OPSWAT.

EBOOK

Proven Deployments in Manufacturing

Table of Contents

01

Introduction

Manufacturers today are producing far more than physical goods. They are generating vast streams of data across increasingly connected operations. From predictive maintenance logs to CAD files and supplier communications, each digital file plays a critical role in keeping production lines moving. But every file also presents a potential entry point for advanced cyberthreats targeting the industrial sector.

As IT and OT systems become more intertwined, manufacturers face unique cybersecurity challenges. Many industrial control systems weren't built with security in mind, yet they now share networks with internet-facing applications and cloud services. A single compromised file can bring operations to a halt, damage equipment, or even put worker safety at risk, disrupting entire supply chains and causing long-term financial and reputational harm.

This e-book delivers practical insight into protecting your most valuable assets without compromising uptime. We'll examine the evolving threat landscape, explore why traditional defenses often fall short in OT environments, and highlight proven strategies used by leading manufacturers to secure both their IT and OT systems.

02

Common Cybersecurity Challenges

Cybersecurity in manufacturing presents a unique set of challenges that go beyond the concerns of typical IT environments. Industrial systems are deeply interconnected, often reliant on aging infrastructure and proprietary protocols that were never designed with cybersecurity in mind. As IT and OT environments converge, the attack surface expands dramatically—and the consequences of a breach extend far beyond data loss.

Malicious actors are increasingly targeting industrial environments with ransomware, file-borne malware, and attacks on connected devices. These threats can bring production to a standstill, damage equipment, and cause cascading disruptions across global supply chains. Understanding these risks is essential to building security strategies that protect uptime, safety, and intellectual property

Fragmented IT-OT Visibility

Manufacturing networks often lack unified monitoring across IT and OT systems, making it difficult to detect threats moving between zones in real time.

Legacy Systems at Risk

Industrial control systems can remain in use for decades. Many lack modern protections, are difficult to patch, and are expensive or disruptive to replace.

Uncontrolled File Flows

Files transferred between departments, suppliers, or devices often bypass centralized inspection. This creates blind spots where threats can slip through unnoticed.

Removable Media Exposure

USB drives, laptops, and portable devices frequently enter secure environments. Without proper controls, they can introduce malware that halts production or corrupts systems.

Compliance Requirements

Manufacturers must meet a range of regulatory standards including NIS2, IEC 62443, NERC CIP, ISO 27001, and GDPR. Each requires provable security controls across IT and OT systems.

Data Integrity Blind Spots

Without tamper-proof inspection and policy enforcement, attackers can alter data used in critical processes, jeopardizing quality, safety, and trust.

Workforce-Centric Risks

Employees, contractors, and vendors may unintentionally expose systems to threats through phishing, poor security practices, or misconfigured access.

Connected Device Vulnerabilities

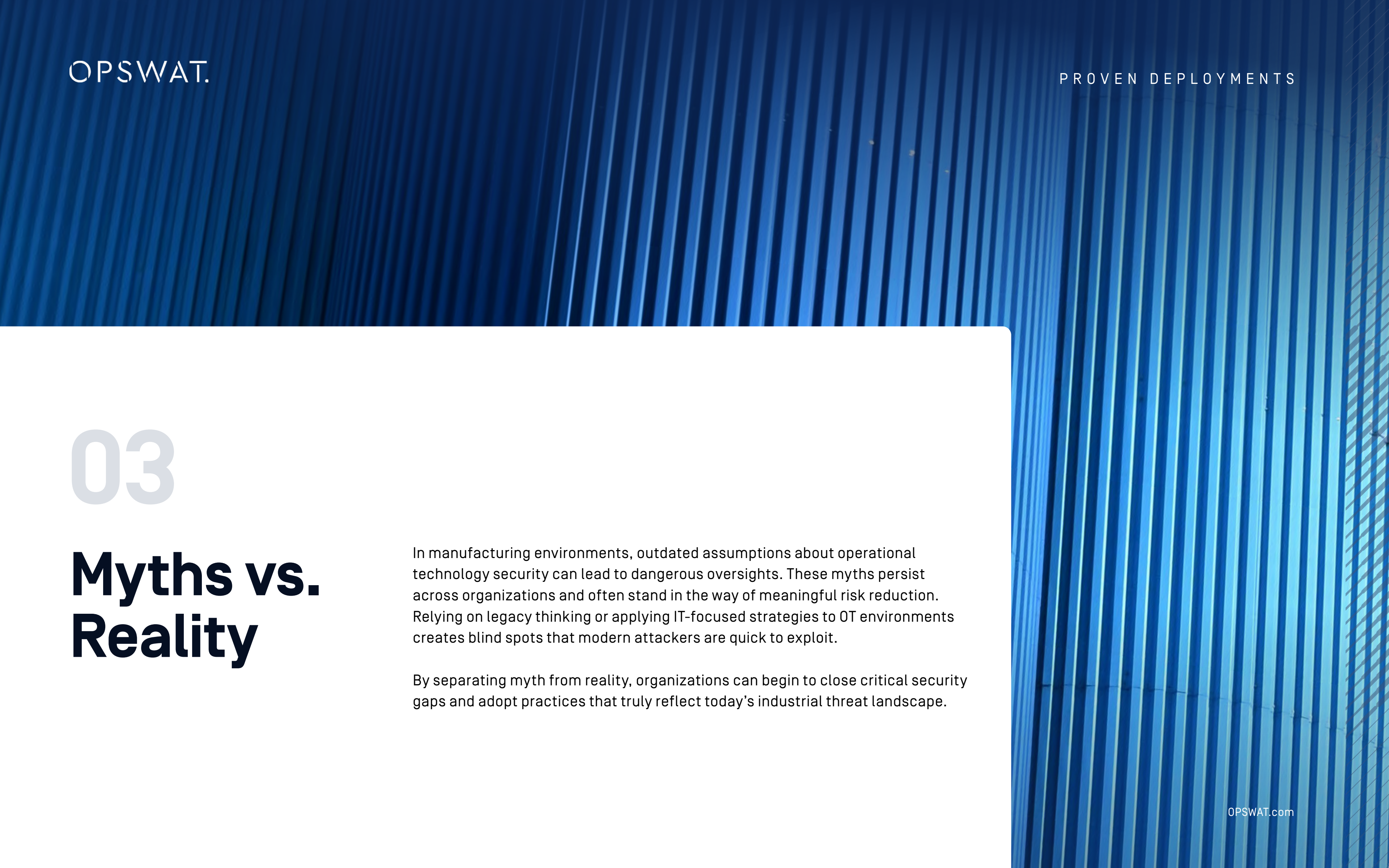
Industrial IoT sensors, robotics, and automation platforms increase operational efficiency but also expand the attack surface if not properly secured.

Downtime and Disruption Costs

Any cyber incident that stops production can result in missed orders, financial losses, and long recovery times. In many cases, downtime is not an option.

Third-Party and Supply Chain Risks

Vulnerabilities in supplier systems can become pathways into your network. Attackers exploit trusted relationships to infiltrate industrial environments.



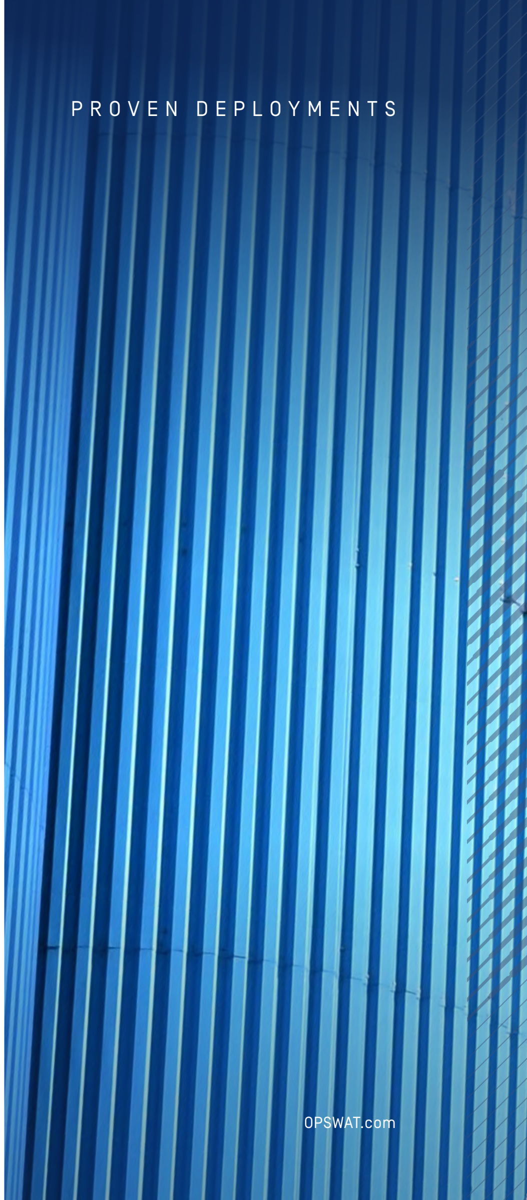
03

Myths vs. Reality

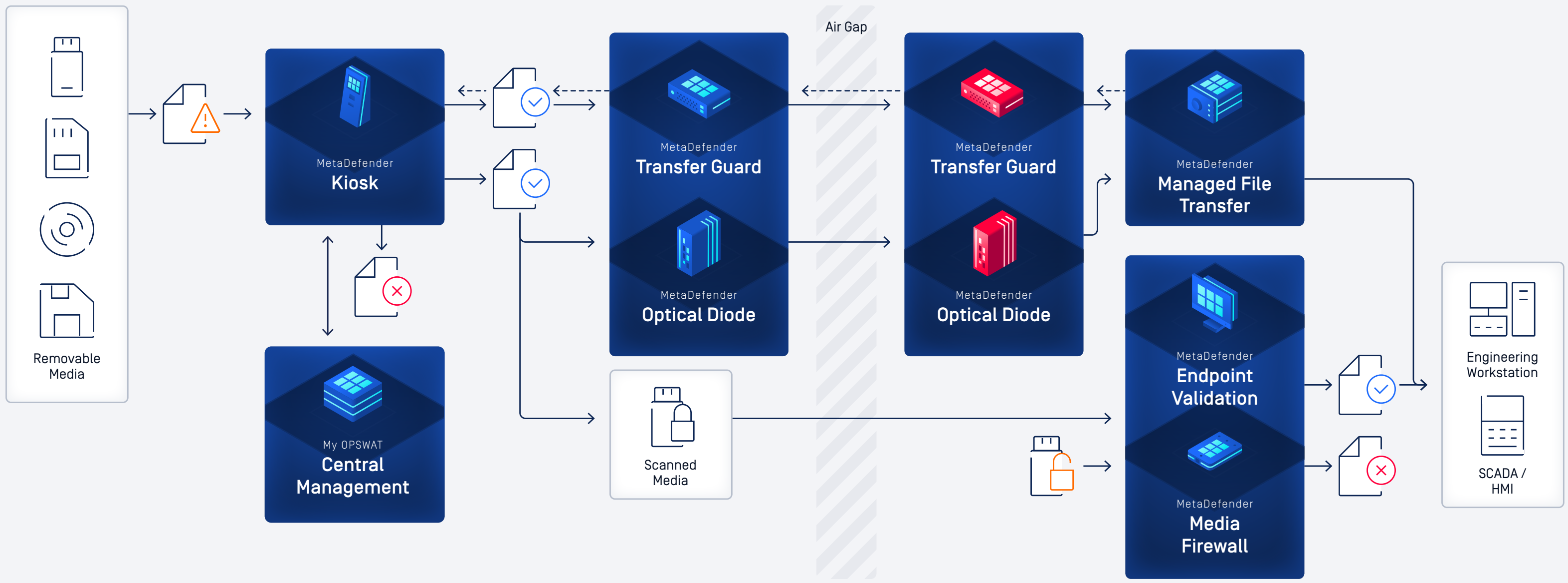
In manufacturing environments, outdated assumptions about operational technology security can lead to dangerous oversights. These myths persist across organizations and often stand in the way of meaningful risk reduction. Relying on legacy thinking or applying IT-focused strategies to OT environments creates blind spots that modern attackers are quick to exploit.

By separating myth from reality, organizations can begin to close critical security gaps and adopt practices that truly reflect today's industrial threat landscape.

Myth	Reality
1. We have full visibility into our OT systems.	Most organizations overestimate their visibility. In reality, few have complete monitoring across all assets. Gaps in device inventory, asset telemetry, and network segmentation allow threats to go undetected.
2. Malware is our biggest problem.	Malware remains a threat, but phishing, business email compromise, and application-layer intrusions are rising rapidly. Focusing only on malware overlooks broader attack vectors that often serve as entry points.
3. OT and IT should be secured the same way.	IT security practices don't translate directly to OT environments. OT systems prioritize availability and safety, require different patching timelines, and depend on proprietary protocols that need tailored defenses.
4. OT security is not a board-level issue.	OT security is increasingly becoming the responsibility of CISOs and executive leadership. As industrial systems face growing regulatory pressure and targeted attacks, board-level visibility is now essential.



