Honeywell | Industrial Cybersecurity

SECURE MEDIA EXCHANGE

World's Strongest Industrial Cybersecurity Solution for USB Protection

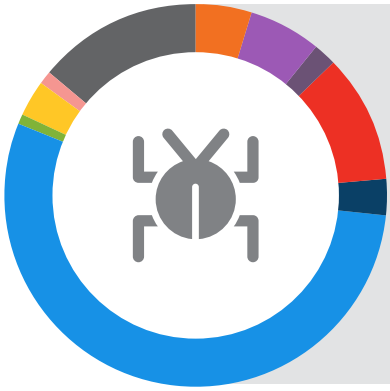
Removable Media Help Keep Operations Running

Since discovery of the Stuxnet computer virus, industrial organizations have struggled with finding secure ways to use and monitor removable media. Unfortunately, many cybersecurity tools and strategies have failed to adapt to evolving operational demands.

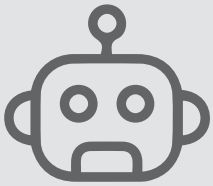
They also create excessive cost and burden, and do not address changing vulnerabilities.

Check. Check. **Go.**

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



55%
TROJANS



11%
BOTS

55%	Trojans	11%	Bots	6%	Hacktools	5%	PUAs	3%	Viruses
3%	Adware	2%	Rootkits	1%	Worms	<1%	Spyware	14%	Other/Unclassified

Although a significant portion of malware found on industrial control systems is propagated by removable media, it's virtually impossible to run today's plants without the use of portable devices like flash drives and USB memory sticks. In addition to employees using removable media to manage industrial controls, third-party integrators and service providers rely extensively on USB exchanges to implement frequent updates to systems at client facilities.

According to the recent Honeywell Industrial USB Threat Report:

- Of the locations studied, nearly half (44%) detected and blocked at least one malicious or suspicious file that represented a security issue
- Of those threats blocked by SMX, 1 in 4 (26%) had the potential to cause a major disruption to an industrial control environment, including loss of view or loss of control, and 16% were targeted specifically against Industrial Control System (ICS) or Internet of Things (IoT) systems
- 15% of the total threats detected and blocked were high-profile, well-known threats, including Stuxnet (2%), Mirai (6%), TRITON (2%), and WannaCry (1%).

You can download the complete report here – www.hwll.co/USBReport

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

- There is no safe, network-based capability for updating digital systems
- 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 cost, burden and risk.

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

Of the
threats blocked:

15%
Are well-known threats
e.g. Mirai, Stuxnet, TRITON, WannaCry

9%
Designed to exploit USB

16%
Targeted ICS or IOT

26%
Potential to cause major disruption to ICS
e.g. loss of view or loss of control

Secure Media Exchange (SMX) for Safe and Productive Use of Removable Media

With years of experience managing security for its industrial customers, Honeywell Process Solutions has introduced a new addition to its cyber risk reduction portfolio—Honeywell Secure Media Exchange (SMX). This intelligent device and cybersecurity gateway protects facilities from USB-borne attacks or misconfigurations.

The SMX solution provides:

- *Immediate and tailored USB port security for industrial networks*
- *Simple removable media scanning solution for operations and plant managers*
- *Ongoing security updates managed and maintained by Honeywell*
- *Better visibility into USB usage and threat activity across multiple locations*
- *Threat protection against advanced USB threats*

Honeywell SMX bridges the divide between IT and OT requirements for safer process manufacturing. It delivers vendor-agnostic threat research updates while securely closing security gaps. It can integrate site security with electronic security to modernize industrial risk posture, and empowers and enables plant managers to realistically embrace cybersecurity.

Find more details at www.becybersecure.com.

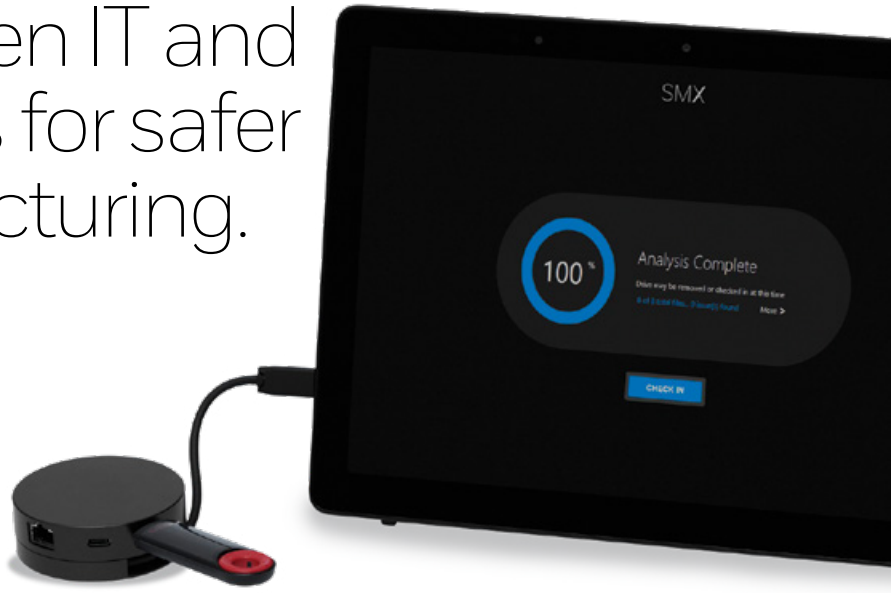
Benefits to Industrial Operators

By monitoring, protecting, and logging use of removable media at industrial facilities, SMX provides the following key benefits:

- *Reduces site disruptions caused by malware and other security threats transmitted via USB*
- *Protects plant operations by allowing safe USB equipment updates by service providers and employees*
- *Reduces the risk of malicious exploitation of USB ports by monitoring and controlling removable media use throughout the plant*
- *Limits the time horizon for new attacks to be launched against operations with an evergreen repository of vendor-agnostic threat detection updates*
- *Enforces security policy by disabling unchecked devices*
- *Modernizes plant security by combining a user-friendly USB scanning kiosk with secure, cloud-based industrial threat updates*
- *Advanced enterprise threat intelligence reporting capabilities*
- *New model – SMX ST comes with the same technology features but is slimmer, lighter and at a lesser price*
- *Simplifies compliance by providing logs of removable media activity and users*
- *Improves service update productivity by simplifying cybersecurity check-in and check-out procedures*
- *Provides unparalleled visibility into removable media risk when combined with Honeywell Risk Manager*

Discover additional benefits at www.becybersecure.com

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



SMX RT Rugged Environment

- Metal Enclosure
- Glove Touch Screen
- Wall Mounted
- Gorilla Glass
- Shock-Absorbent

SMX ST Non Rugged Environment

- Light-Weight
- Touch Screen
- Tabletop Kickstand

	FEATURES	SMX RT	SMX ST
TECHNICAL	Threat Intelligence Solution (Advanced Cloud Based Threat Detection)	✓	✓
	Cellular Capability	✓	✓
	Records Security Photos for Forensics	✓	✓
PHYSICAL	Ruggedized Metal Enclosure	✓	N/A
	Wall Mounting Brackets	✓	N/A
	Front and Rear Facing Camera	✓	✓
	Multi-Port	N/A	✓
	Pop Out Kickstand	N/A	✓
	Shock-Absorbent/Damage Resistant	✓	N/A
	Glove Touch Capable Screen	✓	N/A
	Gorilla Glass (High Durability and Visibility)	✓	N/A

SMX Protects Against Advanced USB Threats

BADUSB

- *Manipulation of USB firmware.*
- *USB device will act as a HID - Human Interface Device (e.g. a keyboard), and can execute scripts.*

RUBBER DUCKY

- *A keystroke injection tool disguised as generic USB drive.*
- *Computer recognizes the USB as a "normal" keyboard and automatically executes the preprogrammed rubber ducky scripts.*
- *Execution speed around 1000 words per minute!*

BASH BUNNY

- *A fully featured Linux computer with the ability to execute all Rubber ducky scripts, as well as more complex attacks leveraging data connections (e.g. Ethernet over USB or Ethernet control model - ECM)*
- *Can also impersonate mass storage or serial devices*

Increasing Threat Complexity

First Threat Detection Tool of its Kind

Secure Media Exchange reduces cybersecurity risk and limits operational disruptions by monitoring, protecting, and logging use of removable media throughout industrial facilities. The SMX gateway security device simply resides in your physical "front desk" or the 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 security checks involve a powerful combination of intelligence feeds and multiple types of industrial threat detection techniques, as well as Honeywell Cybersecurity Lab researcher updates.

As part of an innovative private hybrid cloud subscription service, managed by Honeywell, SMX delivers vendor-agnostic ICS threat updates for evergreen protection (Learn more about Honeywell's Threat Intelligence solution,) SMX security checks involve a powerful combination of intelligence feeds and multiple types of industrial threat detection techniques, as well as Honeywell Cybersecurity Lab researcher updates. Self-learning capabilities and automation ensure that the combination of SMX and Threat Intelligence solution protect against current and emerging USB-borne threats.

After initial security analysis upon USB check-in, SMX continues removable media monitoring to enforce your plant's policy. 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 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 a cloud-based industrial cybersecurity threat updates. And it 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 Industrial Cybersecurity Risk Manager, your process control network risks and threats can be prioritized and mitigated for a more robust industrial security posture.

Rely on Security Technology— Not Just 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 minimizing security risks and related disruptions, digitally and physically.

As a pioneer in industrial security, Honeywell heavily invests in people, process and technologies that help secure critical infrastructure from cyber threats. We are committed to keeping plants running smoothly despite increasing threats to digital control systems. Our products and services are not limited to Honeywell control systems, but can protect a diverse operations infrastructure.

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 partner to help protect the availability, reliability and safety of your plant automation system, as well as safeguard people and processes involved in all facets of your operation.

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

Honeywell is a proven industrial security partner that offers:

- Tailored solutions to efficiently secure industrial controls, 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
- Track record of completing 1,000s of global industrial cybersecurity engagements
- Mature solutions with 400+ managed industrial cybersecurity sites

For more information

To learn more about Honeywell Secure Media Exchange (SMX) visit www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road
Zhangjiang Hi-Tech Industrial Park
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

BR-17-17-ENG | 01/19

Honeywell