OPSWAT.

Protecting the World's Critical Infrastructure

Cybersecurity Solutions Built for Any Critical Network

OPSWAT.

Government
Communications
Transportation
Energy
Dams
Nuclear
Chemical
Agriculture
Emergency and Public Safety
Commercial
Manufacturing
Financial Services
Healthcare and Public Health
Defense Industrial Base
Water and Wastewater Treatment

Trusted Globally to Defend What's Critical

OPSWAT solutions are trusted by more than 1,500 organizations, governments, and institutions around the world to protect their critical networks. More than 100 enterprise partners trust OPSWAT technologies to enhance their cybersecurity capabilities. This positions OPSWAT as an industry leader across the 16 defined critical infrastructure sectors.

Simplifying Complex Cybersecurity Challenges

After two decades spent protecting the most critical networks around the world, we've learned that the primary cybersecurity challenges faced by organizations across the spectrum can be broken up into three parts: Network Complexity, Technology Gaps, and Training Gaps.

We simplify how these challenges are solved with a one-to-one approach that addresses each challenge directly. OPSWAT protects the world's critical infrastructure with our patented, industry-trusted technology and battle-tested products, unrivaled service and support, and award-winning OPSWAT Academy.

OPSWAT.

Solving Critical Cybersecurity Challenges

OPSWAT protects the world's critical infrastructure with an end-to-end cybersecurity platform, providing multiple lines of defense across all levels of IT and OT systems.

OPSWAT's growing portfolio of products and solutions solves a wide spectrum of specific customer challenges across critical networks.

opswat.com/solutions

Application Security

File Upload Security
Malware Protection for Storage

Supply Chain Security

Software Security
Hardware Security
Network Asset Inventory

Network Infrastructure

Removable Media Security
Transient Cyber Asset
Asset Supply Chain Security
Industrial Firewall
Cross Domain Solutions

Endpoint Management

Patch Management
Compliance Enforcement
Advanced Endpoint Protection
Vulnerability Management
Remote Access Security

Security Operations

Threat Intelligence
Malware Analysis

Cloud Security

Application Access Control
Threat Prevention
Infrastructure Protection

Email Security

Phishing Protection
Zero-Day Malware Detection
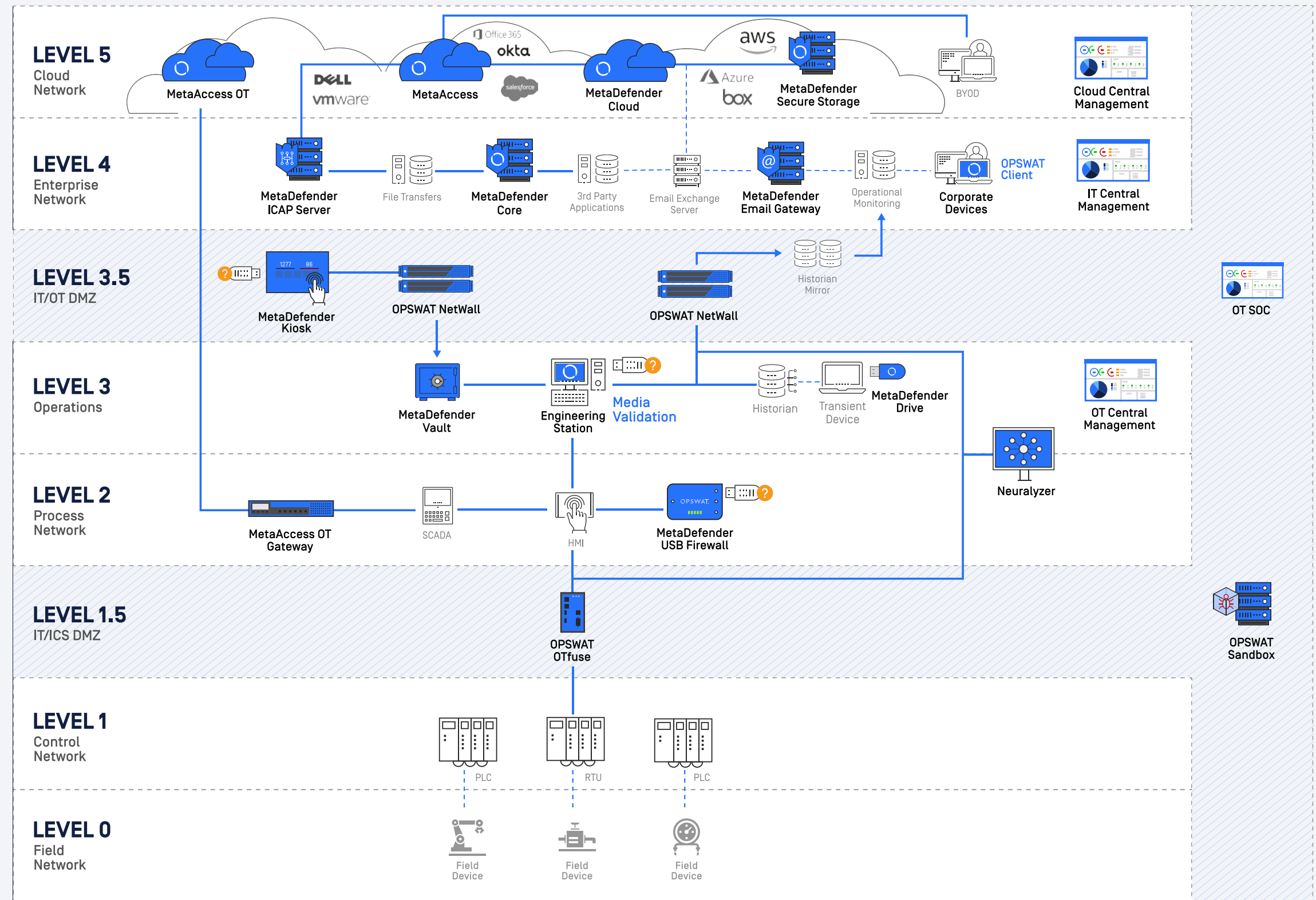Unknown Exploit Prevention
Data Leakage Protection

OEM & SDK

Endpoint Security SDK
File Security
Device Security
Threat Intelligence
Malware Analysis
Free Tools

OPSWAT.

End-to-End Cybersecurity Platform

OPSWAT has spent the last 20 years evolving our end-to-end cybersecurity platform to give public and private sector organizations the critical advantage needed to protect the most complex networks. Built on our "Trust no file. Trust no device.™" philosophy and integrated by design, we're solving our customers' challenges as their singular point of cybersecurity, creating critical lines of defense across every level of their infrastructure.

LEVEL 5
Cloud Network

MetaAccess OT
MetaAccess
MetaDefender Cloud
MetaDefender Secure Storage
BYOD
Cloud Central Management

DELL
vmware
Office 365
okta
salesforce
aws
Azure
box

LEVEL 4
Enterprise Network

MetaDefender ICAP Server
File Transfers
MetaDefender Core
3rd Party Applications
Email Exchange Server
MetaDefender Email Gateway
Operational Monitoring
Corporate Devices
OPSWAT Client
IT Central Management

LEVEL 3.5
IT/OT DMZ

MetaDefender Kiosk
OPSWAT NetWall
OPSWAT NetWall
Historian Mirror
OT SOC

LEVEL 3
Operations

MetaDefender Vault
Engineering Station
Media Validation
Historian
Transient Device
MetaDefender Drive
OT Central Management

LEVEL 2
Process Network

MetaAccess OT Gateway
SCADA
HMI
MetaDefender USB Firewall
Neuralyzer

LEVEL 1.5
IT/ICS DMZ

OPSWAT OTfuse
OPSWAT Sandbox

LEVEL 1
Control Network

PLC
RTU
PLC

LEVEL 0
Field Network

Field Device
Field Device
Field Device

Trust no file.
Trust no device.

Our Cybersecurity Philosophy

We believe that all files and devices are malicious until they are confirmed otherwise. Our philosophy is a cybersecurity approach that emphasizes the importance of assuming all files and devices as potential threats, regardless of their source or reputation. This philosophy helps to proactively safeguard digital assets and reduce the risk of cyberattacks, and is rooted in four key principles.

