KEEPER
Cybersecurity Starts Here

DATASHEET

Manufacturing Industry Brief

Stolen User Credentials Put Manufacturers at Risk

target for phishing attempts are manufacturers[1]

most common target for cyberattacks[2]

of data breaches target user credentials[3]

increase of ransomware attacks between Q4 '19 & Q1 '20[4]

Vulnerable IT Systems Put Operational Technology (OT) Systems at Risk

The manufacturing industry is powered by operational technology (OT) systems, the highly specialized hardware and software that monitors and controls the physical equipment and processes used in today's automated manufacturing plants.

Historically, OT and IT systems were siloed from each other, which shielded OT systems from cyberattacks. However, as manufacturing became increasingly computer-driven, IT and OT networks became interconnected. While this interconnectivity enables holistic management of production systems, it enables cybercriminals to use IT systems as backdoors into OT systems.

Cyberattacks on OT systems can damage plant equipment, causing production bottlenecks and even putting human health and life at risk. In 2014, cybercriminals used a spear phishing campaign to obtain user credentials to a German steel mill's corporate IT network. Once inside the mill's IT systems, the cybercriminals accessed OT systems and manipulated the controls for a blast furnace, causing massive damage to plant equipment.[5]

OT systems are also vulnerable to ransomware attacks, which can damage equipment, put employees in danger, and halt operations. In October 2020, Steelcase, the world's largest office furniture manufacturer, suffered a ransomware attack that forced it to shutter operations for two weeks. It is believed that attackers accessed Steelcase's network after obtaining a set of admin credentials, then deployed the ransomware payload.[6]

In addition to attacks on OT systems, manufacturers have long been targets for cyberespionage perpetrated by nation-state actors or competitors who are seeking to steal valuable digital intellectual property (IP), such as product design schematics. Often, cyberspies enlist the help of malicious company insiders. According to Verizon, 27% of cyberattacks on manufacturers involved espionage activities, and 25% of attacks involved company insiders misusing their credentials.[7]

Exacerbating these problems, many manufacturers are small businesses that lack comprehensive cybersecurity defenses. In addition to being soft targets for cybercrime, these small manufacturers are more likely than large enterprises to experience significant downtime as they attempt to restore operations following an attack.

Keeper Protects Your IT Systems, OT Systems, and Digital IP

Keeper enables manufacturers to secure their number-one vulnerability, their employees' passwords, enabling them to address password security across their entire data environment and protect both their IT and OT systems.

A security dashboard in Keeper's Administrative Console provides an overview of weak passwords, password reuse, and 2FA enforcement, along with role-based access controls (RBAC) to enforce least privilege policies that prevent users from accessing data and systems that have nothing to do with their jobs. 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.

In addition to giving administrators complete control over employees' password usage, Keeper helps prevent employees from entering their credentials on phishing sites. Many phishing sites are carefully designed to look just like the "real" webpage they are impersonating, right down to a phony URL that is only a bit different. These phony URLs may get past the naked eye, but they don't get past Keeper. If a user tries to use Keeper to auto-fill their login credentials on a phishing site, Keeper notifies them that there's no match for that URL in their vault, a big red flag that they're about to be scammed.

Secure More than Just Passwords with Keeper Secure File Storage

Digital IP is the lifeblood of today's manufacturing industry. In addition to securing employee passwords, Keeper helps manufacturers 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 company 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).

[1] IndustryWeek [2] Dark Reading [3] Verizon [4] Beazley [5] BBC News [6] Bleeping Computer [7] Verizon DBIR