Zero Trust Maturity Across the Federal Government

"Never trust; always verify," is emerging as the new slogan for information security in a cloud-based world. At its core is Zero Trust – the idea that access to agency resources should be restricted until the user has proven their identity and access permissions, and the device has passed a security profile check. Are Federal agencies migrating to a Zero Trust mindset?*

Laying the Foundation

While **only one out of three** Federal agencies have an active Zero Trust initiative …

93% of agencies have implemented at least one security solution that maps to a modern Zero Trust strategy
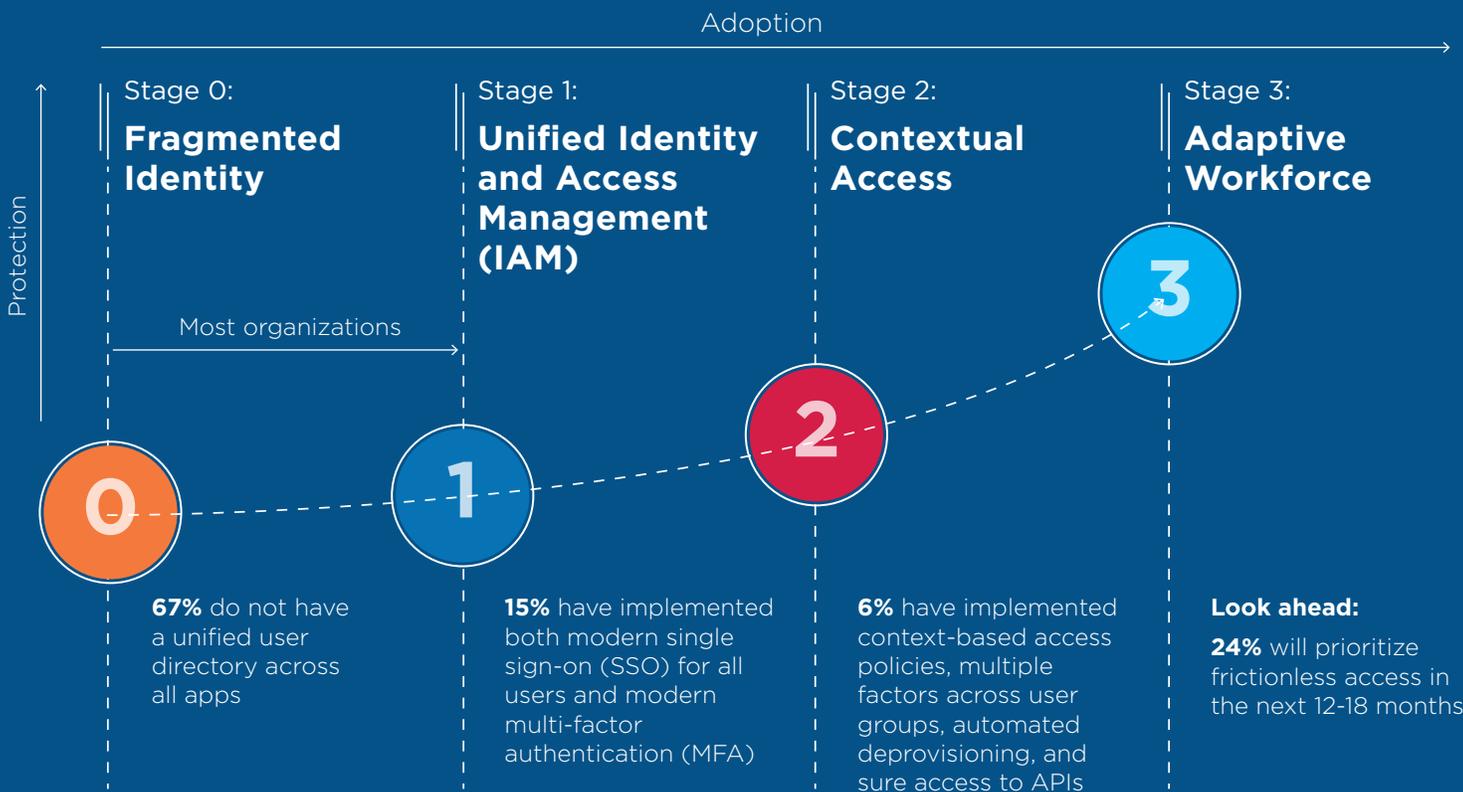
93%

Agencies continue to forge ahead because the notional ideas of Zero Trust are critical to securing today's perimeter-less landscape.

