

Lieberman Software Helps Fortune 500 Industrial Manufacturer Achieve Security Compliance

Customer Profile

With more than \$4 billion in annual revenue, this multi-industry manufacturing leader has operations in many countries around the world.

Situation

In order to meet its Sarbanes-Oxley (SOX) regulatory compliance requirements the manufacturer needed to regularly change and audit the use of administrator credentials on financial reporting-impacted systems.

Solution

The company deployed Lieberman Software's Enterprise Random Password Manager to manage, secure and audit privileged accounts throughout the network.

Result

The manufacturer now maintains unique administrator passwords for each of its systems, and is auditing use of these passwords - per its SOX regulatory compliance requirements.

The Situation

It's been said that the demands of regulatory compliance are leading the way for IT. In the case of one global Fortune 500 multi-industry manufacturer headquartered in the Southeastern United States, maintaining compliance with the Sarbanes-Oxley (SOX) mandate requires frequently changing, and auditing the use of, administrative credentials on all corporate systems.

For the CISO of this manufacturer, meeting strict SOX requirements was also an opportunity to remedy a serious security threat – shared administrator passwords.

The CISO explained, "We researched some of the major IT data breaches and advanced persistent threats and saw that having the same administrator password on multiple systems was a no-brainer of an attack vector for hackers. Whether it's done by a nation state or a run-of-the mill criminal, the ability to exploit shared passwords and move laterally across an organization is a very real threat."

The shared account password threat the CISO wanted to mitigate involves powerful administrative-level credentials that grant elevated permission to access data, run and install programs, and change configuration settings throughout the network. An attacker who can exploit even one of these common privileged passwords inside an organization can leapfrog from system to system, continuously extracting sensitive data.

Large, multi-site enterprises – including this Fortune 500 manufacturer – typically have many thousands of privileged accounts.

"We're globally dispersed, with more than 17,000 Windows end points, including servers," the CISO explained. "Additionally, we have legacy applications and older technology, which are more difficult to manage, but also have privileged accounts that need to be found and tracked."

The manufacturer's IS team had previously attempted to manage its administrator and sa passwords by storing them in a vault and releasing them to users when needed. One of the drawbacks with this process, though, is that vaults do not provide a method for tracking who accessed the passwords, or when the passwords were last changed – standard requirements of regulatory compliance mandates like SOX.

The Solution

The CISO embarked on an evaluation of the privileged identity management market, seeking a scalable enterprise-level product that could not only help his company meet SOX compliance, but could also provide each account in the network with unique, complex passwords to remove the threat of shared passwords.

Following his evaluation, the CISO chose Lieberman Software's flagship privileged identity management product - Enterprise Random Password Manager (ERPM).



ERPMM helps control access to proprietary data by auditing administrative credentials on systems and applications in the IT infrastructure. It provides the accountability of showing who on the IT staff had access to sensitive data, at what time and for what stated purpose. This information can be provided to security auditors to verify compliance with regulatory mandates.

“One of the biggest factors in our decision to deploy ERPMM was its ability to permit delegated administration,” the CISO said. “It lets us delegate which particular groups of people can check out passwords for which particular groups of systems.”

Another primary driver in the CISO’s decision to purchase ERPMM is the product’s ability to automatically find all privileged accounts in the network. During a password change process ERPMM will update all of the passwords for the privileged accounts, and then propagate these changes every place in the network where the passwords are used.

“That’s a really powerful feature,” the CISO commented, “because it’s one thing to manage a password change. But to be effective you also have to include all of the supporting technologies that are using that password. In a Windows environment that includes things like services and scheduled tasks. Otherwise you could end up with system lockouts and downtime.”

The CISO contracted Lieberman Software Professional Services to assist with the deployment of ERPMM throughout the enterprise.

“I was pleased with professional services,” the CISO said. “They were very good about working with us to architect a solution that met our dispersed network topology. We have sites with varying network bandwidth and latency, so the proper placement of ERPMM zone processors [scheduling services deployed remotely to manage customer systems in the associated region] was appreciated.”

The Result

Once the deployment was complete the manufacturer began making the regular privileged password changes needed to meet SOX compliance and security best practices. ERPMM also streamlined the way in which the company’s IT staff performed their jobs.

“ERPMM helped to change the way our IT staff look at password security because they no longer need to know the password for every computer,” the CISO said. “There’s a little bit of letting go and a little bit of culture shock, but despite that, ERPMM has been well received internally.”

Part of the reason has been ERPMM’s ability to increase security within the company, while also reducing the workload for IT.

“Previously, from the people, process, technology triad, we focused on the people and the process, but not on the technology,” the CISO explained. “With ERPMM, we’re able to focus on the technology aspect of resolving the shared account password problem, which frees up our IT staff for other projects. And from an attack vector perspective, we’ve really stymied the shared administrator password threat.”

“ERPMM can absolutely meet an organization’s IT compliance and security requirements with a minimum of investment, and without a lot of long-term internal support requirements.”

After running ERPMM for several months in a large enterprise environment, the CISO is confident in its ability to meet his compliance and security obligations.

“ERPMM can absolutely meet an organization’s IT compliance and security requirements with a minimum of investment, and without a lot of long-term internal support requirements. The next time we have a SOX audit, I expect to pass.”

About Lieberman Software Corporation

Lieberman Software provides privileged identity management and security solutions to more than 1000 customers worldwide, including 40 percent of the Fortune 50. By automatically discovering and managing privileged accounts everywhere on the network, Lieberman Software helps secure access to sensitive systems and data, thereby reducing internal and external security vulnerabilities, improving IT productivity and helping ensure regulatory compliance. The company developed the first solution for the privileged identity management space, and its products continue to lead this market in features and functionality. Lieberman Software is headquartered in Los Angeles, CA with an office in Austin, TX and channel partners throughout the world. For more information, visit www.liebssoft.com.



LIEBERMAN SOFTWARE

www.liebssoft.com | P 800.829.6263 (USA/Canada)
P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152
1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067
© 2012 Lieberman Software Corporation.
Trademarks are the property of their respective owners.