SECURE MEDIA EXCHANGE SMX

Enforceable Enterprise USB Device & Removable Media Cybersecurity Solution for Operational Environments

Honeywell

REMOVABLE MEDIA KEEPS OPERATIONS RUNNING

In today's current cybersecurity climate, OT leaders are looking for a low effort USB Device Management solution that solves a problem to a big pain. Not only is there a need to find ways to more safely use and monitor removable media, USB device regulatory compliance requirements are also on the increase. Unfortunately, many cybersecurity tools and strategies have failed to adapt to evolving operational demands, while creating excessive cost and labor burdens to deal with evolving hardware-based threats like Rubber Ducky's or Bash Bunny's.

Throughout industries such as refining, pulp & paper, oil & gas, mining & minerals, pharmaceuticals, power generation, buildings, manufacturing and aerospace, removable media is critical to maintaining the availability and security of facility processes, and yet they introduce potential security risks.

Despite IT policies banning USB usage, removable media is often used across industrial control networks because:

- The diversity of system platforms from multiple vendors makes it difficult to centrally manage updates
- The long lifespan of equipment creates a mix of legacy and modern systems, all requiring ongoing updates.

Limitations of Existing Solutions

Within a manufacturing facility, there is a need to balance the requirement for swift software updates with the task of protecting critical assets against disruption or malicious attack.

This comes at a time when industrial networks are changing dramatically to more digitally interconnected software and systems. The days of air-gapped architectures are over, with digital connectivity opening up more opportunities for hackers to attack.

Unfortunately, information technology (IT) security approaches are frequently unsuitable for production and manufacturing environments. Even if these approaches are acceptable for the organization's business network, they might be catastrophic in an operational technology (OT) environment. IT-related anti-virus (AV) software is known to miss OT vulnerabilities, and IT monitoring tools can create control network traffic that interferes with important process commands.

USB security workarounds such as maintaining auxiliary engineering workstations for updates and patching, or using unsecured file transfer techniques can create excessive costs, burden and risks.

Lastly, traditional USB scanners don't solve the removable media security problem for industrial sites since they require continuous AV software updates to stay current and are designed to detect IT-related threats only.

HONEYWELL SMX

Reduce risk by enforcing active policy controls for USB Devices across your organisation.

Honeywell SMX extends leading industrial USB cybersecurity across the OT Enterprise, with the Enterprise Threat Management portal.

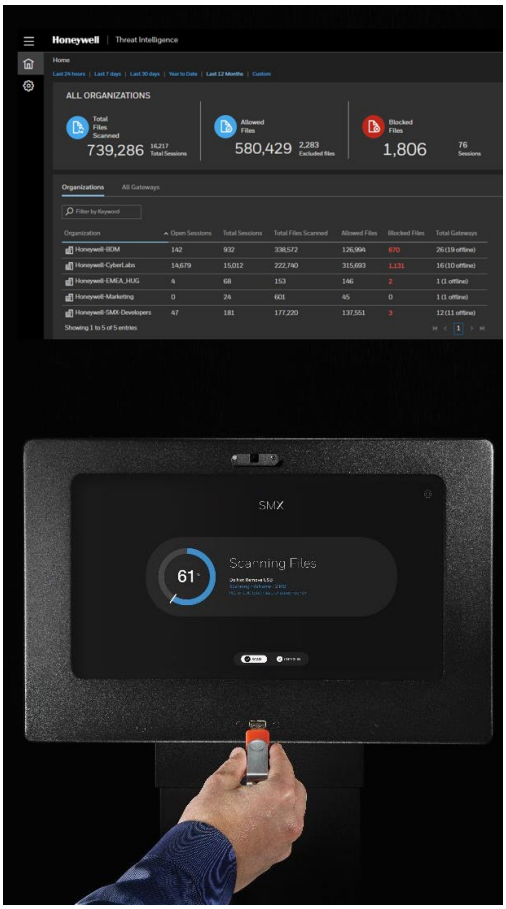
Honeywell SMX allows for visibility and management of USB devices, activity, and content across the organization – including remote sites, offshore facilities, air-gapped automation environments, and other challenging areas.

WHY HONEYWELL SMX?

- No surprises! Manage USB devices across the enterprise
- Better defend networks from hardware threats (cell phones, keyboard, etc.)
- Increase efficiency while updating and patching your production environment with custom file policies
- Stay on top of emerging OT threats with proactive research, malware analysis & deep web mining

WHAT IS HONEYWELL SMX?

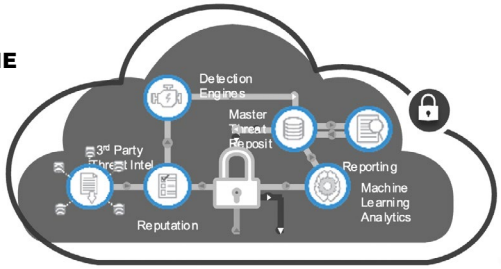
- Enterprise Threat Management Portal – Manage removeable media, logs and files remotely
- Enforcement Driver – All storage media must be scanned before use
- SMX Solution – Fully managed rugged, micro or portable scanning station for any environment. Better protect your environment from hardware-based threats e.g., rubber ducky, cell phones
- GARD Engine – Industry leading OT threat detection



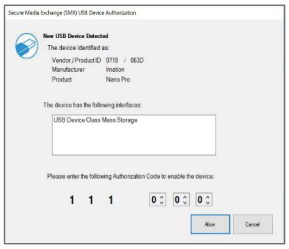
HONEYWELL SMX 5 KEY COMPONENTS

1 SMX SYSTEMS

2 GARD THREAT ENGINE
Global Analysis, Research & Defense

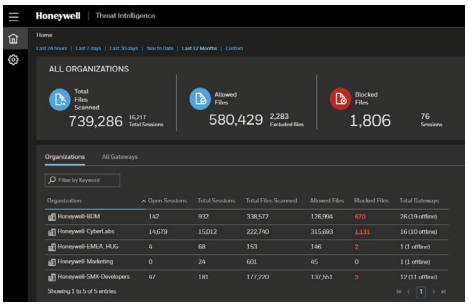


AIR GAP

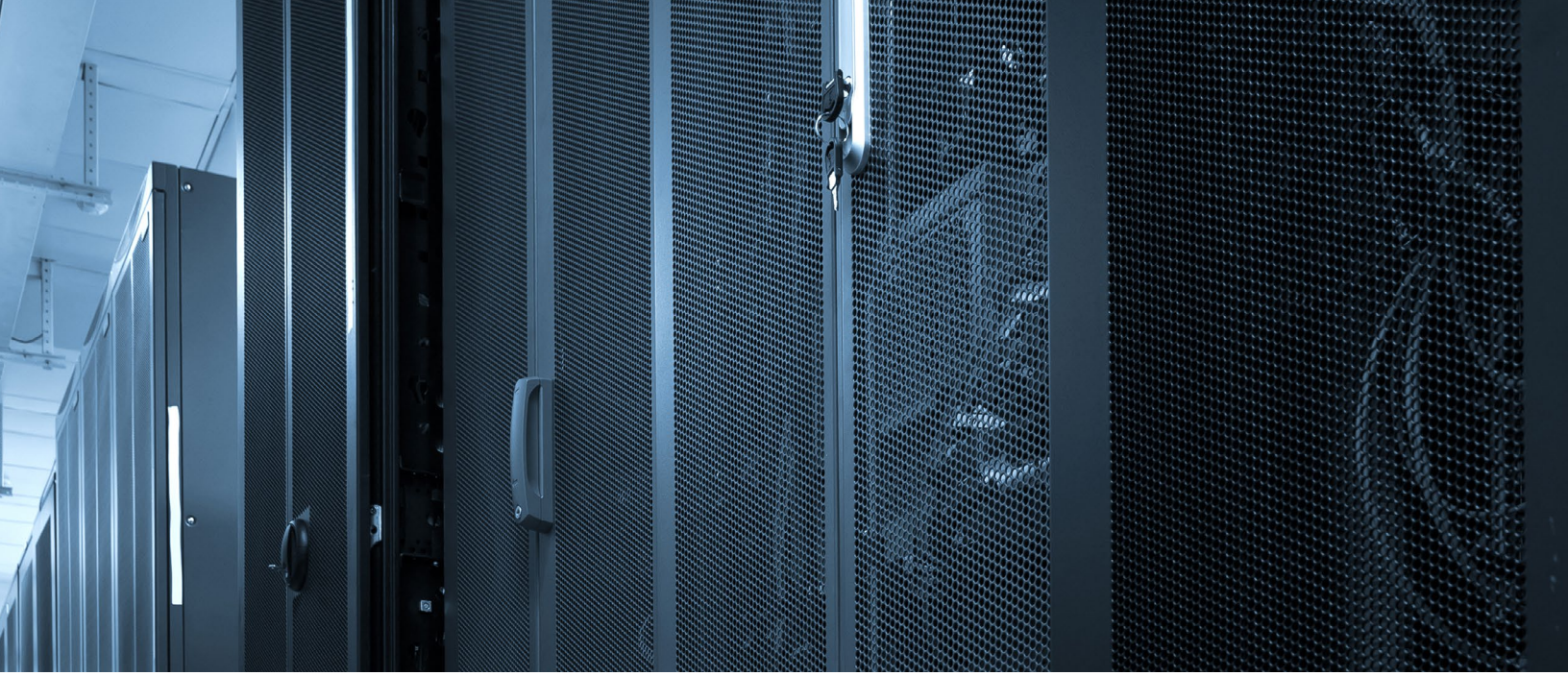


3 SMX CLIENT ENFORCEMENT DRIVER

4 ENTERPRISE THREAT MANAGEMENT PORTAL



5 GARD THREAT RESEARCH TEAM
Global Analysis, Research & Defense



FIRST THREAT DETECTION TOOL OF ITS KIND

SMX is designed to assist a customer in reducing their cybersecurity risks and limits operational disruptions by monitoring, better protecting, and logging use of removable media throughout industrial facilities. The SMX gateway security device simply resides in your physical "front desk" or a site location of your choice. A consumer-driven touch screen—which works even with gloves on— intuitively prompts visitors to insert their removable media as part of check in procedure. Malware and other security threats are detected before they can be transmitted by USBs to critical infrastructure in the facility.

SMX delivers vendor-agnostic ICS threat updates for evergreen protection.

SMX security checks involve a powerful combination of intelligence feeds and multiple types of industrial threat detection techniques, as well as Honeywell's Cybersecurity Global Analysis, Research and Defense (GARD) threat research team.

Self-learning capabilities and automation ensure that the combination of SMX and Threat Intelligence capability better protect against current and emerging USB-borne threats. After initial security analysis upon USB check-in, SMX better protects plant safety and operations by allowing service providers and employees to safely use convenient and pervasive removable media for equipment updates.

It modernizes plant security by combining a consumer-friendly USB scanning device with cloud-based industrial cybersecurity threat updates.

The SMX solution simplifies compliance and site reviews by providing logs of removable media activity throughout the plant.

SMX includes support for ISA-99 and IEC 62443 requirements. In concert with additional Honeywell solutions such as Honeywell Forge Cybersecurity Site, your process control network risks and threats can be prioritized and better mitigated for a more robust industrial security posture.

Helps protect against weaponised USB devices such as Rubber Ducky, OMG Cable, Bash Bunny, OMG Plug, Flipper Zero and others.

RELY ON ENFORCEABLE SECURITY TECHNOLOGY, NOT JUST AN HONOR SYSTEM POLICY

Some cybersecurity providers ignore the current situation and expect industrial operations to stop for security, which is unrealistic. They recommend policies banning the use of removable media altogether, and rendering physical ports inoperable.

