



iIDENTITY DAYS

okta

Preventing Identity Phishing Attacks

Webinar Phishing Resistant MFA & Passwordless



Nicolas Milosavljevic
Senior Solution Engineer, Okta

Safe harbor

This presentation contains “forward-looking statements” within the meaning of the “safe harbor” provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, long-term financial targets, product development, business strategy and plans, market trends and market size, opportunities, positioning and expected benefits that will be derived from the acquisition of Auth0, Inc. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as “expect,” “anticipate,” “should,” “believe,” “hope,” “target,” “project,” “goals,” “estimate,” “potential,” “predict,” “may,” “will,” “might,” “could,” “intend,” “shall” and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, the market for our products may develop more slowly than expected or than it has in the past; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; we may fail to successfully integrate any new business, including Auth0, Inc.; we may fail to realize anticipated benefits of any combined operations with Auth0, Inc.; we may experience unanticipated costs of integrating Auth0, Inc.; the potential impact of the acquisition on relationships with third parties, including employees, customers, partners and competitors; we may be unable to retain key personnel;

global economic conditions could worsen; a network or data security incident that allows unauthorized access to our network or data or our customers’ data could damage our reputation and cause us to incur significant costs; we could experience interruptions or performance problems associated with our technology, including a service outage; the impact of COVID-19 and variants of concern, related public health measures and any associated economic downturn on our business and results of operations may be more than we expect; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any unreleased products, features or functionality referenced in this presentation are not currently available and may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.



Agenda

01 Phishing attacks – Why, What and How?

02 How Can Okta Help?

03 Investments and Key Takeaways



01

The why, what and how of phishing attacks



NIS 2 – Effective at end of CY24

Fines for non-compliance with the NIS Directive can be severe, ranging from a maximum amount of at least 10 million euros or 2% (for essential entities) to a maximum amount of at least 7 million or 1.4% (for significant entities) of the company's total global annual revenue for the preceding financial year, whichever is greater.

The first and most crucial step is to implement multi-factor authentication to secure all accounts, in lieu of passwords. Given the sophistication of modern day cyberattacks and the cyber arsenal available at an attacker's fingertips, the reliance on passwords as a reliable form of defense must end.




Not all authenticators provide the same level of protection


Knowledge
"something you know"

Possession
"something you have"


Inherence
"something you are"




Password




Security Question




SMS, Voice, Email OTP




OTP with Push




Physical Token OTP



PIV / CAC +Biometric



FIDO2 WebAuthn



Okta FastPass



Low Assurance

High Assurance



Phishing is on the rise

61%

Increase in phishing attacks (5/1/21-4/30/22)

Source: Phishing Landscape 2022: An Annual Study of the Scope and Distribution of Phishing

1M+

Total phishing attacks in Q1 2022

Source: PHISHING ACTIVITY TRENDS REPORT, 1st Quarter 2022

Phishing Reaches All-Time High in Early 2022

Phishing Attacks, 2Q2021 - 1Q2022



Source: APWG Phishing Activity Trends Report



Phishing Attack Vectors

Identity Attacks



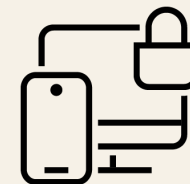
Identity

- Credentials Stuffing
- Email Phishing
- Phone / SMS Phishing
- OTP Interception Bots
- Adversary/Man in the Middle Attack
- MFA Push Fatigue Attack
- OAuth Consent Phishing

Prevent Phishing Attacks:

Okta's Phishing Resistant Authenticators and Access Policies protect against Identity phishing attacks.

