KEEPER
Cybersecurity Starts Here®

DATASHEET
Energy Industry Brief

Financially Motivated Cybercriminals Threaten Energy Providers

64%
of energy industry leaders say that sophisticated cyberattacks are a top challenge[1]

56%
report at least one shutdown or operational data loss per year[2]

54%
expect an attack on critical infrastructure in the next 12 months[3]

Cybersecurity is Crucial as Energy Providers Digitize

The energy industry is powered by operational technology (OT) systems, the highly specialized hardware and software used to generate, transmit, and distribute power. Historically, OT and IT systems were siloed from each other, which shielded OT systems from cyberattacks. However, as the utility industry digitally transforms, OT systems are being connected with IT systems, enabling energy providers to replace centralized power generation with distributed systems of natural gas and renewable energy.

Digitization makes energy delivery more efficient, benefiting both utility customers and the environment, but it also enables cybercriminals to breach OT systems simply by compromising a set of employee login credentials. Cyberattacks on OT systems can damage energy grid assets, causing power outages, damaging the environment, and putting human health and life at risk.

In addition to nation-state cybercriminals who are seeking to damage utility grids, the energy industry is a prime target for financially motivated ransomware attacks, as utility providers have an incentive to pay up quickly. In October 2020, multinational energy company Enel Group was hit by a ransomware attack[4] for the second time in the calendar year; attackers demanded a $14 million ransom payment to release decryption keys.

The COVID-19 pandemic has left energy providers especially vulnerable. With many employees working remotely, cybercriminals can take advantage of insufficiently secured remote workforces and undermanned facilities.

Keeper Helps Energy Providers Secure Critical Infrastructure

Keeper enables energy providers to protect their OT systems by securing the most vulnerable part of their IT networks, their employees' passwords.

Every employee is provided with a secure digital vault. A security dashboard in the Admin Console provides an overview of weak passwords, password reuse, and 2FA enforcement, along with role-based access controls (RBAC) to enforce least privilege policies. Administration may be delegated according to department or by team leader, and folders and records can be securely shared and revoked. If an administrator or employee leaves the company, their vault can be automatically locked and securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

Secure More than Just Passwords with Keeper Secure File Storage

In addition to securing employee passwords, Keeper helps organizations prevent theft of digital IP and other sensitive data by enabling them to store sensitive files, documents, digital certificates, private keys, images, and videos in a highly secure, encrypted digital vault. Employees can securely share files with colleagues with confidence, knowing that only the intended recipients can access the shared files.

Keeper uses PBKDF2 to derive authentication keys based on the user's Master Password, then generates individual record-level AES-256 encryption keys locally on the device to encrypt each stored file. Keeper's cloud only holds the encrypted ciphertext of each file. Sharing between users is performed using PKI to ensure that only the recipient of a shared file can decrypt it. Keeper's zero-knowledge encryption methods ensure that only the user can access and decrypt their stored files.

Defend Against Third-Party Vendor Breaches with BreachWatch™

Even if your password security is solid, your organization could be compromised through one of your vendors. With remote workforces having rapidly expanded, cybercriminals are taking advantage of the myriad of SaaS solutions that businesses are deploying to enable their remote workforces.

Data breach victims are typically the last ones to know they've been compromised. It can take a breached organization months, even years to detect a breach, but cybercriminals don't wait. When they steal login credentials, they put them to use very quickly, either by launching their own cyberattacks or by putting them up for sale on the Dark Web - the part of the World Wide Web that is only accessible by means of special software.

Keeper's BreachWatch for business protects your organization against third-party vendor breaches. BreachWatch for business doesn't depend on public breach notifications. It scans Dark Web forums and notifies organizations in real-time if any employee passwords have been compromised. This allows IT administrators to force password resets right away, minimizing the risk of cybercriminals using them to breach company systems.

Simplify Compliance Enforcement & Reporting

Keeper simplifies compliance monitoring and reporting with robust internal controls through delegated administration, enforcement policies, event tracking, monitoring, and reporting, as well as customizable audit logs and event reporting.

Email Auto-Provisioning

Easily and quickly provision Keeper vaults to tens or thousands of users, with a domain match on email addresses. With minimum administration, large-scale deployment can be accomplished using an existing email channel or portal.

Flexible Provisioning

Keeper supports the ability to seamlessly provision users and teams from Microsoft Azure AD or other identity platforms using the SCIM protocol. Keeper also supports API-based, command line provisioning through the use of Keeper® Commander SDK. The Keeper Commander SDK is open-source Python code that is available for download from Keeper's Github repository.

Microsoft Active Directory Synchronization

Keeper® AD Bridge synchronizes to Microsoft Active Directory or OpenLDAP. This enables rapid user provisioning and automatically adds Nodes (organizational units), Users, Roles, and Teams. Keeper enables RBAC and the ability to track roles when employee positions or job duties change. This includes automatically locking vaults when employees depart the company.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. In 2020, Keeper was named PCMag's Best Password Manager of the Year & Editors' Choice for the third time. Keeper has also been named PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM).

Keeper Third-Party Attestations and Certifications

[1] Siemens [2] Ibid [3] Ibid [4] Information Security Buzz