Now Honeywell innovation extends plant protection to removable media and keeps operational metrics on track by decreasing security risks and related disruptions, digitally and physically. As a pioneer in industrial cybersecurity,

Honeywell heavily invests in people, processes and technologies that improve cybersecurity threat protection for critical infrastructure. Honeywell is committed to working with you to assist you in keeping plants running smoothly despite increasing threats to digital control systems. Our products and services are not limited to Honeywell control systems, they can also better protect a diverse operations infrastructure.

SMX continues removable media monitoring by enforcing active policy controls across your orgainsation. It prevents unchecked USB devices from using USB ports, while keeping the port active for authorized devices. Upon visitor or employee check-out, SMX checks the device again for anomalies, and later supports forensics by logging device information.

SMX ENHANCES PROTECTION AGAINST ADVANCED USB THREATS

Honeywell SMX bridges the divide between IT and OT requirements for safer process manufacturing

KEYLOGGERS
Data extraction and password theft

KEYSTROKE INJECTORS
Hidden "inside attacks" able to bypass anti-malware

SERIAL
Direct COM access able to bypass network security

STORAGE
Malware delivery and data extraction

AUDIO / VISUAL
Espionage, spyware

NETWORK
Rogue access points and network backdoors

Honeywell USB Firewall Technology creates an enforceable USB security program providing granular control over which USB based devices (storage media, mouse, cell phones, etc.) can connect and how each device operates. One can think of this as a "USB device firewall". Additionally, all storage drives must be scanned by SMX before they connect ensuring that all files are checked in before they can be used on the critical network.

HOW GARD WORKS

How do you know if a file is "good" or not? There's a lot to consider ...

THREAT RESEARCH

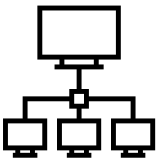
- Proactive threat research
- Threat mining and hunting
- OT Threat focus

MULTISOURCE THREAT INTEL

- Multiple threat reputation feeds
- Early-day threat detection
- Malware multi-scans
- Threat hunting & Darkweb mining

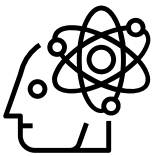
CONTENT WHITELISTING

- Multi-vendor firmware & software validation
- Custom file policies



OPERATIONAL TELEMETRY

- Thousands of deployed sensors
- Incident data from Honeywell's global SOC
- Public and Private Sector information sharing



HUMAN INTELLIGENCE

- Research from 7 Honeywell cybersecurity centers of excellence

---

CHALLENGE

There are so many threats, that endpoint anti-malware can detect less than 1% of known malware, leaving no room for industry-specific threats. Cloud threat detection helps, but isn't available to air-gapped networks.

SOLUTION

The GARD Threat Engine provides a more secure and connected threat detection engine designed to find more threats than commercial solutions ... and it works with Honeywell Forge Cybersecurity offerings to protect air-gapped networks.

IMPACT

Better threat detection to help protect Honeywell customers from the most relevant threats facing industrial, building, and aerospace customers.

+20%

THREAT DETECTION OUTPERFORMS MOST COMMERCIAL AV SOLUTIONS

-7%

POTENTIAL FALSE POSITIVES EXTRA LEVELS OF VALIDATION MEANS FEWER FALSE POSITIVES

Group showed that almost half of the enterprises polled had suffered a successful malware attack even though they were running anti-virus software.

– ENTERPRISE STRATEGY GROUP

SMX VS TRADITIONAL ANTI-VIRUS USB SCANNING

SMX is not just an AV scanning station! It's so much more...

