



Major Television Network Protects Its Prized Data Assets with Enterprise Random Password Manager

The CIO of a major television network knows that protecting the organization’s confidential information needs to be a top priority. Yet he faces the same challenge encountered by IT security staff in all industries. How do you restrict access to sensitive content that IT administrators should never see, while still granting them all the privileges necessary to perform critical repairs with no loss of productivity?

The Situation

“People who have the keys to the kingdom, the IT administrators, have freedom to move about anywhere,” said the CIO. “Absent the right kinds of encryption solutions, they can look at data that’s not intended for their eyes. So while we don’t want to handcuff them from being able to support our IT assets when needed, they shouldn’t be able to roam freely in and out of folders where they don’t belong.”

And as a publicly traded company, the television network is subject to compliance with the diligence and governance regulations of Sarbanes-Oxley (SOX).

“We have a very procedural audit process which revolves around Sarbanes-Oxley. This requires deliberate, documented audits, once a month,” the CIO said.

The organization’s IT infrastructure supports television stations in all major U.S. markets and operates out of multiple datacenters and server rooms. Hundreds of servers and thousands of client systems make up their environment with a mix of Windows, UNIX and Linux operating systems. To protect the organization’s data assets the CIO required a solution that could manage any of these components, reliably and affordably, while helping to meet their company’s regulatory compliance and security initiatives.

Customer Profile

Top U.S. television network with stations in every major market.

Situation

Needs to protect sensitive data – without adding unnecessary staff or system overhead. Motivated by Sarbanes-Oxley compliance goals.

Solution

Enterprise Random Password Manager was deployed to control access to privileged accounts and to report who had access, at what time, and for what purpose.

Result

The television network eliminated anonymous access to sensitive data and improved its compliance with Sarbanes-Oxley and other

The Solution

The CIO’s team began its evaluation of privileged identity management products but was initially discouraged by the high costs of many offerings. As part of its investigations the team considered not only purchase and support costs, but also the infrastructure and management overhead introduced by products that require the deployment of software agents to manage each system.

Research then led the team to Lieberman Software’s Enterprise Random Password Manager (ERPM). ERPM is a privileged identity management solution that automatically discovers, updates, stores, and enables secure recovery of local, domain, and process



account passwords throughout the enterprise – without requiring any agents or scripts.

“All of the products we looked at, other than ERPM, required agents, but we are agent-averse,” the CIO said. “If we follow every vendor’s desire to load agents, eventually all of our servers will be bogged down with the sole purpose of supporting those vendors’ products. So being agentless in our deployment is an important differentiator for ERPM– as is its price point.”

“We see our organization as being aggressively frugal and pragmatic. Our answer to every technical challenge isn’t to just throw money at it. We prefer no-nonsense, no unnecessary frills, and only the most necessary of products. For our organization ERPM provides a cost-effective solution to a specific data protection problem.”

“Either we couldn’t find, or there doesn’t exist, a product that is really a competitive equivalent of ERPM.”

The Result

Using in-house IT personnel, ERPM was rolled out to all targeted systems. According to the CIO, compared to other deployments ERPM was “relatively easy.”

The organization is now using ERPM to control service and administrative accounts for all Windows domain controllers, as well as its UNIX application environment. By doing so, their television stations are meeting SOX and other regulatory requirements pertaining to privileged account security.

“Acquiring ERPM was definitely motivated by our desire to maintain governance,” the CIO stressed. “We recognized that that there were a lot of opportunities for data to be lost, compromised, or otherwise mistreated because too many people had too much

“Either we couldn’t find, or there doesn’t exist, a product that is really a competitive equivalent of ERPM.”

freedom with their permissions, and due to the number of programs that required service accounts. There was no governance over the potential for people to abuse those service accounts and then cover their tracks.”

Maintaining significantly more accountability and control over their prized, proprietary data assets has provided a significant, strategic value for the television network.

“ERPM is allowing us to achieve our goal of restricting access to certain libraries where no one, including systems administrators, is allowed to go,” the CIO emphasized. “It’s a product we deployed to solve a very specific problem. ERPM is a strategic cog in the machine.”

About Lieberman Software Corporation

Lieberman Software provides privileged identity management and security management solutions to secure the cross-platform enterprise. By automating time-intensive administration tasks, Lieberman Software increases control over the IT infrastructure, reduces security vulnerabilities, improves productivity, minimizes business disruption, and ensures regulatory compliance. Lieberman Software pioneered the privileged account security market, having developed its first product to address this need in 1999. The company is headquartered in Los Angeles, CA with a support office in Austin, TX.

For more information, see www.liebsoft.com.