Advancing Zero Trust IT with PAM and IAM

Integrating Privileged Access Management (PAM) and Identity Access Management (IAM) is essential to your identity security strategy.

Clarence Hinton
Chief Strategy Officer and Head of Corporate Development
CyberArk

The need for strong Privileged Access Management (PAM) controls has continued to increase as IT teams look to secure what have become highly distributed computing environments due to the pandemic, digital transformation, cloud migration and the shift left.

Not only are end users more likely to be accessing corporate resources from anywhere, but they now expect it, noted Yuval Moss, CyberArk VP Identity Security, in his talk, "What is Identity Security?"

While several years ago only small groups of users (mostly IT admins) were considered privileged, this isn't the case in today's cloud and hybrid environments.

What's more, it's become apparent that each machine – and even individual components of an application – have an identity that needs to be managed. Without the right controls in place, any of these identities can become a privileged identity, opening doors to valuable data and assets.

Similarly, the attacker landscape is evolving. Cyber attackers have increased in number, sophistication and aggression. These factors have combined to lead to an exponential increase in cybersecurity threats facing enterprises across the globe.

A Security-First, Least Privilege View of Identity-Related Risk

Rather than managing PAM and Identity Access Management (IAM) platforms in isolation, CyberArk is making a compelling case for integrating these capabilities via a unified software as a service (SaaS) platform to achieve and maintain Zero Trust security in the most friction-less way possible.

The company, as part of that effort, showed how organizations can apply policies based on identity and least privilege access rules to desktops or even specific end users using either single sign-on (SSO) or biometric tools.

"PAM and IAM are coming together," said Khizar Sultan, Senior Director for Product and Solution Strategy at CyberArk during a "Why Integrating PAM and IAM Is Essential to Your Identity Security Strategy" session. "Identity winds up actually being the new perimeter for security."

CyberArk also stressed the need to protect end users by enabling policies to isolate sessions using a continuous authentication mechanism that makes

CyberArk is making a compelling case for integrating PAM and IAM capabilities via a unified software as a service (SaaS) platform to achieve and maintain Zero Trust security in the most friction-less way possible.

certain end users are active in a session, in addition to protecting them from cyber attacks aimed specifically at browsers. As an extension of that capability, it's critical to enable an audit trail that tracks all actions made during a session.

In general, managing the lifecycle of passwords and privileges based on identity within the context of a task will be crucial. End-users need to be able to assign a higher level of privilege in a just-in-time fashion to complete a specific task, based on their specific identity or the role they play within an organization.

The goal is to enable organizations to implement Zero Trust policies in a way that doesn't jarringly disrupt business process workflows. Naturally, there will also be a need to provide the monitoring tools so that IAM and PAM capabilities are being optimally employed.

Most organizations had already begun to gradually transition toward Zero Trust IT architectures. The COVID-19 pandemic simply accelerated that shift once IT organizations realized many employees would continue to work from anywhere for the long run.

The challenge is finding a way to seamlessly implement Zero Trust principles and capabilities so employees, customers, and business partners won't either reject out of hand or, more likely, waste countless hours trying to find a way to workaround.

Learn more at www.cyberark.com. ■

Michael Vizard, Freelance Writer and Editor at RCF Media, who covers Cybersecurity issues, contributed to this article.

About The Author

Mr. Hinton is Chief Strategy Officer, Head of Corporate Development at CyberArk. He is responsible for formulating, assessing and executing strategic growth initiatives.

Prior to CyberArk, Hinton served as Senior Vice President of Corporate Development at Nuance Communications, where he was responsible for identifying, developing and executing acquisitions, divestitures, minority investments and joint ventures.

Hinton holds an MBA from Harvard Business School and a Bachelor of Science degree in Engineering with honors from the University of Pennsylvania.