KEEPER

Industry Brief: Higher Education

Keeper Security Government Cloud Password Manager and Privileged Access Manager for Higher Education

FR AUTHORIZED StateRAMP TX-RAMP

Colleges And Universities Are Targets

Higher education institutions are a primary target of cybercriminals, both because of the vast amounts of student and staff data they possess and due to the potential for large payouts.

Universities, community colleges and private educational organizations often have limited cybersecurity budgets and large attack surfaces due to ever-changing student populations and heterogenous IT resources between departments.

Student and Staff Data Is at Risk

Colleges and universities maintain a wealth of personal information including names, addresses, birth dates, and sometimes even Social Security numbers of students and staff. This data can be sold on the dark web or used for identity theft.

Campuses Lack of Robust Security

Many colleges and universities do not have a Privileged Access Management (PAM) solution in place. Legacy PAM solutions are often too costly, too complex and too difficult to manage for time and budget-strapped higher education IT teams.

Failure To Act Is Costly

Recovering from a cyberattack can be expensive. Organizations might need to hire external experts, replace compromised hardware, purchase new software or pay ransoms. In addition, universities are often required by law to protect student data. A breach can lead to legal consequences, potential lawsuits and fines.

Colleges and Universities Are Under Attack

200

There were nearly two hundred reported ransomware attacks targeting US universities between May of 2022 and June of 2023.[1]

74%

The percentage of data breaches that are due to the human element, with stolen or weak passwords acting as a primary vector for cybercriminals.

56%

Over half of IT teams report they’ve tried to deploy a PAM solution, but didn’t fully implement it due to complexity.

$3.7M

Data breaches cost higher education and training organizations $3.7M on average in 2023.[2]

[1] University of Hawai’i News

[2] Higher Ed Dive

KEEPER

Industry Brief

Higher Education

Cybersecurity Starts with Protecting Your Passwords, Secrets and Credentials

Keeper Security Government Cloud (KSGC) Password Manager and Privileged Access Manager delivers enterprise-grade password, passkey, secrets and privileged connection management in one unified platform.

Bonus >>> Keeper provides a free personal password manager to all students

Keeper gives higher education institutions the visibility and control they need to prevent credential-based cyberattacks by enabling IT administrators to manage employee password use and systems access throughout the data environment.

Keeper provides privileged account session management, secrets management, Single Sign-On (SSO) integration, privileged account credential management, and powerful credential vaulting and access control.

Protect Passwords and Credentials

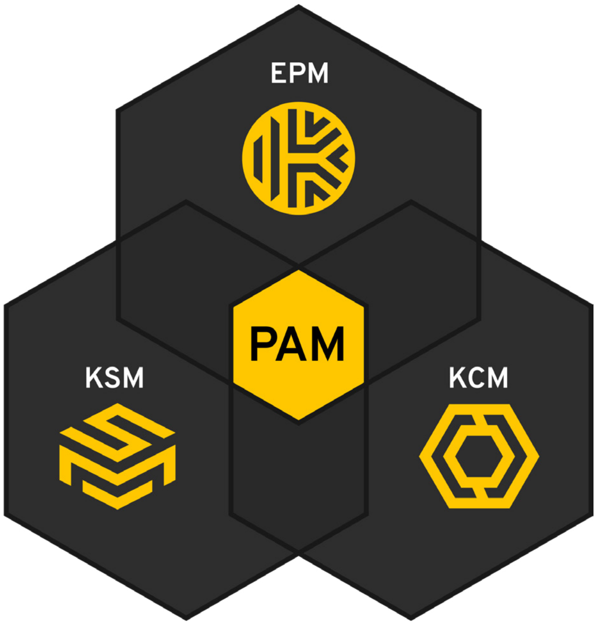
Keeper's unique security architecture protects data and systems with a solution that is quick to deploy and easy to use. Securely store, share and manage passwords across the entire organization.

Simplify Secure Remote Access

Securely manage your remote connections from anywhere – no VPN required.

Streamline Compliance and Audits

Provide on-demand visibility of access permissions to your organization's credentials and secrets.



KEEPER PASSWORD MANAGER

Enables organizations to securely manage, protect, discover, share and rotate passwords and passkeys with full control and visibility to simplify auditing and compliance.

KEEPER SECRETS MANAGER

Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.

KEEPER CONNECTION MANAGER

Provides an agentless remote desktop gateway for instant privileged session management, remote infrastructure access and secure remote database access with RDP, SSH keys, database and Kubernetes endpoints – without the need for a VPN.