Endpoint Attacks



Device / Browser

- Malware
- Ransomware

Network

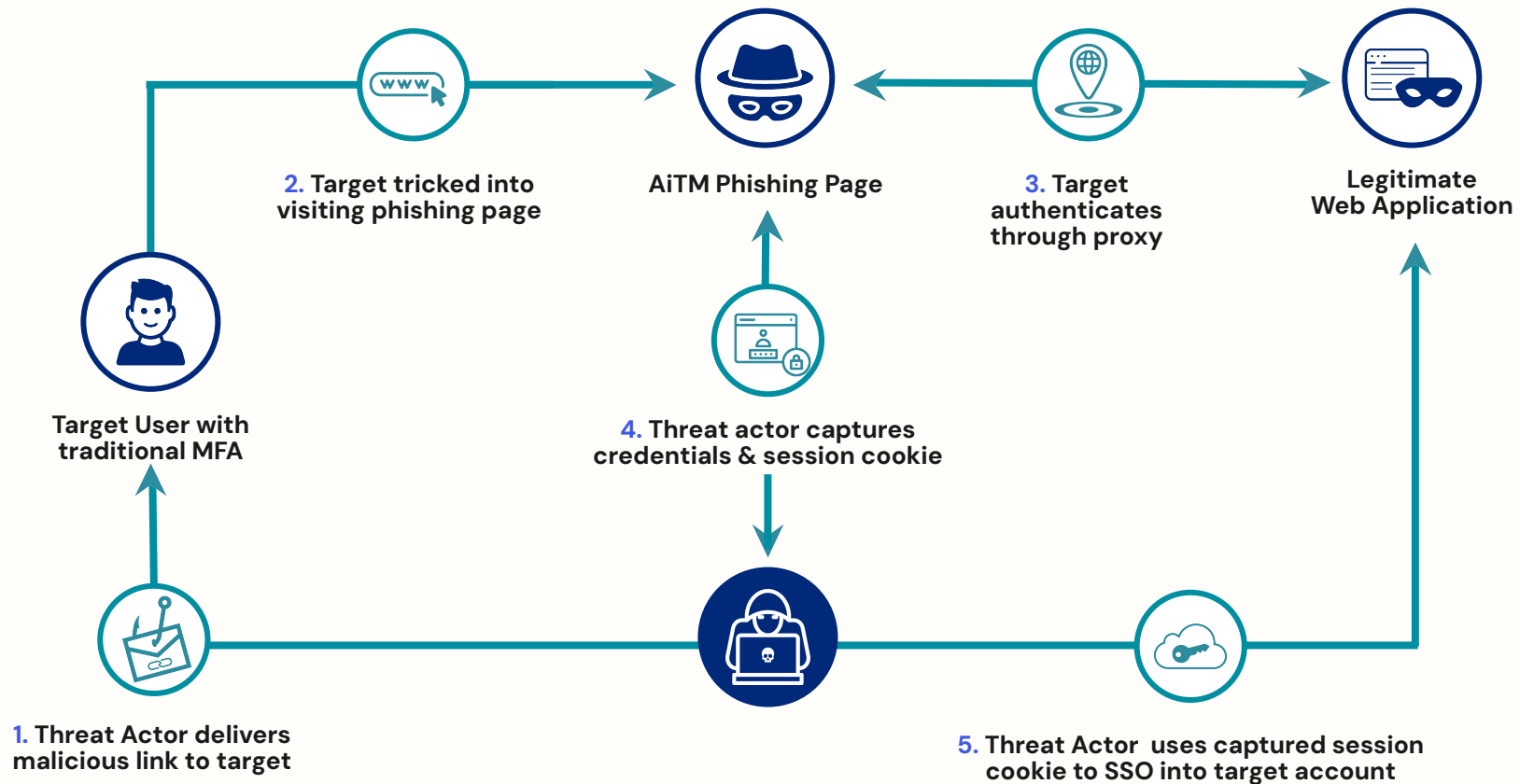
- DNS Hijacking
- Insecure Networks
- Stolen Session Hijacking

Minimize Phishing Surface:

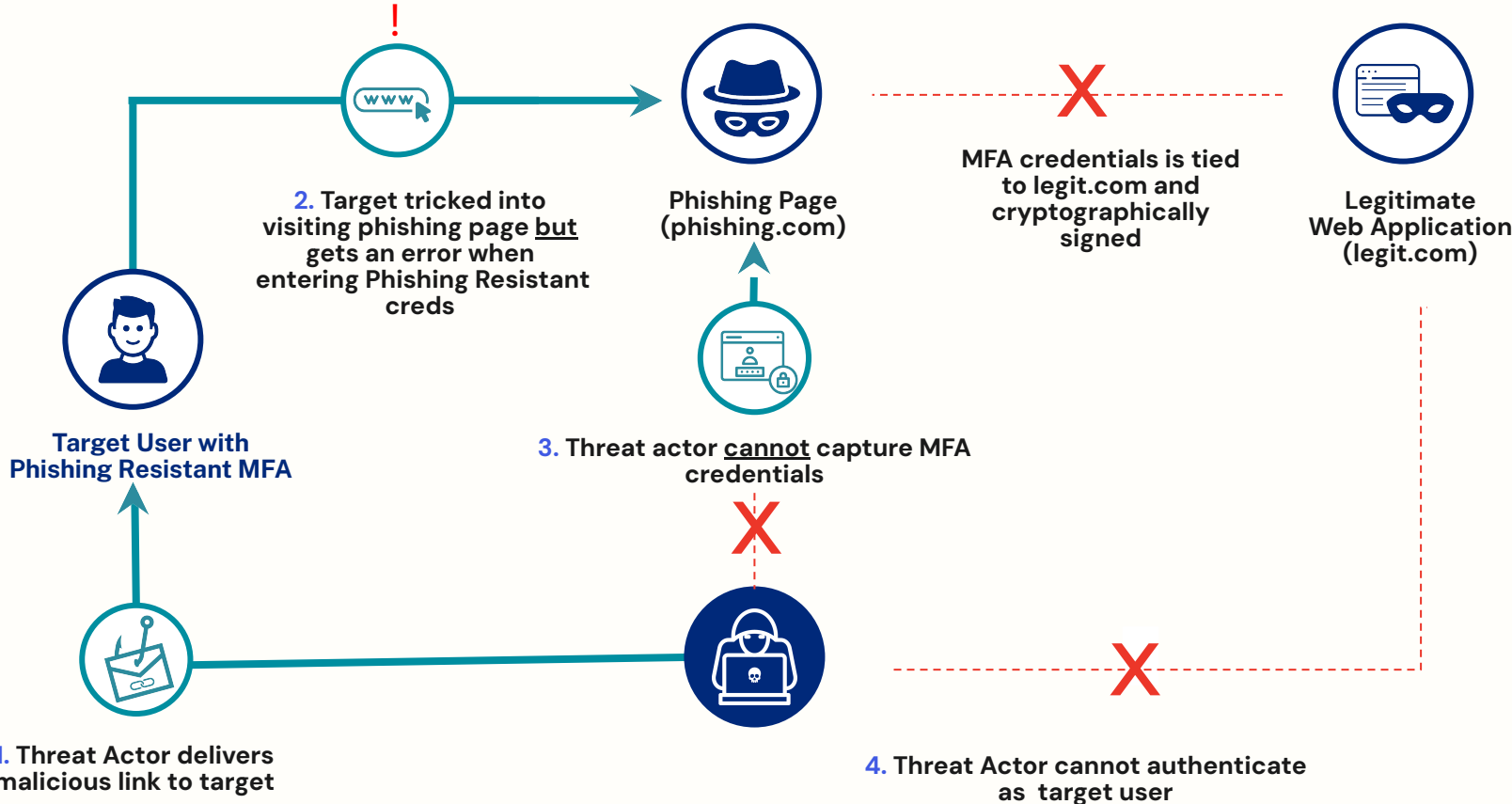
Okta's Third Party Integrations, Device Signals and AMFA Policies can help detect and minimize attacks.



Phishing Attack with MFA Bypass: AiTM* Phishing Proxy



Phishing Attack **Blocked** with Phishing Resistant MFA



How does Phishing resistant authenticator work?

3 major properties



No Shared Secrets

A credential keypair is cryptographically signed and private key is stored in the Hardware Security Module



Origin Bound

A credential keypair is tied to a specific domain mitigating the threat of phishing



Trusted

Authenticator attestation helps verify the public key is from a trusted authenticator



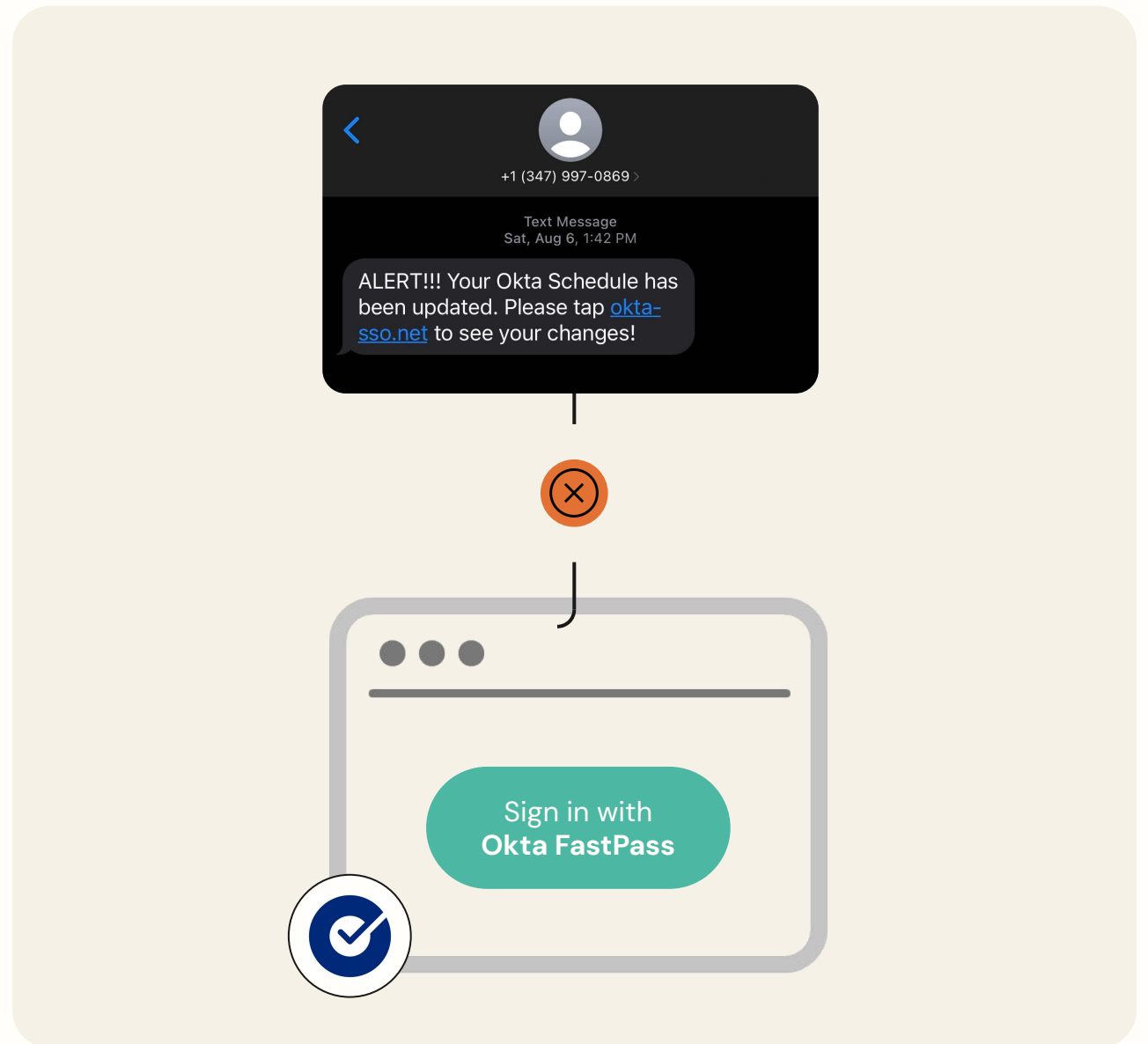
Advanced phishing resistance for Okta FastPass

What is it?

Ensures authentication requests are coming from the correct server.

Benefits

Ensures stolen keys cannot be used to access Okta protected sites and apps.



Why Okta FastPass



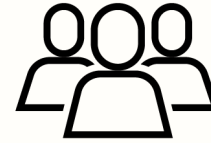
Secure passwordless login to resources

Passwordless authentication to any SAML, OIDC, or WS-Fed app in Okta. Can be coupled with your choice of device management tool.



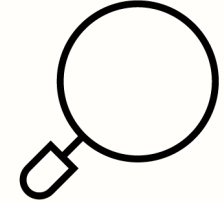
Enforcement of phishing resistant authentication flows

FastPass is phishing-resistant for managed and unmanaged Windows, iOS, Android, and macOS devices.



