Enhancing government identity security through zero trust

In the evolving cybersecurity landscape, a robust identity and privilege management strategy, underpinned by a zero trust approach, is crucial for government agencies to protect against threats and ensure secure, seamless operations.

In today's rapidly evolving threat environment, government agencies face increasing risks from sophisticated cyber attackers who exploit vulnerabilities to gain unauthorized access. With the rise of digital transformation and remote work, these threats have grown more complex, requiring a fundamental shift in cybersecurity strategy. Alarmingly, about 80% of hacking-related breaches involve the misuse of privileged credentials, underscoring a significant weakness in many organizations' defenses. To counter these risks, a zero trust approach to cybersecurity has become indispensable, placing identity management at its heart.

For government agencies navigating this challenging digital landscape, ensuring robust identity security is more important than ever. Implementing a comprehensive Identity, Credential, and Access Management (ICAM) program as part of a zero trust strategy enables agencies to manage users, applications, and data cohesively. This approach ensures that only authorized users have the appropriate access to necessary resources at the right time, substantially reducing the risk of unauthorized access.

During a recent NextGov/FCW Identity Security Workshop, industry experts discussed the importance of integrating ICAM into an agency's security posture. In a session with Michael Saintcross, BeyondTrust's federal vice president, and Kelvin Brewer, Ping Identity's director of public sector sales engineering, the two shared insights into how agencies can approach zero trust to ensure productivity and security.

Here's what they had to say:

THE CHALLENGE OF DIVERSE IDENTITY PROVIDERS

Adopting a zero trust framework is vital for government agencies aiming to enhance security while ensuring a seamless user experience. One of the most significant challenges these agencies face, however, is managing the diversity and complexity of identity providers (IDPs).

"When you look at the complexity of what's happened in the identity industry and how IDPs have become so diverse, it's not just the fact

> **"When you look at the complexity of what's happened in the identity industry and how IDPs have become so diverse, it's not just the fact that there are so many different IDPs, but also the amount of data stored in those IDPs."**
>
> KELVIN BREWER
> Director, Public Sector Sales Engineering, Ping Identity

> "Conditional access is the ability to pull all these variables in and look at what kind of risks a user presents to me today..."
>
> MICHAEL SAINTCROSS
> Federal VP, BeyondTrust

that there are so many different IDPs, but also the amount of data stored in those IDPs," Brewer explained. This diversity can complicate security efforts, making it harder to maintain a strong security boundary while managing multiple identities across different systems.

To address this challenge, Brewer emphasizes the importance of an integrated approach that leverages the strengths of various IDPs. This strategy involves orchestrating the myriad data points associated with different identities to make informed, risk-based decisions in real time.

By consolidating data from various sources into a unified identity management framework, agencies can enhance security while ensuring legitimate users have the access they need without unnecessary barriers. This approach not only prevents unauthorized access, but also aligns security measures with zero trust principles.

THE POWER OF COLLABORATION AND CONDITIONAL ACCESS

Another critical component of ICAM is managing elevated privileged access across an organization. According to Saintcross, agencies face challenges identifying and controlling privileges across multiple environments, including cloud services, databases, and network devices. Privileged identities are often dispersed throughout an organization, making it difficult to discover and manage these critical access points.

To effectively secure these environments, Saintcross suggested agencies adopt a comprehensive strategy that covers all areas. This involves not only managing user identities, but also implementing controls that govern who has privileged access and under what conditions. Additionally, conditional access is crucial for federal agencies as it allows them to dynamically adjust access controls based on the current risk level, enhancing security without compromising productivity.

"Different variables can increase the risk for an organization to allow someone to access any of their resources," said Saintcross. "Conditional access is the ability to pull all these variables in and look at what kind of risks a user presents to me today, at this moment, because it's probably different than it was even an hour ago."

By integrating identity management with privileged access solutions, agencies can mitigate risks associated with privilege escalation—a common tactic used by attackers to gain unauthorized access.

Saintcross and Brewer agreed that no single vendor is the answer, but rather that agencies should leverage powerful orchestration tools to integrate different technologies smoothly. By combining their capabilities, Ping Identity and BeyondTrust offer a unified solution that manages both general user and privileged access, simplifying deployment and enabling faster, more effective security solutions.

Discover how BeyondTrust and Ping Identity are helping agencies bolster their identity security.