SECURE MEDIA EXCHANGE

SMX: Enterprise Solutions

Deploy, Optimize and Enforce USB Device Controls Across Multi-Site Organizations to Enable In-Depth Protection for OT Environments

Honeywell

The Benefits of Honeywell SMX with Honeywell Cyber Threat Intelligence + Google Threat Intelligence (GTI)

"The majority of breaches are due to human error" (source: Verizon's 2021 Data Breach Investigations Report (DBIR).

In the rapidly changing OT threat landscape, maintaining regulatory compliance and security for multi-site organizations is becoming increasingly crucial. Balancing resources, budgets, and safety adds to the complexity. SMX, combined with the Honeywell Cyber Threat Intel and GTI, is designed to offer robust security for removable media in OT environments.

The Honeywell SMX Enterprise offering is designed to be a cost-effective and secure managed solution, featuring centralized reporting and compliance.

As digital transformation accelerates within the OT cybersecurity perimeter, the pressure on existing capabilities intensifies. While adopting new technologies like IIoT and meeting sustainability targets is essential, implementing robust controls is equally critical. Amidst these changes, enterprises require enhanced protection against human error and malicious intent.

Honeywell Cyber Threat Intelligence focuses on OT (operational technology) threat detection, analysis, and defense.

With the integration of Google Threat Intelligence (GTI) and Cyber Threat Intelligence now offers the following enhanced capabilities and features in addition to its existing offerings:

- File upload and advanced malware analysis capabilities
- Contextual analysis and threat information
- IOC (Indicator of Compromise) reputation and enrichment capabilities
- Adversary Tactics and Techniques Detection (ATTD)
- Executive and detailed reports
- Integrated dashboard for threat insights
- Integration with SOC/SIEM/SOAR tools to automate analysis
- Identification and prioritization of threats

MULTI-SITE MANAGEMENT

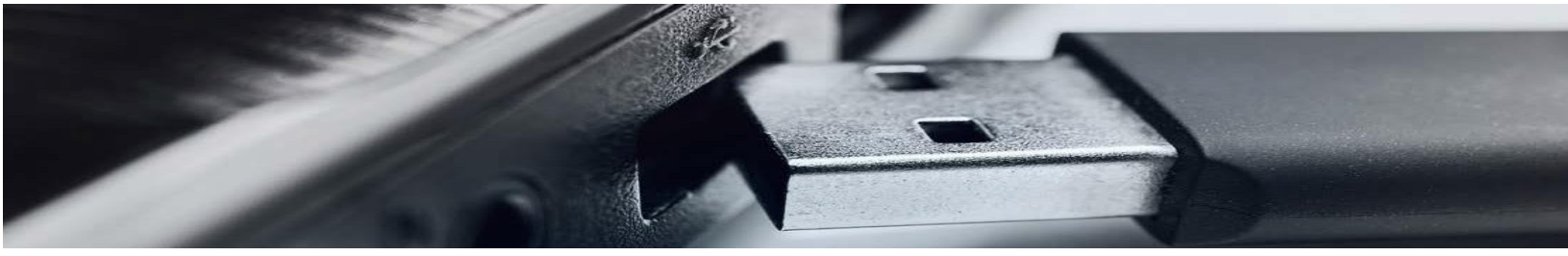
Managing the USB devices and removable media brought into your sites can be challenging. The SMX solution offers five key strengths that provide comprehensive USB device protection:

1. SMX Gateway
2. Cyber Threat Engine + GTI
3. SMX Client Driver
4. Enterprise Management Portal
5. Cyber Threat Research Team

SMX enterprise deployments allow Honeywell to collaborate closely with you to design, configure, and deploy your SMX fleet. All SMX patches and updates are managed automatically, with alerts sent to designated contacts. If needed, we can integrate SMX with your existing IT SOC.

