OPSWAT.

OPSWAT Inc.
398 Kansas Street
San Francisco, CA 94103
1.415.590.7300

www.opswat.com

OPSWAT.

Protecting organizations from content and device based threats

OPSWAT is trusted by more than 1,000 organizations worldwide from government, military, and intelligence to banking, healthcare, and utilities, including more than 90% of nuclear power plants in North America.

For more information, please contact **sales@opswat.com**

OPSWAT.

Trust no file. Trust no device.

San Francisco (HQ)
398 Kansas Street
San Francisco, CA 94103
+1.415.590.7300

United Kingdom
20 Market Place
Kingston upon Thames
Surrey, KT1 1JP England
+44.1483.361021

Japan
Level 27, Tokyo Sankei Building
1-7-2 Otemachi Chiyoda-ku
Tokyo 100-0004 Japan
+81.3.3242.6386

Hungary
H-8200 Veszprém
Zrínyi Miklós utca 3. Hungary
+36.1.580.9140

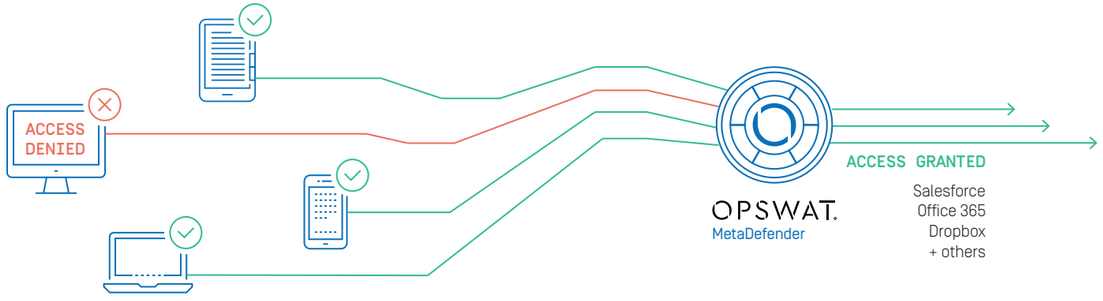
Romania
2nd Martin Luther Street
300054 Timişoara, Romania
+40.771.162.153

Vietnam
17th Floor, Sai Gon Giai Phong Newspaper Building
436 – 438 Nguyen Thi Minh Khai Street
Ward 5, District 3, Ho Chi Minh City, Vietnam
+84.28.7107.8886

SOLUTIONS

Secure Device Access

As an increasing number of organizations migrate to the Cloud, coupled with the rise of BYOD, the need has never been greater for cloud access control and device management. OPSWAT protects organizations from device based threats by preventing risky devices from accessing local networks and cloud applications such as Office 365, Salesforce and Dropbox. Using MetaAccess, threat intelligence and compliance technologies, OPSWAT performs extensive security and compliance checks, as well as remediation, before allowing devices to connect to local networks and cloud applications. OPSWAT also offers APIs to add cloud access control to your existing security solutions. Offering intuitive end user experiences, flexible polices and configurations, OPSWAT helps you achieve compliance and device security at a reasonable initial cost and a low ongoing overhead expense.

