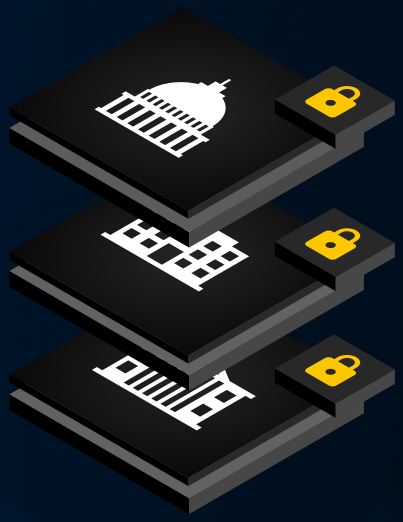
KEEPER®

Solutions Brief

# Adoption of Zero-Trust Architecture In Government Agencies



Public servants access secure databases and applications across various platforms and networks. To successfully adopt a zero-trust architecture (ZTA), IT teams must provide the right solutions and training to ensure that every employee in the organization is securely accessing sensitive data.

The Office of Management and Budget (OMB) has created standards and objectives for agencies to achieve ZTA by 2024. The five pillars of ZTA, released by the Cybersecurity Infrastructure and Security Agency (CISA), lay out the base requirements for solutions that address how employees and contractors protect and access each pillar: Identity, Devices, Networks, Applications and Workloads and Data.

## Zero-Trust Means Securing the Human Element

A major goal of ZTA is to secure the most vulnerable part of an organization: the employees and contractors who work and deliver on agency missions. Ensuring secure access to systems, data and applications means securing the credentials and managing the privileges of every person who requires access. By providing employees with an easy-to-use, zero-trust solution, organizations can ensure all employees and contractors support the five pillars of ZTA when accessing mission-critical data.

## How to Quickly Adopt Zero-Trust, Zero-Knowledge Solutions

Immediate and swift actions must be taken to meet the OMB's ZTA requirements. Following are three simple, effective measures that can be executed to minimize vulnerabilities and risks inherent in the human element.

1. Partner with vendors that apply ZTA strategies internally and within their solutions offerings. Agency Strategy Implementation Leads can glean best practices and lessons learned from industry partners that have also been combatting phishing and cyberattacks by investing in technology that protects and educates employees. Phishing attempts and cyberattacks can be combatted with agency-wide adoption of password management.

2. Make sure applications and programs support multi-factor authentication (MFA) or can enforce MFA policies. Verizon's DBIR 2021 noted that "Organizations that neglected to implement multi-factor authentication, along with virtual private networks (VPN), represented a significant percentage of victims targeted during the pandemic."[2] Enforcement and adoption of MFA policies through Keeper's Admin Console allows ZT Strategy Implementation Leads to that ensure all personnel are using MFA and that networks and devices are adhering to the ZTA tenet to "never trust, always verify."[3]

3. Protect and prioritize securing the human element. Eighty-five percent of successful data breaches involve the human element.[2] Provide your organization with security solutions that meet rigorous compliance standards, are easily adopted, and seamlessly integrate with existing cybersecurity solutions such as single sign-on (SSO), privileged access management (PAM), and your organization's security information and event management (SIEM) solution. To successfully improve the security posture of an organization, leadership must consider how employees and contractors adapt to new measures and empower them to keep mission-critical tasks afloat, whether team members are working in-office or remotely. Implementation and support provided by ZT technology partners needs to be readily available to all team members.

# Begin Your Zero-Trust Journey with Password Management

Comprehensive implementation of ZTA is a marathon, not a sprint. However, Keeper's enterprise-grade password security and encryption platform enables government agencies to hit the ground running by shoring up the all-important human element.

## Protect Access to Applications, Systems, Secrets, and IT Resources

Keeper's Admin Console provides IT admins with organization-wide visibility and control of user password practices while empowering the entire organization with zero-trust, zero-knowledge security for applications, systems, secrets and data.

## Secure Against Social Engineering Attacks

Keeper safeguards your organization against phishing and other social engineering attacks that fuel data breaches and ransomware by ensuring that every employee and contractor follows cybersecurity best practices such as strong, unique passwords and MFA.

## Monitor Devices and Control User Access

Keeper utilizes real-time risk analytics to provide insights and visibility into device security monitoring, data access and device-based access controls and validation. IT admins can use the Admin Console to implement role-based access controls (RBAC) to ensure that only authorized users can access sensitive, mission-critical systems and data.

## Insights and Immediate Action on Compromised or Weak Credentials

Security audit scores and Keeper BreachWatch alerts provide IT admins with immediate insight into vulnerable and compromised credentials, so that they can force password resets before compromised passwords can be leveraged by cybercriminals.

Keeper seamlessly integrates with existing identity and access management (IAM) solutions and is easy to deploy and scale. Learn more about how Keeper Security can help you build the foundation of a successful ZTA strategy by visiting **keeper.io/publicsector**.

## About Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-trust, zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage, advanced reporting and messaging. Named PC Magazine's Best Password Manager & Editors' Choice and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award, Keeper is trusted by millions of people and thousands of organizations to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2 (Type 1 and 2) and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects organizations of all sizes across every major industry sector.

Keeper is FIPS 140-2 validated and is the only enterprise password management solution listed on the FedRAMP marketplace.

## Contact the KSGC Team

**Email:** publicsector@keepersecurity.com
**Phone:** +1 202.946.4575
**Website:** keeper.io/publicsector

Sources: [1]zerotrust.cyber.gov/federal-zero-trust-strategy [2]verizon.com/dbir [3]forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify