OPSWAT.

WHITE PAPER

Secure Manufacturing Processes from External Media Threats

How Needs-Based Cybersecurity Systems Improve Uptime

EXECUTIVE SUMMARY

The Risks

- Cyberattacks targeting manufacturing processes and operational technology can cause unplanned downtime, missed financial targets and loss of consumer trust
- Production networks often require physical access to manage, which introduces portable media and removable devices, such as USB and HDD, as a primary source of risk
- OT networks that are not regularly updated are especially vulnerable to modern malware and malicious actors

The Challenge

- Third-party vendors and contractors introduce supply chain risks, such as vulnerable software updates
- Security and needs in manufacturing environments are more complex because of their unique nature
- Lack of visibility into OT assets can make it difficult to properly plan out a cybersecurity system

The Solution

- Cybersecurity processes and programs need to be a benefit to manufacturing teams and not hinder the efficiency of processes
- Organizations need a solution to secure removable devices and to protect manufacturing assets by scanning for malware and vulnerabilities before outside media enters a critical domain
- The physical presence of a cybersecurity kiosk protects the perimeter of manufacturing environments to minimize unplanned downtime and create a culture of cybersecurity for all who enter the site

Manufacturing networks and systems tend to be isolated from IT systems, both physically and logically, which makes cybersecurity for these systems more complex. Even air-gapped networks are vulnerable to the direct physical access that IT and OT teams, engineers, and contractors require to operate, maintain, update, audit, and manage these systems.

This physical access represents a security risk, such as ransomware, malware, botnets, worms, and other attacks that can gain access through compromised files and portable devices, such as CDs, DVDs, USB, and HDD.

Incidents involving malicious USB devices are well documented:

- An Italian Defense contractor was hit by a massive data exfiltration attack initiated by using an infected USB
- A critical infrastructure in the Middle East was infected with the Copperfield malware after an employee plugged in a USB drive to an engineering station to watch a movie
- The U.S. secret service confiscated a malware-infested thumb drive at President Trump's Mar-a-Lago resort
- The FBI issued a warning after the FIN7 hacking group attempted a widespread delivery to U.S. households of USB drives containing malicious firmware
- An international technology corporation invariably delivered customers infected devices with the Storewize installation tool
- The "USB drop" tactic is still a popular approach used by attackers with alarming success percentages

History has shown that malicious insiders and agents of espionage are indeed likely to leverage removable media devices as an attack vector as a hapless employee is likely to unwittingly install a vulnerable software update. It doesn't matter if you have isolated your networks, if you don't have security controls for portable and removable media, you are leaving an unlocked door to malicious actors.

When the cost of cyberattacks includes the interruption of production and leads to unplanned downtime, skimping on security leads to even higher costs in the long run. It is important not to overlook the fundamentals of protecting production networks. Physical security controls, such as locked doors, cameras and guards are common approaches to protecting access to control systems. As organizations consider how to implement effective cybersecurity solutions to control portable media access, the physical presence of a cybersecurity kiosk is an excellent approach, otherwise these unmanaged devices create vulnerabilities when granted unfettered access to an OT network.

CYBERSECURITY THREATS POSE A MAJOR RISK TO PRODUCTION TARGETS

Ransomware against industrial entities increased by 500 percent from 2018 to 2020, a trend that is likely to continue into the future. External threats range from foreign nations to financially motivated cybercrime, and both look increasingly similar. Other threats may emerge as insider attacks: a careless employee may become an unforeseen source of risk, or a vulnerable software update may enter through the supply chain.

SECURITY RISKS

Removable Media as Attack Vector

Removable media is a significant concern since it can contain malicious hardware/firmware, malware in hidden partitions, as well as infected files. This risk is dramatically compounded since using USB drives bypasses other security layers such as secure web and email gateways. The USB can then directly compromise the target machine, leading to initiating an attack propagation within the organization. In fact, researchers in the Ben Gurion University in Israel documented over 20 methods in which a USB device can be used as an attack vector. None of these attacks involve malicious files, but rather an exploitation of the device itself. To mitigate these risks, it is essential to create a physical barrier that will prevent connecting portable devices directly to endpoints.

The Danger of Transient Cyber Assets

Unlike removable media, transient cyber assets such as laptops and power system simulators are designed to perform managerial, monitoring, and diagnostic tasks on the ICS. These assets will not stay connected to the system for more than 30 days, but even then, they are still significant threat vectors. They could be affected by malware before being deployed into an ICS, which causes widespread infection. Worse yet, because transient cyber assets are not permanently based on site, malicious actors can steal them and make unwanted changes to the ICS. The Maroochy attack is a classic case that illustrates how much damage these assets can cause if they fall into the wrong hand.

Accidental Insider

The accidental insider includes IT and OT team members, engineers, and other personnel with direct access to OT environments and manufacturing systems. These individuals may inadvertently copy a malicious file onto a portable media device, which is transferred into an OT environment, or they might unintentionally copy confidential information in the process of exporting data and analytics. These careless employees don't mean to be the source of an attack—in fact, they rarely know that they are—but this is one instance where ignorance is not bliss.

Malicious Insider

The actions of malicious insiders and accidental insiders appear the same, but their motivation is completely different. A malicious insider may knowingly introduce malware and vulnerable software updates, or they may intentionally steal away trade secrets, but they are motivated by financial incentives, a personal vendetta, or recruited by foreign nation-states, making them similar to cyberespionage agents.

Data Loss and Theft

Few things are more important to your company than proprietary technologies, formulas, and patents in your manufacturing process. DLP must be a key pillar in your cybersecurity program to ensure the protection of your data and processes. Industrial espionage is a real and pervasive threat that requires mitigation through Data Loss Prevention techniques. This threat vector includes contractors as well as company insiders. Exfiltrating company SCADA recipes, client information, employee private information, network diagrams, etc. can be accomplished through many vectors to include embedding information in images, or in the clear as raw files brought out of facilities on portable media. Sometimes exfiltration can be done unintentionally as well via support or log files exports.

Supply Chain Vulnerabilities: Third-Party Risk

The SolarWinds compromise is a recent reminder that software vulnerabilities can emerge through the supply chain. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) frequently publishes advisories for ICS vulnerabilities. Just like any other technology, these systems need to be updated as vulnerabilities are identified and patched, but it is also important to make sure that new software updates are not vulnerable themselves. Ultimately, these patches are most often applied directly by a removable media device, which is an additional source of risk.

Supply Chain Vulnerabilities: Country-of-Origin Risk

Another third-party risk that can affect the supply chain consists of devices made from countries with ties to malicious actors. These devices might contain intentional vulnerabilities that can be exploited once an attack occurs. Patches must be installed on these devices before they can be deployed to eliminate hidden vulnerabilities.

SO, WHAT CAN YOU DO?

Installing anti-virus (AV) on operational systems is already problematic because any single engine is less than 90 percent effective. AV definitions need to be constantly updated or their detection rates fall even lower. IT systems are usually designed to update directly from an AV vendor (security policy permitting), but the isolated nature of OT networks makes it much more difficult.

Organizations must also be able to verify the source of anti-virus updates and scan downloads for malware. This is particularly important because attackers have been able to compromise update servers and spoof malware within them. Anti-virus signature databases must be updated daily, at all endpoints—a challenging task due to restrictions on internet access and in patch delivery systems.

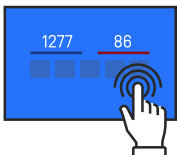
Patch management is similarly important and difficult. Vulnerabilities are common because there are many legacy systems in use, so any network connectivity could expose a single vulnerability to attack. The first step of patch management is to determine if systems are vulnerable to attack, and the rest of the process is similar to updating anti-virus definitions: verify the source of the patch and scan it for malware.

Portable media can be essential for updating anti-virus and patch management, so a policy that forbids their access is impractical.

Cybersecurity should not only help to secure your processes but also optimize them. Cybersecurity solutions should not be a headache for operations teams, they should enable them instead. The key is to create a solution that matches your processes to ensure that your teams can work swiftly and easily on what matters most, manufacturing product.

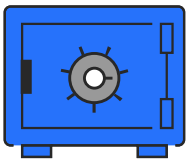
The foundation of a security solution that fits your environment lies in knowing what is available and how these options fit together to form a strong and enforceable security program. The best removable media security programs involve a combination of the following components. Each brings with it different features that can help you to better secure your operations.

OPSWAT SOLUTIONS



MetaDefender Kiosk

- A removable media scanning station to scan for malware, vulnerabilities, and sensitive data, improving control of inbound and outbound content across critical networks
- Turnkey set-up, intuitive configuration, and management to simplify compliance and reporting
- Market-leading, trusted solution that enables secure, audited, authorized, authenticated, and controlled use of media within your most critical infrastructure



MetaDefender Vault

- Secured and audited bi-directional file transfers, with tiered supervisory approval, enabling authenticated, authorized, and verified data extraction from critical infrastructure systems
- Enforce Data Loss Prevention (DLP) policies during Vault-to-Kiosk transfers to proactively redact files found to contain protected data
- Enhance the efficiency of cross domain solutions with the parallel processing of files during client facility check-in and retrieval

USB Firewall

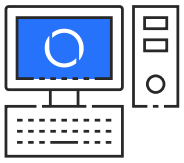
- Enforce file authentication and media protection in isolated networks without any software installation on end points

MetaDefender Drive

- Scan laptops, workstations, and servers to identify any risks associated with malware, sensitive data loss, vulnerable binaries, and foreign-country-originated software

NetWall Unidirectional Security Gateway

- Enable lossless, unidirectional data communications and secure transfer of software updates and other files to the protected domain
- Transfers data over a non-routable protocol, isolating the protected domain from the untrusted network
- Supports connecting multiple MetaDefender Kiosk to multiple MetaDefender Vaults based on established workflows



OPSWAT Client

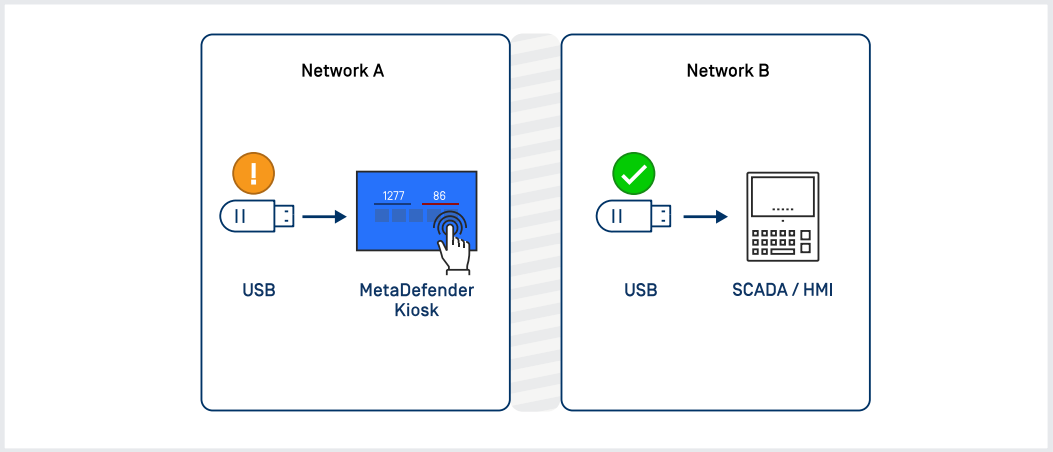
- Authenticate files and authorize access to prevent threat actors from modifying or introducing compromised files after validation at the OPSWAT kiosk on secured end points

DEPLOYMENT SCENARIOS

MetaDefender Kiosk - Standalone Protection in 3 Steps: Control the flow of data into and out of your organization

- Insert the media device into MetaDefender Kiosk
- MetaDefender Kiosk works as a media scanning station to check files from the device
- Detailed report will be generated after the scan is completed

A common portable and removable media protection mitigation that meets and exceeds NIST, NEI, NERC CIP, ISO/IEC, and ISA/IEC requirements is to place OPSWAT MetaDefender Kiosks at key check point entrances, critical SCADA network locations, and research facilities to verify all media before use.