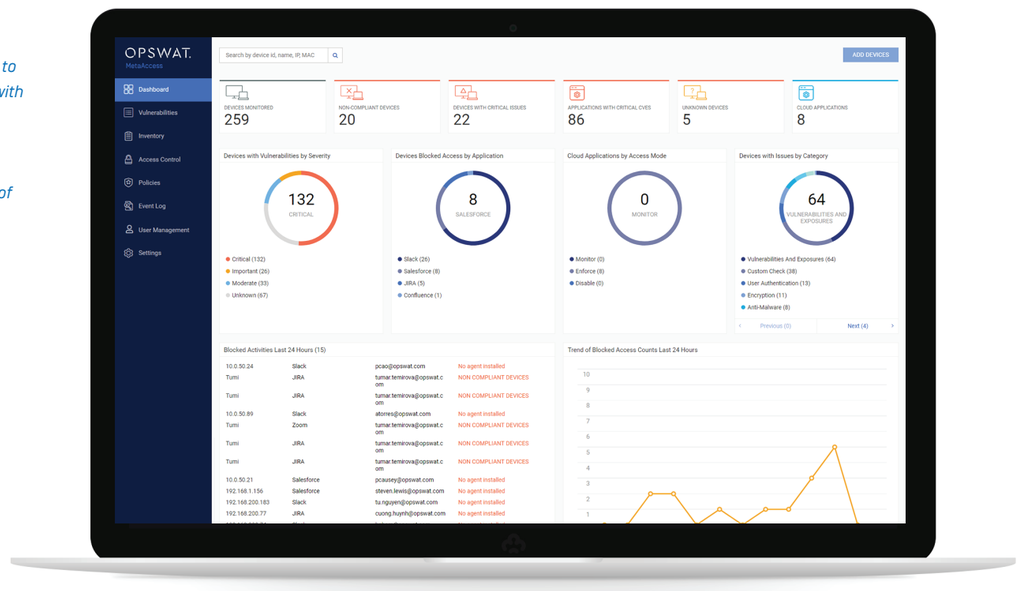


MetaAccess

MetaAccess protects against device based threats. It secures corporate data by ensuring that only compliant devices are allowed to access local networks and cloud applications. It helps organizations meet regulatory requirements through zero-day detection, classification, assessment, and management of more than 5,000 security applications backed by OPSWAT's industry-leading certification program. MetaAccess provides full application inventory tracking, vulnerability classification, and helps IT organizations prioritize patch management. It also prevents malware infections by offering unique threat detection with multi-scanning technologies combined with portable media content inspection and access control. It has an intuitive end user experience and provides full visibility to security administrators.

"MetaAccess enables us to provide our many users with increased usability, and secure network and resources access, while maintaining a high level of security for the bank's network."

IT Director
Large global bank



MetaDefender Platform

Modern enterprises of all types and sizes face an increasing number of challenges from major attack vectors, including email, BYOD, the Cloud, and web portals. OPSWAT created a platform for preventing and detecting cyber security threats on multiple data channels and devices. The platform is powered by patented technologies and is controlled by a flexible workflow engine to efficiently prevent advanced threats. OPSWAT main use cases include isolated network protection, web and email security, and secure device access.

The Technologies

Data Sanitization

Data sanitization, also known as Content Disarm and Reconstruction (CDR), is an advanced threat prevention technology that does not rely on detection. Instead, data sanitization assumes all files are malicious and rebuilds each file ensuring full usability with safe content. The technology is highly effective for preventing known and unknown threats, including zero-day targeted attacks and threats that are equipped with malware evasion technology such as Fully Undetectable (FUD) malware, VMware detection, obfuscation and many others.

MetaScan

OPSWAT multi-scanning technology increases detection rates, reduces outbreak detection times and provides resiliency for anti-malware vendor issues. OPSWAT pioneered the concept of multi-scanning files with more than 30 anti-malware engines available to deliver enhanced protection from a variety of cyber threats.

Data Loss Prevention (DLP)

OPSWAT helps prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive data in files and emails, including credit card and social security numbers. OPSWAT DLP supports a wide range of file types, including Microsoft Office and Adobe PDF.

MetaAccess

MetaAccess technology enables access control based on the device health and security status. This patented technology ensures that only devices compliant to security policies will access cloud and local applications.

Vulnerability Assessment

OPSWAT vulnerability assessment technology identifies application and file-based vulnerabilities before and after they are installed. OPSWAT uses 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.

#1 OPSWAT DATA SANITIZATION RANKING BY US GOVERNMENT AGENCY

20K+ INSTALLER AND APPLICATION VULNERABILITIES DETECTED

100M+ DEVICES PROTECTED

2B+ THREATS IN OUR THREAT INTELLIGENCE DATABASE

Compliance

OPSWAT device compliance technology minimizes ongoing risk by offering zero-day detection and management of newly updated software and components powered by our industry-leading certification program.

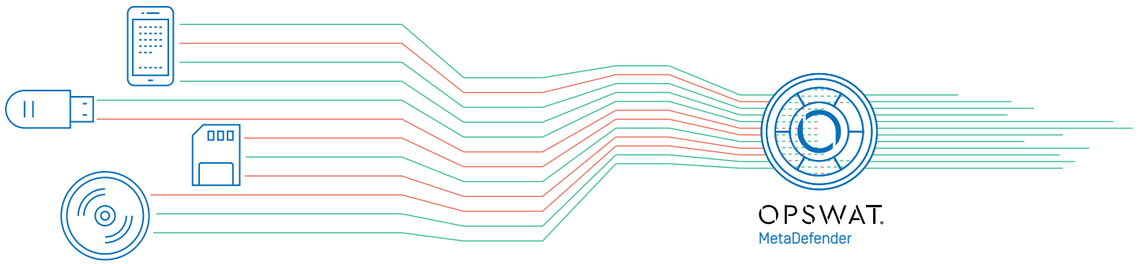
Threat Intelligence

OPSWAT enables developers to leverage millions of data points from millions of in-the-wild devices. Developers, IT administrators and organizations can easily integrate our up-to-date malware threat intelligence data into their existing tools or solutions to effectively protect their organization against threats.

SOLUTIONS

Isolated Network Protection

Critical networks are especially challenging for security practitioners because isolated and air-gapped networks are vulnerable to attacks from portable media and other file transfer technologies. OPSWAT creates a secure end-to-end process for transferring files to and from isolated networks, which is widely used in manufacturing, energy, government, banking, pharmaceutical, and entertainment industries.



MetaDefender Kiosk

MetaDefender Kiosk serves as a security checkpoint for preventing cyber security threats from entering isolated networks via peripheral devices. Kiosk offers software and hardware form factors for any type of deployment environment. Kiosk is used by organizations that require the highest level of security, including critical infrastructure, government agencies, and financial institutions. MetaDefender Kiosk is used by the majority of North American nuclear operators, making MetaDefender the leading hardware-based portable media detection and file sanitization solution for the North American nuclear industry.

MetaDefender Vault

MetaDefender Vault is a protected network storage location that can sit anywhere on a network and can be used with MetaDefender Kiosk for processed file storage. The technology enables the transfer of secure files into and out of isolated networks without the need to transport portable media into a facility. Guests and users can access all certified and checked files from MetaDefender Vault while leaving all USB drives at the perimeter. Checkpoints across isolated networks can be established strategically for visibility, audits, and malware prevention, wherever necessary.

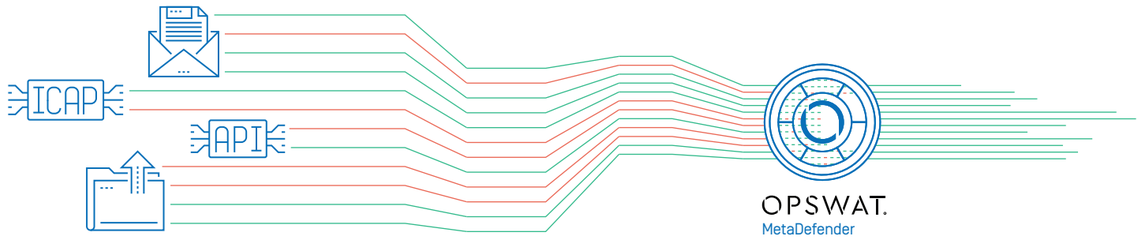
"Our MetaDefender Kiosks give us the added confidence in our ability to help keep our network malware-free."

Ed Koeller
Security Analyst, Ameren

SOLUTIONS

Web & Email Security

File uploads and email are essential to business productivity. However, both are increasingly vulnerable to malicious attacks via content-borne malware. OPSWAT protects organizations against cyber security threats from email and file uploads.



MetaDefender Email Security

MetaDefender email security solutions protect against email-borne threats that evade sandboxes and bypass advanced threat protection solutions. MetaDefender Email Security prevents zero-day attacks and unknown threats.

MetaDefender ICAP Server

MetaDefender ICAP Server protects against advanced threats entering organizations via network traffic and can be seamlessly integrated with ICAP-enabled devices. ICAP includes integrations to traditional Intrusion Prevention Systems (IPS), forward/reverse-proxy servers and storage devices.

MetaDefender Core

MetaDefender Core provides advanced content security with a flexible API for DevOps and security development teams. OPSWAT APIs are at the core of multiple OPSWAT technologies including multi-scanning, data sanitization, vulnerability assessment, DLP, and threat intelligence.

MetaDefender Cloud

MetaDefender Cloud API provides enterprise malware researchers, incident response teams, and technology providers with comprehensive APIs to leverage MetaDefender Cloud's advanced threat prevention, detection, threat intelligence, and binary reputation technologies.

"We use OPSWAT's MetaDefender as one of the tools in our arsenal that protects our email users against advanced malware threats. We've been using the product for many years now. OPSWAT's multi-engine scanning technology is fast, easy to integrate, and has been highly effective in our pursuit of offering the best security available to our customers. OPSWAT has been a great company to work with and I highly recommend them."

Chris Cain

VP of New Technologies,
AppRiver