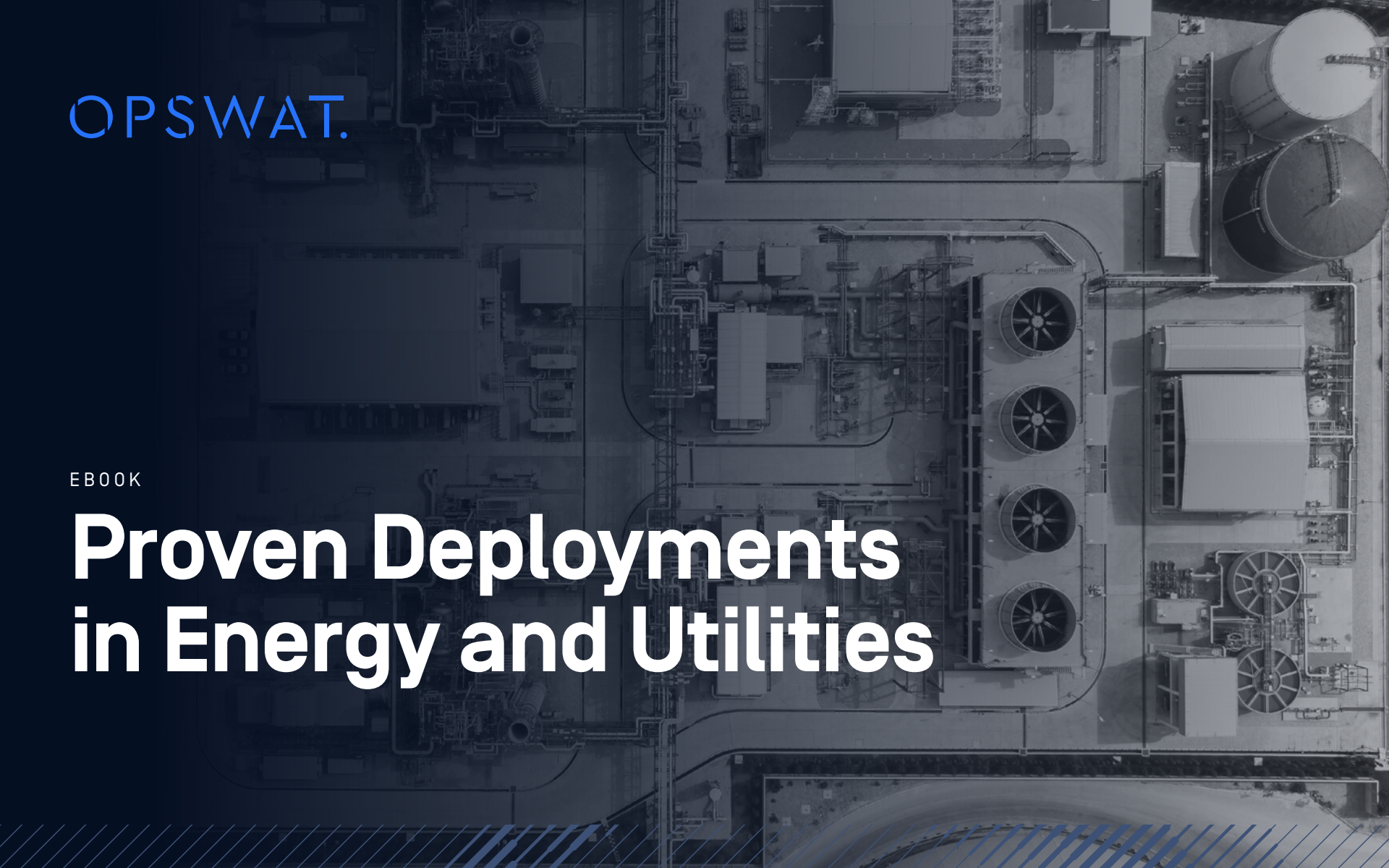
OPSWAT.



EBOOK

Proven Deployments in Energy and Utilities

Table of Contents

01

Introduction

The energy and utilities sector has been a primary target of cyberattacks by both independent and state-sponsored threat actors. With infrastructure modernization and digitized operations, attack vectors increase in number and complexity.

Within the OT environments of modern infrastructure, field teams often rely on USB drives and external laptops to transfer data, apply patches, and perform maintenance tasks. Third-party contractors also access air-gapped environments with minimal security oversight, leading to data flows between IT and OT systems without visibility or comprehensive control. In addition, inbound hardware often carries complex, preloaded software and unverified components, introducing potential supply chain vulnerabilities.

These are not speculative causes of cyberattacks. There have been various alarming incidents in recent years:

- Cyberattack on a German nuclear plant that led to operational disruptions
- FrostyGoop malware attack that left 600 apartment buildings with no power for two days
- Cyberattack on a Florida water treatment plant where hackers remotely manipulated the toxic chemical levels of the water supply

Critical infrastructure industries, including Energy and Utilities, are strictly regulated, and failing to meet compliance comes at a high cost. For instance, the Sellafield nuclear site received a £332,500 fine after being found with significant cybersecurity shortfalls. A U.S. utility was similarly penalized with a record $10 million fine for widespread NERC CIP violations, highlighting critical gaps in its cybersecurity practices.

02

Common Cybersecurity Challenges

Maintaining Compliance with Traceable Records

At a US-based energy utilities company, a compliance officer was responsible for enforcing policies to maintain compliance with industry standards like NERC CIP and NIST, which require strict control over removable media and transient cyber assets. The compliance officer ensured that the policies were implemented, but failed to provide complete logs, records, or sufficient trail during an audit. The reporting and logging mechanisms implemented lacked consistency, leaving the team with no way to prove that procedures were enforced.

Legacy Systems Outpaced by Modern Threats

A plant engineer at a gas processing plant was using a 20-year-old control system to monitor pressure and flow. The aging hardware and outdated operating system could not support modern endpoint security, leaving critical assets exposed. This also created significant vulnerabilities due to the system's lack of support for features such as real-time threat detection, patch management, and secure remote access.

Blind Transfers from IT to OT

At a utility company, the IT lead was sending software updates into the OT network using a shared folder that contained unscanned files. The OT manager had no visibility into what was coming, and no action was taken to control how it was being handled, making this transition a blind spot. Both sides assumed that the other had it covered.

Unscanned Removable Media

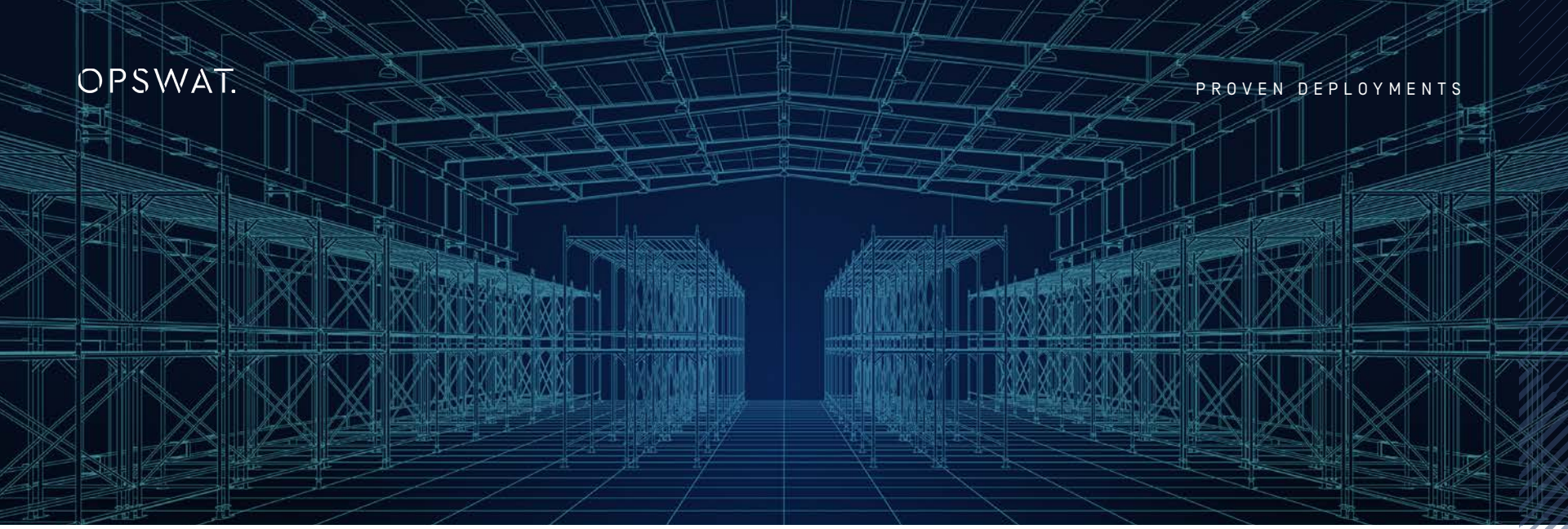
A field technician at a power generation facility used a USB drive to patch and update the SCADA system, assuming it was safe because it had been scanned three months prior. The same drive had been used on other substations for patching and hadn't been re-scanned. Skipping frequent security checks, which commonly occur in OT environments, created a direct path to a compromised network.

No Centralized Visibility or Control

The compliance officer of an energy production company was tasked with reviewing security practices across multiple power plants ahead of an audit. One facility had a removable media scanning kiosk with no policy enforcement, another used outdated AV, and a third did not have any removable media policies or transient devices control protocols in place.

Inbound Hardware Leads to Increased Downtime

An engineering contractor arrived at a nuclear power facility with a laptop preloaded with software and unverified components, many lacking proper origin validations. The site's security manager granted it access to the OT zone after a quick antivirus scan due to the urgency to maintain uptime. Instead, this action caused a costly breach and actually resulted in increased downtime. Such action not only exposed critical infrastructure to threats but also violated key OT security guideline frameworks such as NIST SP 800-82 and IEC 62443.



03

Myths vs. Reality

Myth	Reality
1. Air Gaps Ensure Security.	Malware comes in different forms and can bypass air gaps and make its way into isolated systems through various methods, such as USBs and third-party vendor laptops.
2. Field Operators Always Follow Policies.	In practice, policies and safe use instructions slow down field operators, and they are often overlooked unless a physical enforcement mechanism is in place.
3. Not Having Prior Incidents Means a System is Secure.	In reality, some of the most dangerous cyberthreats went undetected. Some took years until they were first detected.
4. Preventive Measures are Enough.	Having effective preventive measures on paper does not mean that they will be properly enforced during field operations.
5. Internal Use Ensures Data Safety.	Even the internally used removable media and employees' internet-connected laptops still pose significant risks to secure, isolated environments.

OPSWAT.

04

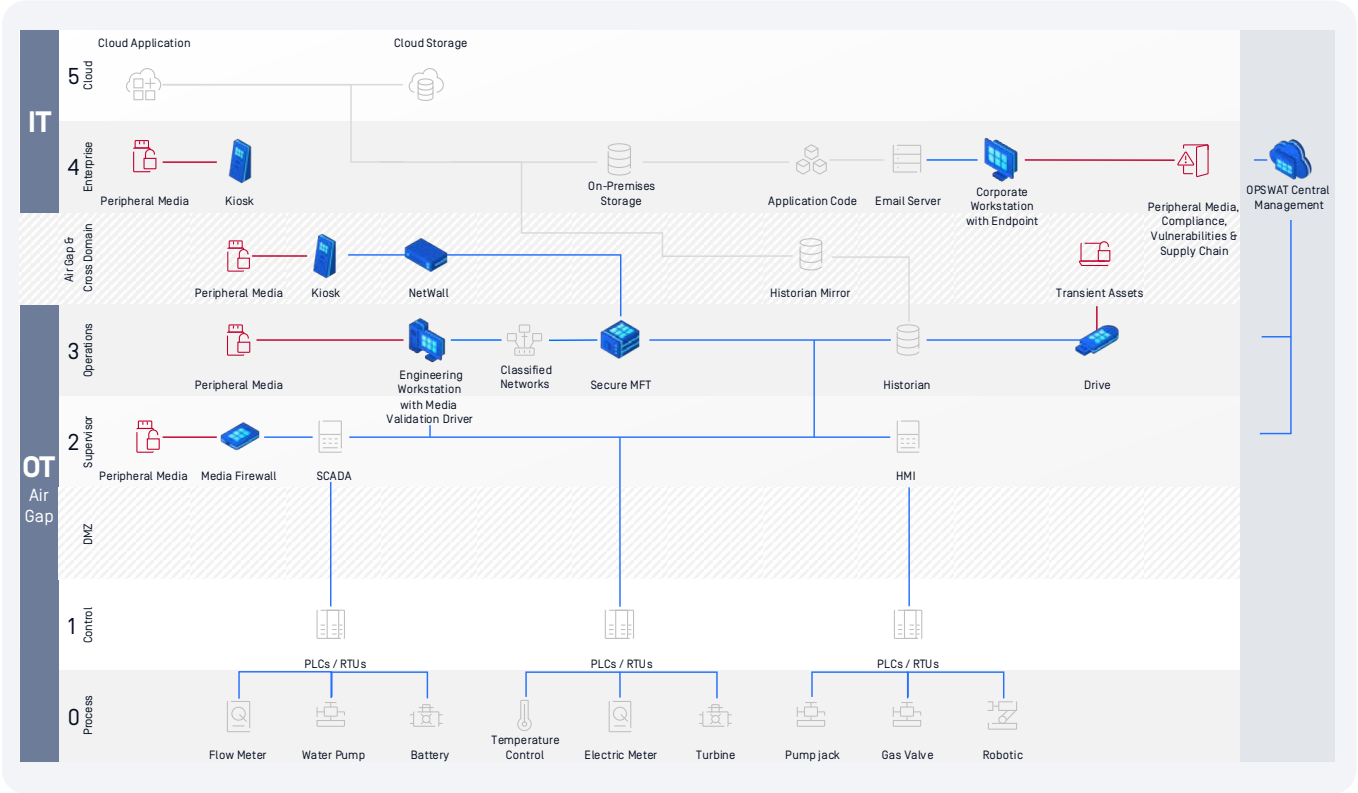
Comprehensive, Purpose-Built Solutions to Address Real-World Challenges

Practical Solutions for Every Role

OPSWAT solutions have earned the trust of global energy companies' security experts, enabling them to standardize security protocols across all sites. With solutions tailored to address the specific needs of various roles within the cybersecurity world, field operators and security leadership at companies deploying OPSWAT products and solutions have had their specific concerns addressed to maintain cyber resilience and enhance security posture.

The Role	The Need	OPSWAT Solution
Compliance Officer	Audit-ready scan reports and logs	Centralized proof of compliance to support regulatory audits with a unified view
Plant Operator	Safe and easy-to-use security tools to enforce security policies without risking system downtime	Secure, comprehensive, and efficient scanning solutions to mitigate threats at the point of entry
CISOs and Security Leadership	Holistic visibility across all sites, including security posture, tools in use, and emerging threats.	Centralized control to enforce consistent policies, streamline access, and ensure compliance across all sites, with real-time visibility and easy policy updates

Multi-Layered End-to-End Protection



OPSWAT solutions enable energy and utility organizations to secure file transfers and data across secure zones. It enables organizations to manage and authorize user access, files, and devices, helping security teams mitigate risks posed by vulnerabilities, malicious code, and unauthorized access of transient cyber assets and removable media.

End-to-End Protection

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 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 Media Firewall
Enhances the defense-in-depth removable media cybersecurity strategy for IT and OT by enforcing the scan policies and validating that all files have been scanned by MetaDefender Kiosk. It ensures that boot sectors and file contents of inserted portable media are inspected, audited, sanitized, and approved prior to use.

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 Managed File Transfer
Offers secure, policy-driven file transfers across networks. It ensures that all file transfers are secure and automates the process of transferring files from IT to OT environments.

MetaDefender Netwall
Enforces strict controls over data entering and exiting air-gapped networks, significantly reducing the risk of sensitive information leaks in the event of a breach. It impedes attackers from extracting data, even if they manage to implant malware in air-gapped environments.

My OPSWAT Central Management
Helps enforce consistent scan policies by providing centralized control over security configurations across all endpoints. Administrators can define, deploy, and monitor scan policies from a single dashboard to support compliance and simplify the enforcement of standards.

OPSWAT.

MetaScan™ Multiscanning

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.

*According to Statista's State of Malware Worldwide report

Deep CDR™

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.

*OPSWAT Deep CDR is the first technology ever to achieve 100% rating by SE Labs.

Adaptive Sandbox™

Adaptive Threat Analysis

Adaptive Sandbox uses advanced emulation technology for zero-day malware detection, extracting key IOCs (indicators of compromise) 10x faster and 100x more efficiently 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.

OPSWAT.

Proactive DLP™

Detect Sensitive Data and Protect Against Data Leakage

Proactive DLP technology 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. Proactive DLP supports 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.

Country of Origin

Instant Detection of a File's Geographic Origin

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

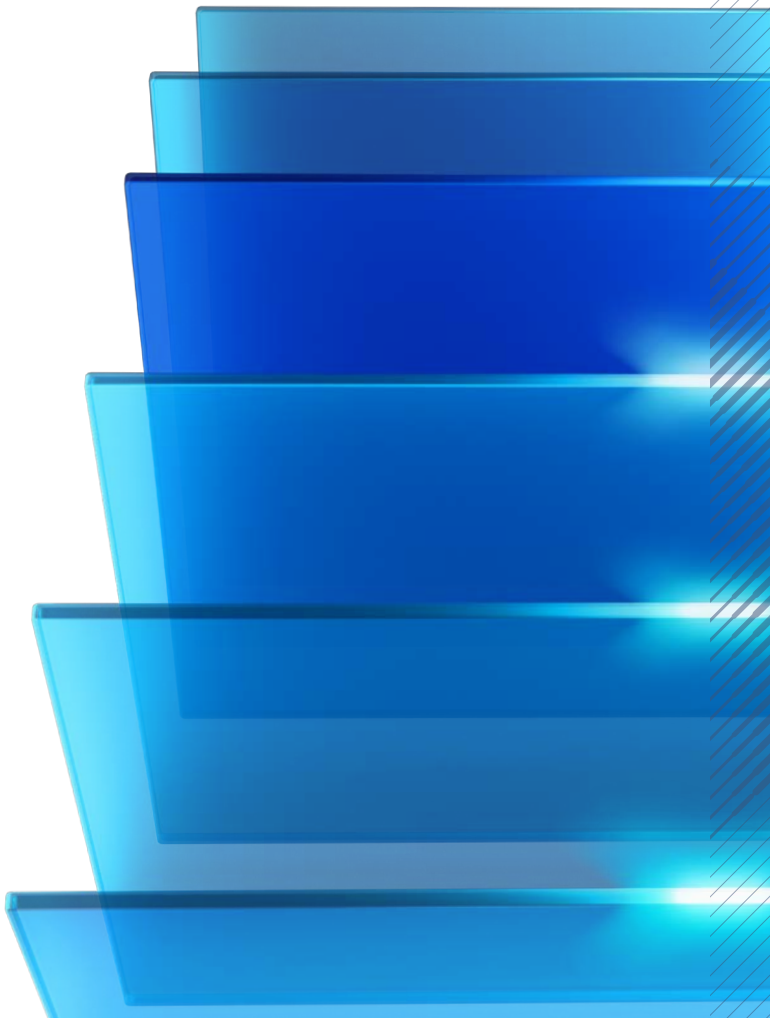
Detect Application Vulnerabilities Before They Are Installed

By using this patented technology (U.S. 9749349 B1), File-Based Vulnerability Assessment technology detects application and file-based vulnerabilities before they are installed. This technology correlates vulnerabilities to software components, product installers, firmware packages, and many other types of binary files, which are collected from a vast community of users and enterprise customers.

05

Use Cases and Proven Deployments

The following are real-world case studies, presenting challenges that OPSWAT customers have faced and how those challenges were addressed using OPSWAT solutions. These stories demonstrate success stories when cybersecurity solutions are designed around people, roles, and pressures of critical infrastructure:



USE CASE #1

Total File Security at Dounreay Nuclear Facility

Customer: Dounreay Nuclear Facility

Region: Dounreay, Scotland

Employees: 1,500 employees

Deployed Solutions: MetaDefender Core, MetaDefender Kiosk, MetaDefender Drive, MetaDefender Managed File Transfer

A nuclear research and development site faced significant cybersecurity challenges during the decommissioning process involving an outdated file security system that required a manual scanning process, provided limited threat detection, and entailed prolonged file validation.

Challenges

- Designing the need for advanced file security measures beyond the capabilities of conventional antivirus and endpoint security solutions.
- A single-engine legacy antivirus was not capable of detecting advanced threats.
- Manually scanning files using the sheep dip system[1].
- Validating files took days to finalize.
- The system was not auditable.

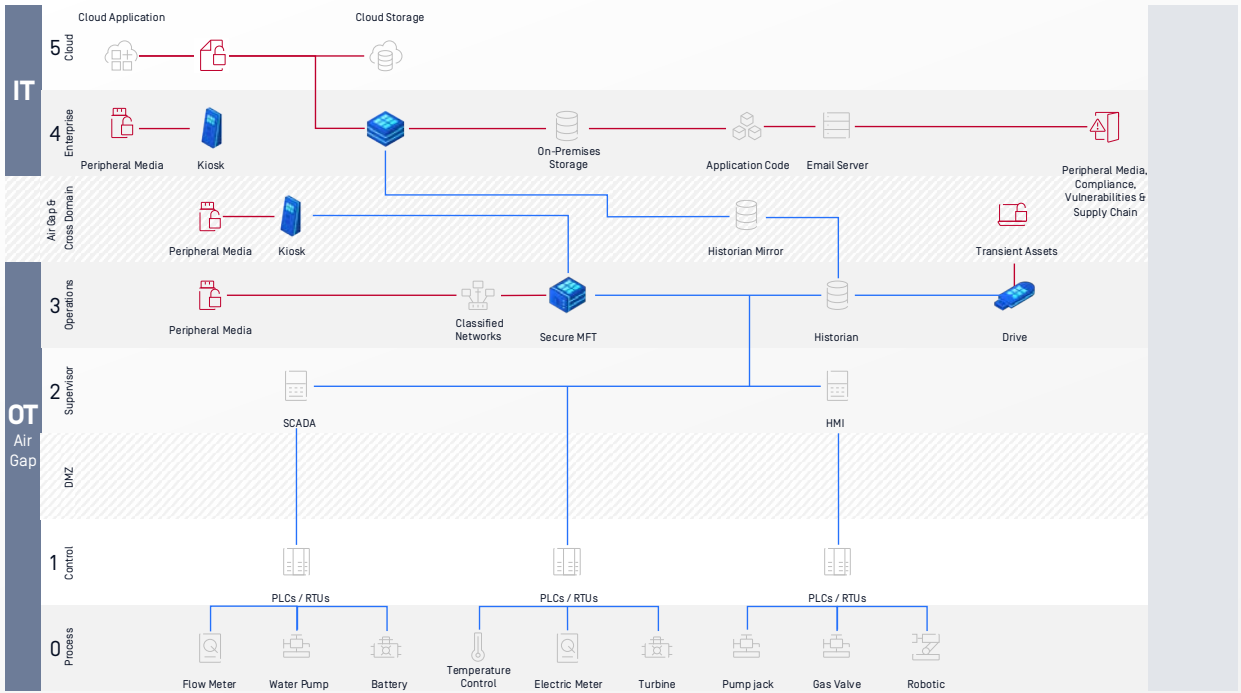
Deployment Outcomes

- **Reliability and Flexibility:** MetaDefender Core and Kiosk safely scanned and stored web-uploaded and physically brought-in files, replacing the manual process.
- **Secure Supply Chain:** MetaDefender Drive scanned third-party laptops before site entry, preventing malware from vendors.
- **Safe File Uploads:** MetaDefender Managed File Transfer in a DMZ, allowing pre-uploaded files to be scanned securely.
- **Increased Efficiency:** Scanning and securing removable media in hours, down from three to five days.

1. The outdated, legacy "sheep dip" manual file security system, where files or devices are scanned by a single antivirus engine, presented major challenges.

USE CASE #1

Total File Security at Dounreay Nuclear Facility



USE CASE #2

Protecting the Supply Chain of Hitachi Energy

Customer: Hitachi Energy

Region: Zürich, Switzerland

Employees: 40,000+

Deployed Solutions: MetaDefender Core, MetaDefender Kiosk Mobile

Enhanced resilience against emerging threats to support compliance through last-mile supply chain security.

Challenges

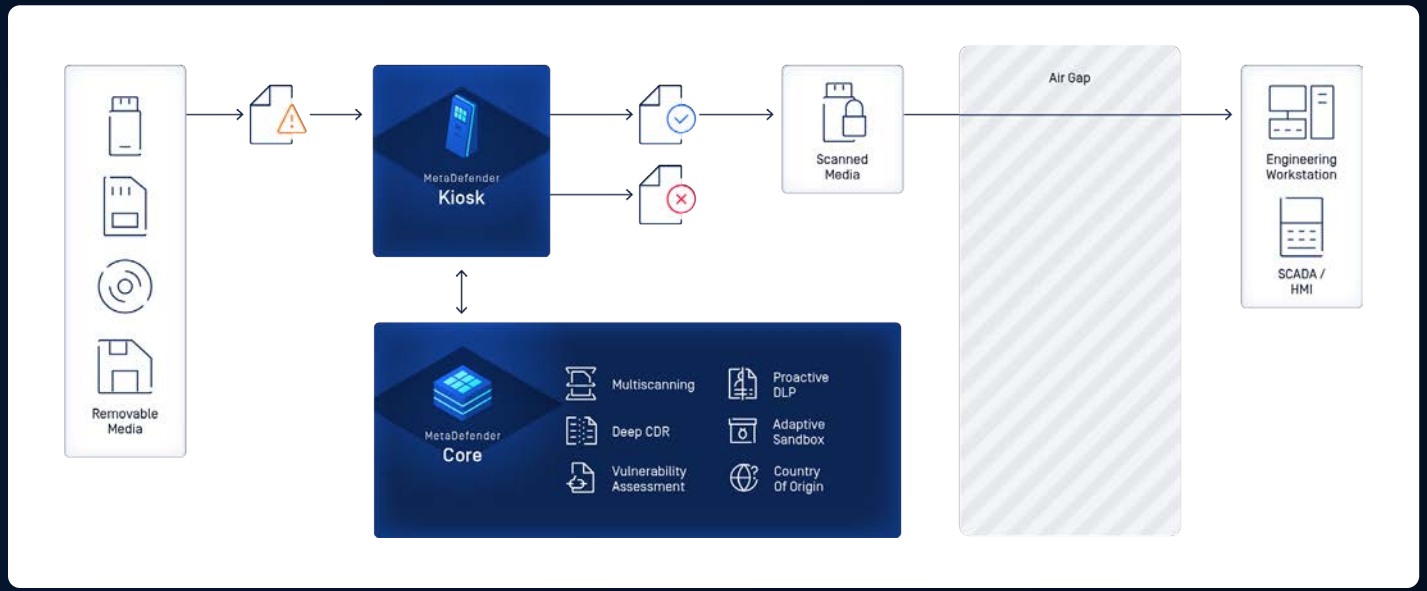
- Safeguarding supply chains against cyberthreats
- Ensuring security for a global organization with service engineers in 90 countries and multiple development centers
- Mitigating the risk of becoming a supply chain vulnerability.

Deployment Outcomes

- **Streamlined, Global Control:** Global Cybersecurity Management adopted MetaDefender Core to unify services and simplify processes across sites.
- **Remote Scanning:** MetaDefender Core was integrated into daily workflows so developers and service engineers could scan files on the go, even in remote sites with limited connectivity.
- **Last-Mile Supply Chain Security:** Engineers in low-connectivity areas used MetaDefender Kiosk Mobile appliances to access updates and scan media securely.

USE CASE #2

Protecting the Supply Chain of Hitachi Energy



USE CASE #3

Protecting Omaha Public Power District

Customer: Omaha Public Power District

Region: United States

Employees: 1,700+

Deployed Solutions: MetaDefender Kiosk

Standardized secure USB scanning across field sites using MetaDefender Kiosks, enabling policy-driven protection across field locations without slowing down operations.

Challenges

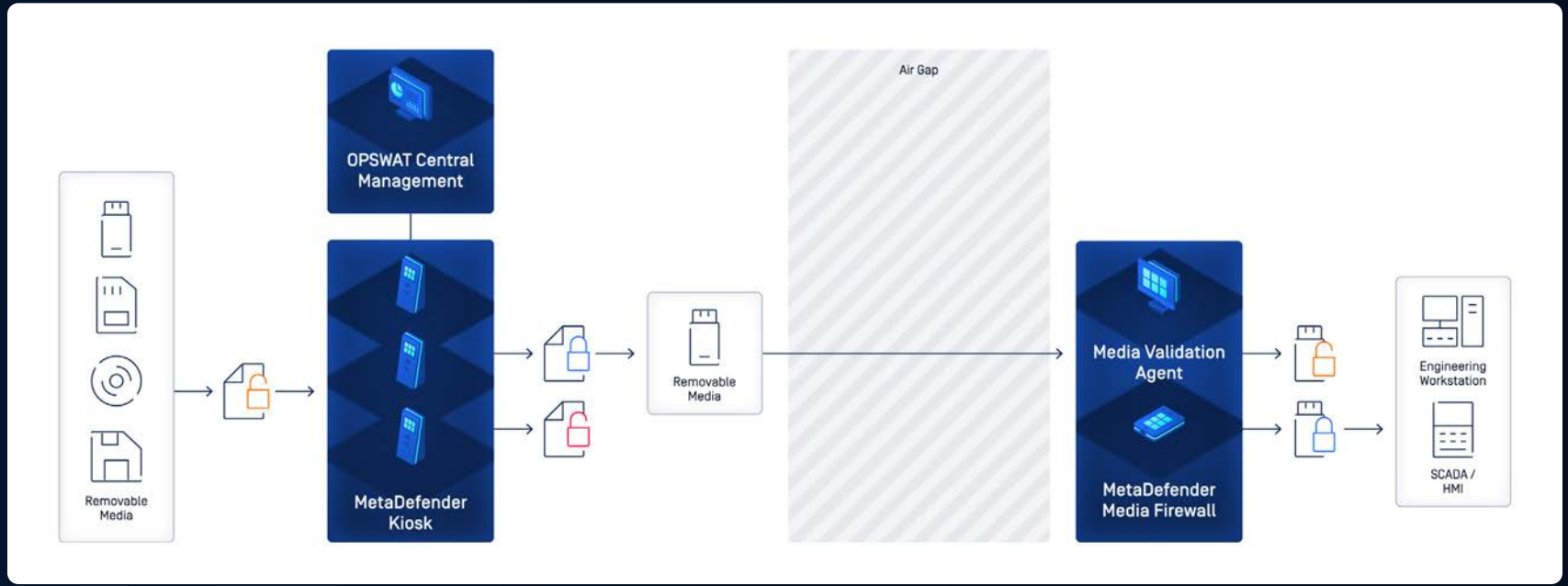
- Expanded attack surface with data transfers across multiple vital networks
- Increased operational complexity due to frequent ICS system upgrades
- Stringent industry regulations with compliance failure fines of up to $10M

Deployment Outcomes

- **Role-Based Control Policy Enforcement:** MetaDefender Kiosk has enabled site security admins to configure detailed security policies for different user groups across sites.
- **Complete File Management:** Security teams could prevent files based on types, size, or other data from entering critical networks.

USE CASE #3

Protecting Omaha Public Power District



USE CASE #4

Preventing Removable Media-Borne Threats for Global Energy Organization

Customer: Global Energy Organization

Region: United States (Offices Worldwide)

Employees: 3,000+

Deployed Solutions: MetaDefender Kiosk

The organization replaced an end-of-life security solution with MetaDefender Kiosk to secure removable media at scale, reducing risk across critical facilities.

Challenges

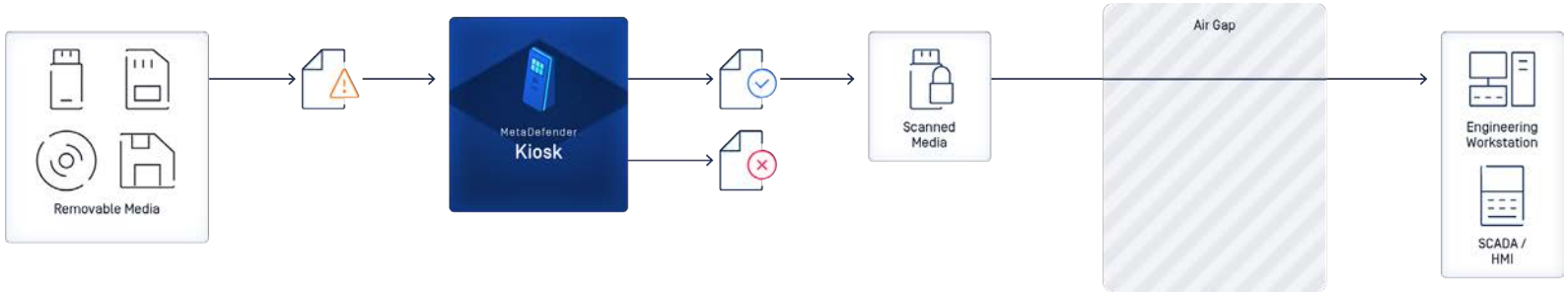
- Removable media scanning solution reached end-of-life
- The need to replace existing security measures
- Finding a suitable removable media solution and enhancing the overall security posture

Deployment Outcomes

- **Simplified Scanning Workflows:** Field teams securely controlled data flows in three simple steps: insert media, process files, and review results.
- **Seamless Integration Capabilities:** MetaDefender Kiosk was integrated smoothly into the existing OT system, enhancing overall security posture while ensuring minimal operational disruption.

USE CASE #4

Preventing Removable Media-Borne Threats for Global Energy Organization



USE CASE #5

Building a Perimeter of Defense Around Essential Energy Infrastructure

Customer: Fossil fuel energy producer and distributor

Region: United States

Employees: 3,000+

Deployed Solutions: MetaDefender Kiosk, MetaDefender Managed File Transfer

A US-based energy company secured data transfers and ensured cybersecurity compliance with OPSWAT's MetaDefender Kiosk and MetaDefender Managed File Transfer. Their proactive approach has fortified their operations against malware and zero-day attacks, making their facilities more resilient in the face of evolving cyberthreats.

Challenges

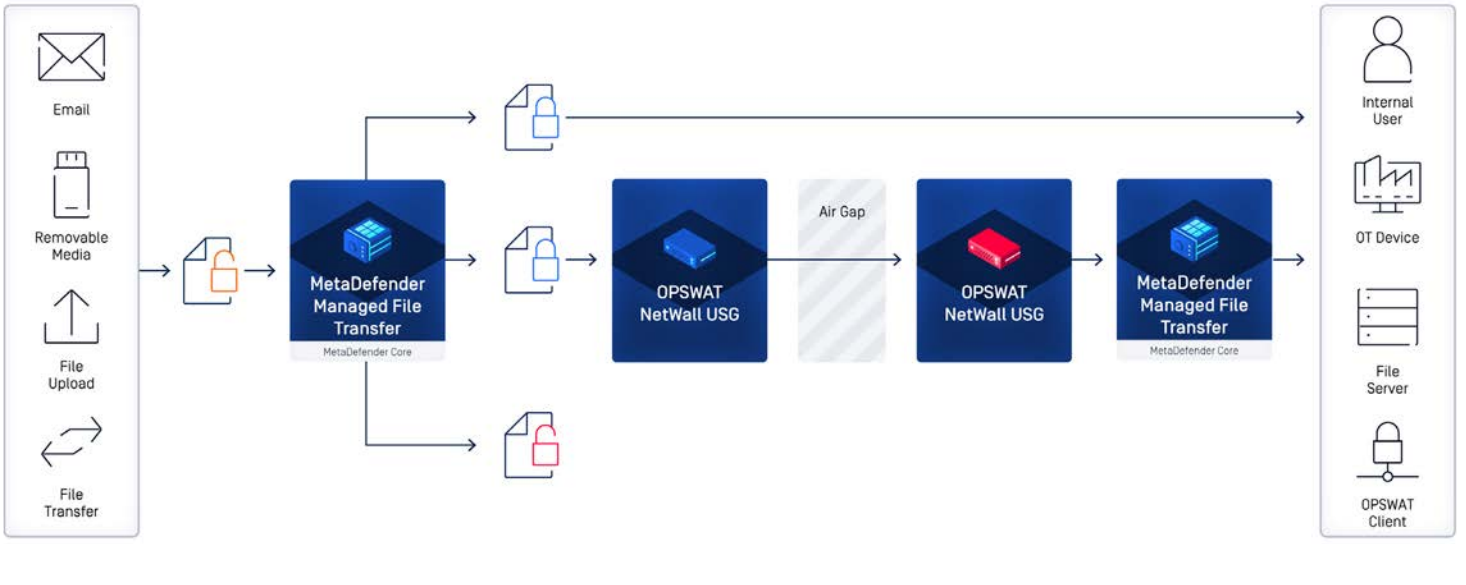
- Data is often transferred to air-gapped systems using employees' and contractors' portable devices.
- Frequent use of unsecured removable media, including CDs, USB flash drives, and external hard drives.

Deployment Outcomes

- **Digital Perimeter Control:** Securely manage file and device transfers, even across varying security levels, systems, and physical transfer points.
- **Enforced Secure Data Transfer Processes:** Enforcement of secure file transfer procedures, continuous malware scans, and the addition of digital signatures.
- **Breach Prevention:** Actively monitor and control sensitive data at every transfer point.

USE CASE #5

Building a Perimeter of Defense Around Essential Energy Infrastructure



USE CASE #6

Securely Transferring Real-Time OPC DA/AE Data from OT to IT

Customer: Liquid Natural Gas Producer

Region: Global

Deployed Solutions: Cross Domain Security

When a global liquid natural gas producer required secure, real-time OPC DA/AE data replication, MetaDefender Unidirectional Security Gateway ensured that the data transfers were successful, while not compromising their critical OT network.

Challenges

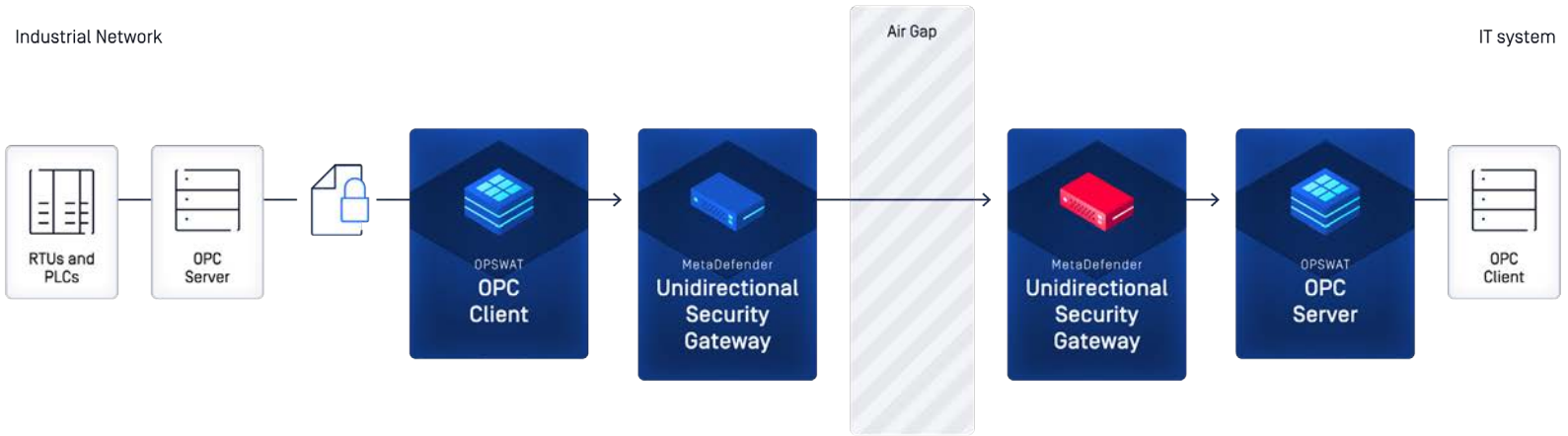
- Unverified data transfer between OT and IT networks exposed the infrastructure to cybersecurity risks.
- Operational disruptions from unauthorized access or malware in the OT network, leading to production losses and safety hazards.
- Data integrity risks caused by compromised data resulted in inaccurate information being used for critical decision-making and potential equipment failures.

Deployment Outcomes

- **One-Way Transfers Guaranteed:** The gateway ensures that data flows only in one direction - from the OT network to the IT network - while providing assured data delivery.
- **Uncompromising Non-Routable Protocol Break:** Created a secure boundary to ensure that the IT network cannot directly communicate with the OT network and prevent cyberthreats from propagating between networks.
- **Native OPC Support:** By natively supporting OPC DA/AE standards, the MetaDefender OPC Connector acted as an OPC Client on the OT network and an OPC Server on the IT network, facilitating seamless and secure data transfer.
- **Real-Time Data Transfer:** Enabled real-time transfer of OPC values and alarms/events to ensure the IT systems receive up-to-date information without delay.