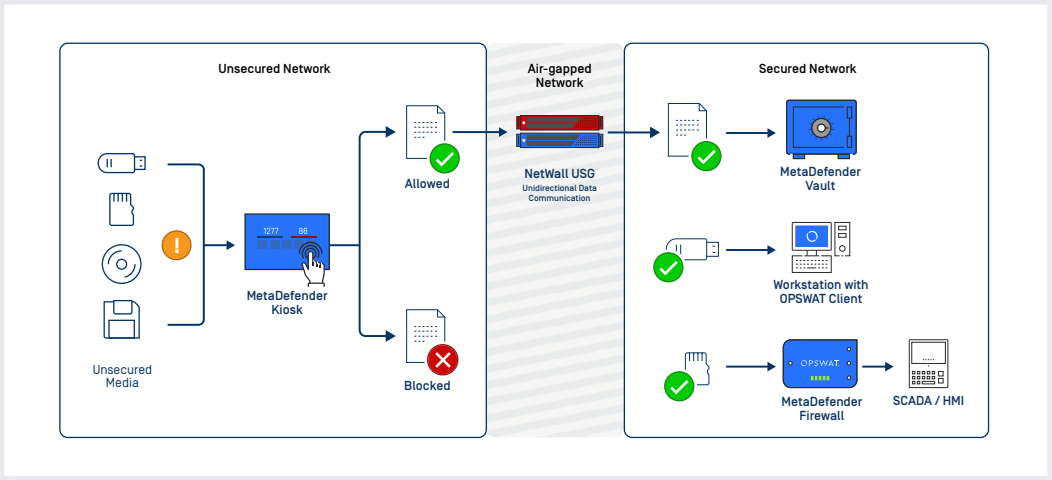
The kiosk confirms the user, the source, and the file types; looks for any malicious partitions and malware; and determines whether the device is secure or if it requires further inspection.

- Allow listing: An administrator can also add enforcement (allow listing) of the specific media devices that are allowed into the facility. The kiosk can restrict media usage to specific pre-screened vendors and types.
- Client Certified Media: Organizations can also provide their own certified media for the copied destination of all sanitized/validated files. In this case, only these media devices would be allowed into the facility with the employee/contractor or under escort.

The OPSWAT MetaDefender Kiosk can better secure content from 20+ media types prior to entering a secure network. MetaDefender Kiosk can be procured as a turnkey system or installed on your preferred hardware. This can be further enhanced in a variety of ways to deter unauthorized data exfiltration.

MetaDefender Kiosk with Closed Loop Media Control

An alternative deployment would include the OPSWAT Client and/or USB firewall to provide additional enforcement on endpoints within the protected network. Only scanned media can be used on these protected machines. A closed-loop system prevents any introduction of malicious content or changes to content while in transit from the kiosk to the destined system. For critical environments where software installation could affect vendor warranty on existing systems, the USB Firewall provides a no-install option for closed-loop control.

