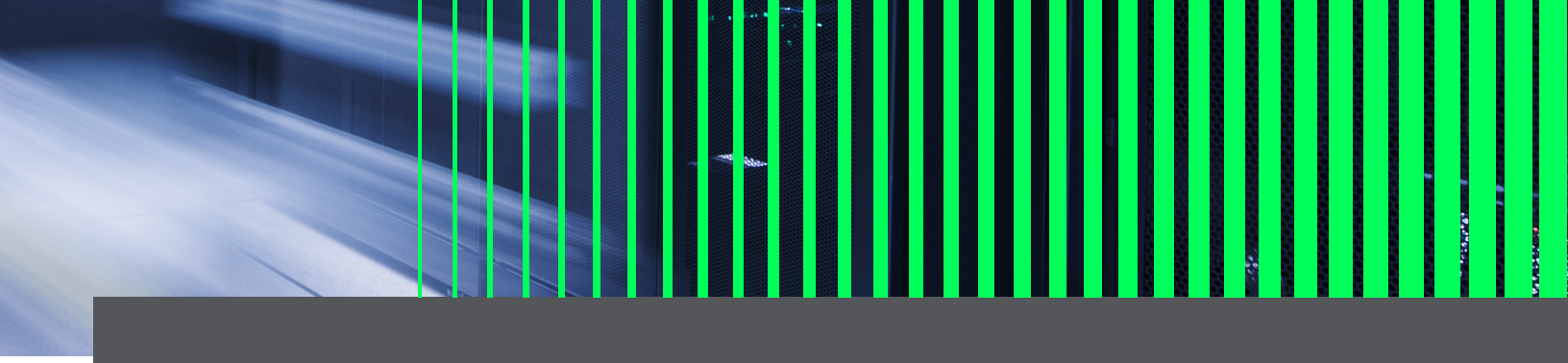

Delinea

GLOBAL ORGANIZATION **CASE STUDY**

Global Organization Leverages Delinea

to achieve PCI compliance, manage privilege across their *NIX environment

Challenges

When the company's lead security analyst joined in 2018, a small group of servers was under the control and management of the Delinea solution. The remaining 1,500 servers were still using local accounts for access and sudo to elevate privilege. The result was an increasingly difficult to manage, insecure environment.

"Every time a user requested access to a server that wasn't managed by Delinea, we created a new local account," says the lead security analyst. "But those accounts add up fast, and with only three technicians tasked with managing them, it quickly became a nightmare — not to mention the fact that every new local account adds another element of risk to the environment."

As part of a Cybersecurity Initiative, the company undertook an extensive evaluation of their infrastructure to identify and address their most critical issues. They found that, despite the focus on compliance to industry standards and government regulations, they were overlooking several key best practices.

Sessions that were directly connected to target systems had no privilege management component in place. Specific privileges within systems were granted and revoked manually. A manual process was also used for privilege elevation. "We wanted to avoid giving full privileged access when possible, so our goal was to elevate privileges to perform critical tasks, and then revoke that privilege as soon as they were completed," he says. "But granting access could take several days. And when privileges aren't granted in a timely manner, delays and interruptions arise that threaten time-to-market deadlines."

Most of the company's operations teams still used root access to perform their duties, which undermined the company's ability to understand who had access to which systems, when they had it, and where they were located.

Background

A large American organization with a global presence was having trouble controlling their privileged access. The company adopted Delinea Privileged Access Management (PAM), implementing a limited number of licenses meant to cover their most critical — and frequently audited — systems. Eventually the company extended Delinea PAM across their entire infrastructure to better manage access and privilege, significantly enhance security, and alleviate pressure on IT staff.

The company was using a competitive product to perform some key security elements, but it didn't provide all the features necessary to maintain a strong security posture.

"The vault we were using didn't provide Microsoft® Active Directory-based authentication to our Linux systems," says the security analyst. "That meant a huge number of servers and thousands of corresponding local accounts across the infrastructure required hands-on management. This was a costly, time-consuming approach, and our IT department was feeling the pressure."

Given the large number of servers and the complexities of managing local accounts manually, they decided to implement a PAM solution across the remaining infrastructure.

Solution

The company needed to manage user access across their entire Linux environment. They needed to easily grant and rescind privileges, and they needed the ability to tie every action taken with a specific person in order to illustrate accountability to auditors. They identified the following features as essential:

Centralized Authentication: The solution would need to centralize discovery, management, and user administration for Linux and UNIX systems through Active Directory.

Multi-factor Authentication (MFA): MFA would be required at both the vault and server level, and so the solution would need to co-exist with the company's existing vault technology.

Least Privilege: The solution would need to provide just enough privilege, granted just-in-time, and for a limited time only. A secure, automated process of privilege elevation would grant administrators the ability to perform tasks without a root password.

Compliance: The solution would need auditing and reporting capabilities to prove an existing secure access methodology and adherence to PCI, GDPR, and multiple countries' privacy laws.

Having already executed a full product evaluation process just a few years earlier, the company opted to expand Delinea across the entire environment. "We had already addressed our compliance issues, and the teams had come to rely heavily on Delinea, so we made the decision to move forward without considering other solutions," he says. "We hired a local vendor to assist with the implementation, so it went as smoothly as we could have hoped."

The rollout across the remaining environment took approximately 18 months. An interview process that involved users, application owners and those responsible for servers was used to analyze thousands of legacy local accounts, and to determine current access and privilege requirements across the organization. "That's what took the most amount of time — cleaning up the local accounts and identifying current access requirements. Otherwise, we could have rolled it out in a week," he says.

Results

With the expansion of the Delinea solution, the company's nearly 2,000 servers now fully leverage Active Directory. User accounts are centrally managed through Delinea PAM, and that has resulted in the removal of thousands of local accounts from Unix servers, dramatically simplifying the identity management process while improving the company's risk profile.

"Delinea provides centralized, Active Directory-based authentication and authorization for our Linux systems, reducing the number of accounts, while tying all access to a specific individual and helping us to remain in compliance with government regulations," says the security analyst. "Delinea methodologies and reports have been instrumental in helping us to avoid non-compliance fines and to identify issues that could negatively impact our business."

Adding and removing individual access from a central location has eliminated the need to scan thousands of servers to determine access rights, and also ensures each individual has a consistent user ID throughout the environment. With appropriate Delinea PAM roles centrally managed from Active Directory, administrators can access any Linux system using their personal Active Directory account. Privileged activity is no longer anonymous, but is tied back to a unique individual.

Granting unrestricted root access is no longer necessary. Users now elevate privileges to perform specific commands through Delinea, and their work is audited. "With Delinea, we've achieved data consistency with our elevated privilege program," says the analyst. "Sudo files and access logs have been consolidated into Active Directory for simplified management. Elevated access is managed across groups of computers, eliminating the need to push static flat files to each server."

The company has effectively integrated two solutions: the first manages root passwords, while Delinea brokers the authentication for most administrative sessions. "We use Delinea to fill any gaps, and for account reconciliation across our Linux environment. With everything in Active Directory, user passwords are managed by Delinea, which ensures they remain in sync," he says.

"Ultimately, Delinea provides us with all the tools we need to build a comprehensive secure access methodology for our entire infrastructure," he says. "By providing Active Directory-based authentication, MFA at the host level, privilege elevation, and auditing and reporting, Delinea satisfies the Privileged Access Management requirements found in the vast majority of audits."

Looking forward

The company recently initiated a hardening project designed to enhance the security configuration of their Linux systems. The ultimate goal is to remove sudo from the environment entirely. This will eliminate the user's ability to create local sudo rules into which the IT department has no visibility — including those used to escalate privilege. Moving forward, the user will only be able to obtain permission for elevated privileges through Delinea.

Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**