Enhance Security Posture for State and Local Agencies

okta

Index

Introduction

Ransomware attacks on city, state and local governments are the latest cyberthreat to hit the headlines in force. From Atlanta to Baltimore to cities across Florida and Texas, these attacks present a significant and unique challenge for resource-strapped local government entities. While ransomware is hardly a new attack type, it is in fashion in large part because these attacks have proven to be extremely lucrative for attackers if successful.

State and local governments' ability to stop ransomware attacks is likely to continue to be tested until agencies are able to deploy stronger mitigation strategies to block these attackers. And as the cat and mouse game continues, public security professionals also must juggle ransomware mitigation alongside a growing list of threats and limited resources to prioritize protecting against this landscape. Security leaders at government agencies need strategies that help mitigate these common and timely attacks, and fast, to get ahead of threat actors today – as well as for whatever strategies these attackers turn to tomorrow.

The Mind of an Attacker

First put yourself into the mind of a hacker. Hacking is a game of inches: you get one thing, and then you try to get the next, until you reach your target (and/or find something better along the way).

Ideally you're looking for something of value. If you can't get it from one compromised system, then you need to go horizontally across other systems. Can you get login credentials? If so, you can try to log in as another user, getting higher levels of access across each system you compromise. Can you get an unsuspecting user to download something, potentially via phishing? In both cases, you now have a foothold onto the target system.

Once you have an initial foothold, an installed program can make all kinds of chained decisions on what to do next. It does not have to be a simple encrypt and declare victory – it could be part of a broader strategy. Your hacker program could call in reinforcements, download new attack programs, schedule them to run, etc. Your goal might not even be a pure encryption game: that piece could be far down the list, with credit cards and bank account numbers as the first target and encryption as the last thing you schedule to run on your way off the system.

When we take a look at what's actually happening to cause public sector system compromise, we see use of similar patterns:

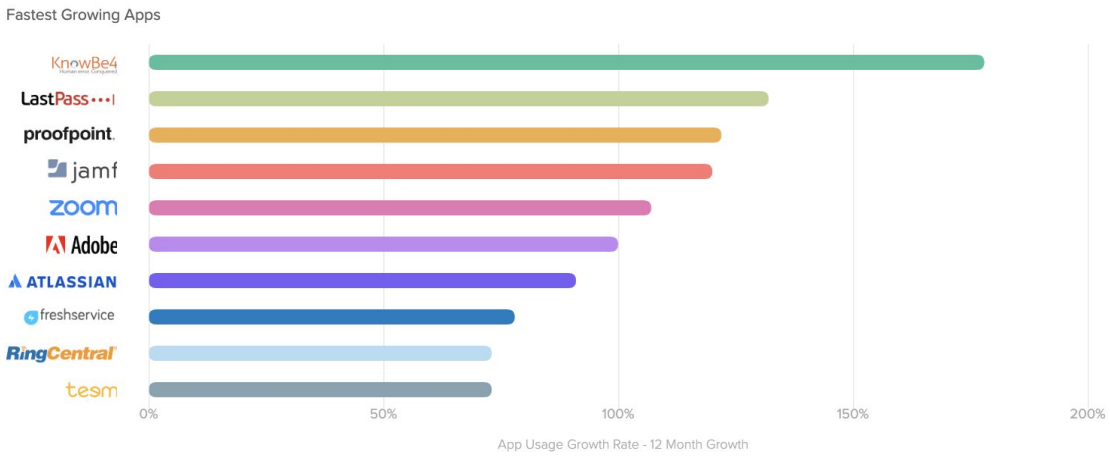
Action	Asset	Count
Social - Phishing	Person - Unknown	155
Social - Phishing	User Dev - Desktop	139
Malware - Backdoor	Person - Unknown	130
Malware - Backdoor	User Dev - Desktop	129
Hacking - Use of backdoor or C2	Person - Unknown	119
Hacking - Use of backdoor or C2	User Dev - Desktop	119
Malware - C2	User Dev - Desktop	100
Malware - C2	Person - Unknown	99
Malware - Spyware/Keylogger	User Dev - Desktop	82
Malware - Spyware/Keylogger	Person - Unknown	81

Table 7
Common threat action and asset combinations within Public breaches, (n=330)

Source: Verizon Data Breach Investigations Report, 2019

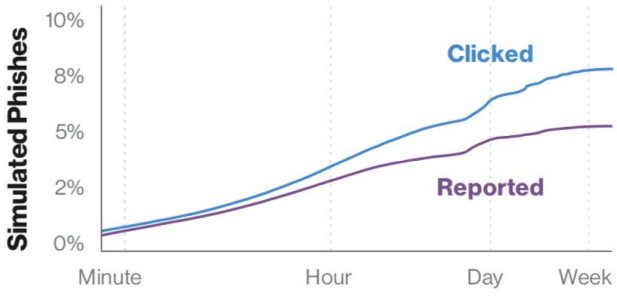
As Verizon puts it, the story from the above table could simply be told as “See Spot Send Malicious Attachments and Gain a Foothold… the familiar phish > backdoor/C2 > use of the newly acquired channel into the network.” While Verizon doesn’t have as much data as to explain what is happening beyond the initial compromise, the report notes that the “inclusion of keylogging malware is a good indicator that additional credential theft and reuse is a likely next step” – and with the use of stolen credentials and phishing as the top two causes of breaches across industries in 2019, it’s unsurprising to see the impact that successful people-oriented attacks can have across the attack chain.

It’s something many organizations are aware of as well: user-focused security apps dominated the fastest growing enterprise apps used by Okta customers in 2018, with KnowBe4, LastPass, and Proofpoint in the top three spots.



Source: Okta Businesses at Work, 2019

KnowBe4’s rapid growth may be due to its fulfillment of a clear market need, yet Okta found only 49% of knowledge workers across industries have ever participated in cybersecurity training at work (Okta Business @ Work 2019). And when we look more closely at phishing simulations in the public sector, a gap still remains in user behavior: the right chart from Verizon’s DBIR 2019 shows how quickly employees in this sector are clicking or reporting on phishing emails:



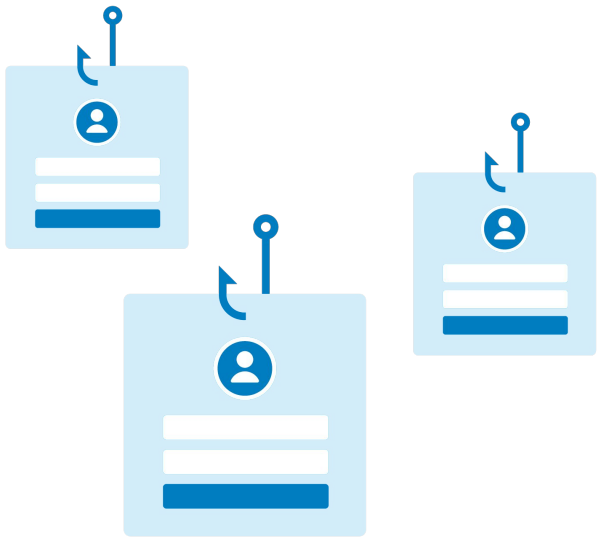
Click, reporting rate in public simulated phishes over time

Source: Verizon Data Breach Investigations Report, 2019

> Early on in the training similar percentages of users are clicking and reporting, but reporting drops off after the first hour, where clicking is more active. Not optimal, but since this was sanctioned and not actually malicious, nothing was done after the initial reporting other than an ‘atta boy.’

Breaking Down the 5 Most Common Identity Attacks

There are a number of vendors who tackle ransomware deployment mitigation specifically, as well as vendors that can help automate backup and recovery of data files. The user piece can be trickier, because it in part puts the dependence on (many) other people to maintain your system security – including teaching them not to click on the link that downloads ransomware onto their machine or hands over their credentials to an attacker. Easier said than done.



Let's look more closely at the top user-oriented attacks:

Attack #1: Broad-based phishing campaigns

Why are phishing campaigns such a popular method of attack? Simply put, the numbers are in the attacker's favor.

A broad-based phishing campaign recognizes that threat agents have to gain access to only a few accounts or one admin account to compromise the organization. Yet with just a light touch of social engineering and a list of email addresses, phishing attacks can successfully compromise 1 out of 20 employees from even a well-trained organization.

Credential theft from phishing is often the first stage of the cyber kill chain. According to the Verizon 2017 Data Breach Investigations Report, 81% of breaches used stolen and/or weak credentials.

Anatomy of the attack

- Attacker acquires a list of emails or phone numbers and designs a generic call to action that's relevant for that list (such as a fake Google login page).
- The phishing message is broadly distributed, and the attacker waits to see which credentials are collected.
- The attacker uses stolen credentials to access the data they are after or adopts that identity for a more targeted attack on a high-value employee.

Attack #2: Spear phishing campaigns

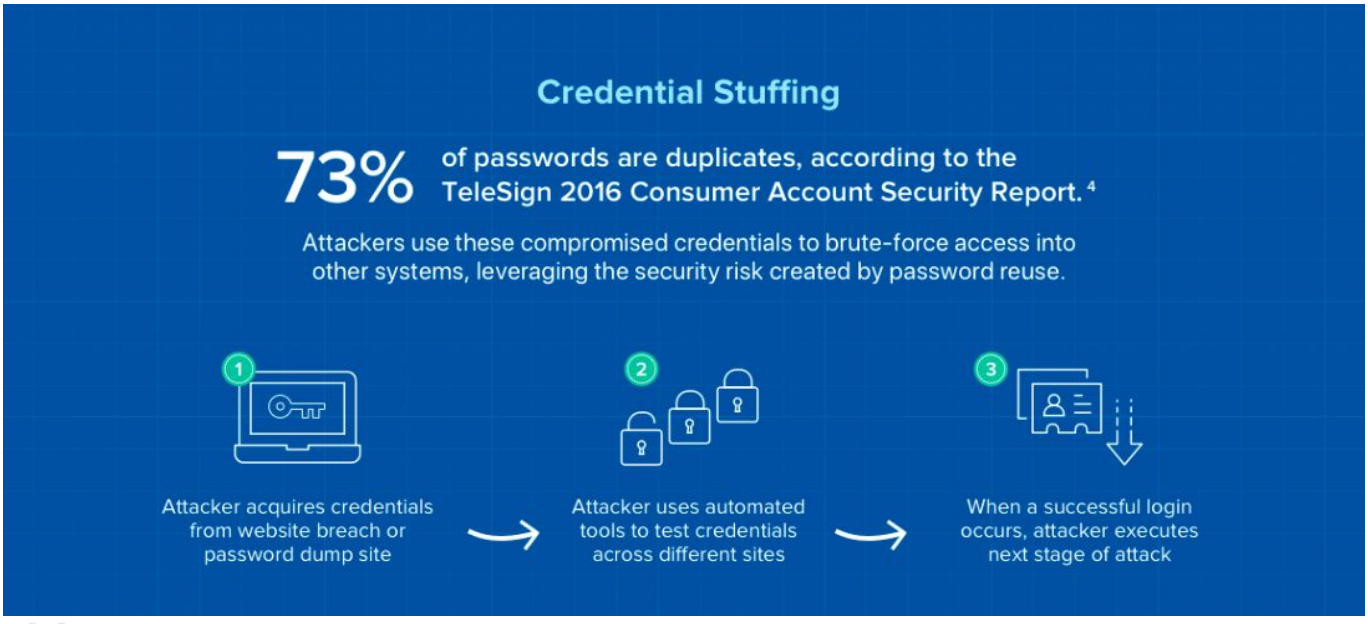
Spear phishing is a targeted form of phishing that often involves more research designing the target list and phishing message. As opposed to broad-based campaigns, spear phishing typically focuses on a small number of employees to evade automated filters. The level of social engineering is also more sophisticated, with messages being more personal and the malicious call-to-action playing on emotions such as curiosity, fear, or rewards.

Anatomy of the attack

- Attacker picks targets carefully, doing extensive research across available resources such as social media or web presence.
- Attacker crafts a phishing message designed to appear legitimate, such as pretending to be a colleague and referencing a topical situation, such as a recent company party that the attacker learned of online.
- The victim is compelled to enter credentials by appealing to his or her emotions, such as a curiosity to see photos from the party behind a fake login page.
- The attacker uses the credentials from the high-value target to access sensitive data or execute the next stage of their attack.

