User Identities in a Zero-Trust World

A key pillar of Zero Trust is identity, which uses capabilities such as multifactor authentication (MFA) to continuously verify the identity of a person or device. ***Hanna Wong,*** *director of public sector marketing for Keeper Security, discusses how organizations can modernize their identity security approach to move toward a Zero-Trust model.*

What's driving interest in Zero Trust?

State and local governments — which have become top targets of phishing, data breaches and ransomware attacks — must be able to prevent cybercriminals from accessing all endpoints, including those associated with a distributed workforce. Prior to the pandemic, employees primarily accessed databases, applications and constituent data from within the secured network perimeter of an office. Now users are connecting from their home networks or unknown networks — even cafes — that don't have the security protections that exist within a physical office. That heightens the need for Zero Trust, which has "never trust, always verify" as a main tenet.

Why are some user provisioning solutions inadequate for government?

A lot of modern solutions cannot provision users or verify credentials for certain legacy systems, so it's important to have a solution that can meet cybersecurity needs throughout the modernization journey. As governments transition from legacy systems, they need to invest in a solution that protects employee passwords and credentials in those old systems and integrates with modern identity and access technology like single sign-on (SSO).

What is a zero-knowledge platform and how does it help organizations strengthen security and compliance?

A zero-knowledge platform means the provider of your credential management solution can't decrypt the information stored there. In terms of security and compliance, that means even if the solution provider's system is breached, the attacker cannot steal your user identities, passwords and other sensitive information and use them to break into your infrastructure.

What capabilities should organizations seek in a credential management solution?

Zero Trust, zero knowledge and the enforcement of MFA are critical. One of the Zero-Trust pillars is identity, and the adoption of identity functions like MFA is central in the Zero-Trust security models developed by CISA and the Office of Management and Budget (OMB). Solution simplicity is also vital. Zero-Trust technologies need to be intuitive to use and easy to roll out — both for IT and non-IT teams. If it's too complicated, it lowers adoption rates and increases security risks. The solution should also support secure intra and interagency collaboration, including the capability to securely share documents, records and resident data.

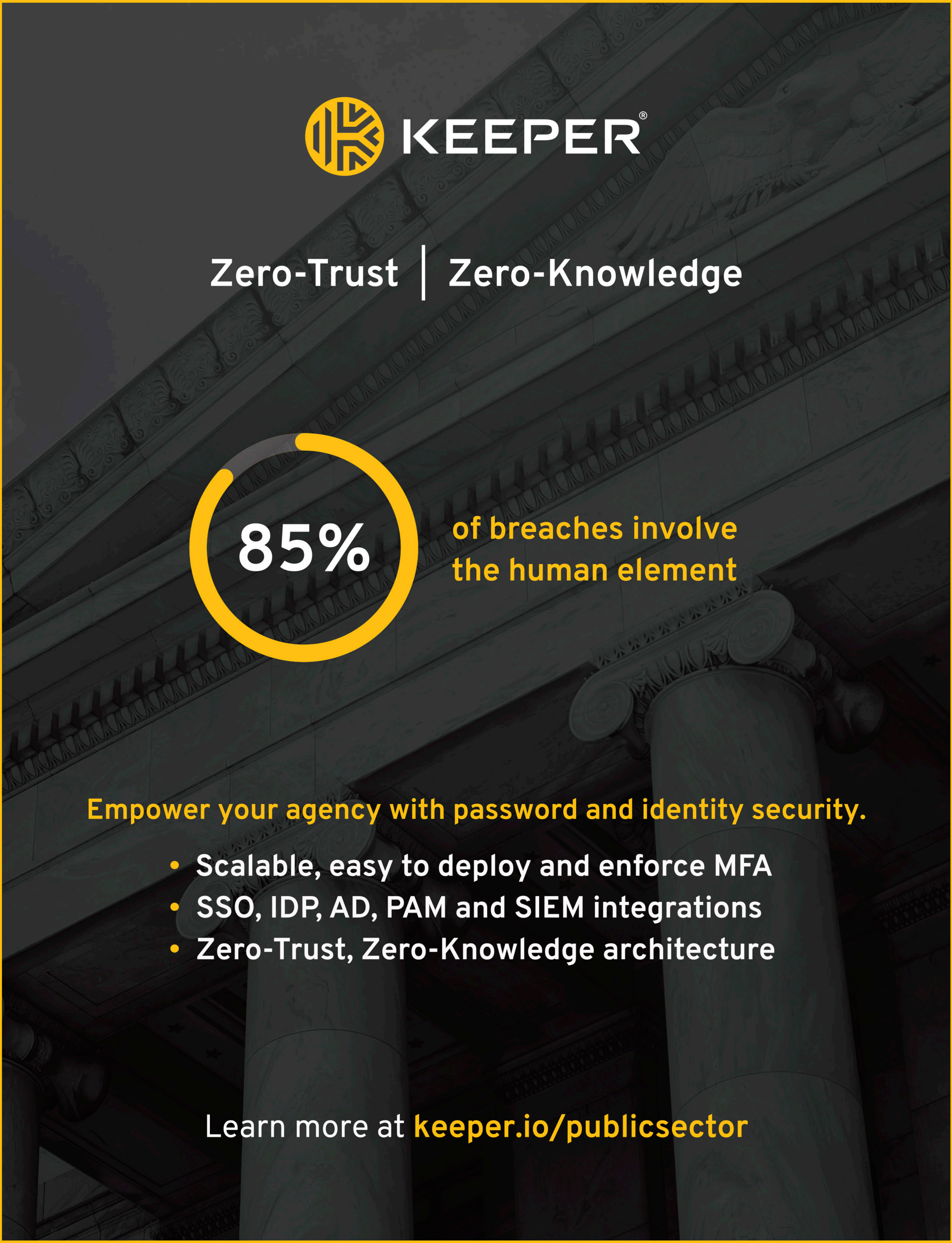
How can organizations maintain strong security while improving user experience?

Government organizations are in different stages of their modernization journeys, so it's important to have a solution that can integrate with the existing identity stack and security stack — for example, security information management solutions that let IT teams view and aggregate data across their cybersecurity and identity solutions. In addition, having a platform that can secure the user credentials for legacy applications while working in sync with SSO is becoming more important. It is a single vault where each user can store credentials for all their systems.

The OMB recently released a memorandum specifying requirements and a 2024 deadline for federal agencies to implement key features of a Zero-Trust model. Where can state and local governments start their own Zero-Trust journeys?

Partnership with industry is always one of the best places to start for this type of implementation and requirement. The leading vendors have already implemented Zero Trust in their architecture strategies internally as well as in their solution offerings, so they can share best practices and lessons learned. Given that organizations have already invested a lot in identity and access solutions, a tangible and easy place to start is by implementing solutions that seamlessly enforce MFA policies across the organization and allow you to receive security audit reports and dark web monitoring alerts. Finally, as mentioned, a solution that is easy to adopt and enables secure collaboration across agencies or departments will make a big difference when it comes to Zero-Trust models.

Learn more at **Carah.io/GT-22-Cyber-Keeper**



KEEPER®

Zero-Trust | Zero-Knowledge

85% of breaches involve the human element

Empower your agency with password and identity security.

- Scalable, easy to deploy and enforce MFA
- SSO, IDP, AD, PAM and SIEM integrations
- Zero-Trust, Zero-Knowledge architecture

Learn more at **keeper.io/publicsector**