keeper

Customer Case Study

University Scores Big with Secure Password Vault

Easy, effective password-sharing solution meets consolidation challenges.

IT departments take many forms in different organizations, often growing up as a confederation of quasi-independent teams that eventually are united within a consolidated unit. That was the case at Oregon State University, the venerable Division 1-A university with operations throughout the entire state.

From IT consolidations can arise greater operational efficiencies, more effective standardization drives and common sense pooling of talent, such as security efforts.

Consolidation can also uncover certain weaknesses. One such deficiency that arose at OSU is that the different teams, pre-consolidation, were each managing mission-critical passwords in a variety of ways. Some kept them on spreadsheets that were freely circulated among team members for password sharing, while others created shared drives to house the various passwords - some of which had not been changed in a decade. Others used simple text files or kludgy, single-user applications. The bottom line is that once consolidation took hold, many users could not easily (if at all) access the systems and information assets they needed to do their jobs in the absence of a unified password management system.

The Search for a Simple, Secure Password Vault

Josh Zojonc, lead infrastructure engineer within the IT infrastructure department, began mapping plans and requirements for a password management system for OSU's needs. One thing he absolutely did not want was any solution that would add complexity to OSU's robust IT operations. Thus, his wish list shaped up like this:

- A solution that was not reliant on OSU's network and would not actually operate on that network
- A fully auditable solution
- A mobile-enabled solution that would allow users to restart servers impacted by a network outage simply by accessing the password vault via a smartphone
- Capabilities for two-factor authentication
- Simple central management
- A password vault that represents a "lightweight," yet powerful solution for highly secure sharing of passwords
- The ability to generate very complex and therefore powerful passwords that no individual need remember

"We wanted it to be simple, yet powerful and effective for our password-sharing needs," Zojonc recalled. "We didn't want a complex solution for storing web passwords that auto-logs users into different sites."

Oregon State University

At a Glance

- Founded in 1868
- Serves more than 30,000 students in multiple locations
- Main campus in Corvallis, OR
- Josh Zojonc, lead infrastructure engineer within the IT infrastructure department
- Recently consolidated several IT teams into a single group
- IT staff of 15 maintains 928 virtual machines

Challenge

To unite users in a consolidated group around a common password management solution for effective, secure password sharing.

Keeper Rises to the Top

Zojonc and his team tested trial copies of several different password management solutions. After doing so, OSU settled on the Keeper Security Password Manager and Secure Digital Vault. “No doubt Keeper offered the best shared-password vault solution to meet our requirements,” he said.

“Overall, the deployment of Keeper was smooth. The expectations we set with users is that they’d have a secure and very easy way to share passwords, a simple solution that didn’t get in their way but still was very effective. That’s what they got.”

Additionally, some users are now utilizing the Keeper solution to share increasingly popular SSL certificates - effectively small files that are installed on a server to allow secure connections from the server to a browser. Other users are leveraging the Keeper solution to store private keys as well.

OSU has realized other benefits since deploying the Keeper solution, including the ability to root out and replace inherently weak passwords. And, of course, the solution replaced the less secure, clumsy method of sharing passwords whereby an instant message initiated the sharing of a password certificate.

The Keeper solution also comes with a security analytics scorecard, which allowed Zojonc to track the security effectiveness as the solution was deployed and used. “Our scores definitely went up,” he noted.

While OSU does not yet have a password refresh policy in place, Zojonc said his department has several automation projects on the drawing board into which he would like to include such a policy, now that OSU has a tool making regular password changes so easy.

Zojonc also had praise for OSU’s working relationship with Keeper’s support staff throughout the evaluation, deployment, and early use phases.