Attack #3: Credential stuffing

Credential stuffing is a form of brute force attack that takes advantage of our struggle to select unique passwords across our various accounts. This is hardly surprising when you consider that the average American internet user has 150 online accounts requiring a password. Yet many of us have had account credentials compromised as part of a data breach (have you checked yours recently?)



Attackers leveraging credential stuffing will use these compromised credentials on several other websites to test if the login details are re-used. And they often are: 73% of passwords are duplicates, according to the TeleSign 2016 Consumer Account Security Report.

These types of attacks can be done at scale by bots, leading to a higher likelihood of these attacks affecting your organization.

According to a recent report from Akamai, “more than 40% of global log-in attempts are malicious thanks to bot-driven credential stuffing attacks”.

Anatomy of the attack

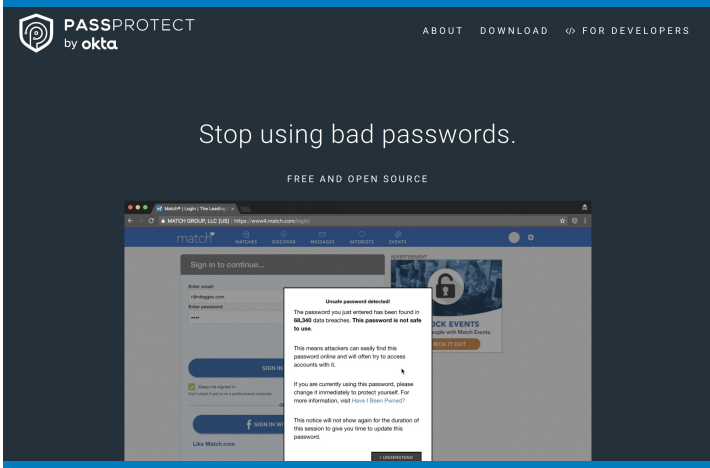
- Attacker acquires credentials from a website breach or password dump site.
- Automated tools are used to test credentials across a variety of different sites.
- When a successful login occurs, attacker harvests the sensitive data or executes the next stage of their breach.

Attack #4: Password spraying

Password spraying is another form of brute force attack whereby an attacker takes advantage of our tendency to rely on common passwords such as “password1” (which according to Pwned Passwords has appeared in a data breach over 2.3 million times).

Anatomy of the attack

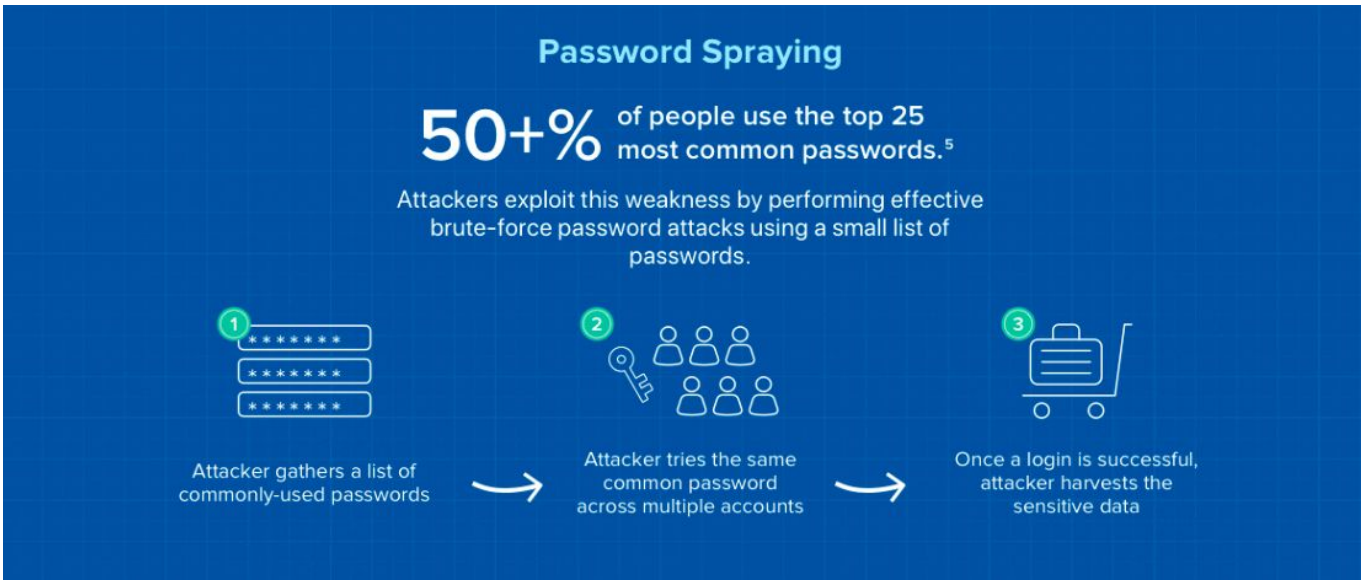
- Attacker uses a small list of commonly-used passwords that match the complexity policy of the domain.
- Instead of trying multiple passwords for one user, the attacker uses the same common password across many different accounts which helps avoid detection.



Do your credentials pass the test?

Okta created PassProtect in 2018 as a free, publicly available Chrome browser plugin that makes it easy for anyone to discover in real-time if a password they’re using has been exposed in a data breach. With a real-time notification, PassProtect quickly alerts users of unsafe passwords on any site, in the moment so they can take immediate action – without compromising privacy.

By using k-anonymity, PassProtect ensures no passwords are ever seen, stored, or sent over the network during the checking process.PassProtect is powered by Have I Been Pwned? and is free, open source and secure.



Anatomy of the attack (con't)

- Once the attacker encounters a successful login, the attacker harvests the sensitive data or executes the next stage of their breach.

Attack #5: Man-in-the-Middle (MitM) attacks

A man-in-the-middle attack on an organization is a highly targeted attack that can result in a full take of credentials and data-in-transit if executed correctly. After intercepting a network connection, an attacker can also take advantage of "session hijacking" that compromises the web session by stealing the session token.

Anatomy of the attack

- Attacker intercepts a network connection, often by leveraging tools to mimic a legitimate wifi access point (such as Starbucks Wifi).
- If data is encrypted, attacker may attempt to decrypt data by tricking the user into installing a malicious certificate or other technique.
- If attack is successful before the initial authentication, the credentials may be stolen as the attacker is monitoring all the user inputs.
- Alternatively, the attacker steals the session token and is able to authenticate into the account and execute the next stage of their breach.

Mitigation Strategies

Okta has built security features directly into our solutions to help customers combat identity-based attacks. Our solutions like Adaptive Multi-factor Authentication and Lifecycle Management help solve security challenges like mitigating the risk of phished credentials, including phishing reverse proxies, and reducing the attack surface area, while solutions like Advanced Server Access and API Access Management extend Okta's strong authentication across applications and down to other critical parts of an agency's infrastructure, namely servers and APIs, respectively.

Risk-Based Multi-Factor Authentication: Security + Usability

Multi-factor authentication is a broad solution that can help prevent credential compromise across the attack types highlighted in the previous section. While it won't be able to stop a user from clicking on the malicious link, it will prevent an attacker who may have compromised credentials from being able to use those credentials as a foothold into your system – requiring an additional burden of proof separate from a username/password before granting access into the system.

WIth Okta, organizations can leverage login context like device, location, and user biometrics to take dynamic actions based on risk level. This means step-up authentication can be automatically implemented in scenarios that have been identified as atypical for a particular user, reducing the burden on admins to create and manage complex policies. Through machine learning, Okta can also refine login context, continually improving security as well as user experience.