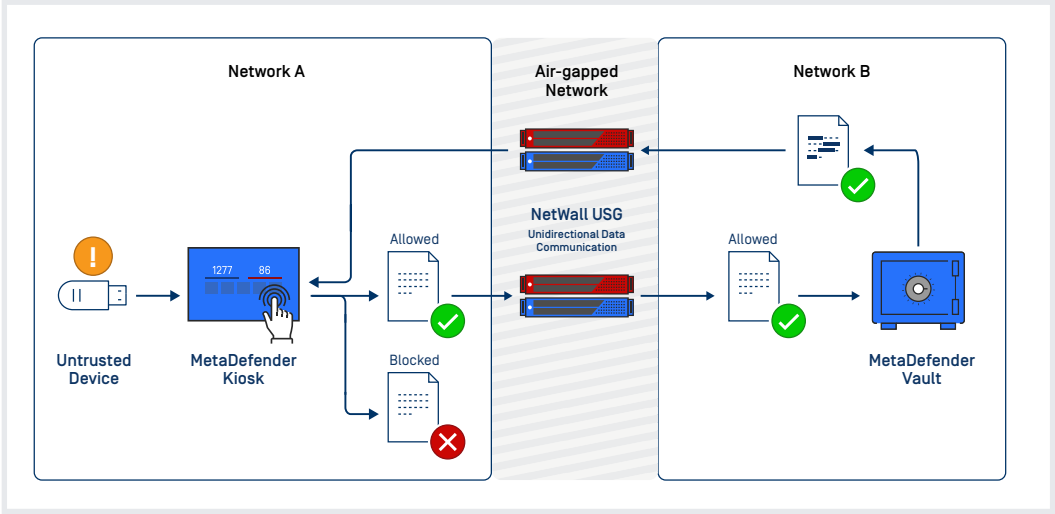


MetaDefender Kiosk to Vault (Enhanced Data Loss Prevention)

Vendors and contractors often need to extract files from a facility for debugging and analysis purposes. In this use case, the data flow can go to and from MetaDefender Vault. Outgoing data starts at the MetaDefender Vault and flow to the Kiosk where the authenticated and authorized user can extract the files using approved media. Data Security and Data Privacy rules are enforced through pre-defined data redaction rules assigned to the relevant workflow.

These data redaction and workflow rules are designed to enhance GDPR, NIST, HIPAA, HITRUST, ISO/IEC, and ISA/IEC data security and data privacy compliance. All data transfers and workflow configuration changes are logged for detailed audit reporting.

A strong “closed loop” option for MetaDefender Kiosk provides for the security of Data at Rest and Data in Transit. In this use case, the Kiosk provides workflow control where files are delivered unidirectionally using NetWall USG to MetaDefender Vault, hosted on the target network. MetaDefender Vault provides tiered supervisory authentication, authorization, approval, and audit reporting when transferring, storing, and retrieving files into and out of protected network segments.

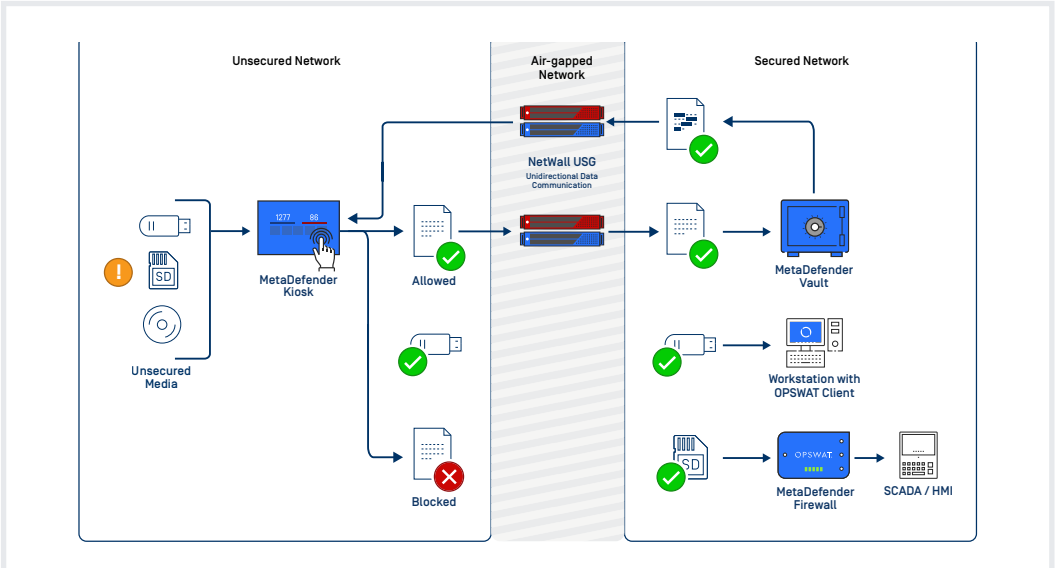


Network A to B is performed by one set of NetWalls for unidirectional communication. A second set of NetWalls will provide the transfer back to kiosk with enforcement for data loss prevention. Isolation between Network A and B is preserved by NetWall's non-routable protocol break between source and destination servers.

All files in MetaDefender Vault are AES encryption secured, monitored, checked for malware using 30+ anti-malware engines, sanitized, and quarantined based on configuration and workflow policies.

