KEEPER
Cybersecurity Starts Here®

Case Study

Oregon State University

Oregon State Rallies Around Password Security

KEEPER®

After consolidating several of their information technology (IT) departments, a leading university needed an easy-to-use, secure and highly efficient password management solution.

Challenge

- Independent IT departments using a variety of password management solutions
- Problems accessing data after IT consolidation

Solution

- Password manager and digital vault
- 2FA protection against unauthorized access
- Automated complex password generation
- Password vault access via mobile devices

Results

- Increased efficiency
- Ability to identify and strengthen weak passwords

About Oregon State University

Oregon State University is an international public research university serving more than 30,000 students. In addition to the main campus in Corvallis, Oregon, the school has a second campus in Bend, Oregon, 15 experiment stations and 35 extensions. Oregon State ranks in the top one percent of higher education institutions in the world.[1]

The Challenge

Oregon State University (OSU) is a multifaceted organization with facilities across the state. Over the years, quasi-independent IT departments had formed to address the organization's growing IT needs. To improve efficiencies and better leverage talent, OSU decided to consolidate these teams into a single unit and standardize processes and procedures.

> **To improve efficiencies and better leverage talent, OSU consolidated their IT teams intoa single unit.**

The consolidation revealed that OSU's IT teams were managing mission-critical passwords in a variety of ways. Some used spreadsheets and freely circulated them among team members for password sharing. Others created shared drives to house passwords, some of which had not been changed in a decade. Still others used simple text files or clunky single-user applications. As a result, after consolidation, many users could not easily access the systems and information assets they needed to do their jobs.

Josh Zojonc, Lead Infrastructure Engineer, started mapping plans and requirements for a password management system to meet OSU's needs without added complexity. "We wanted it to be simple to manage, yet powerful," Josh recalled. "We were looking for a solution that would operate independent of OSU's network, be fully auditable and, of course, be as secure as possible."

The Keeper Solution

As part of their due diligence, Josh and his team tested trial versions of several password management solutions. They chose Keeper because it offered unmatched security and the best shared password vault solution to meet OSU's requirements. Keeper also met the team's criteria to provide two-factor authentication (2FA) capabilities, automated complex password generation and password vault access via mobile devices. "We set expectations with users that they'd have a secure and very easy way to share passwords; in other words, a simple solution that didn't get in their way but was very effective. That's what Keeper delivers."

> **Keeper offers unmatched security and the best shared password vault solution to meet OSU's requirements.**

Some users take advantage of Keeper's ability to share increasingly popular digital certificates, which are small files installed on a server to allow secure connections from the server to a browser. Others use Keeper to store private keys.

[1] Oregon State University ranked among the top 1 percent of world universities," Oregon State University, November 8, 2017

The Results

The most immediate and obvious benefit of the Keeper password manager was eliminating clumsy, less secure methods of sharing passwords. As a bonus, streamlining password management was one of the simpler parts of the IT consolidation, thanks to the Keeper support staff's efforts during evaluation, deployment and early use phases.

The Keeper security analytics scorecard, which tracks effectiveness as the solution is deployed and used, confirmed OSU's security improvements. "Our scores definitely went up," Josh noted. "Now that we have a tool for making regular password changes, we can start incorporating a new password refresh policy into the automation projects we have on the drawing board. Another big benefit is the ability to root out and replace inherently weak passwords, which I know is a major contributor to data breaches."

The Impact

As an internationally renowned university, OSU needs unmatched data security to protect its employees, students and valuable information assets. Weak or stolen passwords lead to more than 80% of data breaches,[2] which means organizations must make password management a high priority. Keeper gave OSU an effective, easy-to-implement solution to simplify and streamline password management during a critical organizational change.

> **Weak password security leads to more than 80% of data breaches.**

About Keeper

Keeper Security develops leading password manager and security software for protecting businesses and client information. Keeper works with companies of all sizes across every industry to mitigate the risk of data breaches, bolster data security and privacy, increase employee productivity and strengthen cybersecurity reporting and compliance.

To learn more about Keeper Security's leading password manager and security software, visit **keepersecurity.com**.

[1] Verizon Data Breach Investigations Report, 2017