# CASE STUDY

Financial services company achieves security goals by implementing IBM Secret Server

## Leveraging PAM tools for audit and accountability

### THE COMPANY

*Originally chartered in 1865, this regional financial services company has nearly 70 locations in Illinois and eastern Missouri. With the twin goals of safeguarding customer information and complying with banking regulations, the company is constantly evaluating its data security posture. They looked at PAM, or Privileged Access Management, utilities as a way to get ahead of the game.*

**THE NEED:** Greater administrative accountability.

The company's Chief Information Officer saw a need for greater administrative accountability for privileged accounts, a topic gaining attention in the banking and financial services field.

Privileged accounts exist to allow IT professionals to manage applications, software, and server hardware. Privileged accounts provide administrative or specialized levels of access based on higher levels of permissions that are often shared.

Unlike user accounts, privileged accounts can be non-human, such as accounts used to run services with elevated permissions.

The power of privileged accounts makes them an attractive target for hackers. IBM has found that 80% of breaches involve privileged credentials. As Chris Hill, Security Practice Leader for LRS® IT Solutions explains, "In a credential attack the attacker will try to gain control of privileged accounts, not just admin accounts but users with elevated privileges as well. Once that has been achieved, the attacker has a better chance to move around laterally around the network and elude alerting systems."

According to IBM, many organizations fail to take even the basic steps to protect privileged accounts. They leave default settings in place, even leaving "admin" as the user name for privileged accounts. In some cases, organizations simply have too many accounts that no one knows about.

**THE SOLUTION:** PAM using IBM Secret Server.

IBM® Secret Server delivers the ability to easily detect, manage, and audit privileged accounts and authentication secrets such as passwords and SSH keys. Its Discover function can locate all privileged accounts in your environment.

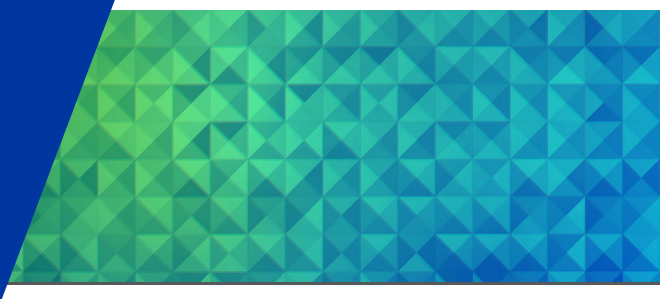
"You run the Account Discovery process, and it finds the privileged accounts that should be managed and controlled," Joshua Brant, Cyber Security Strategist for LRS IT Solutions, said.

Once an organization has all of its privileged accounts in the vault, the security team can securely store passwords and SSH keys and can leverage check-in and check-out functionality for extra accountability. They can also rotate or change passwords automatically.

That's something that many organizations fail to do. Too many privileged accounts are allowed to have a static – that is, a never changing –

*"In a credential attack the attacker will try to gain control of privileged accounts, not just admin accounts but users with elevated privileges as well. Once that has been achieved, the attacker has a better chance to move around laterally around the network and elude alerting systems."*

— Chris Hill
Security Practice Leader, LRS IT Solutions



password, which increases the probability that a hacker will find it and be able to get into an IT environment.

"When IBM Secret Server is fully implemented, it can manage single-use passwords on any privileged account," Joshua noted. "From a security standpoint, that's a panacea."

IBM Secret Server also provides session recording capability. "It can create a video recording of a session or log keystrokes in addition to robust audit logging."

Best of all, IBM Secret Server is flexible; it can be implemented on premises, in the cloud, or as a managed service. The installation is simple, and it's an extremely affordable solution.

**THE RESULT:** Transparency and audit trail

In addition to installing and configuring the Secret Server PAM solution, LRS IT Solutions offers several types of managed service options. For the financial services company, LRS is providing weekly reports of privileged account activity, which is generated by the PAM solution.

"The CIO wanted to be able to monitor what was going on," Chris said. "We're providing weekly reports of things to be aware of, so they now have accountability around privileged accounts, and they have audit trails. Bank auditors love those."

The company has achieved its goal of getting ahead of the game in PAM, has discovered all of its privileged accounts, has administrative control of its privileged accounts, and has even pleased bank auditors. It's a win-win-win.

## ACCOMPLISHED SECURITY GOALS

- Administrative accountability for privileged accounts
- Discovery of all privileged accounts
- Weekly reports of privileged account activity
- Audit trails
- Dynamic passwords for privileged accounts

## SOLUTIONS

- IBM Secret Server
- Installation and configuration services
- Weekly activity reports

LRS IT SOLUTIONS

**Learn more, visit LRSitsolutions.com or call 217.793.3800**

© 2019 All rights reserved. Levi, Ray & Shoup, Inc. LRS and the LRS chevron logo are registered trademarks of Levi, Ray & Shoup, Inc.
IBM is a registered trademark of International Business Machines Corporation in the United States, other countries, or both.