Consistent user experience across platforms and devices

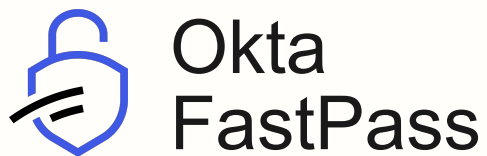
Support and secure a heterogeneous mix of devices, and improve user productivity by reducing user friction at access touchpoints.



Device context to ensure the security of the devices in use

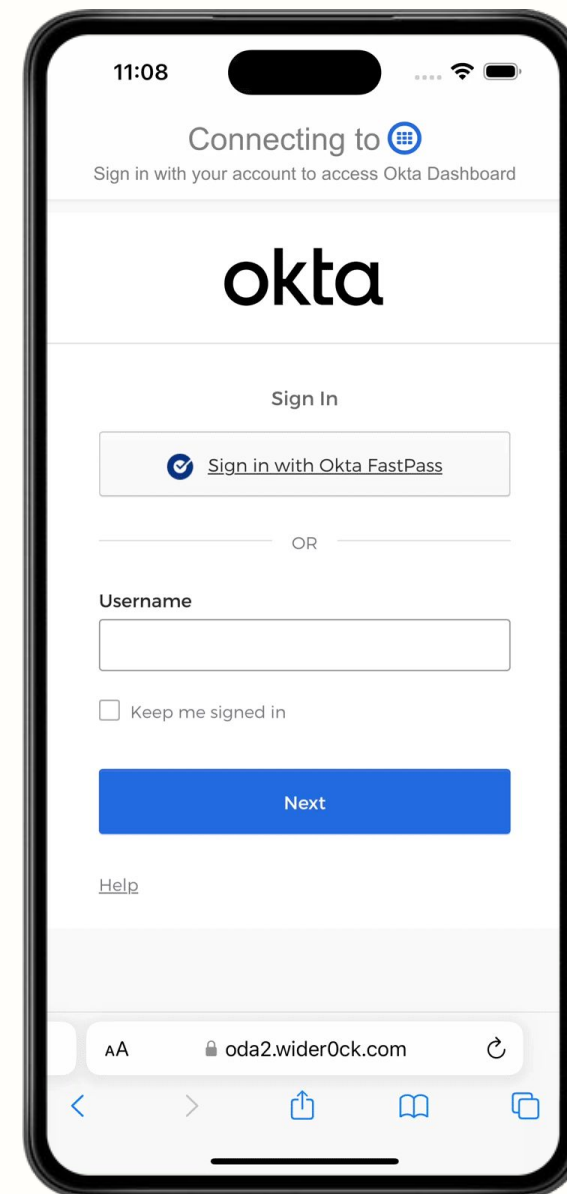
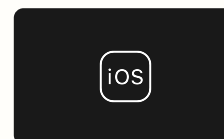
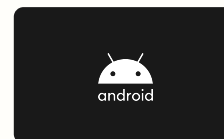
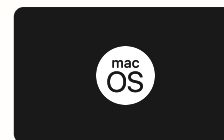
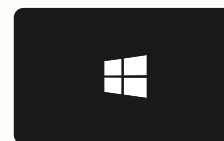
Amplify the security of your devices with device signals for risk aware authentication policies.





Advanced phishing resistance across **any** device and **all** major operating systems.

- ✓ MANAGED DEVICES
- ✓ UNMANAGED DEVICES



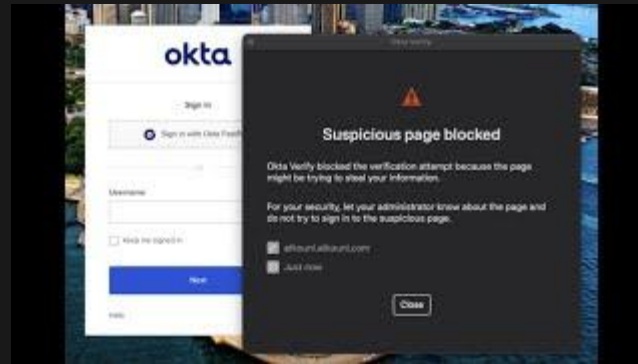
02

How can Okta help?