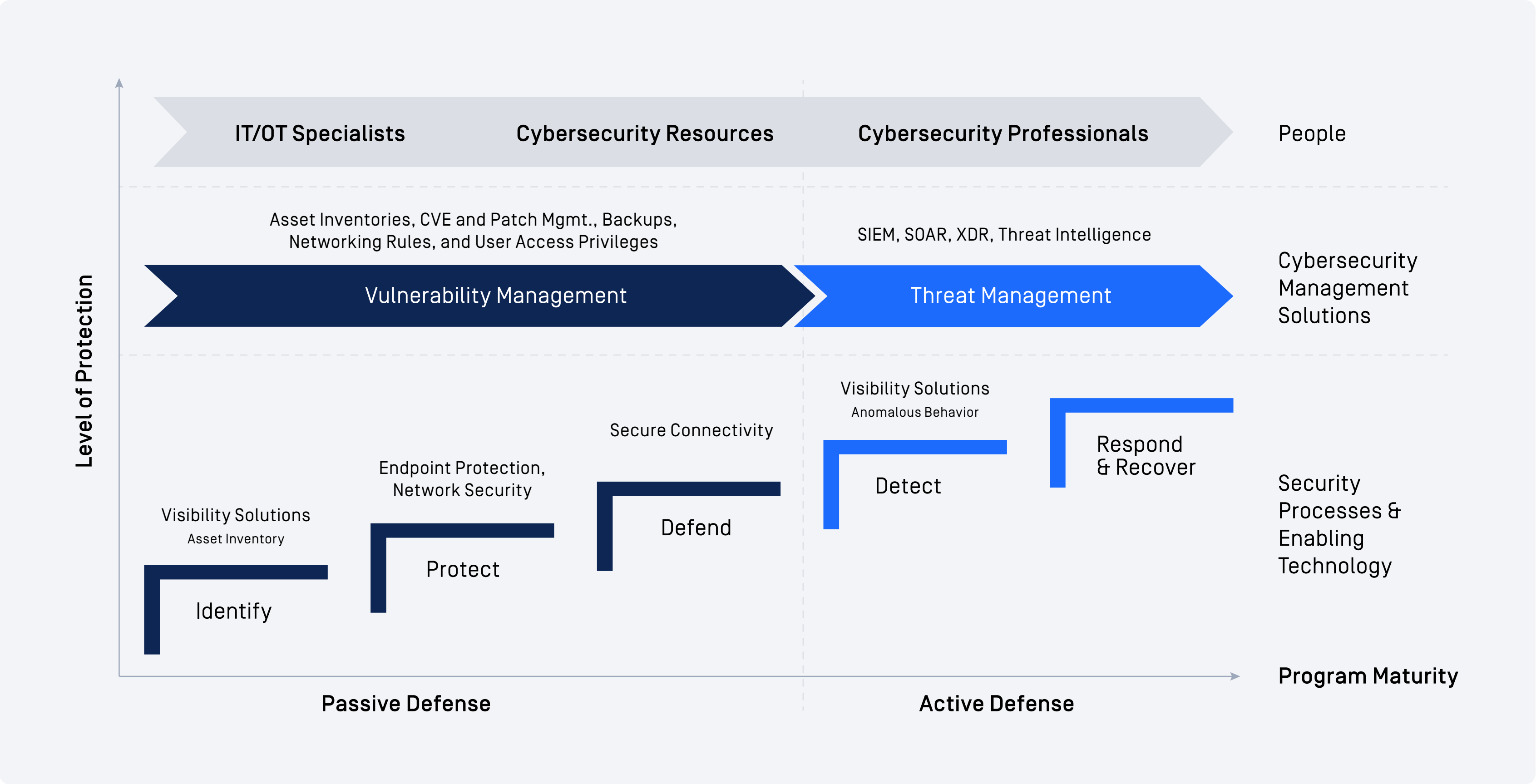
Myth	Reality
5. Regulatory compliance equals security.	Passing audits doesn’t guarantee protection. Many compliant organizations still experience breaches. True resilience comes from proactive, layered defenses, not checkbox compliance.
5. We’ll know if we’re breached.	Breach detection in OT environments is notoriously difficult. Many attacks go unnoticed for weeks or months due to poor monitoring of remediation and limited visibility across legacy systems.
7. Air gaps are enough to protect OT systems.	Air gaps no longer guarantee safety. Due to increased connectivity, digital transformation, and IT-OT convergence, many previously isolated systems are now exposed to remote access and file-based threats.


Removable Media
MetaDefender
Kiosk
My OPSWAT
Central Management
MetaDefender
Transfer Guard
MetaDefender
Optical Diode
Scanned Media
Air Gap
MetaDefender
Transfer Guard
MetaDefender
Optical Diode
MetaDefender
Managed File Transfer
MetaDefender
Endpoint Validation
MetaDefender
Media Firewall
Engineering Workstation
SCADA / HMI

04

Building Cybersecurity Maturity

Cybersecurity maturity, a concept that encompasses the effectiveness and sophistication of an organization's cybersecurity practices, plays a pivotal role in fortifying OT environments against the ever-evolving threat landscape. It is the culmination of comprehensive strategies, technologies, processes, and awareness that empower organizations to proactively detect, respond to, and recover from cyber incidents. By nurturing resilience and elevating cybersecurity maturity, businesses can mitigate risks, enhance operational efficiency, safeguard against financial losses, protect public safety, and ensure the uninterrupted functioning of essential services. This critical cybersecurity concept is visualized clearly in the ARC Cybersecurity Maturity Model.


IT/OT Specialists
Cybersecurity Resources
Cybersecurity Professionals
People
Asset Inventories, CVE and Patch Mgmt., Backups, Networking Rules, and User Access Privileges
SIEM, SOAR, XDR, Threat Intelligence
Vulnerability Management
Threat Management
Cybersecurity Management Solutions
Level of Protection
Visibility Solutions
Asset Inventory
Identify
Endpoint Protection, Network Security
Protect
Secure Connectivity
Defend
Visibility Solutions
Anomalous Behavior
Detect
Respond & Recover
Security Processes & Enabling Technology
Program Maturity
Passive Defense
Active Defense

Multi-Layered End-to-End Protection from the Front Door to the Factory Floor

OPSWAT solutions enable organizations to secure file transfers and data across security domains and zones, authorize users and devices, and mitigate risks from removable media and transient assets.

MetaDefender Kiosk
Protects critical systems by preventing threats introduced by removable media. It comes with scanning performance of up to 13,000+ files per minute and is embedded with industry-leading technologies. MetaDefender Kiosk only enables scanned and sanitized data access to OT environments, protecting organizations at the point of entry.

MetaDefender Drive
Designed to scan laptops thoroughly and ensure they are free from malware before gaining access to OT environments. MetaDefender Drive boots using its own OS to scan laptops and stationary devices. This portable scanning device can be easily integrated into existing security protocols, offering a reliable means of confirming the cleanliness of laptops.

MetaDefender Endpoint
Proactively scans connected devices and ensures endpoint compliance by blocking all removable media usage until security conditions are met. This reduces supply chain risks. It also helps protect critical endpoints from third-party applications by identifying vulnerabilities and supporting remediation through robust patch management, keeping critical assets secure, and minimizing potential attack surfaces.

MetaDefender Endpoint Validation
Alongside MetaDefender Kiosk, MetaDefender Endpoint Validation serves as an additional layer of security, protecting critical assets from peripheral and removable media-borne threats by enforcing scanning and sanitization policies and offering HID and BadUSB protection.

MetaDefender Managed File Transfer
Ensures that all file transfers are secure and automates the process of transferring files from IT to OT environments. Each file is rescanned and verified for unknown threats.

MetaDefender Media Firewall
Ensures that boot sectors and file contents of inserted portable media are inspected, audited, sanitized, and approved before use.

MetaDefender Netwall
Enforces strict controls over data entering and exiting the air-gapped network, significantly reducing the risk of sensitive information leaks in the event of a breach. This would make it significantly harder for attackers to extract data, even if they manage to implant malware in air-gapped environment.

My OPSWAT Central Management
Helps enforce scan policy consistency by providing centralized control over security configurations across all endpoints. Administrators can define, deploy, and monitor scan policies from a single dashboard, which improves compliance and simplifies enforcement of standards, whether antivirus scans, media protection, or other security measures. With real-time visibility and reporting, My OPSWAT Central Management ensures that security policies are consistently applied and easily adjustable as needed.e.

Built With OPSWAT's Technology

MetaScan™ Multiscanning

#1 Market-Leader

Advanced Threat Prevention with Simultaneous Anti-Malware Engines

Every day, 560,000 new pieces of malware are detected*, making it harder for signature-based, single-engine AV software to keep up. Modern threats, especially with the emergence of AI technologies, often bypass traditional detection methods, posing significant risks to OT and ICS environments. MetaScan Multiscanning leverages 30+ leading anti-malware engines and proactively detects over 99% of malware by using signatures, heuristics, and machine learning. This significantly improves detection of known and unknown threats and provides the earliest protection against malware outbreaks.

Deep CDR™

#1 Market-Leader

File Regeneration that Protects from Evasive Malware and Zero-Day Exploits

Deep CDR sanitizes files by extracting potentially malicious objects, scripts, and other out-of-policy content, regenerating safe-to-use files. By focusing on prevention rather than just detection, Deep CDR enhances anti-malware defenses, protecting organizations from file-based attacks, including targeted threats. It neutralizes potentially harmful objects in files traversing network traffic, email, uploads, downloads, and portable media before they reach your network. With support for over 200 file types, including PDFs, Microsoft Office documents, HTML files, and common image types, Deep CDR helps eliminate threats that traditional antivirus solutions may miss.

Country of Origin

Enable instant detection of a file's geographic source

OPSWAT's Country of Origin technology enables instant detection of a file's geographic source. By analyzing digital fingerprints and file metadata to identify restricted locations and vendors automatically, it filters and blocks files from specific origins to support regulatory compliance.

File-Based Vulnerability Assessment

Detect Application Vulnerabilities Before They are Installed

All applications contain exploitable vulnerabilities of varying severity. Our File -Based Vulnerability Assessment improves endpoint security. It detects binaries and installers with known vulnerabilities in files, applications, and software before they are installed on endpoint devices, including IoT devices. It supports vulnerability detection for over 1 million files and over 20,000 applications.

Adaptive Sandbox

Adaptive Threat Analysis

Adaptive Sandbox uses advanced emulation technology for zero-day malware detection, extracting key IOCs with 10x faster and 100x more efficient analysis than traditional sandboxes. It's a vital tool for in-depth threat and malware analysis, helping organizations stay ahead of emerging threats and fine-tune their cybersecurity strategies.

Proactive DLP™

Detect and Block Sensitive Data

Detect Sensitive Data and Protect Against Data Leakage Proactive DLP can help prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive, out-of-policy, and confidential data in files and emails, including credit card numbers and social security numbers. Supporting a wide range of file types, including Microsoft Office and PDF. AI-powered Document Classification detects adult content in images and offensive language in text.

05

Use Cases and Proven Deployments

Let's explore our real-world case studies where user challenges addressed by OPSWAT's solution and outcome were achieved. These stories demonstrate what success looks like when cybersecurity solutions are designed around the people, roles, and pressures of critical infrastructure.

USE CASE #1

A Leading Automaker Strengthened Production Security with OPSWAT MetaDefender Kiosk™

Customer: Global Automotive Manufacturer

Region: United States

Employees: 100,000 employees

This company is a global leader in automotive manufacturing, producing a diverse range of vehicles. They operate on an international scale and prioritize innovation in electric and autonomous vehicle technologies. From manufacturing to the finished vehicle, their approach to cybersecurity is comprehensive, highlighting a company-wide dedication to both safety and protection

Challenges

- **Securing Removable Media:** The US-based automotive manufacturer struggled with securing data transfers that involved peripheral devices and removable media within their complex production environment.
- **Limitations of Previous Solution:** Their existing security system had several drawbacks.
- It used a single scanning engine, limiting its detection capabilities.
- It frequently malfunctioned due to exposure to debris in the production environment.
- It had slow scanning times, causing costly production downtime and increasing vulnerability to advanced threats.

Solution

MetaDefender Kiosk: The manufacturer adopted OPSWAT's MetaDefender Kiosk. This solution is specifically designed for industrial environments and provides:

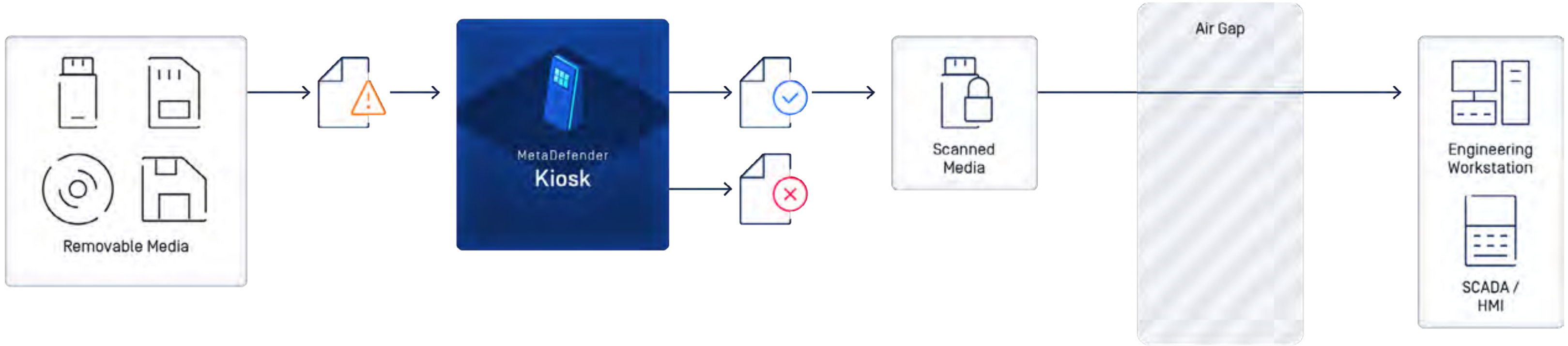
- **Multi-engine Scanning:** It utilizes multiple antivirus engines for comprehensive threat detection.
- **Integration with Visitor Management:** It can be integrated with visitor management systems to streamline security processes.

USE CASE #1

A Leading Automaker Strengthened Production Security with OPSWAT MetaDefender Kiosk™

Results

- **Reduced Failures and Maintenance:** The Kiosk's robust and durable design led to fewer malfunctions and reduced maintenance requirements.
- **High-Speed Secure Scans:** It enables fast scanning of incoming media, preventing disruptions to critical production workflows.
- **Advanced Threat Prevention:** Features like Deep Content Disarm and Reconstruction (CDR) and Proactive Data Loss Prevention (DLP) ensured files were sanitized and sensitive information remained secure.
- **Enhanced Cybersecurity Culture:** Customization options allowed the Kiosk to be branded, helping to foster a stronger cybersecurity awareness within the organization.



USE CASE #2

Abdi Ibrahim Secures Pharma Data with OPSWAT MetaDefender Kiosk™

Customer: Abdi Ibrahim

Region: EMEA

Employees: 5,500 employees

Founded in 1912 by Istanbul pharmacist Abdi İbrahim Bey, Abdi Ibrahim Pharmaceuticals has become Türkiye's leading pharmaceutical company, boasting a portfolio of 250 brands and over 500 products. Operating in 17 countries with 5,500 employees, the company is home to AbdiBio, Türkiye's largest accredited biotechnological manufacturing facility, specializing in hormone production, sterile ophthalmology, inhalation products, injectables, and oncology treatments.

Challenges

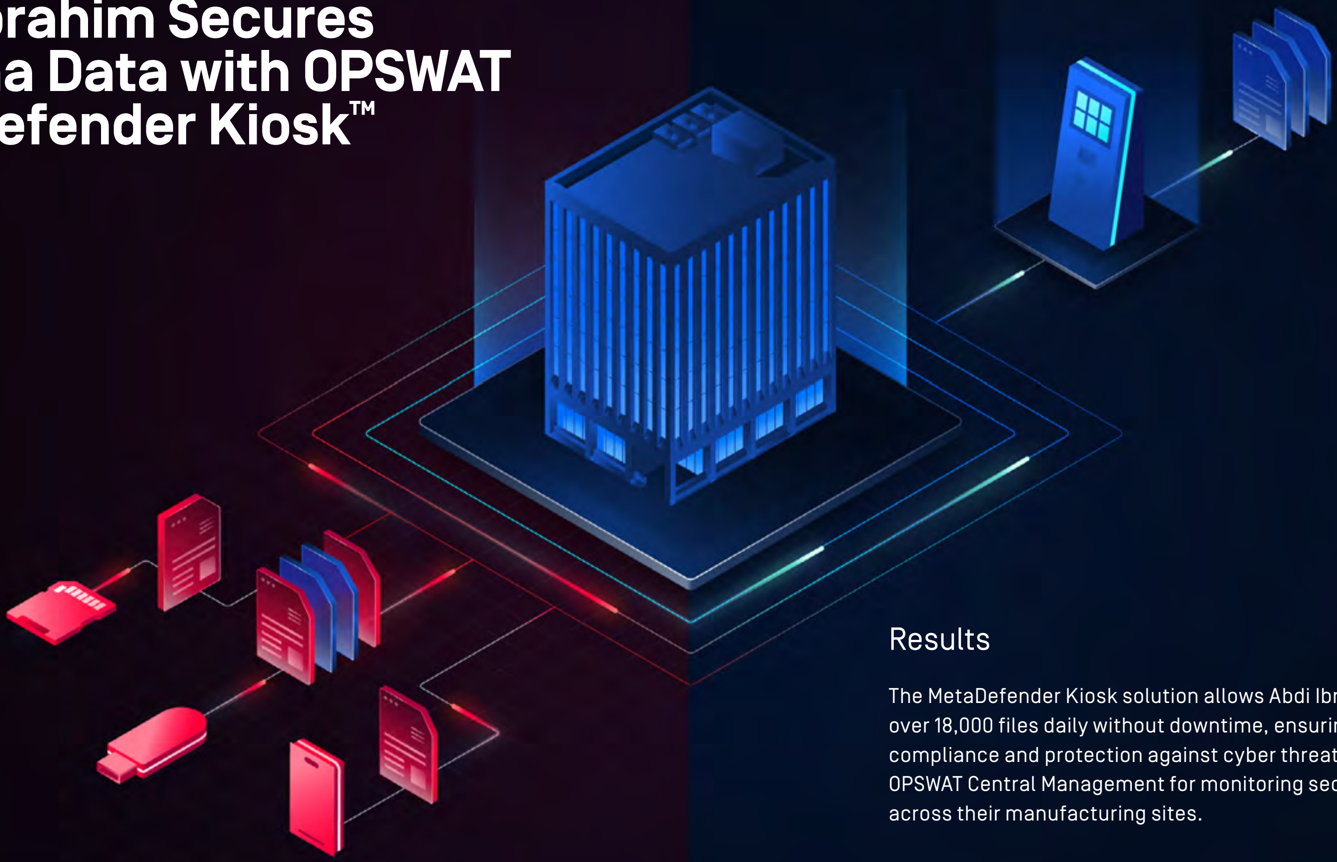
Abdi Ibrahim initially used an air gap for OT asset protection, but this was insufficient against threats from portable media like USB drives

Solution

They integrated OPSWAT's MetaDefender Kiosk to scan and sanitize files, preventing malware and securing file transfers, which was critical for protecting sensitive data like pharmaceutical recipes and OT configurations.

USE CASE #2

Abdi Ibrahim Secures Pharma Data with OPSWAT MetaDefender Kiosk™



Results

The MetaDefender Kiosk solution allows Abdi Ibrahim to scan over 18,000 files daily without downtime, ensuring regulatory compliance and protection against cyber threats. They also use OPSWAT Central Management for monitoring security protocols across their manufacturing sites.

USE CASE #3

Preventing Cross-Domain Threats for a Vietnamese Manufacturer

Customer: Automotive Manufacturer

Region: Asia Pacific

Employees: 1,200+ employees

A leading fertilizer producer and trader in Vietnam, this company, part of a large energy group, focuses on developing comprehensive nutritional solutions for crops to support farmers and the agricultural sector. With significant achievements, they've had a major impact on the Vietnamese fertilizer market.

Challenges

- **Flat Network Design:** The manufacturing plant used a flat network where IT and OT systems were interconnected without proper segmentation. This design made the entire network vulnerable to widespread malware and ransomware attacks.
- **Internal Risks:** Potential threats from employees, contractors, or suppliers pose internal security risks.
- **External Threats:** The company was also exposed to external cybercriminal activities

Solutions

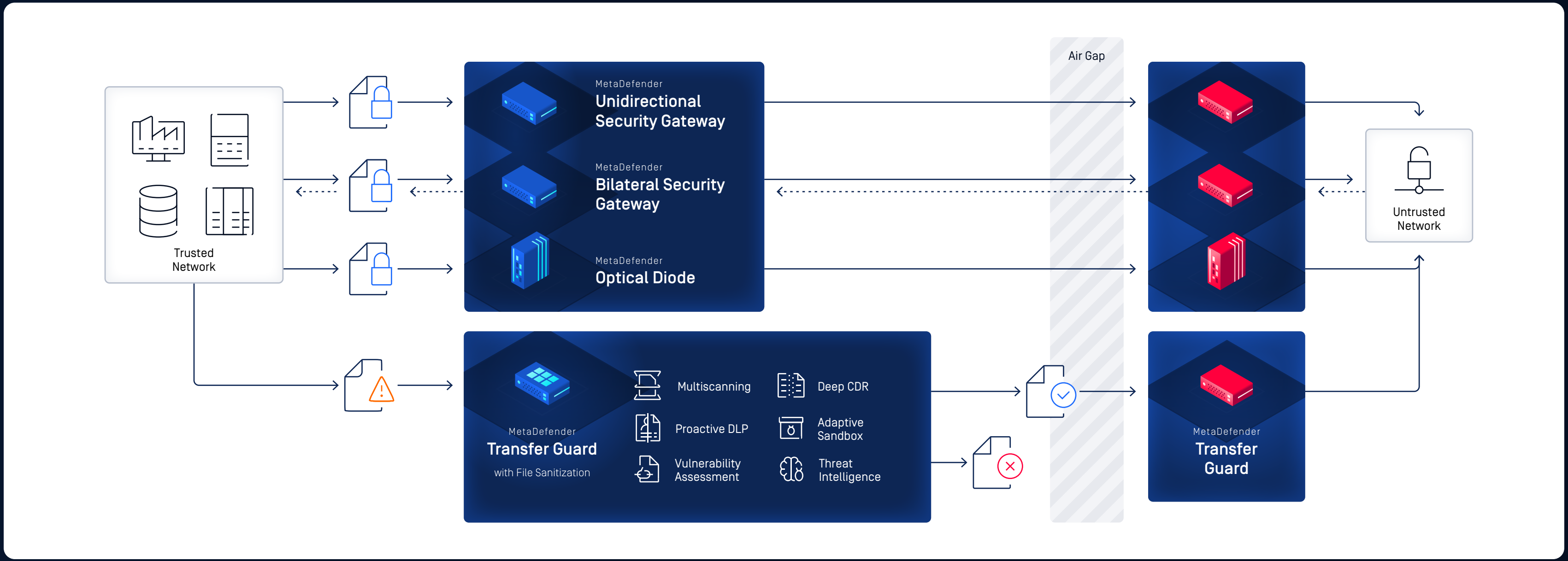
- **OPSWAT MetaDefender Optical Diode:** The manufacturer deployed OPSWAT's MetaDefender Optical Diode, part of the MetaDefender NetWall Suite of Solutions. This hardware-enforced solution establishes a one-way data transfer link, physically separating IT and OT networks.

Results

- **Enhanced Security:** The solution eliminated communication vulnerabilities between IT and OT systems, effectively preventing the spread of malware and external attacks.
- **Simplified Security Management:** It streamlined security operations by removing the need for complex firewall configurations.
- **Compliance Maintenance:** The implementation helped the company adhere to industrial cybersecurity standards.
- **Stable Operation:** The solution contributed to maintaining stable operations even in challenging industrial environments and protected critical infrastructure.

USE CASE #3

Preventing Cross-Domain Threats for a Vietnamese Manufacturer


Trusted Network
MetaDefender Unidirectional Security Gateway
MetaDefender Bilateral Security Gateway
MetaDefender Optical Diode
Air Gap
Untrusted Network
MetaDefender Transfer Guard with File Sanitization
Multiscanning
Deep CDR
Proactive DLP
Adaptive Sandbox
Vulnerability Assessment
Threat Intelligence
MetaDefender Transfer Guard

USE CASE #4

Protecting Agricultural Operations from OT Cyberattacks and Data Tampering

Customer: Agriculture Manufacturing

Region: Global

Employees: 10,000+ employees

The customer, operating in the Agriculture and Food Sector operated on two types of systems: OT – Operational Technology - controlling the machinery, sensors, and systems in their physical operations, and IT – Informational Technology - for business data, communications, and software management.

Challenges

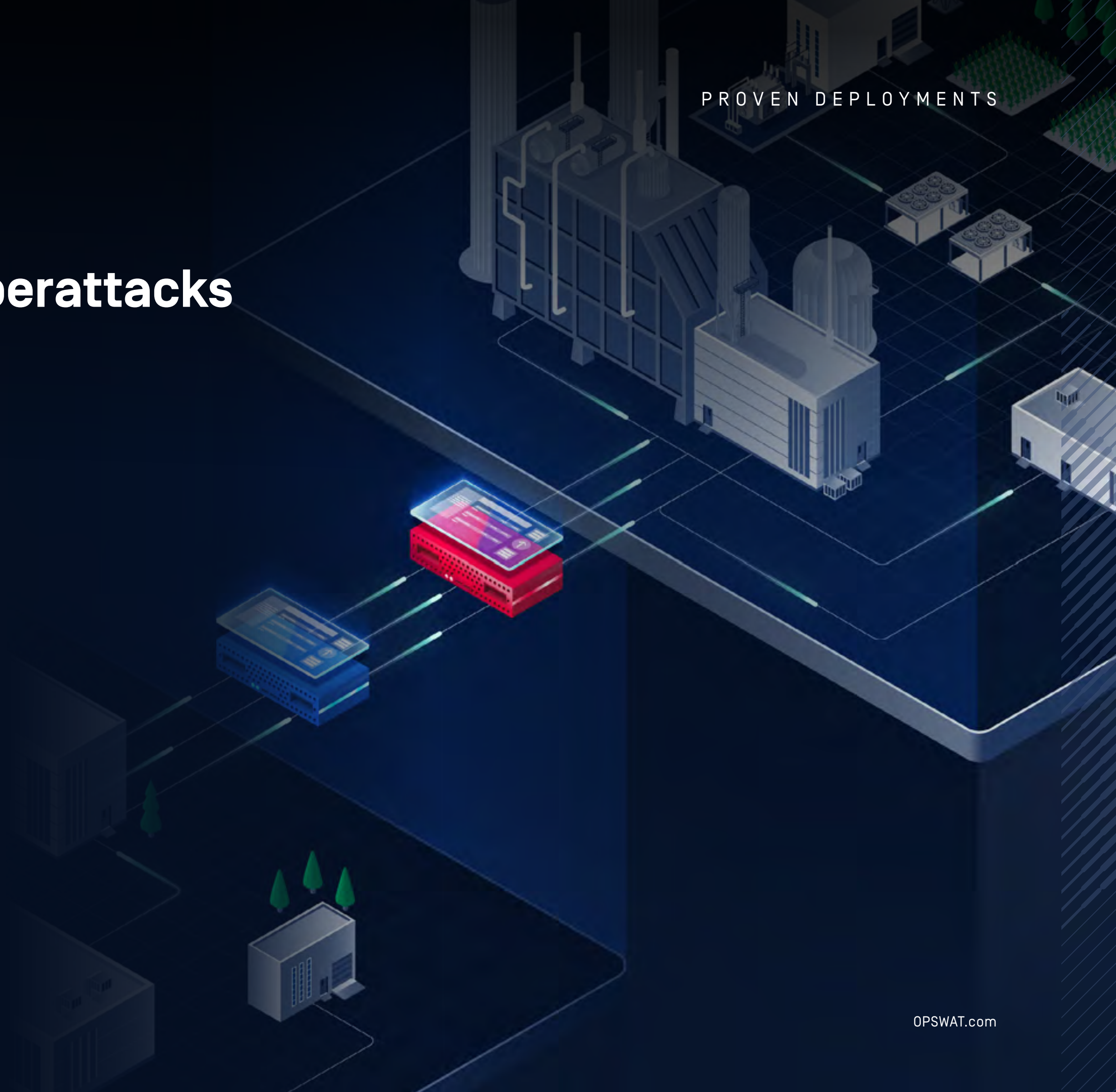
- **Balancing Cybersecurity and Data Visibility:** The agricultural and food sector customer initially air-gapped (completely isolated) their Operational Technology (OT) and Information Technology (IT) systems for security. While this provided protection, it prevented business teams from accessing and monitoring critical OT data, which hindered planning and operational efficiency.
- **Regulatory Compliance:** The need to comply with regulations such as FDA cGMP and FSMA requires ensuring data accuracy, confidentiality, and controlled access.

Solutions

- **MetaDefender Optical Diode:** The customer deployed OPSWAT's MetaDefender Optical Diode, a hardware device within the MetaDefender NetWall Suite. This solution facilitates secure, unidirectional data flow, acting as a "data gatekeeper" to allow data to move from OT to IT systems but not in reverse. This protects vulnerable OT systems from external threats while enabling necessary data visibility.

USE CASE #4

Protecting Agricultural Operations from OT Cyberattacks and Data Tampering



Results

- **Real-time OT Data Access:** Business teams gained real-time access to critical OT data, significantly improving performance monitoring and maintenance planning.
- **Enhanced OT Network Protection:** The solution secured the OT network from cyber threats by preventing two-way communication between OT and IT systems.
- **International Security Standard Compliance:** The MetaDefender Optical Diode is Common Criteria EAL4+ certified, demonstrating its adherence to high international security standards.
- **Regulatory Adherence:** It supports various industrial protocols and aids the organization in meeting crucial regulatory requirements.

USE CASE #5

Securing Data Flow for a Fortune 500 Petrochemical Company with MetaDefender Optical Diode [Fend]

Customer: Petrochemical Manufacturer

Region: Global

Employees: 10,000+ Employees

A Fortune 500 petrochemical company operates 20 refineries across North America, producing essential fuels, lubricants, and petrochemicals used globally. With thousands of employees, the company’s operations rely on DCS [distributed control systems] that continuously generate and transmit critical process data. Maintaining secure and reliable data flow is essential for both regulatory compliance and safe operational performance.

Challenges

- **End-of-Life Firewalls:** The petrochemical company's existing firewall manufacturer announced end-of-life support for their products by 2025. This created a significant risk to the security of the air gap between their IT [Information Technology] and OT [Operational Technology] environments.
- **Vulnerability to Cyberattacks:** The potential loss of the air gap meant increased risks of unauthorized access to critical OT data, operational disruptions, and heightened cyber threats such as ransomware, zero-day exploits, and remote access attacks.
- **Financial Impact:** Downtime caused by security breaches could lead to substantial financial losses.

Solutions

MetaDefender Optical Diodes [Fend XE15]: The company opted to replace their end-of-life firewalls with OPSWAT's MetaDefender Optical Diodes [Fend XE15]. These data diodes provide hardware-level security, enforcing one-way data flow to prevent inbound threats from reaching the OT environment.

USE CASE #5

Securing Data Flow for a Fortune 500 Petrochemical Company with MetaDefender Optical Diode (Fend)

Regulatory Compliance

The solution helped the company meet necessary industry regulations.

Stronger Cyber Resilience

It significantly enhanced the company's ability to withstand and recover from cyberattacks.

Operational Efficiency

The secure and reliable data flow contributes to smoother and more efficient operations.

Long-term Stability

The robust security solution provided long-term stability for the company's critical infrastructure.

USE CASE #6

Protecting an Automotive Manufacturer from File-Borne Threats

Customer: Automotive Manufacturer

Region: Global

Employees: 10,000+ Employees

A global automotive manufacturer with thousands of employees produces vehicles for markets worldwide, focusing on innovative technology and operational efficiency. This company plays a critical role in the global supply chain, with production facilities located across several continents.

Challenges

- **Securing File Scanning, Transfer, and Visitor Management:** A global automotive manufacturer struggled with ensuring robust security across these critical areas of their operations.
- **Ineffective Multi-Vendor Solution:** Their existing security setup, which involved multiple vendors, was difficult to integrate, leading to security gaps and leaving critical infrastructure vulnerable to cyber threats.
- **Rising Cyber Incidents:** The automotive industry has experienced a significant increase in cyber incidents, with a large portion resulting in service and business disruptions

Solutions

OPSWAT's Integrated MetaDefender Platform: The manufacturer adopted a unified approach by implementing key components of the OPSWAT MetaDefender Platform.