This approach offers three key benefits:

- Empowers you to focus on other critical organizational projects.
- Enables your engineers to use removable media confidently, knowing that multiple controls are in place to minimize mistakes or malicious activity.
- The enterprise management console provides visibility and reporting to help you oversee your removable media protection and facilitates auditing for regulatory compliance.



HONEYWELL SMX

Minimize risk by enforcing active policy controls for USB devices throughout your organization.

Honeywell SMX enhances industrial USB cybersecurity across the OT environment with the Enterprise Threat Management Portal. It provides comprehensive visibility and management of USB devices, activities, and content across the organization, including remote sites, offshore facilities, air-gapped automation environments, and other challenging areas.

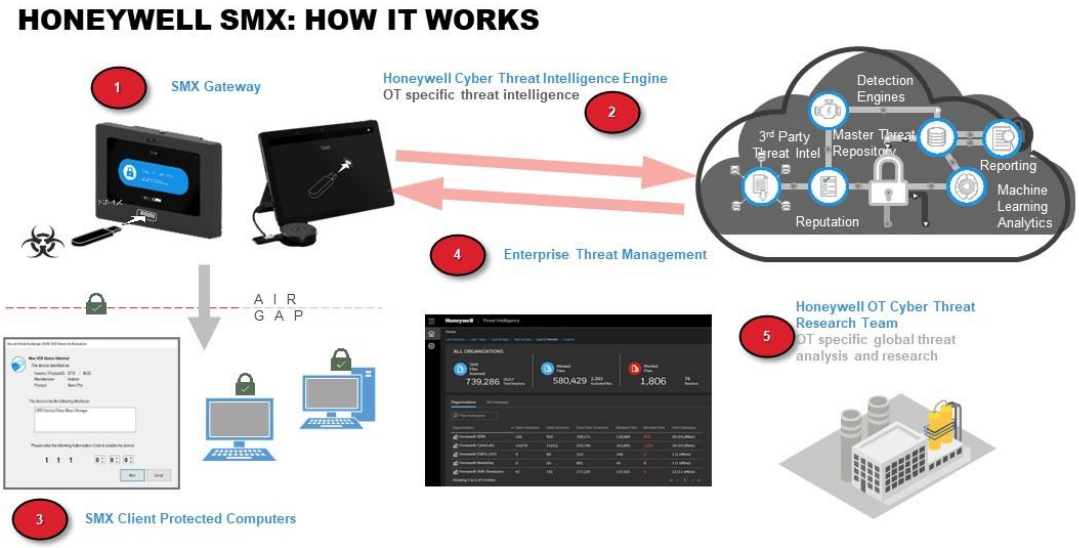
WHY HONEYWELL SMX?

- Enterprise-wide management of USB devices
- Enhanced defense against advanced USB hardware threats
- Custom file policies enable Increased efficiency with custom file policies for well-known files
- Proactive research and malware analysis to stay ahead of emerging OT threats
- The SMX Portable Scanner (PS) is a USB-based scanning solution designed for secure, on-site use in industrial environments. It enables users to scan Windows-based machines and air-gapped systems without internet access.

WHAT IS HONEYWELL SMX?

- Enterprise Threat Management Portal: Remotely manage removable media, logs, and files
- SMX Client: Enforcement driver ensuring all storage media is scanned before use on protected workstations
- SMX Gateway: Fully managed rugged or portable scanning station for any environment, designed to protect OT assets from malicious files and hardware-based threats
- Cyber Threat Engine + GTI: Industry-leading OT threat detection powered by Google Threat Intelligence (GTI)

HONEYWELL SMX 5 KEY COMPONENTS



HOW HONEYWELL CAN HELP

- SMX enterprise solutions simplify the deployment and management of the SMX solution across your organization by offering a managed custom configuration service.
- Honeywell cybersecurity engineers will collaborate with you to understand your specific needs and requirements across your distributed OT/IT environment.
- We work closely with you to determine the best method for deploying your SMX units and the most effective use of your Enterprise Threat Management Portal.
- This custom configuration service ensures that you receive the best possible service and value for your business.