OVERVIEW

Protecting U.S. Government networks, systems, and data against advanced and sophisticated cybersecurity threats from outside attacks is a daily reality. But protecting networks from trusted and privileged users inside the network has led to increased concern and a need to rethink security solutions and services that specifically address insider risks.

While there are many standards and compliance mandates that address the risks of external and insider threats to government, a hacker’s most sought after method of breaching a system is through the acquisition of a privileged user’s password or other credentials. Acquisition of those credentials could allow an adversary to disrupt mission critical operations, compromise sensitive information, exfiltrate or corrupt data, or own or deny service to those systems.

The importance of privileged access management increased after the Office of Personnel Management (OPM) was breached because a privileged account credential was shared with a government contractor who was then hacked, exposing over 22 million government employee records.

The use of a Privileged Access Management (PAM) Solution aligns with important compliance standards, including FISMA, NIST SP 800-53, DFARS, and ISO 27001. And, it aligns with Federal Identity, Credential and Access Management (FICAM), and NIST’s Cybersecurity White Paper that state privileged accounts need to be monitored, actively managed, given least privilege as required, and automatically reviewed.

CHALLENGE

Meeting accessibility and compliance requirements means that IT staff are constantly pushing to allow access for their network and system users while also protecting data, networks, and systems from potential breaches.

Managing inter- and intra-agency network and system access, and a growing remote workforce, means organizations need compliant and secure ways to give privileged users the access and collaboration tools they need to meet administrative goals.

Cybersecurity experts expect that updates to federal requirements related to privileged users and privileged access will include privileged access management, real-time monitoring, and automated responses to potential cybersecurity threats.

SOLUTION

Agencies need to rethink the way they handle privileged accounts from the view of an adversary and minimize potential threats.

Managing and securing privileged user accounts and elevated privileges are a key component of federal government’s cybersecurity standards, including ISO 27001 and NIST SP 800-53 that focus on Access Control, Audit and Accountability, as well as Identification and Authentication security controls. These controls give agencies guidelines on how to manage privileged user accounts, including methods for encrypting passwords.
over government networks, two-factor authentication, strong passwords, real time password updates, and user/access approval workflows.

The use of Local Administrator rights instead of a Least Privilege strategy, and the way agencies and organizations still allow unfettered access to networks by broadly allowing the use of privileged accounts, results in administrator accounts being the most common targets of nation-state adversaries, hackers, and cyber-criminals. Once gained, adversaries could install malware, steal information, compromise systems, and stage attacks against domains, servers and other network-connected devices.

THYCOTIC CAN HELP YOUR ORGANIZATION

Thycotic’s security solutions can help agencies meet requirements for managing, monitoring, and providing visibility into privileged user accounts across an agency’s networks, systems, and devices.

Thycotic Secret Server

- Meet CNSS, OMB/FISMA and NIST requirements and guidelines for protecting privileged user account passwords and credentials.
- Enforce and support multiple top-level security layers including AES 256 encryption, two-factor authentication, 100-character passwords, custom workflow approvals, active session monitoring, and SIEM integration.
- Organize privileged accounts in intuitive nested folders through a simple, customizable dashboard.
- Manage, create, share, and automatically change privileged account passwords.
- Assign user permissions at any level.
- Track password use with audit reports showing access and requested access for every privileged account.
- Alert the team in real time when network passwords are changed.
- Create customized alerts for specific types of access.

Additional Thycotic Solutions for PAM:

**Secure Vault**
Secure accounts with privileged access.

**Discovery and Automation**
Find privileged, yet unknown accounts.

**Session Control**
Proxy, record, and monitor active sessions within critical infrastructure.

**Access Workflow**
Add access approval workflows for sensitive accounts.

**Behavior Analytics**
Alert security team to anomalous behavior on privileged accounts.

**Least Privilege**
Establish, monitor, and manage accounts beginning with least privilege access.

**Application Control**
Allow users to install and update approved software.

**User Management**
Grant workers active directory password reset and AD group self-management that is audited and secure.