USE CASE #6

Securely Transferring Real-Time OPC DA/AE Data from OT to IT



USE CASE #7

Securing Infrastructure for a Major Energy Provider in Vietnam

Customer: Energy Provider in Vietnam

Region: Vietnam (APAC)

Employees: 7,400+

Deployed Solutions: MetaDefender Kiosk, MetaDefender Core, MetaDefender Managed File Transfer.

The Vietnamese energy provider recognized that firewalls alone could not protect their network. They needed a solution that would securely transfer files between their IT and OT environments while ensuring files were malware-free.

Challenges

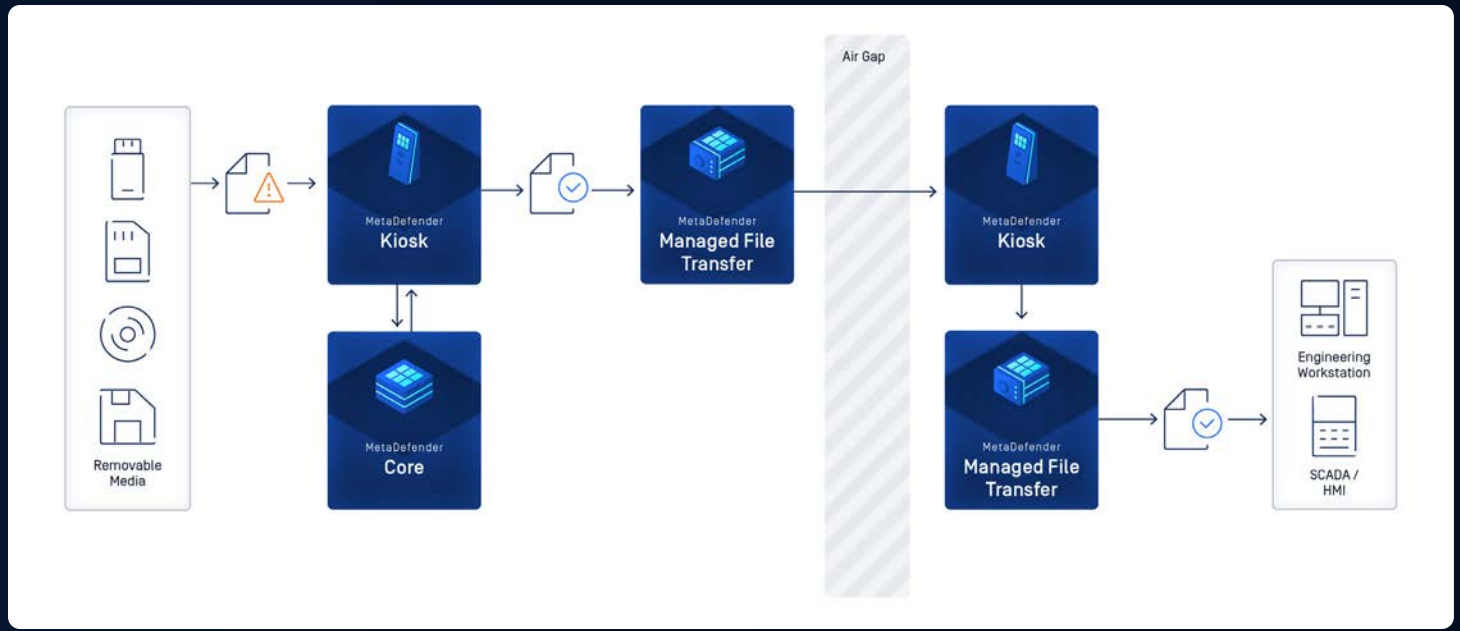
- Rising cyberattacks on Vietnam's critical infrastructure, including energy providers, led to a heightened need for secure file transfers between IT and OT environments.
- Firewalls alone were insufficient to protect against advanced threats and zero-day attacks.
- Removable media, such as USBs and laptops, introduced significant risks, necessitating a more robust approach to malware prevention.

Deployment Outcomes

- **Advanced File Transfer Protection:** Securely scanning, sanitizing, and transferring files between IT and OT environments using MetaScan Multiscanning and Deep CDR technologies.
- **Automated File Transfers:** Reduced manual errors and increased efficiency across their network.
- **Adaptive Threat Analysis: T**o protect against zero-day attacks and advanced persistent threats.

USE CASE #7

Securing Infrastructure for a Major Energy Provider in Vietnam



USE CASE #8

Hardware-Enforced Protection to Secure Data Flow in the Petrochemical Industry

Customer: Fortune 500 Petrochemical Company

Region: North America

Employees: Thousands of Employees

Deployed Solutions: OPSWAT MetaDefender Optical Diode (Fend)

The company relied on firewalls to control outbound data flow from its OT network to its enterprise IT systems. When the firewall manufacturer announced EOL (end-of-life) support by 2025, the company had to make a change and saw the opportunity to both enhance and simplify their industrial cybersecurity protections.

Challenges

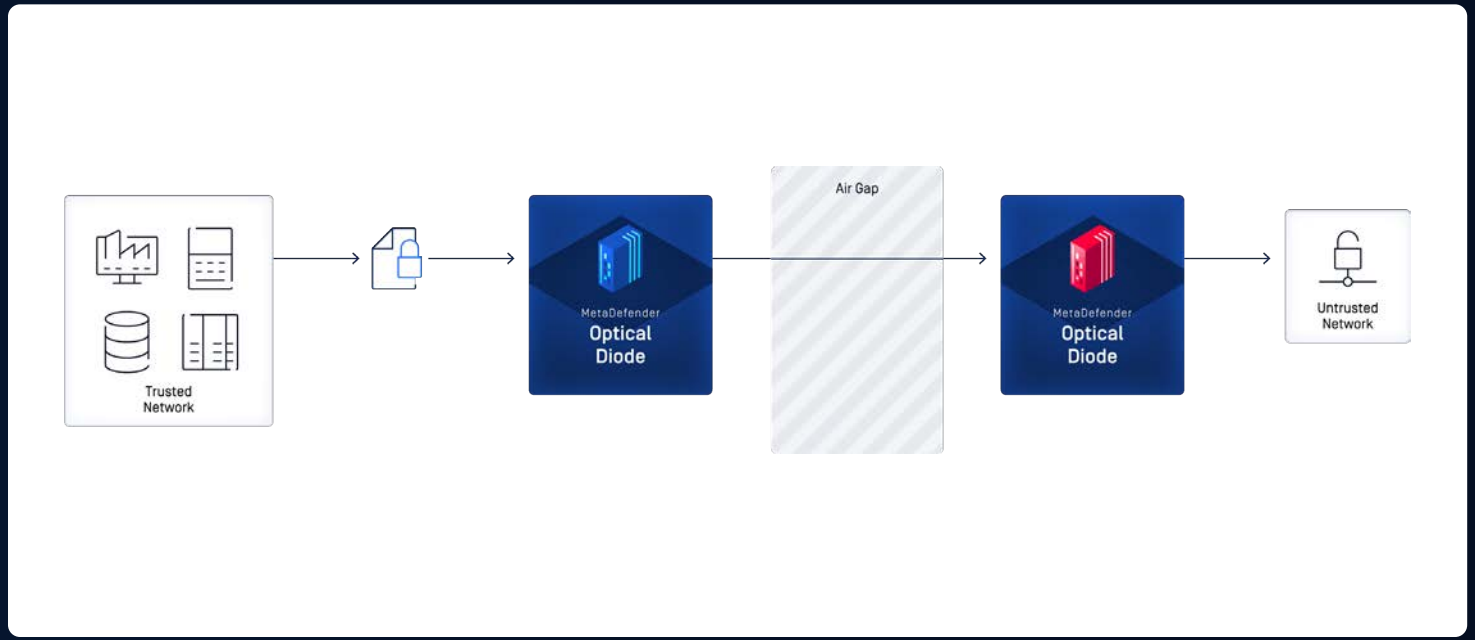
- Without a replacement, refineries risked unauthorized access to critical OT data.
- Lack of secure data transfers slowed down decision-making, affecting production and compliance reporting.
- Firewalls require frequent patching to plug vulnerabilities.
- Downtime caused by an insecure or ineffective replacement solution could result in millions of dollars in lost revenue.

Deployment Outcomes

- **Seamless Integration:** The Fend XE15 diodes were designed to directly replace firewalls with minimal reconfiguration.
- **Zero Maintenance Security:** By eliminating software-based protection, the diodes removed the need for constant patching.
- **Scalability:** The diodes were compact, rugged, and cost-effective enough to be deployed across all refinery locations.

USE CASE #8

Hardware-Enforced Protection to Secure Data Flow in the Petrochemical Industry



USE CASE #9

Fortifying Mining Operations to Drive Safety and Sustainability

Customer:
Global Mining Leader Operates Across Multiple Continents

Region: Global

Employees: 10,000+ Employees Worldwide

Deployed Solutions: MetaDefender Kiosk

For the mining company, secure USB management strengthened mining operations, ensured safety, compliance, and protection from cyber threats.

Challenges

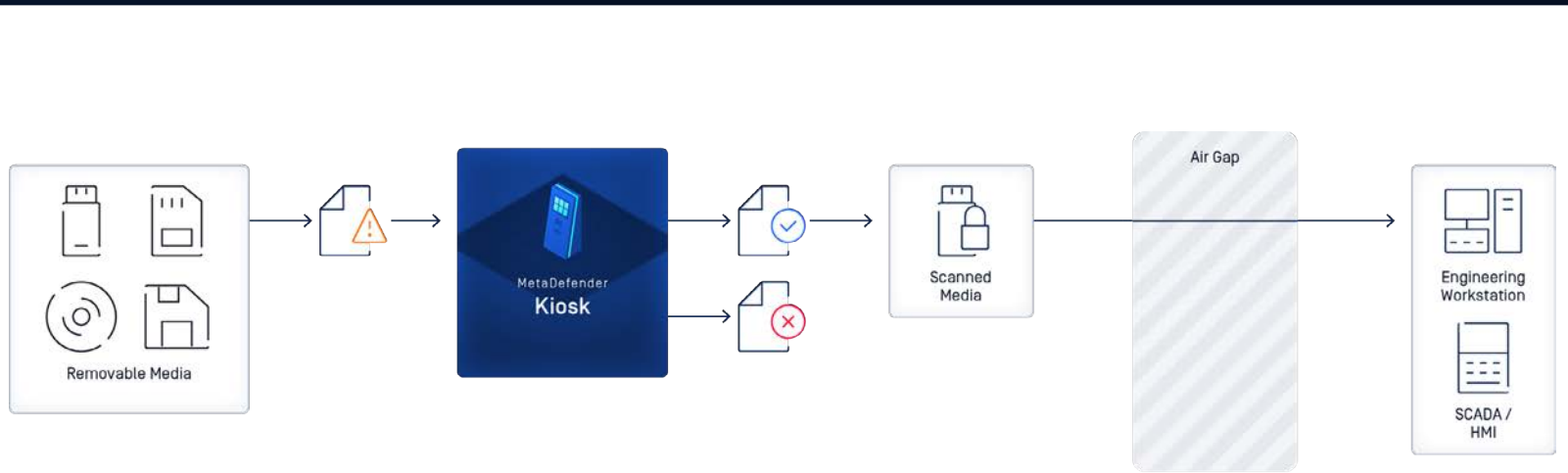
- As part of their modernization efforts, the company faced critical challenges in securing its OT infrastructure.
- Difficulties managing USB devices that are used for critical updates and data transfers.

Deployment Outcomes

- **Sustainability Gains:** With secure smart drills and precision blasting systems, the company continued to reduce greenhouse gas emissions and energy consumption.
- **Streamlined Logistics:** A secure and efficient digital supply chain ensured materials and products moved seamlessly, minimizing delays and enhancing collaboration among stakeholders.
- **Operational Efficiency:** Enhanced operational efficiency, reduced downtime, and enabled better decision-making for asset management and vulnerability patches.

USE CASE #9

Fortifying Mining Operations to Drive Safety and Sustainability



USE CASE #10

Enhancing Renewable Energy Supply Chain Security

Customer: Leading Renewable Energy Producer

Region: Europe and North America

Employees: 5,000+ Employees

Deployed Solutions: MetaDefender Drive

Due to the nature of their business, third-party vendors frequently operate their laptops within air-gapped zones. To ensure the security of these transient devices, the renewable energy producer urgently needed an effective and quick-to-deploy solution to ensure the security of external contractor and vendor laptops.

Challenges

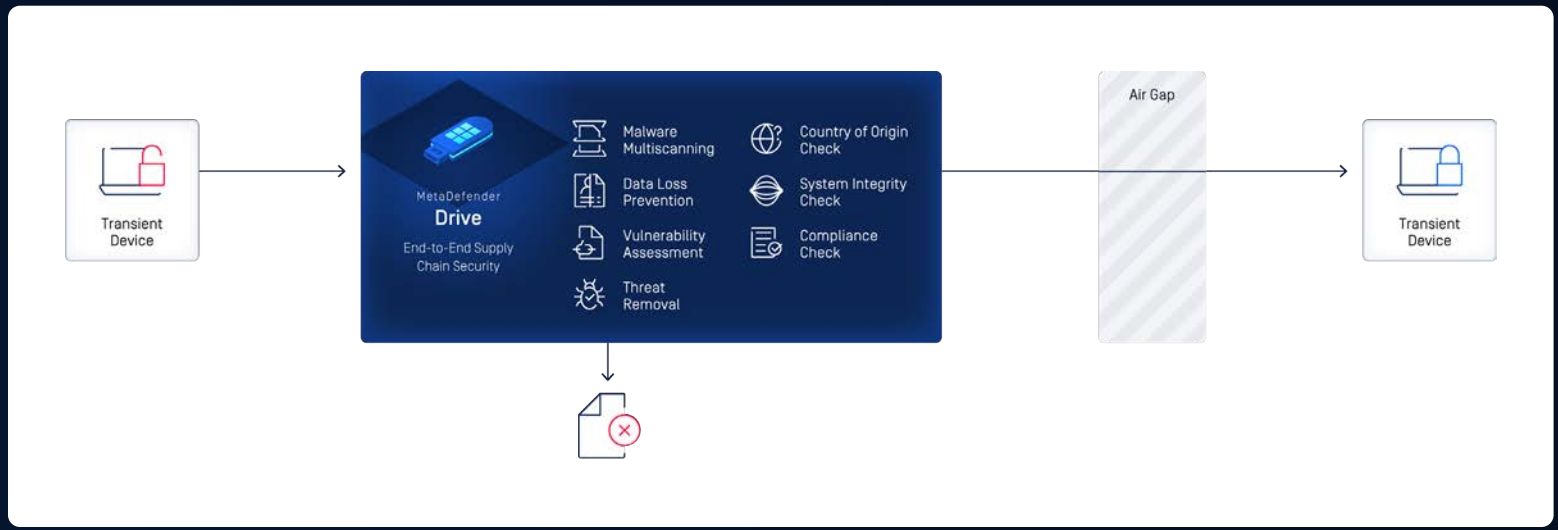
- Relying on a single-engine active scanning solution to secure third-party vendor laptops.
- Limited detection of new and unknown threats.
- Low performance when scanning large files.
- Lack of compatibility with legacy devices.
- A system downtime incident, due to a frozen vendor laptop during a scan.

Deployment Outcomes

- **Streamlined Scanning Process:** With multiple bare-metal scanning routines.
- **Optimized Scanning Speed:** With a scanning rate of 111 files per second, outpacing the traditional solution's 2 files per second rate.
- **Enhanced Integrity Checks:** With the ability to detect boot sector infections.
- **Sensitive Data Protection:** Using Proactive DLP technology.

USE CASE #10

Enhancing Renewable Energy Supply Chain Security



USE CASE #11

Securing Vietnam's Critical Power Infrastructure

Customer:
Major Power Provider Operating a Critical Coal-fired Power Plant

Region: Vietnam (APAC)

Employees: 2,000

Deployed Solutions:
MetaDefender Netwall Unidirectional Security Gateway

A leading Vietnamese thermal power plant faced increasing cybersecurity threats. They needed to secure their infrastructure with advanced cybersecurity solutions tailored to their needs.

Challenges

- Malware infiltration and unauthorized SCADA access attempts.
- The need for a robust solution to secure IT-OT cross-domain data flow.
- Comply with stringent energy sector regulations.

Deployment Outcomes

- **Zero Malware:** While transferring data from IT to OT networks.
- **Improved Resilience:** Against DDoS and advanced attacks.
- **Simplified Regulatory Compliance:** With sector standards (e.g., IEC 62443).
- **Enhanced Operational Efficiency:** Through reduced IT workload.
- **Strengthened Reputation:** As a secure, reliable energy provider.

