KEEPER

Industry Brief: K-12 Education

Keeper Security Government Cloud Password Manager and Privileged Access Manager for K-12 Schools

K-12 Schools Are Targets

School systems are a primary target for cybercriminals, both because of the vast amounts of student and staff data they possess and the potential for large payouts. Cyberattacks targeting K-12 schools in the U.S. rose from 400 in 2018 to over 1,300 in 2021.[1] In addition, debilitating ransomware attacks targeting K-12 organizations have grown 827% since 2021.[2]

Student and Staff Data Is at Risk

Schools maintain a wealth of personal information, including names, addresses, birth dates and sometimes even Social Security numbers of students, staff, and parents. This data can be sold on the dark web or used for identity theft. Schools are critical public institutions, and any disruption to their operations can have serious consequences. This makes them potential targets for ransomware attacks.

Schools Lack Robust Security

Many K-12 school systems do not have the latest security infrastructure in place. Budget constraints, lack of IT personnel or simply not recognizing the potential threats can lead to vulnerabilities in their systems. Student passwords are particularly problematic as IT teams must enforce length and complexity requirements but also ensure students are able to easily log in to password-protected systems such as student portals.

Failure To Act Is Costly

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

Public School Systems Are Under Attack

827%

Ransomware attacks targeting K-12 school systems have increased more than eightfold since 2021.

$9.4B

The total cost of ransomware attacks on K-12 schools in 2022 is estimated to be nearly ten billion dollars.[3]

74%

The number of data breaches due to the “human element” with a majority involving weak or stolen passwords.

9 MONTHS

It takes a K-12 school two to nine months on average to fully recover from a successful cyberattack.[4]

[1] Partnering to Safeguard K-12 Orgaizations from Cybersecurity Threats Report
[2] The Journal
[3] Comparitech
[4] 2022 U.S. Government Accountability Office Report

KEEPER

Industry Brief
K-12 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 educational organizations 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 Employee Passwords and Credentials

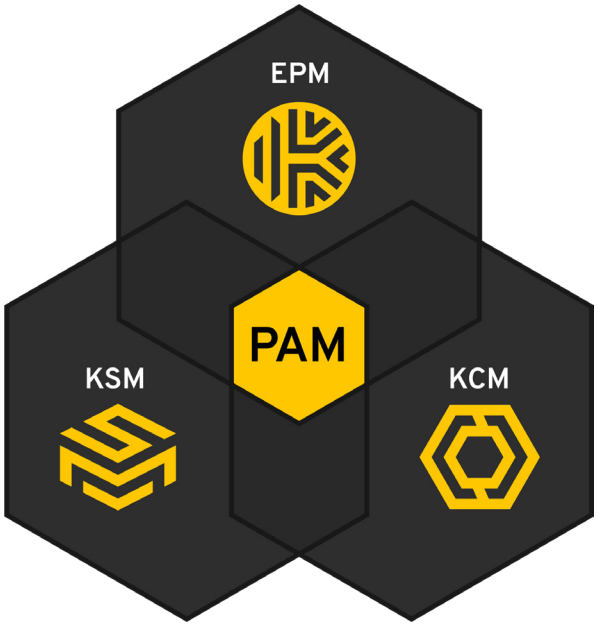
Keeper's unique security architecture protects data and systems with a solution that is quick to deploy and easy to use. Securely store, share and manage passwords across the entire organization.

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.