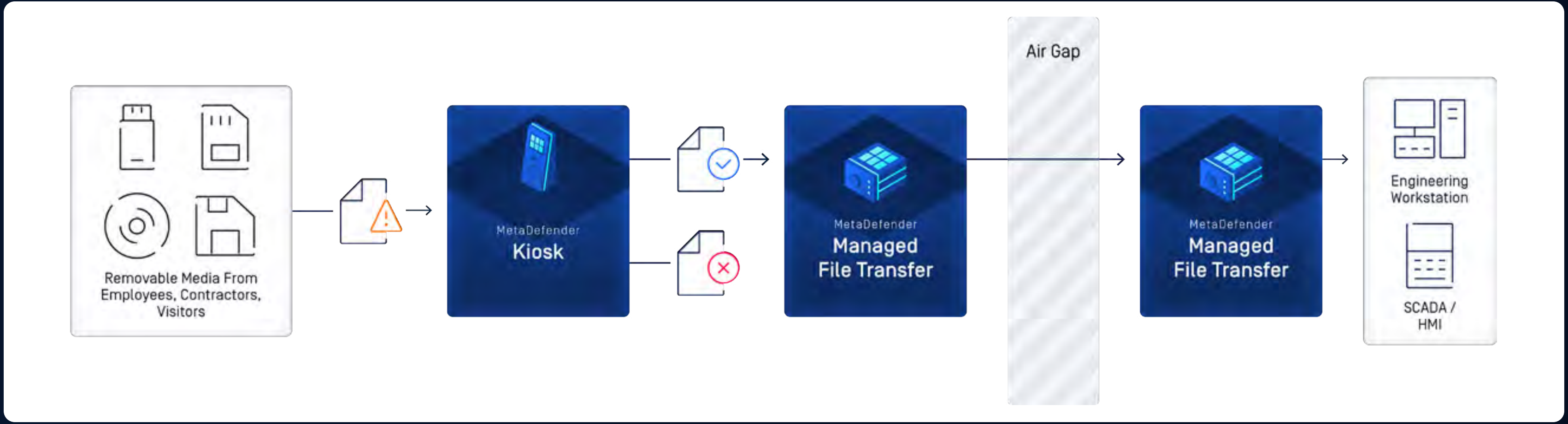
- **MetaDefender Kiosk:** Deployed at entrances and critical control areas for secure visitor management and thorough file scanning.
- **MetaDefender Managed File Transfer:** Used to ensure secure and controlled file transfers both within the internal

USE CASE #6

Protecting an Automotive Manufacturer from File-Borne Threats

Results

- **Improved Operational Efficiency:** The integrated solutions streamlined security processes, leading to greater efficiency in daily operations.
- **Unified Security Enforcement:** The platform ensures consistent security policies and enforcement across the entire infrastructure, eliminating previous security gaps.
- **Advanced Visibility and Control:** The manufacturer gained enhanced insight and control over data movement and potential threats.
- **Vendor Consolidation:** Merging security solutions under a single vendor with reduced complexity and increased efficiency.
- **Robust Threat Prevention:** Technologies like MetaScan Multiscanning (using multiple antivirus engines) and Deep Content Disarm and Reconstruction (CDR) provide strong protection against file-borne threats and ensure data integrity.



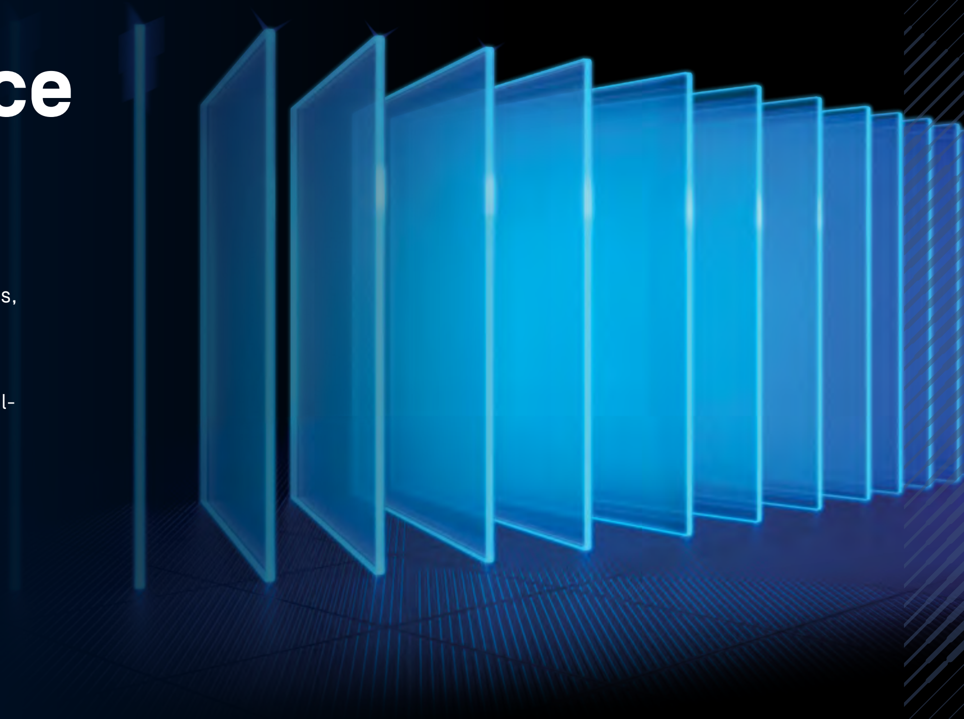
06

Strengthening Resilience Across Manufacturing

Manufacturing organizations face unique cybersecurity challenges from air-gapped OT systems to fragmented file flows and third-party risks. As digital transformation accelerates, legacy tools and manual transfers can no longer keep pace with evolving threats.

Here we have explored common manufacturing security challenges, debunked persistent myths, and outlined a path toward mature, resilient cyber defense. We also showed how real-world manufacturers are deploying OPSWAT technologies to enforce secure file transfers, control removable media, and protect against threats across industrial environments.

As manufacturers digitize and connect more processes, a proactive security approach is essential. OPSWAT's purpose-built solutions help manufacturing organizations secure the flow of data and maintain safe, compliant, and uninterrupted operations.



Are you ready to put OPSWAT on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Visit us at:
opswat.com/get-started
sales@opswat.com

Since 2002, OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,800 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life. Visit: www.opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure