

# Carnegie Mellon University Takes Control of Privileged Identities in Less Than One Day

## Customer Profile

Carnegie Mellon University is a global research university with more than 11,000 students, 84,000 alumni, and 4,000 faculty and staff.

[www.cmu.edu](http://www.cmu.edu)

## Situation

The IT staff required a way to automatically update and securely store privileged account passwords to help protect data.

## Solution

Enterprise Random Password Manager was deployed to the enterprise and operational in less than one day.

## Result

Local accounts are now updated with unique passwords on a daily basis and all sensitive privileged passwords are securely stored in a vault.

IT staff at Carnegie Mellon University know that managing privileged account passwords is a requirement for controlling access to sensitive data. Their challenge was to find a solution that could continuously discover, update and securely store all privileged passwords on the network, and be in full production in the least amount of time.

## The Situation

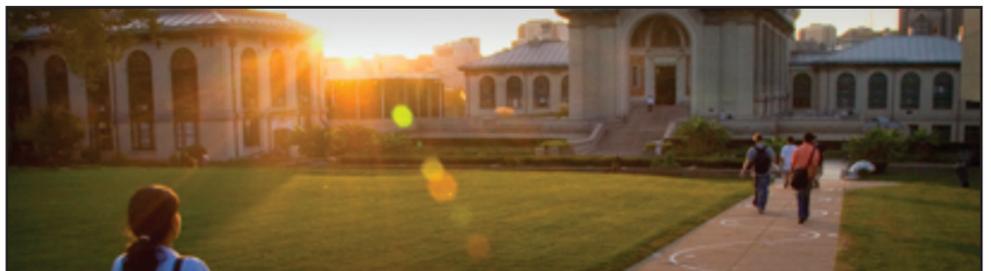
As an advanced research institution with campuses at multiple sites, Carnegie Mellon University is accustomed to having some of its departments operate as independent entities, often with individual IT infrastructures. And while this arrangement helps to empower the institution's research staff, it presents challenges from an IT security standpoint.

"Initiatives like provisioning accounts, setting password policies and configuring users should be centrally managed," said Joe Correy of the Carnegie Mellon IT group.

Correy also includes privileged identity management in his list of strategic priorities. Privileged identities are "super-user" accounts that can access virtually all operating systems, appliances, databases and line-of-business applications in the datacenter. If left uncontrolled, these accounts can provide shared, anonymous access to an organization's IT assets. Common privileged account passwords can potentially be exploited both by insiders and outside attackers, creating a weak link in an organization's security.

Staff at Carnegie Mellon had attempted to manage privileged account passwords manually, first by storing a list of current passwords in a safe and later by writing scripts that changed the passwords. However, these processes were time-intensive, often lacked documentation, were difficult to troubleshoot and provided insufficient reporting. They also offered no way to change privileged passwords frequently enough or detect every credential in need of change.

"I looked at this sideways and thought there must be a better way," Correy said. "I found out that there are privileged identity management products that solve this problem and concluded that it's much more efficient to buy than to build."



Carnegie Mellon University



## The Solution

Correy and his team began researching privileged password management products with the goal to safeguard all major platforms present on the network – including a mix of physical and virtual servers running Windows, Linux and UNIX.

Their investigation led to Lieberman Software's Enterprise Random Password Manager (ERPM). ERPM automates the tasks of locating, tracking, managing and securing the thousands of privileged account passwords dispersed throughout customer networks.

"We evaluated ERPM and decided not to look at other products in this space," Correy said. "The pricing was good and the product met our criteria."

Following the evaluation, the Carnegie Mellon team deployed ERPM to servers in the university's centralized IT department. Correy cited ease of deployment as a significant advantage of ERPM.

"It took less than one day from the time that we started the installation until we changed all of the privileged passwords on our machines. It was that simple."

## The Result

With ERPM, Carnegie Mellon now automatically changes its local account passwords nightly and its SQL Server SA accounts weekly. By doing so, the university secures access to its confidential data and meets the mandates of HIPAA compliance regulations. HIPAA requires documented control and audit trails of the service accounts that grant access to electronic medical records.

IT staff productivity has also benefited from ERPM.

"Previously, when an administrator would leave we'd spend what amounted to days changing all of our privileged passwords and updating the list. It was very cumbersome," Correy said. "With ERPM, when an administrator changes jobs we essentially have the big red button we can press and change all of the passwords in a couple of minutes."

Additionally, ERPM's password store allows the IT staff to secure application passwords in an AES-256 bit encrypted vault that provides delegated, audited access - negating the need to maintain these passwords on a spreadsheet.

*"From the time that we started the installation until we changed all of the privileged passwords on our machines was less than one day. It was that simple."*

With these benefits in place, Correy is turning his attention to additional ERPM features. Future plans include use of the product's delegated workflows for retrieving privileged account passwords. He also intends to start utilizing ERPM to manage the root accounts of Dell DRAC cards on servers in the datacenter.

"ERPM satisfied our purchase criteria on day one," Correy said. "Now we're in the value-add stage."

## 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](http://www.liebsoft.com).



**LIEBERMAN**SOFTWARE

www.liebsoft.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  
© 2010 Lieberman Software Corporation.  
Trademarks are the property of their respective owners.