Adoption Curve

Okta developed a Zero Trust Maturity Curve to help organizations identify where they are today and what their next steps should be. Where do Feds stand?
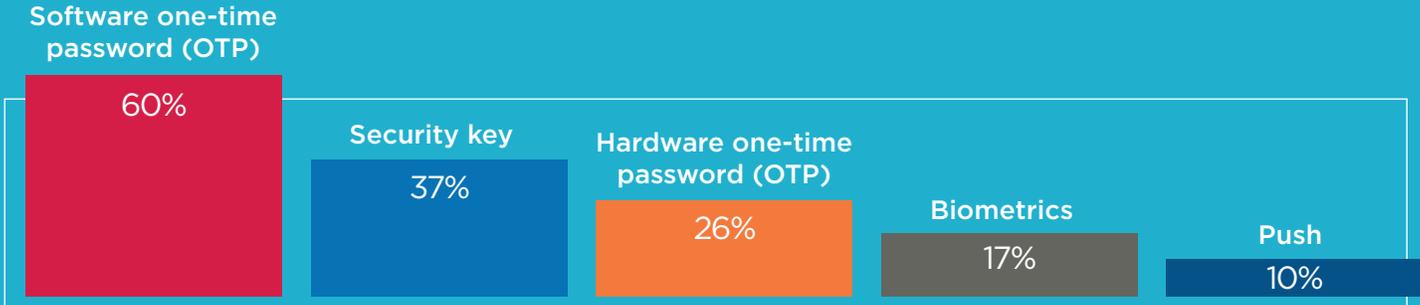
Adoption

Protection

Stage 0:
Fragmented Identity

Stage 1:
Unified Identity and Access Management (IAM)

Stage 2:
Contextual Access

Stage 3:
Adaptive Workforce

Most organizations

0

1

2

3

67% do not have a unified user directory across all apps

15% have implemented both modern single sign-on (SSO) for all users and modern multi-factor authentication (MFA)

6% have implemented context-based access policies, multiple factors across user groups, automated deprovisioning, and sure access to APIs

Look ahead:

24% will prioritize frictionless access in the next 12-18 months

Work-in-Progress

Feds have already implemented or will prioritize **automated provisioning** over the next 12-18 months, both for..

Employees

41%	36%
Complete	Planned

Partners/Contractors

33%	37%
Complete	Planned

While passwords and smartcards (PIV/CAC) still dominate the **MFA landscape at 71%**, agencies are beginning to incorporate other higher assurance factors such as:

Software one-time password (OTP) 60%	Security key 37%	Hardware one-time password (OTP) 26%	Biometrics 17%	Push 10%

2020 Vision

The Zero Trust journey starts with identity – ensuring the right people have access to the right resources at the right time. But there is no silver bullet to Zero Trust, which is why Feds will also integrate other parts of their security stack into their IAM solutions:

44% Cloud access security brokers (CASBs)

37% Orchestration

30% Automation

The Value of 'Zero'

Feds believe Zero Trust can **support their cyber efforts** by:

#1 Reducing the attack surface (57%)

#2 Decreasing cyber incidents (54%)

#3 Increasing workforce productivity (45%)

Okta's Zero Trust solutions help Federal agencies fortify their cybersecurity posture.

To learn more, visit:
okta.com/getting-started-with-zero-trust

*Based on survey of 115 Federal cyber security executives and IT decision makers