Protecting access to a nation's defense secrets

A government-based organization improves security, user experience and savings with a flexible privileged access management (PAM) solution.

Customer: **Government-based defense organization**

Employees: **10,000**

Industry: **Government**

Organizations that develop and manufacture national defense technologies share information on a need-to-know basis. IT security teams control and monitor every detail involving system and cloud access, including password changes, session recordings, and the detection and blockage of any unusual network activity. At the same time, user experience factors into security effectiveness because tools only help if people can use them. A government defense organization with 10,000 employees discovered this important nuance after deploying CyberArk.

The company's IT teams used CyberArk to manage basic privileged access management (PAM). Features such as session recording and public cloud service management didn't work as promised and the time required to add other capabilities made broader adoption impractical. An IT project leader at the company says, "CyberArk was rigid and time-consuming to manage, and we couldn't scale it. Just keeping it stable required 20% of an employee's time each week and 52 days of professional services each year." Any change in user access involved complex manual processes, and each software update took three days. Developers also built a custom app to simplify remote login so that staff didn't have to use the CyberArk interface, which they didn't like.

Challenges

The CyberArk privileged access management solution was inflexible and so difficult to use that it limited deployment and the adoption of features except remote desktop access.

Results

- Cuts time needed to manage PAM by 80%
- Increases PAM users sixfold
- Reduces PAM costs by two-thirds over 5 years
- Deploys in 2 weeks vs. 4 years
- Updates in 2 hours vs. 3 days

Solutions

Third-party ACS helped the organization replace CyberArk with One Identity Safeguard Privileged Access Management to support more users and add capabilities including password vaults and session recording.

When the organization needed to add a network for privileged users, CyberArk's high cost prompted an evaluation of Gartner Magic Quadrant PAM solutions. "The One Identity Safeguard proof of concept impressed us," says the project leader. "One Identity Safeguard's zero-trust model is flexible and its privileged session management is vastly superior to the other PAM options." Safeguard also offered other competitive advantages including excellent support from One Identity and an easy installation process.

"Our deployment of One Identity Safeguard dawns a new era of how we manage access.... We're enhancing security without hindering productivity, and people are asking to use security features."

Project leader, government-based defense organization

Working with its third-party integrator ACS and One Identity as its trusted advisor, the organization deployed Safeguard, including Safeguard for Privileged Passwords, Safeguard for Privileged Sessions and Safeguard for Remote Desktop Access. "In just two weeks of using Safeguard, we accomplished what took us four years to do with CyberArk," says the project leader. "And in 90 days, we were well beyond that milestone." For example, the organization configured Safeguard to interoperate with Active Directory and Azure Active Directory so that users' network, system and cloud-access privileges automatically reflect any changes to their roles.

Reducing time spent on PAM by 80% while adding almost 6x more users

With Safeguard, the company supports 650 privileged users; with CyberArk, it supported only 120. Individual teams now have centralized, self-managed password vaults, and Safeguard automatically blocks network access for the source of unusual network activity. Safeguard also requires less time and fewer skills to manage. Software updates now take two hours rather than three days. One full-time employee now spends 10% of each week managing PAM and needs almost no professional services help. Over five years, the organization is also cutting PAM costs by two-thirds.

"Our deployment of One Identity Safeguard dawns a new era of how we manage access, and we're now fully PAMMED," says the project leader. "We're enhancing security without hindering productivity, and people are asking to use security features. It may be a cliché but it's true. It's the little things that matter. One Identity Safeguard works as stated — and it does so effortlessly."

"One Identity Safeguard's zero-trust model is flexible and its privileged session management is vastly superior to the other PAM options."

Project leader, government-based defense organization

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest