SECURE MEDIA EXCHANGE SMX

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

HONEYWELL FORGE
Cybersecurity+

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

REMOVABLE MEDIA KEEPS 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 labor burden, and do not address changing vulnerabilities.**

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 cost, burden and risk.

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

HONEYWELL SMX

HONEYWELL FORGE Cybersecurity+

Reduce risk by enforcing **USB & increase efficiency with file policies**

Honeywell SMX extends leading industrial USB cybersecurity across the OT Enterprise, with the Enterprise Threat Management portal and integration into the Forge Cybersecurity Suite.

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?

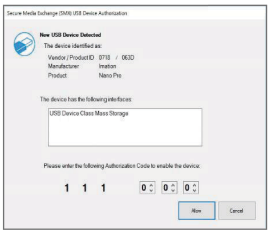
- No surprises! Manage USB devices across the enterprise
- Better defend networks from hardware threats (cell phones, keyboard, etc.)
- **Increase efficiency while** updating and patching your production environment **with custom file policies**
- Stay on top of emerging OT threats with proactive research, 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 System – Fully managed rugged 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

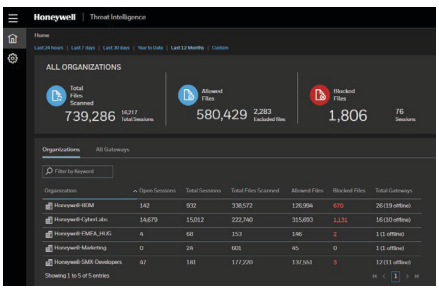
1 SMX SYSTEMS



3 SMX CLIENT ENFORCEMENT DRIVER

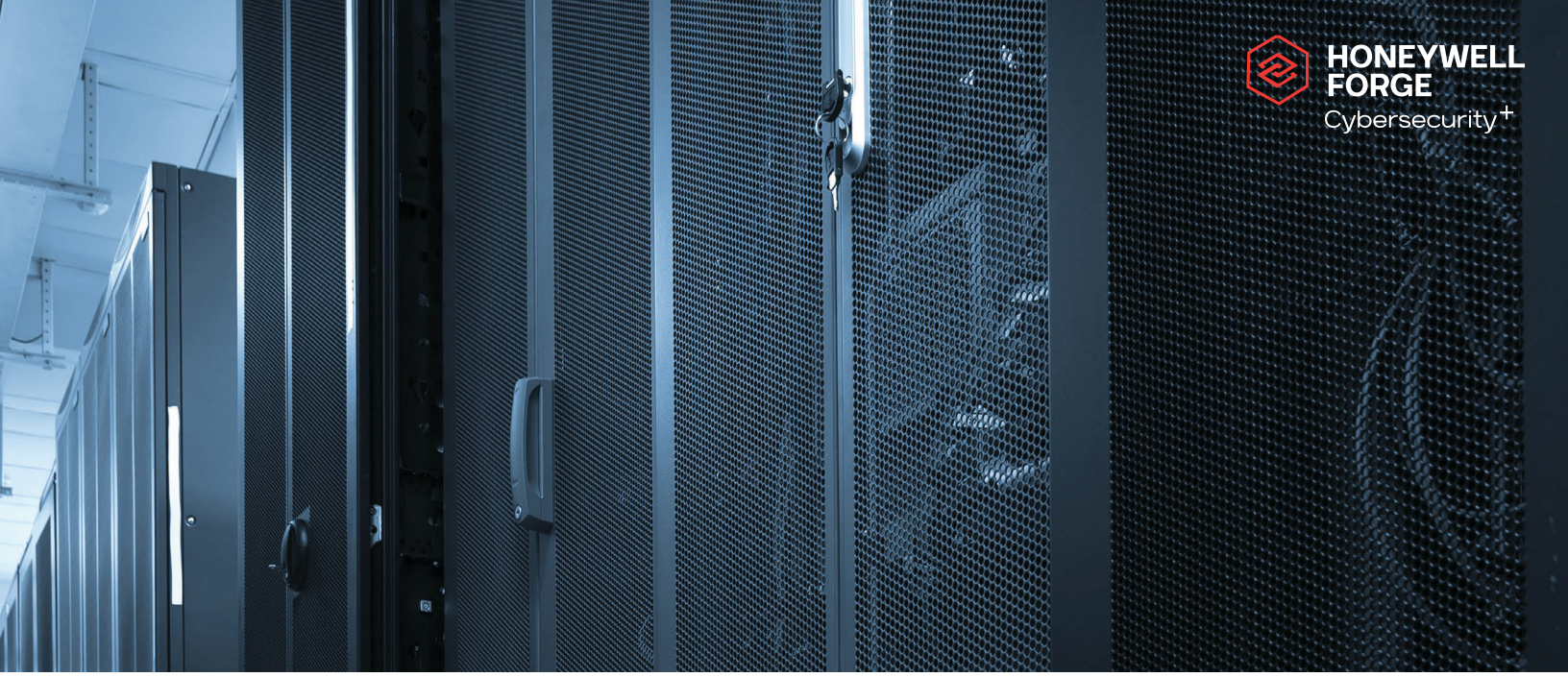
2 GARD THREAT ENGINE
Global Analysis,
Research & Defense

4 ENTERPRISE THREAT MANAGEMENT PORTAL



5 GARD THREAT RESEARCH TEAM
Global Analysis,
Research & Defense

OTD BİLİŞİM GLOBAL VAD



FIRST THREAT DETECTION TOOL OF ITS KIND

Secure Media Exchange reduces cybersecurity risk 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 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 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 solution 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 more 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.

SMX 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.**

HONEYWELL FORGE Cybersecurity+

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 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 better 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 better protect a diverse operations infrastructure.

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 BETTER PROTECTS AGAINST ADVANCED USB THREATS

Energy
Food
Manufacturing
Aerospace
Oil & Gas
Shipping
Buildings
Pulp & Paper
Water & Waste Water

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 TRUST 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.

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

HOW GARD WORKS

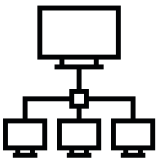
How do you know if a file is "good" or not? There's a lot to consider …

MULTISOURCE THREAT INTEL

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

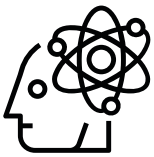
CONTENT WHITELISTING

- 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

GARD provides a more secure, **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

A recent study by the Enterprise Strategy Group showed that almost half of the enterprises polled had suffered a successful malware attack even though they were running anti-virus.

– ENTERPRISE STRATEGY GROUP

HONEYWELL FORGE Cybersecurity+

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

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

HONEYWELL INDUSTRIAL CYBERSECURITY

USB THREAT REPORT 2021

GROWING RISK OF USB THREATS TO INDUSTRIAL SYSTEMS

79 %

OF THREATS HAVE THE POTENTIAL TO CAUSE A MAJOR DISRUPTION IN ICS **(UP FROM 59%)**

↑30 %

INCREASE YEAR OVER YEAR OF USB USE IN PRODUCTION FACILITIES

37 %

OF THREATS ARE DESIGNED TO LEVERAGE REMOVABLE **MEDIA (UP FROM 19%)**

50 %

OF THREATS PROVIDING REMOTE ACCESS

45 %

TOTAL # OF USB THREATS REMAIN CONSISTENT (FROM 44%)

OTD BİLİŞİM GLOBAL VAD

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.

Trojans **30 %**

Designed for USB **37 %**

Targeting OT **30 %**

Establish remote Access **51 %**

According to the recent Honeywell Industrial **Cybersecurity USB Threat Report:**

Overall, the threat of **USB-borne malware** continues to be a serious and growing concern. Threats capable of propagating over USB, or specifically exploiting USB media for initial infection, rose from **19%** in 2019 to just over **37%** in 2020–the second consecutive year of significant growth in this area. Of the threats seen, **Trojans** dominated again by comprising **76%** of the malware detected. In addition, more threats in 2020 were **wormable**, and **52%** (up from **34%**) were able to provide remote access or remote control. This illustrates the continuation of a trend identified in last year's report: adversaries are leveraging USB removable media **as an initial attack vector,** at which point they will attempt to establish remote connectivity to download additional payloads, exfiltrate data, and establish command and control. Combined with a corresponding increase in threats targeting industrials (from **28%** to **30%**), this supports the theory that USB removable media **are being used to penetrate the air-gapped** environments found in many industrial and OT environments.

THREATS CONTINUE TO GET MORE SEVERE

Of the threats blocked, another trend continued from 2019: the malware was more capable of causing a disruption to industrial control systems, up to **79%** from **59%. This is true despite a** slight decline in ransomware, which was a significant contributor in 2019. The increased severity of threat comes from increasingly multi-functional malware, which is capable of directly **impacting target systems** (20%), **downloading stage-2 payloads (9%)**, or **opening backdoors**, establishing direct **remote access**, and **command and control (52%).**

CONTENT-BASED MALWARE AS AN INITIAL VECTOR INTO OT

A new trend identified in 2020 showed that a significant amount of threats specifically leveraged altered or infected documents. **There was a continued increase in trojans (malware disguised a** legitimate software), with a seeming shift from the impersonation of executable files and archives (.exe, .zip, etc.) to document files (Office documents, PowerShell scripts, .PDF files, etc.). In addition to the high **number (76%)** of trojans overall, 12% of the total threats detected leveraged native document structures with embedded scripts and macros. This rise in **content-based malware** seems to correspond to more subjective shifts **in how many organizations operated during 2020 and would indicate that** adversaries were attempting to take advantage of these changes. Because **there is no pre-existing data** concerning file metadata, it is impossible to draw a conclusion here, **although it is something that will be** observed in the future.

Similar findings were also published by McAfee Labs, who saw a **103%** increase in office malware and a **117%** increase **in PowerShell malware.** [2]

HOW HONEYWELL CAN HELP

HONEYWELL FORGE Cybersecurity+

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 better 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 cybersecurity partner that offers:

- Tailored solutions to better 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

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

OTD BİLİŞİM GLOBAL VAD