points of vulnerability such as compromised credentials or incorrect provisioning or authentication.

Fight these attacks, with identity-led security

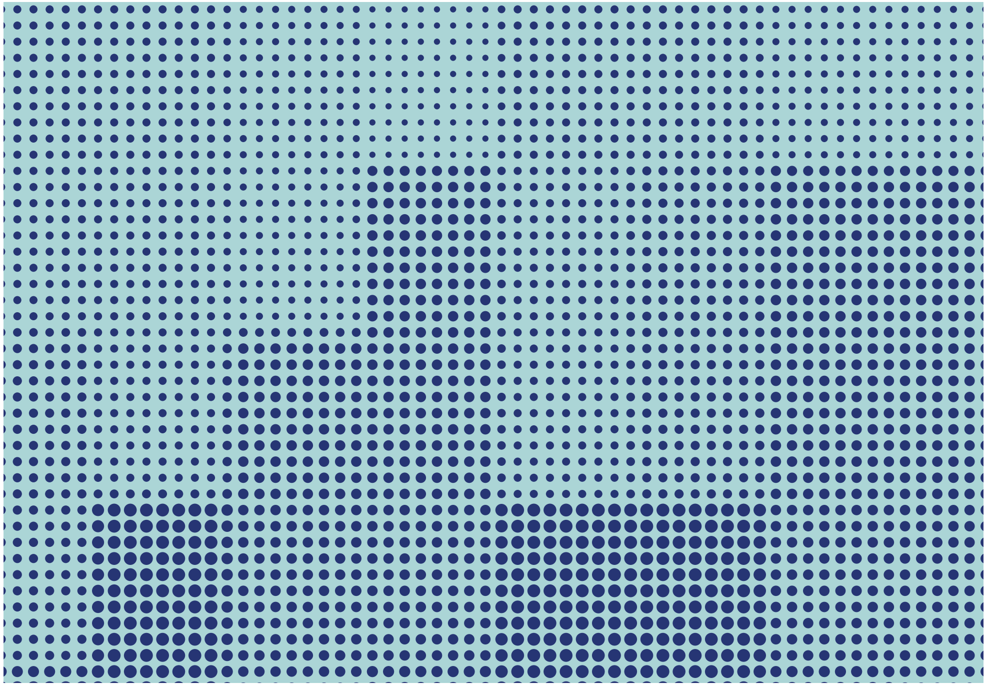
The top cyberattack methods are widespread and sophisticated, but they have a critical shortcoming: since they have to take control of credentials or access points in order to work properly, they can be prevented with a powerful identity solution. That's why identity is not only useful for a modern security stack, but a critical component. In short, identity is (and should be) fundamental to security.

With people at the perimeter, identity solutions can help shape enterprise security models by establishing a central control point across users, devices, and networks. This starts by deploying strong authentication across applications and services, establishing a strong barrier on top of weak or compromised credentials and stopping phishing and brute force attacks in their tracks.

A robust identity platform will also centralize identity and access control with tools like single sign-on, reducing the reliance on weak credentials and instead implementing stronger authentication policies based on federated identities. Centralizing access controls also enables IT and security teams to oversee and unify policies across all applications and servers.

With modern identity, you can also automate provisioning and deprovisioning, ensuring all users have the right level of access to the right resources, at the right time. This goes a long way towards reducing your attack surface and mitigating lateral movement within your systems once a bad actor or malicious internal user gains access to your systems.

Enhanced visibility and response capabilities are another benefit of deploying identity at the core of your security strategy. Context- and risk-based access policies are able to flag unusual activity to security admins so that they can take immediate action, stopping threats such as MitM attacks in their tracks.