SMX

- ✓ Analyze files using the full power of GARD
- ✓ Also scans using local AV as a failsafe
- ✓ No administration required: a full self-service kiosk
- ✓ Works in air-gapped environments
- ✓ Enforce scanning via 'check in' process
- ✓ Enforce scans at end nodes w/driver-level defenses
- ✓ Protects against non-file attacks and malicious USB devices and UAPs

ANTI-VIRUS SCANNING STATION

- ✓ Scan files for a subset of known malware
- ✗ Requires administration to maintain and patch server
- ✗ Requires administration to update AV signature files (no auto-updates in air-gapped environments)
- ✗ Requires customer interaction to log in, initiate scans, interpret results
- ✗ No way to enforce that users are performing scans
- ✗ No way to enforce scan results at end nodes
- ✗ No protection against malicious devices or UAPs

THE VALUE OF AN SMX FLEET DEPLOYMENT

“Over 90% of breaches are due to human error”. In the ever-evolving OT threat landscape, it’s becoming increasingly important to keep on top regulator compliance for multi-site organisations, while also juggling resources, budgets and of course safety.

The SMX FLEET offering is a Cost Effective, Low Overhead “Set it and forget it solution”

The digital transformation within the OT cybersecurity perimeter is increasing pressure on an already stretched capability. While embracing new technologies such as Industry 4.0, IIoT and sustainability targets is important, it’s also critical to implement strong controls. Even better would be a protection in depth, no overhead capability to protect your business from human error and/or malicious intent.

With the human element in mind when updating air gapped systems across multiple sites. We listened carefully to customers feedback and worked hard to pull a capability together that could help automate and simplify the challenges of running multi-site cybersecurity for USB Devices could include:

- Understand what unique challenges your engineers and executives must deal with
- Provide a cross site deployment and management capability
- Fully integrate SMX with your SOC
- Make sure resident and visiting engineers find the system easy to use.
- Ensure SMX Fleet is linked to your cyber response plan
- Alert management

MULTI-SITE MANAGEMENT

Manually keeping track of all engineer work, be that internal staff of visiting engineers, is an arduous task.

There are 4 main strengths within the SMX system that helps deliver a USB Device protection in depth capability:

- GARD Threat Engine
- Management Console
- Client Security Driver
- USB Firewall

SMX Fleet enables us to work closely with you to understand your specific needs and capabilities. We then work with you to define the best way to design, configure and deploy your SMX Fleet. All SMX patches and updates are managed automatically. Alerts are delivered to nominated contacts and if required, we can integrate SMX with your existing IT SOC.

This delivers you 3 benefits:

1. **Empowering you to spend your time and mental bandwidth on other critical organisational projects**
2. **Enable your engineers to move freely and secure in the knowledge that there are multiple controls in place to minimise mistakes or malicious activity**
3. **When you also factor in the visibility and control the management console provides, you may have what**

CUSTOMER DEPLOYMENT HOW WE CAN HELP

The “White Glove” service is to help ensure the best possible service and value is delivered to you and your business

- SMX fleet solution can help simplify the deployment and management of your distributed SMX investment by offering you a fully managed “white glove” service
- Highly skilled OT engineers will engage with you to understand your specific needs and requirements across your distributed OT/IT estate
- We work closely with you to help define the best method to deploy your SMX units as well as the most effective use of your threat management portal

HONEYWELL INDUSTRIAL CYBERSECURITY USB THREAT REPORT 2021

THREATS DESIGNED FOR USB EXPLOITATION RISE TO 52%. GROWTH INDICATORS SLOW, BUT THREAT LEVELS REMAIN DANGEROUSLY HIGH.

DOWNLOAD THE COMPLETE REPORT

81%

OF THREATS HAVE THE POTENTIAL TO CAUSE A MAJOR DISRUPTION IN ICS (UP FROM 79%)

32%

INCREASE YEAR OVER YEAR OF USB USE IN PRODUCTION FACILITIES

52%

OF THREATS ARE DESIGNED TO LEVERAGE REMOVABLE MEDIA (UP FROM 37%)

51%

OF THREATS PROVIDING REMOTE ACCESS

45%

TOTAL # OF USB THREATS REMAIN CONSISTENT

OVERVIEW

By looking at a very specific vector into industrial automation environments, we get a unique opportunity to analyze the real malware threats that industrial organizations face.