1.

Assume all files are malicious.

2.

Assume all devices are compromised.

3.

Embrace a zero-trust approach.

4.

Adopt a defense-in-depth strategy.

Deep Content Disarm & Reconstruction (CDR)

Deep Content Disarm and Reconstruction (Deep CDR) technology protects from known and unknown file-borne threats by sanitizing and reconstructing files. Any possible embedded threats are neutralized while maintaining full usability with safe content.
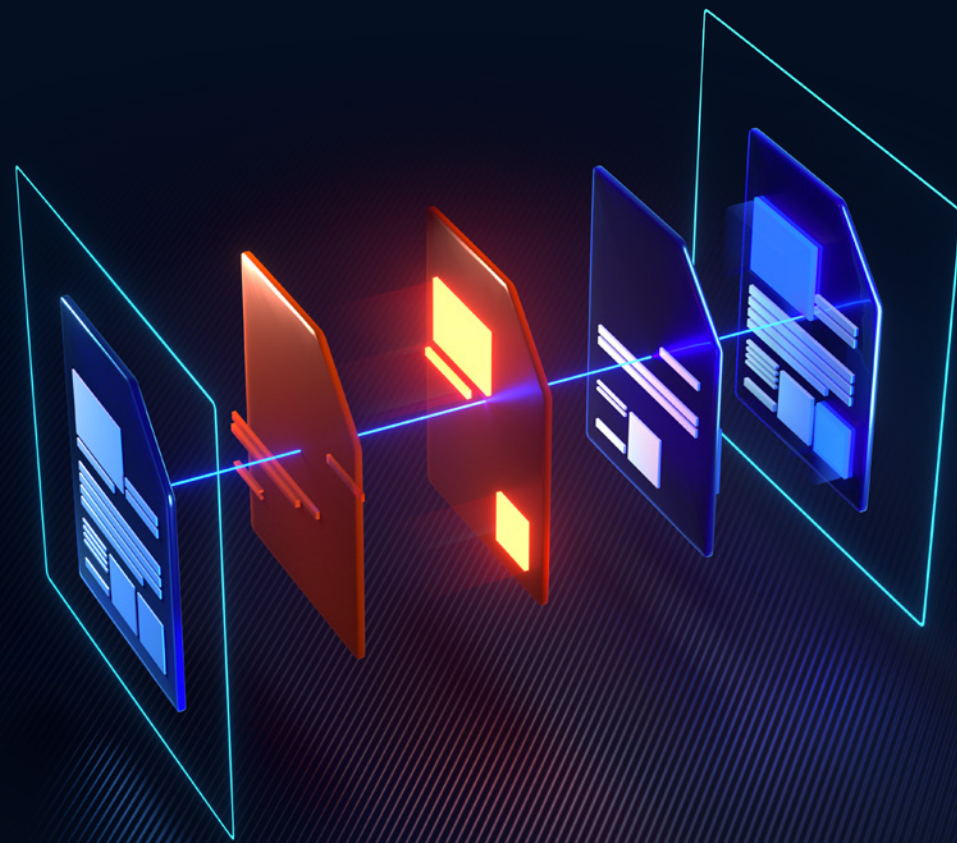
Industry-Leading Patented Technology

Our comprehensive platform is underpinned by patented foundational technologies that are trusted worldwide to secure critical networks. Purpose-built to protect critical environments, these technologies provide industry-leading advanced prevention against known and unknown threats, zero-day attacks, traditional malware, AI malware, and more.

Multiscanning

Multiscanning technology 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 threats and provides the earliest protection against malware outbreaks.

Adaware · AhnLab · Avira · Bitdefender · ClamAV®
COMODO · CROWDSTRIKE · F5 · EMSISOFT · eset
IKARUS security software · INCA · K7 SECURITY · LIONIC Security Solution Provider · McAfee
Microsoft · nG · Quick Heal · RocketCyber · SOPHOS
SYSTWEAK · TG Soft · WEBROOT · X VIRUS
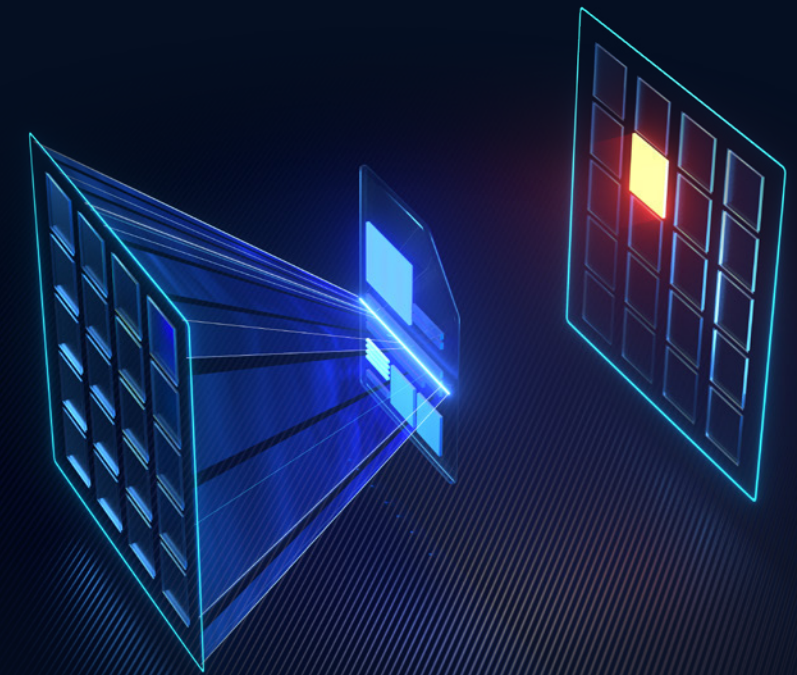
Proactive Data Loss Prevention (DLP)

Proactive DLP helps prevent sensitive and confidential information in files from leaving or entering systems by content-checking files before they are transferred. This helps enterprises meet regulatory requirements like HIPAA, PCI-DSS, and GDPR.
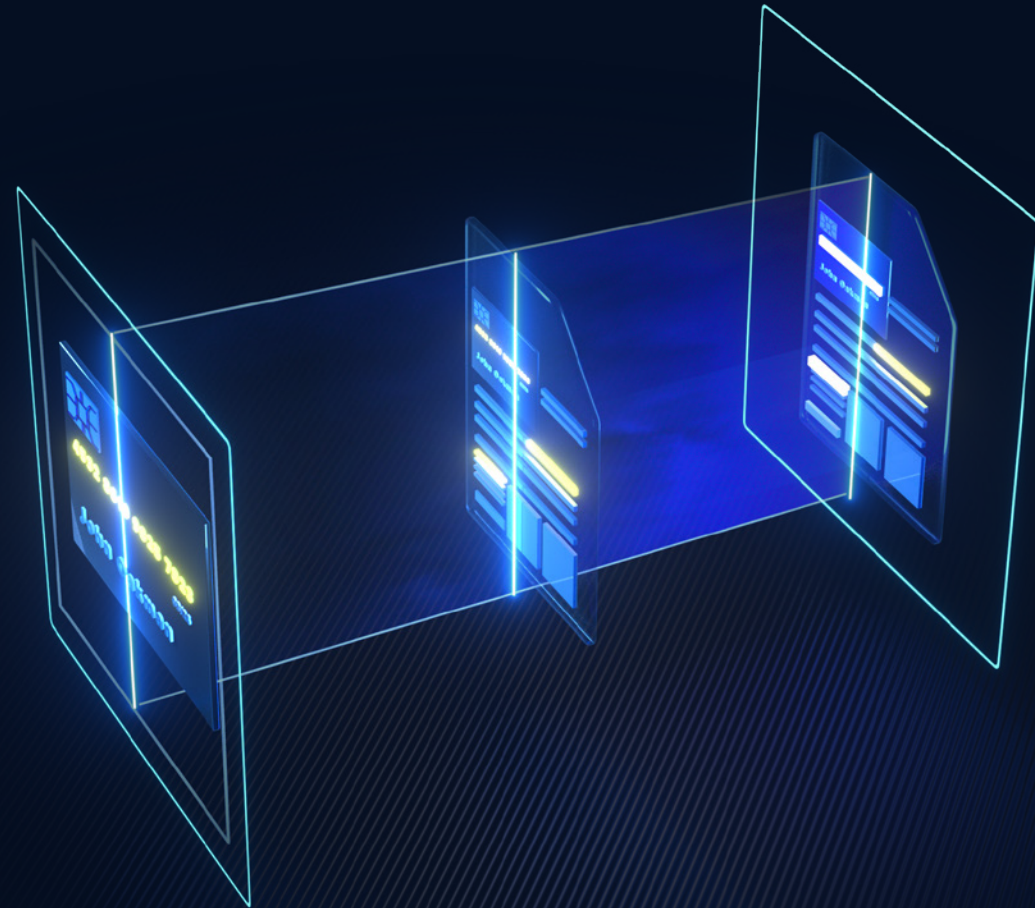
Next-Generation Sandbox

Next-Gen Sandbox offers a complete set of malware analysis technologies including, threat agnostic analysis of files and URLs, emulation of all targeted applications (Microsoft Office, PDF readers, and more), a focus on Indicator-of-Compromise (IOC) extraction, and Rapid Dynamic Analysis engine for targeted attack detection.

Threat Intelligence

Our Threat Intelligence Platform analyzes millions of data entries from thousands of in-the-wild devices across the world and develops a cloud-based database with billions of data points for binary reputation, vulnerable hashes, malware outbreak samples, and many other security intelligence data.

File-Based Vulnerability Assessment

File-Based Vulnerability Assessment technology detects application and file-based vulnerabilities before they are installed. We use our patented technology to correlate 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.

Country of Origin Detection

Many organizations are experiencing heightened requirements to examine the supply chain security of software running on their systems, particularly ones from foreign adversaries. OPSWAT automates binary scans on a target system and determine in which country the publisher resides.

OPSWAT.

Industry-Trusted Portfolio

From IT to OT and everything in between, OPSWAT's products and solutions can be integrated or deployed across every attack surface, providing unrivaled and simple to use, end-to-end cybersecurity at every level—from the cloud to the plant floor.
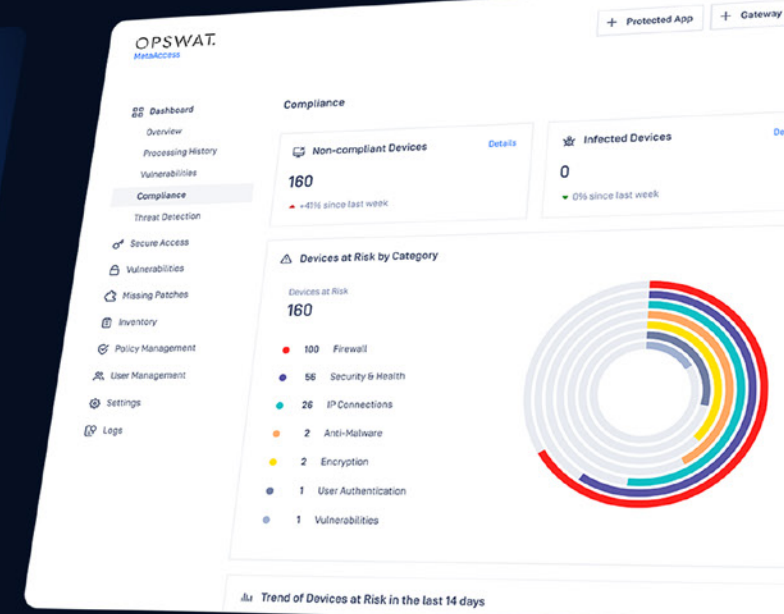
opswat.com/products

Software Solutions

- MetaDefender Core
- MetaDefender ICAP Server
- MetaDefender Vault
- MetaDefender Secure Storage
- MetaDefender Email Gateway
- MetaDefender Cloud Gateway
- OPSWAT Filescan

- MetaAccess
- MetaAccess NAC
- MetaAccess SDP
- OPSWAT Endpoint SDK
- OPSWAT Central Management
- OPSWAT Client

Hardware Solutions

- MetaAccess OT
- MetaDefender Drive
- MetaDefender Kiosk
- MetaDefender USB Firewall

- OPSWAT NetWall
- OPSWAT Neuralyzer
- OPSWAT OTfuse

Critical Support

OPSWAT's support team provides comprehensive, scalable coverage via phone, chat, or cases that you log with us through our portal. To best meet your support needs, we offer a variety of plans to choose from:

Silver
7am to 7pm business day portal and chat support and four-hour response time for blocker severity issues.

Gold
24-hour business day portal, phone, and chat support and one-hour response time for blocker severity issues.

Platinum
24x7x365 coverage via phone and portal, 24-hour business day chat support, one-hour response time for blocker severity issues, and customer success management.

U.S. In-Country Platinum
Everything included in the Platinum tier with the guarantee your support specialist is responding from the US.

Diamond
24x7x365 coverage via phone and portal, 24-hour business day chat support, one-hour response time for blocker severity issues, customer success management, and complete Managed Services support.

opswat.com/support

Expert Services

Our team of subject matter experts bring years of experience in cybersecurity and risk mitigation to make sure you get the most out of our solutions.

Managed Services
Trust OPSWAT professionals to get the most out of your cybersecurity solutions with expertly managed product support, security services, and incident response.

Implementation Services
No one knows OPSWAT solutions better than us. Get started the right way with a customized and validated implementation of your cybersecurity solution.

OT SOC
A 24/7 centralized security operations center powered by industry-trusted expertise.

Cybersecurity Assessments
Avoid gaps in your posture and compliance with a comprehensive and actionable cybersecurity analysis.

opswat.com/services

OPSWAT
academy™

All 16 critical infrastructure sectors are increasingly at high risk of cyberattacks, yet tens of thousands of mission-critical jobs remain vacant.

The award-winning OPSWAT Academy was developed to address the CIP cybersecurity skills shortage through courses that promote the best practices and practical approaches successfully implemented in the most secure critical infrastructure environments.

<div>opswatacademy.com</div>

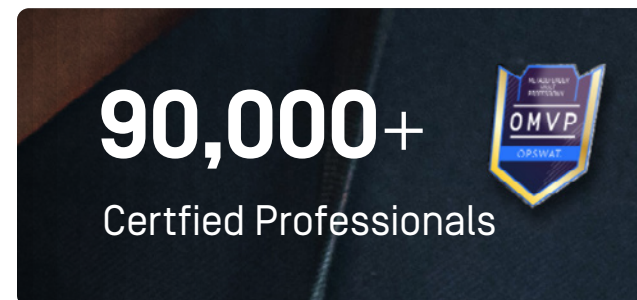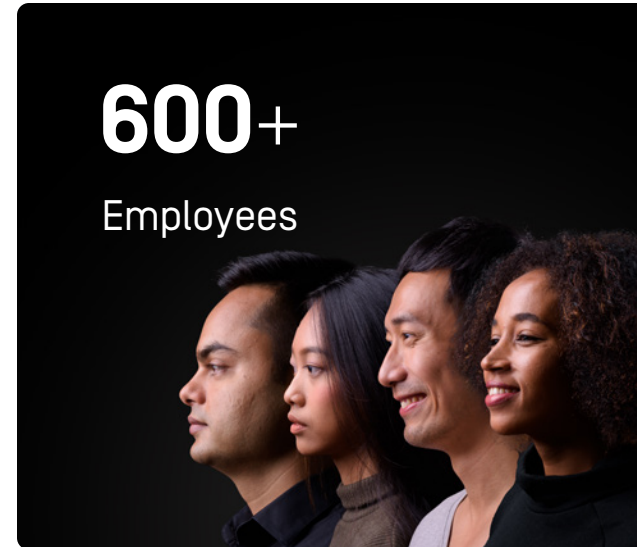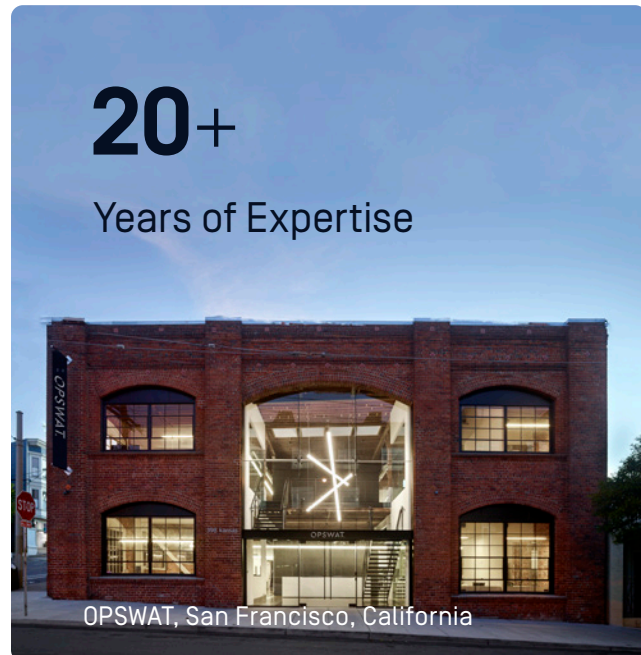# CIP Cybersecurity Certifications

Associate Certifications

File Security Associate

Secure Storage Associate

Cross-Domain Security Associate

Web Traffic Protection Associate

Email Security Associate

Legacy Systems Associate

Network Security Associate

Endpoint Compliance Associate

Professional Certifications

MetaDefender Core Professional

MetaDefender Kiosk Professional

MetaDefender Drive Professional

MetaDefender Vault Professional

MetaDefender ICAP Professional

MetaDefender Email Gateway Security Professional

MetaAccess Endpoint Security Professional

MetaAccess NAC Professional

OPSWAT.

Twenty Years of Innovation

OPSWAT's cybersecurity platform provides governments, enterprises, and small and mid-sized businesses in more than 60 countries with comprehensive end-to-end protection, purpose-built for the most complex and critical IT and OT networks.

Benny Czarny
CEO, Founder, and
Chairman of the Board

"The future of OPSWAT is brighter than ever as we continue to innovate and protect the world against an evolving cyberthreat landscape. With our unwavering dedication and industry-leading solutions, we are laser-focused on ensuring a safer and more resilient future for all.

60+
Countires

1500+
Customers

20+
Years of Expertise

OPSWAT, San Francisco, California

600+
Employees

100+ million
End Points Protected

App Remove
5 out of

Antiphising
10 out of 1

100

Anti-malwa
30 out of 3

90,000+
Certfied Professionals

OMVP

Accolades

2023 Cybersecurity Excellence Awards
Gold – ICS/SCADA Security
Gold – Web Application Security
Gold – CS Solution

2023 Globee Awards
Bronze – Cybersecurity

2022 CyberSecurity Breakthrough Awards
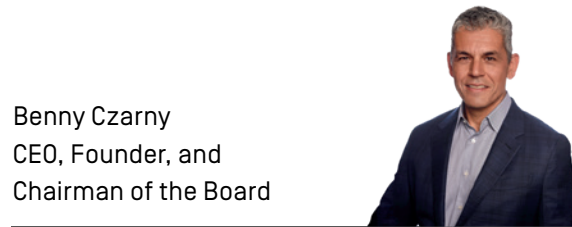Prof Certification Program of the Year

2022 CIOCoverage
Top 10 Leading VMware Partner

2023 The Channel Co.
CRN Partner Program Guide

2022 Cybersecurity Excellence Awards
Gold – Cybersecurity Education Provider
Gold – Content Disarm & Reconstruction
Gold – Critical Infrastructure Security

Put OPSWAT on the front lines of your cybersecurity strategy.

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years 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 1,500 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.