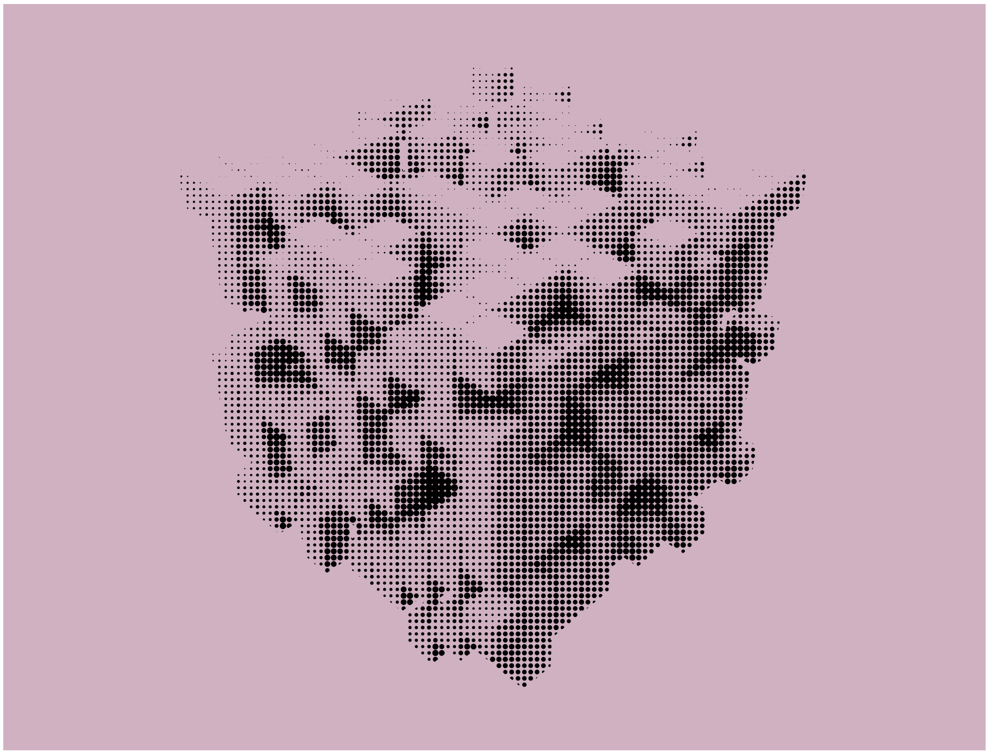


Establish an identity framework with Zero Trust at the core

Placing identity at the center of your security stack is a powerful way to build a Zero Trust security architecture for your organization. The core principle of Zero Trust is to “never trust, always verify,” meaning that all access requests are thoroughly vetted, and all users are considered untrusted until their identities are proven. That allows you to spot potential threats proactively, before they develop into a full-scale data breach, rather than reactively once it’s too late. That’s why identity is the new security control point, and building a Zero Trust architecture is accepted as the best practice for security teams irrespective of industry.

Identity enables Zero Trust by not only strengthening the identity layer behind your login screens, but by ensuring login policies can be centrally managed at scale. That includes automating the identity lifecycle, empowering IT to determine which employees are provisioned to which resources. At the end of the day, it’s about ensuring the right people have the right levels of access to the right apps and tools in the right context. That’s what Zero Trust requires—and it’s what identity allows.

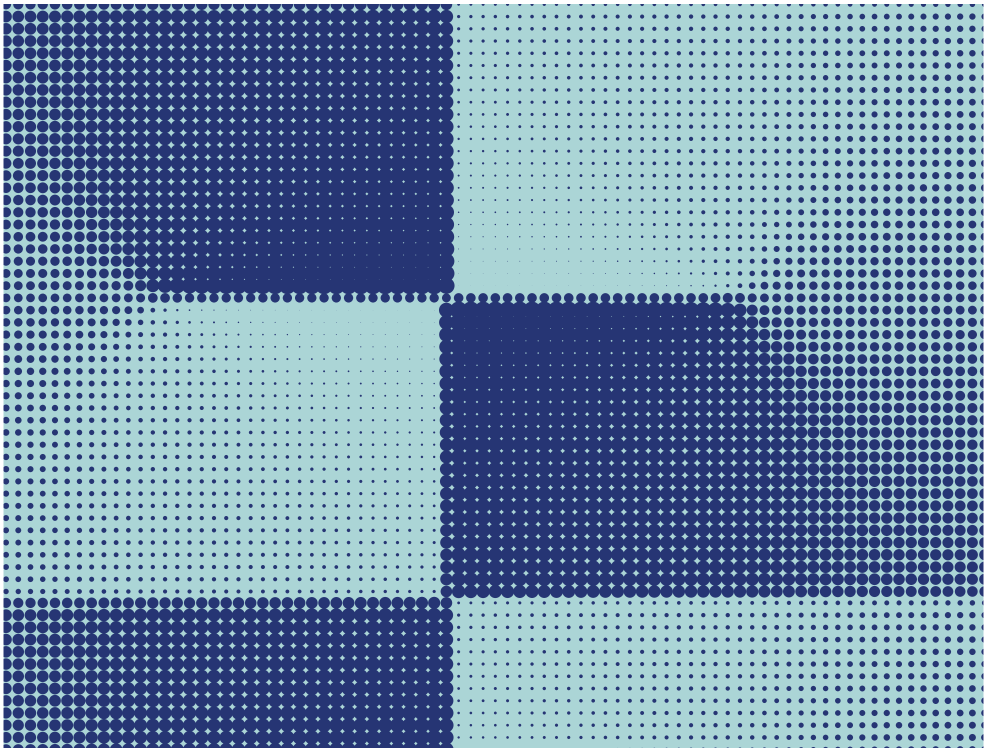
The right security stack is imperative, because it lays the foundations for further innovation and scale. As digital transformation initiatives move forward—reliable, flexible systems must be in place to protect people, data, and resources.



Investing in identity helps solve security challenges

Adopting a robust identity solution covers your access management and user management needs, and ensures you have a comprehensive security layer to keep your organization safe from the most common and damaging cyberattacks. Not to mention, emerging malware continues to focus on stealing credentials, meaning that identity future-proofs your enterprise for the biggest risks today and tomorrow. When laying the foundation of your security strategy, put identity first.

Learn more *about how companies such as FedEx are utilizing Okta's identity solutions as part of their Zero Trust architecture strategy.*



About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 7,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 10,000 organizations, including JetBlue, Nordstrom, Slack, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to https://okta.com