Extending Strong Authentication Beyond Applications: Advanced Server Access + API Access Management

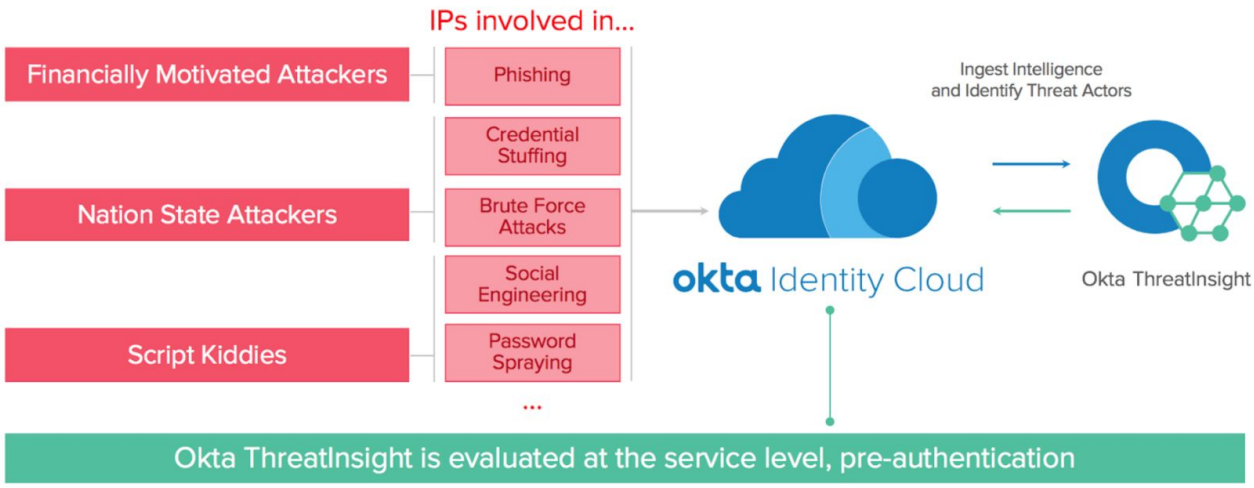
There are many layers of technology that security needs to protect in order to prevent today's threat actors from gaining access, from applications to servers to even APIs. In fact, in their December 2017 report "How to Build an Effective API Security Strategy," Gartner analysts Mark O'Neill, Dionisio Zumerle, and Jeremy D'Hoinne predicted that "[b]y 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise web applications." Agency security teams need to ensure that they're taking steps to build in additional protections across all areas of their infrastructure to limit entry points as well as to minimize potential movement if an attacker does gain a foothold into a system.

By extending the same strong authentication to APIs and infrastructure with Okta API Access Management and Advanced Server Access, respectively, Okta enables IT and security teams to place stronger policies and controls around these core technologies – limiting access and applying additional layers of security to help strengthen the overall posture of a government agency.

Okta ThreatInsight: Leveraging Network Effects

Agencies can further benefit from insights gathered from the Okta Integration Network to block suspicious login attempts at their agency.

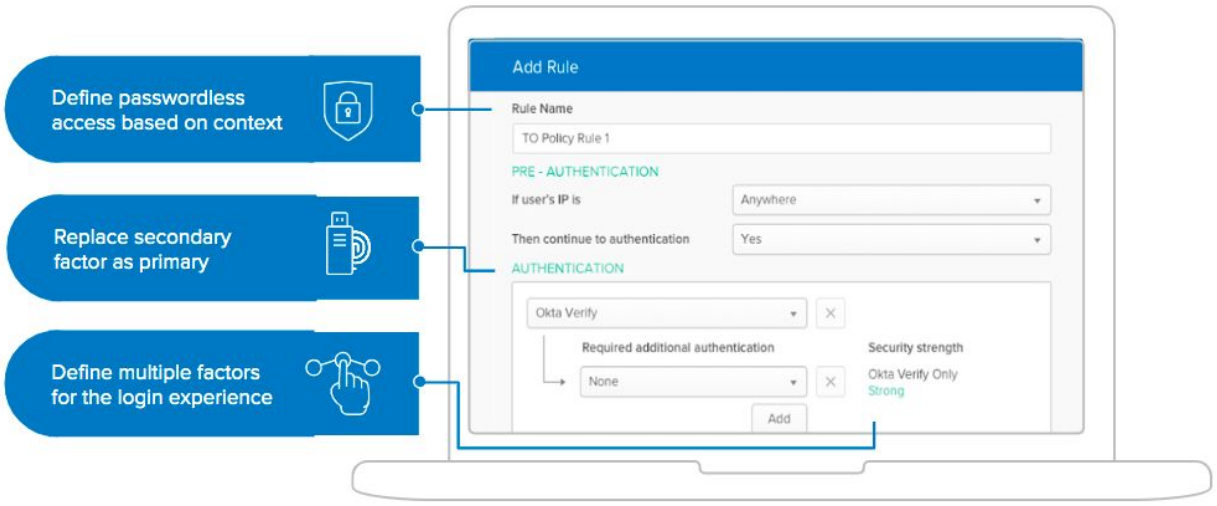
Okta's network effects can help prevent threat actors from compromising user accounts while also mitigating account lockout at the pre-auth level. More specifically with Okta ThreatInsight, agencies can leverage threat intel generated by Okta's security program and take action by applying step-up authentication in ambiguous cases. This allows organizations to benefit from network effects and intel that an individual organizations do not have visibility into.



Going Passwordless: Security that Also Improves the End User Experience

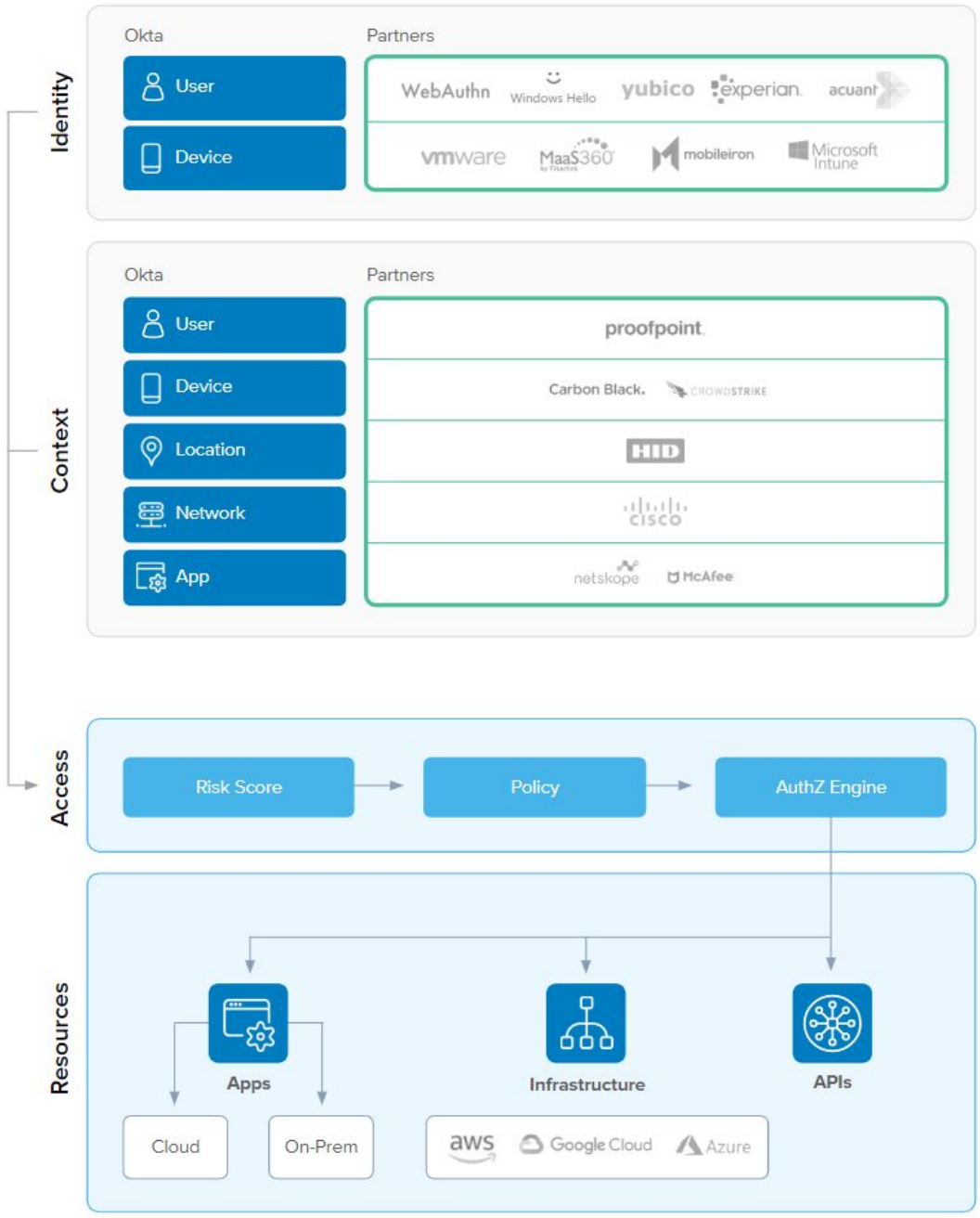
Account lockouts are one of the consequences IT and security teams must grapple with from authentication attacks. As many organizations implement temporary account lockouts when an account has exceeded a set number of failed login attempts, identity attacks can result in DoS-like results with end users unable to access resources. Pre-authentication sign-on policies, factor sequencing, and passwordless authentication can be an effective countermeasure to prevent these attacks and lockouts.

