Delinea

LARGE HOSPITAL SYSTEM **CASE STUDY**

Delinea Secret Server

High security architecture and enterprise PAM eliminate risk of Pass-the-Hash attacks

Challenges

As cyberattacks against the healthcare industry continue to rise, the hospital's IT team is on high alert. "We're always looking at the latest techniques bad actors are using and trying to build up our protections," explains the Senior Systems Analyst for IS Infrastructure Services.

As a key component of its security architecture, the hospital recently shifted from using Secret Server primarily as an enterprise password management vault to a mature privileged access management solution.

Routine penetration tests flagged IT operations practices that could potentially allow malicious hackers to capture privileged passwords. When Domain Administrators were troubleshooting technical issues, the method they used to connect and log into systems opened the door to Pass-the-Hash attacks. Administrators were leaving password hashes behind on remote endpoints. Attackers could potentially scrape system memory or use other techniques to obtain those passwords and gain entry to the IT environment as a privileged user.

Solution

High-security architecture

The security team decided to implement Microsoft's credential tiering system, known as Privileged Access Workstations (PAWs). In a PAWs model, administrative tools and applications for critical functions are on a privileged workstation and all other activities are executed on a standard user workstation. In a simultaneous use scenario, a single workstation can be used for both privileged tasks and daily activities; the physical hardware runs a single PAW operating system locally and contacts a remote desktop service for user applications.

Background

A large hospital has been a Delinea customer since 2012, when the IT team first began using Secret Server to protect and manage encryption keys. As the hospital's security practices developed, their use of Secret Server expanded. The IT team moved away from manual processes and chose to create and store all passwords in Secret Server. They put password management policies in place for all privileged accounts, including hospital service accounts, to enforce character count and complexity.

> If we didn't use Secret Server and work within this tiering model, our environment would be easily compromised. It's our mitigation against Pass-the-Hash."

→ Senior Systems Analyst, IS Infrastructure Services, Large Hospital System

The security team needed to make sure PAM best practices aligned with the new tiering system to allow for secure credential management and access control, as well as RDP. They validated the setup of Secret Server with Delinea's professional services team, which ensured RDP was set up correctly and the hospital IT staff had a secure way to log in through the web interface.

They began implementing Secret Server for all Tier 0 workstations and progressed to Tier 1 for test and development. They then onboarded all application development teams to Secret Server. Today, it is mandatory for all IT and technical teams to use Secret Server. Passwords are changed automatically each day without any interruption to services or workflow. Two-factor authentication and checkout features of Secret Server provide extra layers of protection for privileged accounts. Using RDP, Domain Administrators have no need to see passwords to access workstations and support users.

Distributed Engines

The hospital's high security requirements called for the addition of Distributed Engines, a Windows service which handles work such as password changing, heartbeat, discovery, and more. The architecture now has one Distributed Engine handling Tier 0 systems and one for Tier 1. An encrypted RDP tunnel connects Tier 1 to Tier 0, so there's no way to get from one to the other directly. You can't see the passwords in either tier.

The enterprise-scale architecture has also improved the performance of Secret Server. Previously, the hospital used web servers to manage both the web interface and log in experience as well as password management. Now, with the adoption of Distributed Engines, web servers are focused only on managing on the front end, including the log in and web interface. In addition to providing faster log in and processing, the same Distributed Engine can change all passwords at once.

✓ Impact

With the high security architecture and best-in-class PAM solution, the hospital now clears penetration tests for password vulnerabilities with flying colors.

The security team built custom reports and dashboards to visualize syslogs collected from Secret Server. With the visualizations they can demonstrate thousands of connections that have been successful without introducing vulnerabilities into the process. Secret Server is also part of the hospital's SIEM design so the IT team can collect and analyze data centrally.

In addition to pen testers and auditors, hospital executives also see the clear benefits of the multi-layered security system. "The pen tests made it very clear to them that there was a problem, so their awareness was high," says the Systems Analyst. "But, they didn't really understand what each component does. Now, I show them the security design and they get it immediately. They see the tiering model and they see Secret Server right in there. A picture is worth a thousand words."

> The hospital's high-security architecture has three tiers:
>
> - Domain Admins - Tier 0
> - SysAdmins - Tier 1
> - Users and developers - Tier 2