Demo

Setting up Phishing
Resistant Authenticators
and Policies with Okta



What Okta Offers – Defense in Depth



First line of defense – **Policies**

- Sign on Policies: Manage and restrict access

Second line of defense – **Authenticators**

- Passwordless
- Phishing Resistant Authenticators

Third line of defense – **Contextual Access**

- Device (MDM & EDR) Signals
- Device Assurance checks
- Location / Network Zones, ThreatInsight
- Risk Signals, Behaviour Detection

Fourth line of defense – **Observability**

- Logging, Reporting and Auditing
- Security Workflow Templates



Contextual Authentication Policies

Name	Behavior type	Details	
New City	Location	Location granularity	City
		Evaluate against past	20 authentications
New Country	Location	Location granularity	Country
		Evaluate against past	10 authentications
New Device	Device	Evaluate against past	20 authentications
New Geo-Location	Location	Location granularity	Latitude - Longitude
		Evaluate against past	20 authentications
		Radius from location	20 kilometers
New IP	IP	Evaluate against past	50 authentications
New State	Location	Location granularity	State or Region
		Evaluate against past	15 authentications
Velocity	Velocity	Velocity	805 Km/h

Network Zones

Restrict access to critical apps and data by IP or Dynamic Zones

Behavior Detection

Machine Learning based pattern recognition

Risk Detection

Device Assurance

Unmanaged Device Checks

Re-authentication frequency

AND Re-authentication frequency is

- Every sign-in attempt
- Never re-authenticate if the session is active
- Re-authenticate after:

Re-authentication

Re-authenticate the user at every sign-in attempt

AND Possession factor constraints are

- Phishing resistant
- Hardware protected
- Exclude phone and email authenticators

Authenticators

Enforce phishing resistant flows for access to sensitive apps



Choosing Phishing Resistant Authenticators

Admin Setup

THEN

THEN Access is

- Denied
 Allowed after successful authentication

AND User must authenticate with

Possession factor

AND Possession factor constraints are

- Phishing resistant
 Hardware protected
 Exclude phone and email authenticators

AND If Okta FastPass is used

- The user must approve a prompt in Okta Verify or provide biometrics
 The user is not required to approve a prompt in Okta Verify or provide biometrics

Your org's authenticators that satisfy this requirement:

1 factor type

Okta Verify³ or FIDO2 (WebAuthn)³

³ Phishing resistance may vary based on combinations of apps, browser, operating system, and more. [Learn more.](#)

End User View

okta

Verify it's you with a security method

@ john.smith@atko.com

Select from the following options



Use Okta FastPass
Okta Verify

Select



Security Key or Biometric
Authenticator

Select

[Back to sign in](#)



Phishing Resistant Authenticators at Okta

Choose based on your deployment needs

	FIDO2 WebAuthn Roaming Security Key	Okta Fastpass	FIDO2 WebAuthn Platform Authenticator	Passkey Multi Device FIDO2 Credentials	PIV Smart Card
Phishing Resistant	✔	✔ deployment dependent	✔	✔	✔
Hardware Protected (TPM/Secure Enclave)	✔ authenticator dependent	✔ system dependent	✔ authenticator dependent	✘	✔
Authenticator Bound	✔	✔	✔	✘	✔
Browser / OS Support	✔	✔	✔	Platform dependent	Limited mobile support
Self Service Enroll & Recovery	✔	✔	✔	✔	✘
Deployability	Additional Hardware	✔	✔	✔	Additional Hardware



Monitoring for Possible Account Takeover Attempts

“When this happens”
Event

“If this”
Function

“Do this”
Action

“Do that”
Action

“Do that”
Action

1



MFA Authenticator Reset followed by MFA Activation



Check if event performed by the actual user

okta

Clear User Sessions
Put user in a temporary monitoring group



Log event in a monitoring table



Send Alert with event details

2



Run this flow every 24 hrs

okta

If user's monitoring period expired, remove from group



Clean up the monitoring table



03

Investment and Key Takeaways



Key Takeaways



Go passwordless

Adopt phishing resistant authenticators



Set authentication policies

Leverage device, behavioral and network signals



Enforce observability

Deploy security orchestration





Thank You!





Q&A



Nicolas Milosavljevic

Senior Solution Engineer, Okta

nicolas.milosavljevic@okta.com