With Okta Modern Passwordless, because there is no password involved at all, there's even less chances for account lockouts from failed login attempts since attackers would be incapable of using credential stuffing or password spraying as the primary (or only) factor presented to the user would be a higher assurance ‘something you have’ (i.e. a hard token) or ‘something you are’ (i.e. biometrics). You can also layer on Okta contextual access policies so that you can specify factor, sequence, and when to prompt based on risk signals like user, app, device, and location.



Integrating Identity Across Your Security Stack

As a part of a holistic Zero Trust security strategy, Okta also works closely with other vendors across the security stack to help agency leaders build strong identity and access security controls into their holistic security programs:



Zero Trust Reference Architecture

Zero Trust Reference Architecture

1. **Identity**
   Okta leverages insights both into the user and device identity as a first step to identity-driven Zero Trust security, including additional context from partners such as identity proofing providers like Experian and Acuant or MDM/UEM leaders like VMware, MobileIron or Microsoft Intune.

2. **Context**
   Okta then pulls in context for the specific authentication attempt across categories to detect and identify potential anomalies. For example, Okta can take in context such as device posture, geolocation, network IP or even context on the targeted resource itself (i.e. is this a sensitive app/system the user is attempting to authenticate into?) and feed that insight into its risk engine.

3. **Access**
   Okta's machine learning-powered risk engine then evaluates across this context to see if there are any anomalies in the user's typical authentication patterns. An agency can then set policies to step up authentication should any inconsistencies arise. If the user successfully completes the second factor, Okta can authorize access into the target resource, such as a cloud or on-prem app, or into infrastructure.

4. **Analytics and Orchestration**
   Okta also can tie this contextual and authentication insight into a SIEM or a SOAR to further evaluate and take action should any anomalies arise throughout the authentication and authorization process.

Okta Integrations for Additional Phishing Protection

In addition to vendors across endpoint, network, and data protection, Okta also partners closely with security vendors such as Proofpoint for additional phishing protection. The Okta and Proofpoint integration, for example, leverages insights from Proofpoint's Targeted Attack Protection (TAP) so organizations can take action on very attacked users (VAPs) and those users that have potentially clicked on a phishing link (Threat Response Auto-Pull or 'TRAP'). Users identified as VAP or TRAP are automatically grouped in Okta so administrators can set stronger access policies or limit app access until the threat is mitigated.

Taking Action Today

There is no silver bullet when it comes to modern cybersecurity. Security executives must constantly work to stay ahead of attackers, mitigating both today's latest threat trends as well as stopping those consistent attacks such as credential harvesting.

For state and local governments, the priorities are clear: there's a reason that security and risk management and identity and access management bookend the list of State CIO's 2019 Strategies, Management & Process Solutions priorities (NASCIO State CIO Top 10 Priorities, 2019). By focusing on protecting people, and their identities, agencies can take immediate action to mitigate some of the most prevalent and impactful threats against their ecosystems.

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 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,550 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, visit us at www.okta.com or follow us on www.okta.com/blog.