MetaDefender Kiosk to Vault with Client and Firewall (Enhanced Data Loss Prevention with Scanning Enforcement)

Another possible configuration is to fully enforce the use of the OPSWAT Client and USB Firewall.

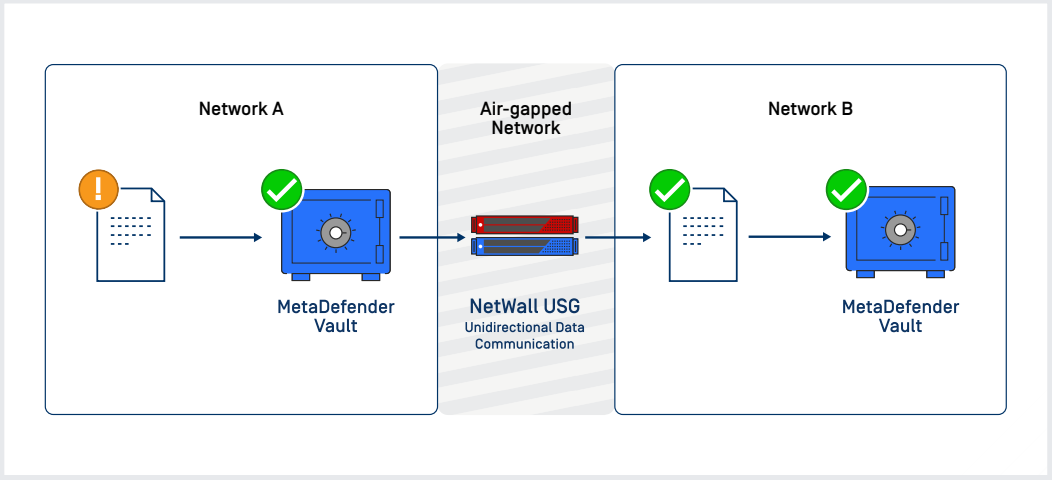


The OPSWAT client, when used in conjunction with MetaAccess, can report all files copied from local drives to removable media.

How does this process work?

- Users enter all media into the Kiosk and select MetaDefender Vault as the destination
- File processing begins immediately by Vault in parallel to the facility entry workflow so the user does not need to wait on local processing but can proceed into the facility
- The Kiosk Ticketing system provides the user with a unique temporary printed code that provides timed network access to the validated/sanitized files stored in MetaDefender Vault hosted by the client from within the facility
- For high security "Security-in-Transit" environments, NetWall USG can be added to further secure network transfers from MetaDefender Kiosk to Vault. This network device can be added to secure traffic as one-way only and guard against the potential misconfiguration (intentional or malicious) of firewalls.

MetaDefender Vault to Vault



For operational purposes, files will need to be securely transferred between these security zones in a controlled, monitored, and logged process.

With OPSWAT MetaDefender Vault installed in each Security Zone or production networks, movement of files can be multi-tier supervisory approved, secured in transit, audited, and secured at rest.

BENEFITS OF REMOVABLE MEDIA SECURITY DEPLOYMENTS

Advanced Threat Protection for OT Assets

- Serves as a barrier to prevent USB devices containing malicious firmware/hardware from directly being able to connect to OT endpoints
- Scan removable media, files, patches, and updates for malware, vulnerabilities, and other suspicious content before it enters a critical domain
- Protect critical assets and manufacturing systems, from vulnerable software updates
- An industry-leading anti-virus multi-scanning technology enables the simultaneous analysis of portable media threats with multiple anti-malware engines, vastly increasing detection rates, decreasing outbreak times, minimizing false positives, and providing resilience

Zero-Day Threat Prevention for Portable Media and Files

- "Trust no file. Trust no device." to prevent zero-day attacks and enforce zero-trust security
- Deep Content Disarm & Reconstruction (Deep CDR) cleanses and reconstructs suspicious files by actively removing malicious content and superfluous data from more than 100 common file types, including .doc and .pdf
- Multi-level archive processing, accuracy of file regeneration, and in-depth views of what is being sanitized and how enable organizations to make informed management decisions to define configurations that best meet your use case
- All processing, analysis, and file transfer information for media is audited, logged, consolidated, and provided in centralized dashboard reports as well as for Syslog/SIEM export. Complete integration with Active Directory for user authorization and activity tracking is provided

