KEEPER SECURITY

New year, new CMMC password requirements

Companies can satisfy several CMMC controls with a password manager and privileged access manager rooted in zero trust

Mike Eppes
Keeper Security

The much-anticipated CMMC 2.0 proposed rule was officially published in the Federal Register on Dec. 26, 2023. The final rule is expected to be out sometime this spring. Although the rule is long and complex, the basic purpose of the Cybersecurity Maturity Model Certification (CMMC) program is to ensure that every organization that does business with the Defense Department is certified via a third-party audit that demonstrates its basic cyber hygiene.

One area of cyber hygiene that the new CMMC rule addresses is password management. The majority of CMMC's current security controls are based on the National Institute of Standards and Technology's Special Publication 800-171 Revision 2, which was released in 2020. NIST 800-171 Revision 3 will be released in the coming months and will include new requirements for passwords. Defense contractors will need to account for these new requirements, such as changing passwords when they have been compromised and ensuring that new or updated passwords are not on lists of commonly used, expected or compromised passwords.

Adopting a zero trust mindset

These seemingly simple requirements are of vital importance to our nation's security. DOD is entrusted with highly sensitive, classified information. And contractors often have access to controlled unclassified information, such as personally identifiable information, health documents, proprietary material and information related to legal proceedings.

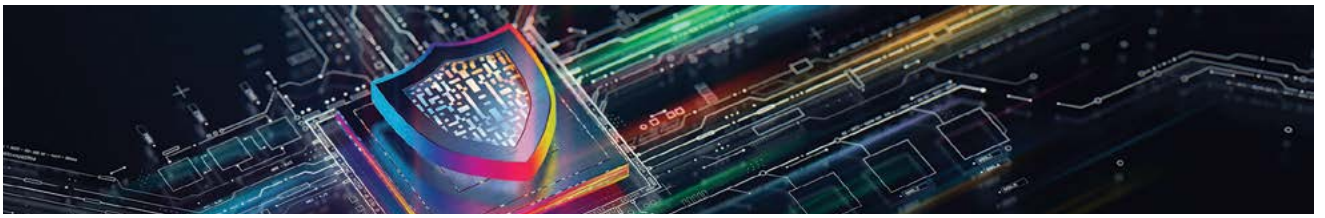
Every member of DOD, including contractors, must adopt a zero trust mindset. This "never trust, always verify" attitude requires companies and individuals to take responsibility for the security of their data, devices, applications and assets. It also means users are granted access only to the data they need and only when needed.

> "A 'never trust, always verify' attitude requires companies and individuals to take responsibility for the security of their data, devices, applications and assets."

With zero trust, password management is one of the simplest ways to protect sensitive systems and data. Seventy-four percent of all breaches involve the human element, with the majority due to weak or stolen passwords. Yet most IT administrators have no visibility, security or control over their employees' passwords and credentials.

A FedRAMP-authorized solution

Keeper Security gives IT and security teams visibility into the strengths and weaknesses of their organizations' passwords and alerts administrators when



iStock

passwords have been compromised or when users are not complying with organizational password policies, such as prohibitions on password reuse. This approach allows administrators to proactively address weaknesses and prevent data breaches.

Keeper Security Government Cloud (KSGC) is a password manager and privileged access manager that is FedRAMP-authorized to protect against cyberthreats. The zero trust solution is further strengthened with zero knowledge security. KSGC provides an advanced cloud authentication and network communications model built for the highest levels of privacy, security and trust.

Each end user is provided with a vault to store passwords, and the contents of the vault are protected with multiple layers of safeguards and encryption. Decrypting a user's vault requires decryption of the data key, which can include a user's master password. For users who log in with single sign-on or passwordless technology, elliptic curve cryptography is used to encrypt and decrypt data at the device level.

KSGC is also StateRAMP-authorized and validated under FIPS 140-2. Hundreds of defense industrial base organizations rely on Keeper to protect their passwords, secrets and privileged credentials from the dynamic threats facing our nation's military.

It's expected that the CMMC proposed rule will be final by the end of 2024 and start to appear in contracts in 2025 so it's important to start preparing now. Many people look at CMMC as another security checklist, but I hope it's also encouraging companies to make a long-term commitment to zero trust by securing every user on every device and in every location. ■

Mike Eppes is director of public sector at Keeper Security.