This is important because there are only a few actual vectors into OT (Operational Technology) environments: the network, limited to specific information conduits between operational and business networks; physical access by authorized users; and supply chain through which hardware and software enters a mill, plant, refinery, or other industrial automation facility.

Removable media falls into two of these categories: physical access (thumb drives and other media physically carried into a facility); and the supply chain. This report focuses specifically on malware (intrusive software) found on USB storage devices used to carry files into, out of, and in between industrial facilities.

The results of the Honeywell Industrial Cybersecurity USB Threat Report are based on malware detected and blocked by technology deployed globally by Honeywell. All data is anonymous, and therefore no correlation can be made to specific organizations, industries, or geographic regions. However, all data is derived from production OT facilities, presenting a unique glimpse at the types of malware threats facing industrial environments via USB removable media.

Note: Malicious USB devices and peripherals crafted specifically to attack computers via the USB interface, while increasingly popular and highly effective, are not included in this report (please refer to the Honeywell USB Hardware Attack Platforms Report).

THE CHALLENGE

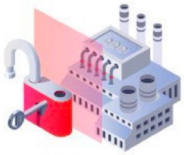
Now in its fourth year, the Honeywell Industrial Cybersecurity USB Threat Report has shown a clear trend: threats continue to become more prominent and more potent.

- Threats designed to propagate over USB or specifically exploit USB for infection rose to 52% from 37%.
- Threats designed to establish remote access capabilities remained steady at 51%.
- Threats capable of causing loss of control or loss of view increased to 81%, up from 79%.

Previous versions of this report showed massive increases, even doubling in many cases, this year the growth of many indicators slowed. These more moderate increases indicate the level of threats utilizing this vector may have plateaued **– although they do so at dangerously high levels.**

Designed for USB **52%** From 37%

Designed for USB **81%** From 79%



Industrial Specific **30%** Steady-High

Remote Access **51%** Steady-High

Remember 45 to 98% of dropped USB sticks will be plugged in

Source: Tischer, Durumeric, Foster, Duan, Mori, Bursztein, Bailey" "Users Really Do Plug in USB Drives They Find"
– Univ. of Illinois, Univ. of Michigan Google, Inc. 2016

HOW HONEYWELL CAN HELP

Recent years have seen a major increase in security incidents related to industrial control systems. As new threats emerge and the industrial security landscape evolves, you need an experienced and trusted vendor to help you protect the availability, reliability and safety of your plant automation system, as well as help you improve safety for people and processes involved in all facets of your operation.

Honeywell Industrial Cybersecurity Solutions are specifically designed to help you defend your control infrastructure and plant operations. These broad solutions leverage our industry-leading process control and cybersecurity know-how, recognized experience and advanced technology, combined with partnerships delivering cutting-edge offerings from leading cybersecurity partners.

Honeywell is a proven industrial cybersecurity vendor that offers:

- Improved security for your industrial controls systems without impacting processes
- Global/regional industrial cybersecurity service hubs close to our customers
- Extensive coverage of industrial control networks
- Ability to support our customers from security assessments to cybersecurity program development

WHO IS HONEYWELL

- Trusted partner for Operational Technology (OT) cybersecurity
- 100+ years of OT & 20+ years OT cybersecurity domain expertise
- 300+ employees focused on OT cybersecurity
- 1000s of secure remote
- access installs & over 5000 projects delivered
- Complete portfolio of industry proven cybersecurity products, services & solutions
- Vendor neutral solutions
- Global capabilities & local presence

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

ISA GLOBAL CYBERSECURITY ALLIANCE Founding Member

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.becybersecure.com

Secure Media Exchange 2022 | Rev 1 | 11/2022

THE FUTURE IS WHAT WE MAKE IT

Honeywell