USE CASE #11

Securing Vietnam's Critical Power Infrastructure

Security Gateway Architecture

Secure Data Replication Mechanism

Flexible Integration

User-Friendly Management Interface

Trusted Support

USE CASE #12

Enhancing Intrusion Detection and Prevention in Critical Energy Infrastructure

Customer: Leading Global Energy Company

Region: Global Operations with Multiple Sites in North America, Europe, and The Middle East

Employees: Around 15,000 Employees Globally

Deployed Solutions:
MetaDefender OT Security, MetaDefender Industrial Firewall

The global energy company faced a critical challenge in securing its vast and geographically dispersed infrastructure. Their diverse portfolio includes conventional oil and gas operations, condensate, natural gas liquids, and natural gas.

Challenges

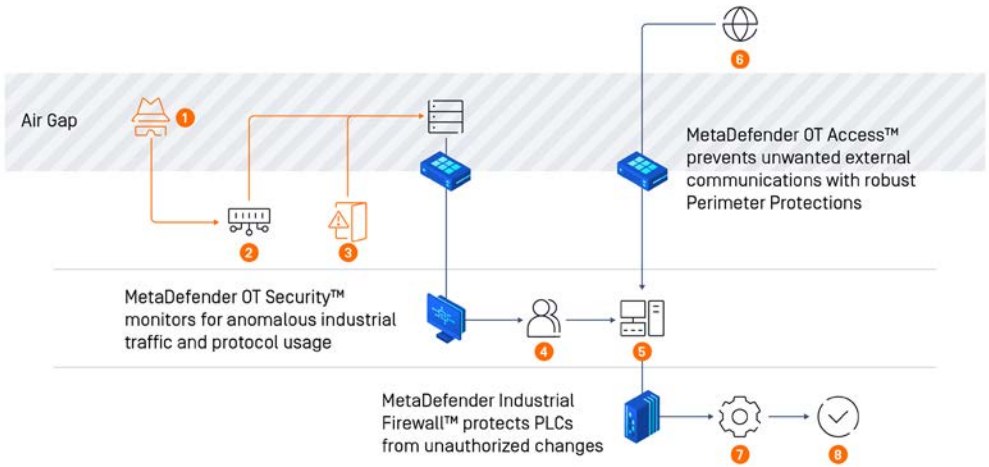
- Lack of comprehensive oversight of OT assets and CPS spread across various locations.
- Inability to monitor and control processes between critical OT devices, leading to potential security blind spots.
- Lack of real-time insight into OT network activity and vulnerabilities, hindering operational efficiency.
- Unmonitored or unpatched devices within the OT environment posed significant cybersecurity threats.
- Risk of fines and penalties due to non-adherence to a variety of regulatory requirements.

Deployment Outcomes

- **Comprehensive Visibility:** Gained visibility at scale into all OT assets across multiple locations.
- **Proactive Threat Detection:** Real-time monitoring and alerts enabled faster identification of suspicious activities.
- **Enhanced Security:** Leveraged AI-powered learning for enhanced security posture.
- **Operational Efficiency:** Enhanced operational efficiency, reduced downtime, and enabled better decision-making for asset management and vulnerability patches.
- **Improved Regulatory Compliance:** Helped with full NERC CIP compliance, reducing the risk of fines and penalties from auditors.

USE CASE #12

Enhancing Intrusion Detection and Prevention in Critical Energy Infrastructure



USE CASE #13

Securing Operations for a Vietnamese Power Corporation

Customer: Key Entity in Vietnam's National Power System

Region: Vietnam (APAC)

Employees: Thousands of Employees in 27 Provinces

Deployed Solutions: MetaDefender Kiosk Tower

With the high risks of malware threats and data leaks due to uncontrolled device usage among field engineers, our client needed to effectively protect their IT and OT networks.

Challenges

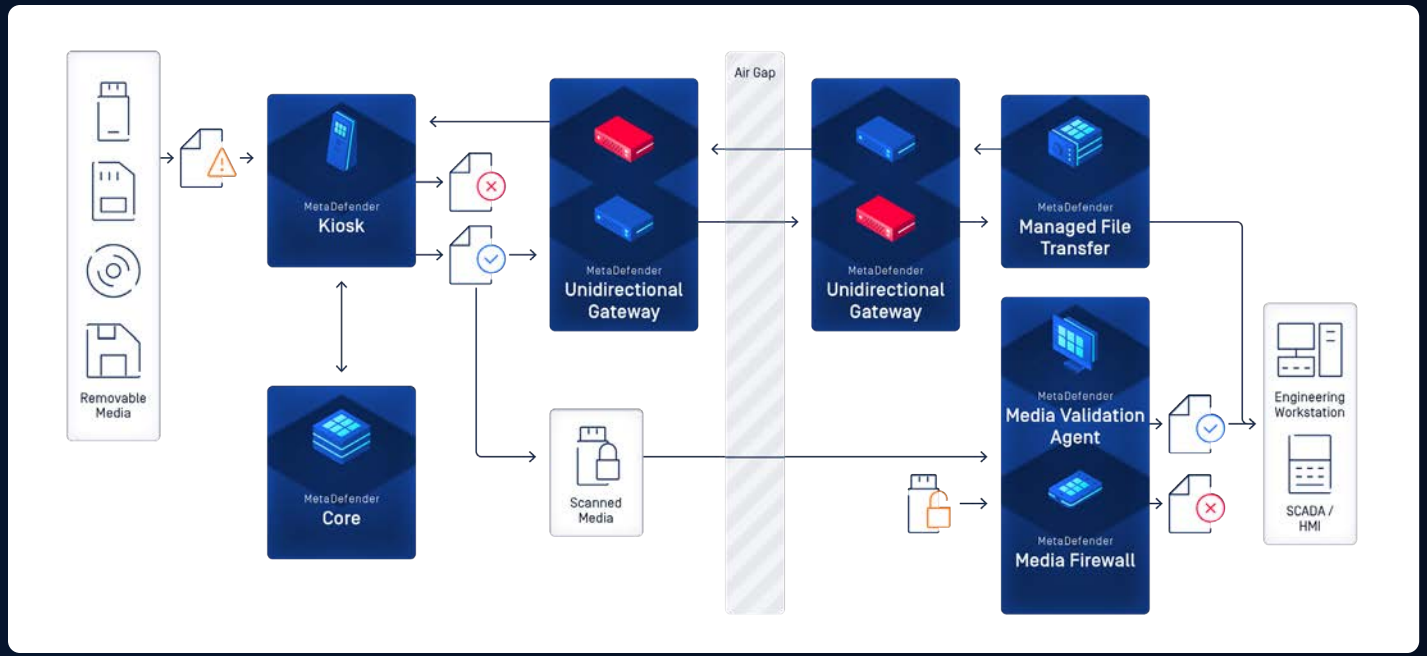
- Cybersecurity risks from peripheral devices like USBs and external hard drives used by field engineers.
- Lack of a secure system for device control, leading to unregulated devices potentially introducing malware into SCADA and control systems.
- Increased exposure to threats due to unsupervised devices, heightening the risk to critical infrastructure.

Deployment Outcomes

- **Multi-Engine Virus Scanning:** Equipped with multiple antivirus engines, Kiosk Tower provided the deep, reliable malware detection needed for devices entering sensitive environments.
- **Deep CDR:** This advanced file sanitization technology neutralizes threats by removing harmful elements such as macros, hidden scripts, and malicious JavaScript from files.
- **Comprehensive Device Authentication:** Beyond scanning, Kiosk Tower conducts thorough device checks, detecting fake devices and preventing data theft.
- **Quick, User-Friendly Processing:** The kiosk operates at high speed, allowing efficient device inspection without disrupting workflow.
- **24/7 Support and Compliance:** In addition to meeting local compliance mandates, OPSWAT's dedicated support team provided valuable implementation guidance and troubleshooting.

USE CASE #13

Securing Operations for a Vietnamese Power Corporation



06

Securing Energy Infrastructure with Future-Proof Technologies

From remote facilities and aging nuclear control rooms to renewable energy fields and critical power grids, every layer of critical infrastructure faces constant cyberthreats on different levels. Today's cyberthreats demand a proactive, defense-in-depth approach to OT cybersecurity. By investing in modern, purpose-built solutions, organizations can reduce their risk profile, enhance safety, and ensure operational continuity.

OPSWAT's end-to-end platform simplifies the complexities of OT cybersecurity challenges with easy-to-deploy, integrate, configure, and manage solutions and technologies. The MetaDefender platform has a proven track record of thousands of deployments that have solved major issues and empowered teams to act with confidence, boost regulatory compliance, and build operational trust.

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