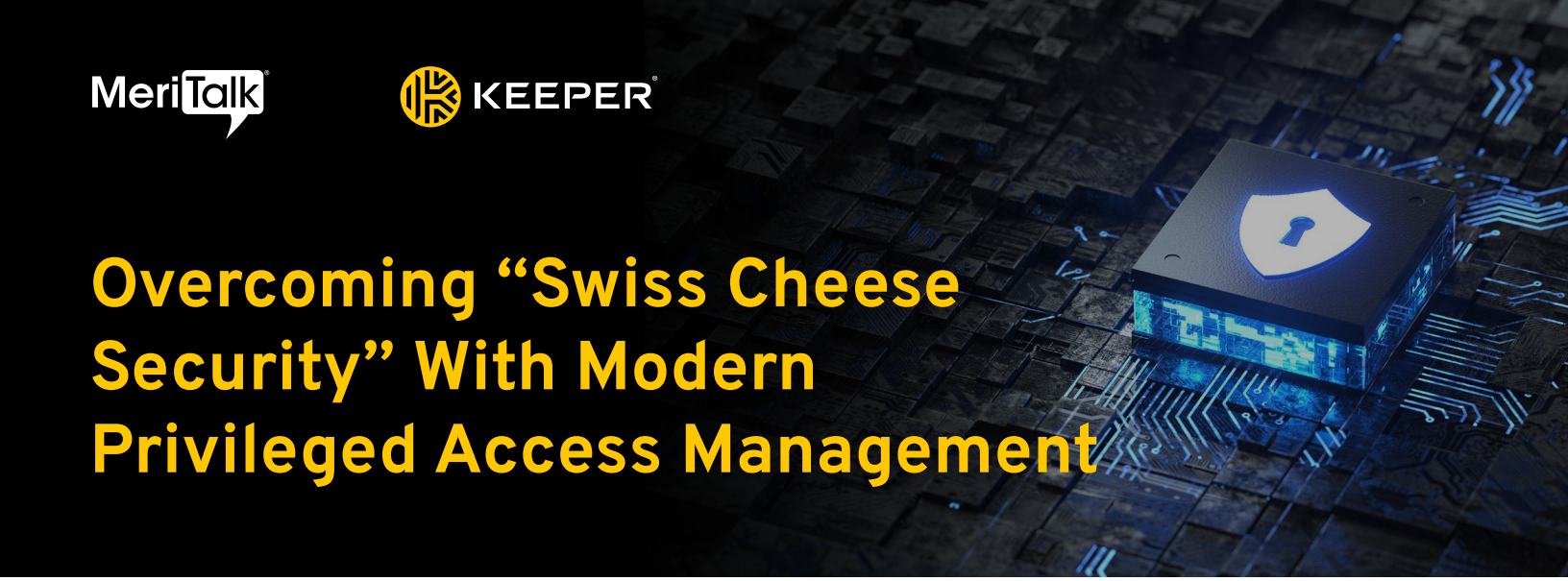

Overcoming "Swiss Cheese Security" With Modern Privileged Access Management

Legacy privileged access management (PAM) solutions, rooted in a perimeter-centric security model, can become security liabilities for Federal agencies. In an interview with MeriTalk, James Scobey, chief information security officer (CISO), Keeper Security, discussed his recent move to Keeper from the U.S. Securities and Exchange Commission (SEC), Federal agencies' progress toward zero trust security architectures, and why modern PAM solutions are a foundational element of zero trust.

MeriTalk: You joined Keeper Security in October 2024 after serving as CISO for the SEC. What's been the biggest change as you get settled at Keeper?

Scobey: As a CISO in a large Federal agency, you're often advocating for cybersecurity. At a cybersecurity company like Keeper, everyone is already obsessed with cybersecurity. The focus is on driving forward and finding more innovative ways to meet customers' mission needs and objectives.

MeriTalk: In your role at Keeper Security, you're focused on corporate cybersecurity and product cybersecurity. Would you say that focus is an even split? What are some of your early goals?

Scobey: Product security and corporate security are fundamentally inseparable. Attackers look for any vulnerability, regardless of where it exists, and will exploit weaknesses in either area to compromise an entire organization. This interconnected reality means that I take both very seriously.

On the corporate side, my major focus is ensuring our detection and response capabilities advance, because as Keeper is adopted by more organizations, we become a bigger and bigger target, and our ability to detect and respond and defend our environment must scale along with that.

On the product side, some of our goals in 2025 are to advance our FedRAMP authorization from Moderate to High and to achieve IL5 for our defense customers. I'm also very focused on advocating for modern PAM.

MeriTalk: You have some concerns about current implementations of PAM. What are your top three concerns, and why?

Scobey: First, in a traditional PAM environment, you have firewalls that segment the user environment, the deployment environment, the production environment, and the development environment. To enable the functionality of the PAM solution, you put holes in those firewalls, creating what amounts to "Swiss cheese security" – a perimeter riddled with entry points. The PAM actually becomes a security liability.

Second, development teams are laser-focused on shipping code, and when the legacy PAM system slows them down, they will resort to workarounds. They create and manage development environments outside of the purview of security teams. This leads to unauthorized password storage, credential sharing, and the creation of unmonitored admin accounts, all of which pose significant security risks.

Third, legacy PAM solutions also suffer from a lack of quality capabilities across the stack. If you have a legacy PAM solution stack that does hundreds of things but only a few of them well, organizations typically implement just 10 to 15 percent of available capabilities. The rest is embedded technical debt that is a burden on security teams and administrators.

MeriTalk: In some cases, once users authenticate to a PAM system, they gain broad access to resources. This is contrary to the principles of zero trust, which focus on identity and data security, rather than perimeter-based security. Looking back on your time in government, how would you assess Federal agencies' progress toward zero trust adoption? What challenges remain?

Scobey: One of the first things I want to do when I come into an organization is log into the systems and see what I get access to. Many times, I find that teams don't know what they're granting access to, so that's a problem for sure.

Thinking about zero trust across the zero trust pillars, I think the Federal enterprise has done a great job of addressing the identity pillar with multifactor authentication, secure access service edge networks, and endpoint detection tools, as well as consolidating identity providers.

Moving forward, agencies' next steps with identity should include enterprise secrets management to protect authentication stories in scenarios that don't involve personal identity verification or common access card authentication. Concerning the application pillar, agencies struggle with legacy systems that can't support modern secure development practices. Perhaps most critically, the data pillar requires a fundamental mindset shift in many agencies. Instead of focusing on protecting systems, agencies need to recognize that attackers target data itself – requiring controls that protect information as it flows across systems and transit points.

MeriTalk: How does Keeper Security apply zero trust principles to identity and access management – especially privileged access management?

Scobey: Keeper Security's zero trust approach aims to minimize attack surface, enforce least privilege, and provide comprehensive visibility and control over privileged access. The platform integrates with major identity providers while supporting advanced authentication methods, including passwordless options and biometric verification.

The solution implements just-in-time privileged access management, where users receive only the credentials they need for a limited period – and inactive privileged users are automatically signed out. Automated secrets management features like password rotation and secure credential sharing prevent developers and users from resorting to insecure workarounds that often compromise traditional PAM systems.

Critical to the zero trust model is comprehensive visibility through detailed audit trails and security information and event management integration, enabling security teams to monitor authentication events that typically fall outside primary identity provider oversight. Optional session recording provides security teams complete visibility into activities on sensitive systems.

Lastly, our zero-knowledge security architecture ensures encryption keys never leave the client side, which means that Keeper Security cannot access agencies' encrypted data. That's crucial, because if Keeper were ever compromised – which has never happened – the attacker would not be able to access agencies' encrypted data via our systems.

MeriTalk: If you could offer one piece of advice to Federal agency CISOs and CIOs as they continue to work on zero trust initiatives, what would it be?

Scobey: Prioritize PAM as a foundational element of zero trust architecture. It's often considered a secondary or tertiary step while agencies focus on network segmentation or endpoint security. That's a mistake, because compromised privileged credentials are the primary attack vector and the most significant indicator of a Federal breach. Start your implementation with privileged accounts that have access to the most sensitive systems and data. Keeper provides automated discovery capabilities that help identify those accounts quickly. You can't defend what you don't know is there, which is often a problem for CISOs.