Security Hardening Best Practices

Security is a shared responsibility, and it is recommended that customers have an overall security program to protect their organization, manage risk and adjust for constantly evolving threats. While AspenTech products contain some security controls, it is best for an organization to have an overall security program that leverages best practices. This includes a program that follows industry best practices, such as defense in depth, least privilege access and training of its personnel. The following are examples of typical industry standards that customers should consider as part of their overall security defense.

Hardening Your Organization for Security

We recommend the following best practices for hardening your organization for security:

- **Develop a Security Policy:** Establish clear security policies and procedures that align with industry standards. Standards may include best practices such as the NIST Cybersecurity Framework, ISO 27001 and ISO 9001.
- **Employee Training:** Conduct regular cybersecurity awareness training to educate employees about phishing, social engineering and other common threats.
- **Access Control:** Least privilege access to systems, devices and applications. Implement role-based access control (RBAC) to ensure employees have access only to the information necessary for their roles.
- **Incident Response Plan:** Develop and regularly update an incident response plan to quickly address security breaches.

Desktops

We recommend the following best practices for hardening desktops:

- **Patch Management:** Ensure all operating systems and applications are up-to-date with the latest security patches.
- **Antivirus Software:** Install and regularly update antivirus software to protect against malware.
- **User Account Control:** Limit administrative privileges and use standard user accounts for daily tasks.
- **Encryption:** Use disk encryption to protect sensitive data stored on desktops.
- **Firewall:** Enable and configure the built-in firewall to block unauthorized access.

Windows Servers

We recommend the following best practices for hardening Windows servers:

- **Patch Management:** Regularly apply security patches and updates to the server operating system and applications.
- **Antivirus and Anti-Malware:** Install and configure antivirus and anti-malware solutions.
- **Access Control:** Implement least privilege access and use strong authentication methods.
- **Disable Unnecessary Services:** Turn off services that are not required to reduce the attack surface.
- **Log Management:** Enable logging and regularly review logs for suspicious activity.

Cloud Instances

We recommend the following best practices for hardening cloud instances:

- **Secure Configuration:** Ensure cloud instances are configured securely according to best practices.
- **Access Control:** Use identity and access management (IAM) to control access to cloud resources.
- **Encryption:** Encrypt data at rest and in transit.
- **Monitoring:** Implement continuous monitoring and logging to detect and respond to security incidents.

Network Operations

We recommend the following best practices for hardening network operations:

- **Firewall Configuration:** Configure firewalls to block unauthorized access and monitor traffic.
- **Network Segmentation:** Segment the network to limit the spread of potential threats.
- **Intrusion Detection and Prevention:** Deploy intrusion detection and prevention systems (IDPS) to monitor and block malicious activity.
- **Secure Protocols:** Use secure communication protocols, such as HTTPS, TLS, or SSH.
- **Regular Vulnerability Assessments:** Conduct regular vulnerability assessments to identify and mitigate network security risks.