Vulnerability Mitigation for Supply Chain Risks

- Prevent supply chain risks from vulnerable vendor software, updates, and patches before they are installed, which may inadvertently or intentionally bypass security policy
- Country-of-origin analysis ensures non-compliant software does not enter your environment
- Multi-scanning technology increases detection rates of malware, exploits, and vulnerabilities

Malware Analysis for Accelerated Incident Response

- Increase the speed of your mean time to detection and response with proactive malware analysis for portable media
- Multi-scanning combines the inputs from analysts located in various malware labs around the globe to enhance intelligence for localized attacks

Data Loss Prevention for Air-Gapped Networks

- Bi-directional Proactive Data Loss Prevention identifies and redacts protected data before it enters or is extracted from critical domains

Flexible Deployment and Management

- Flexible deployment options for air-gapped networks, centrally managed networks, and cloud-connected management
- Support more than 20 media types, including USB, CD/DVD, memory cards, phones and external HDDs

CONSIDERATIONS FOR PORTABLE MEDIA SECURITY

In conclusion, the use of portable and removable media has increased data mobility and overall productivity within manufacturing IT and OT infrastructures worldwide. However, without audits, control, security inspection, sanitization, authorization, and authentication processes, the use of portable and removable media also increases cyber risk exposure to both air-gapped and networked critical infrastructure systems.

Uncontrolled media can allow malware to penetrate our most critical systems as well as enable corporate secrets and private information to be extracted without authorization or knowledge.

While imperative to the protection of manufacturing facilities, securing portable media devices is not easily done, and there are many requirements that can impact the portable media security policies for operators of critical infrastructure. In many cases, there is no single source for an organization's portable media security policy, and individual facilities may require unique security policies. For example, acceptable media types and the appropriate architecture can vary between different facilities, based on their unique requirements, expectations, and geographic location.

With increasing pressure to limit network access to control systems, dependence upon USB removable media to transfer information, files, patches and updates is greater than ever. At the same time, history tells us that USB drive threats are a threat vector impacting manufacturing environments and critical infrastructure organizations.

How can you trust portable media entering and exiting your facilities?

When cyber risks can disrupt critical infrastructure, what is the cost of waiting to act?

When making risk mitigation decisions every organization will draw the line differently. Yet remarkably, it is the 'lowest hanging fruit' or the easiest solution that will result in the biggest reduction of risk, and it can be obtained at the lowest cost. In this case, providing protection for portable media use often rises to the top.

Security and Compliance Solutions by OPSWAT

Network and Systems Protection, Data at Rest, Data in Transit, Policy Management, and Data Privacy

OPSWAT provides cloud, hybrid, and local solutions to enable standards and regulatory compliance. Their many solutions scopes include Zero-Trust Networking, Software Defined Perimeters, Network Access Control, Email Protection, Policy Enforcement, Systems and Endpoint Protection, Data Transfer and Data at Rest Authorization and Protection, and more. Compliance scopes include ISA/IEC 62443, HIPAA, AWIA, GDPR, HITRUST, ISO/IEC 2700X and others.

Critical Infrastructure needs OPSWAT Solutions

OPSWAT protects the highest security environments from ransomware and other critical infrastructure dangers. As a premier partner in enforceable end-to-end removable media security solutions across OT and IT organizations, OPSWAT offers peace of mind and confidence in enforceable security processes by simplifying the complexities of controlling inbound and outbound content from air-gapped networks. Protect your company now. Connect with one of our critical infrastructure cybersecurity experts today.

Contact OPSWAT

Trusted by over 1,500 enterprises and government organizations worldwide, OPSWAT is a global leader in IT, OT and ICS critical infrastructure cybersecurity solutions and Deep Content Disarm and Reconstruction (CDR). Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device poses a threat. Threats must be addressed at all locations at all times – at entry, at exit, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize the risks of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.

OPSWAT.

Protecting the World's Critical Infrastructure