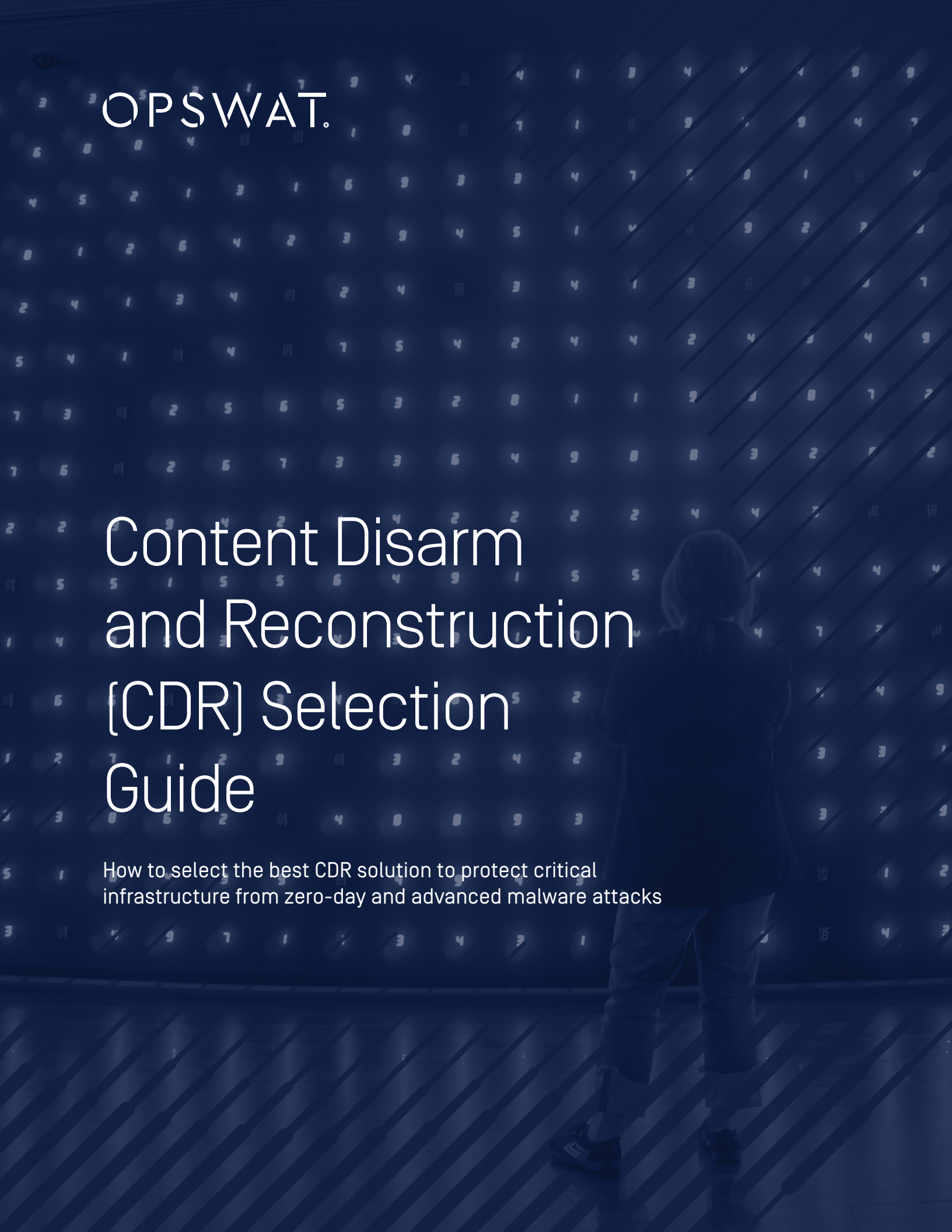
OPSWAT.

Content Disarm and Reconstruction (CDR) Selection Guide

How to select the best CDR solution to protect critical infrastructure from zero-day and advanced malware attacks



Overview

This guide provides an overview of Content Disarm and Reconstruction (CDR) technology and how you can select the best CDR solution to protect your business from emerging cybersecurity threats and how you can protect your infrastructure.

The guide is organized into three sections:

1. How CDR and data sanitization can be used to prevent known and unknown malware from entering an organization
2. Key questions to ask when selecting a CDR solution
3. How OPSWAT Deep CDR provides an advanced level of threat protection superior to other options in the market

SECTION 1

Using CDR Technology to Combat Emerging Threats

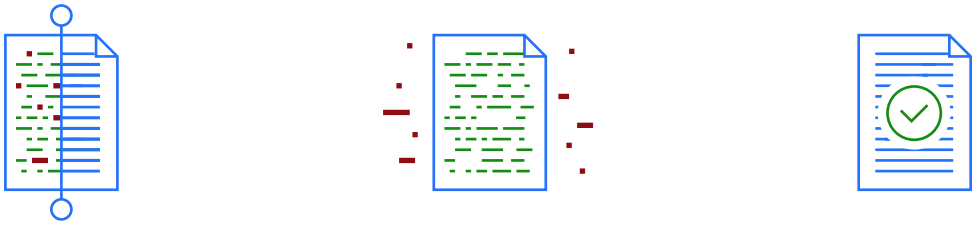
What is CDR?

CDR stands for content disarm and reconstruction. CDR, also known as data sanitization, is an advanced threat prevention technology that does not rely on detection—it follows the zero-trust philosophy and assumes all files are malicious, and sanitizes and rebuilds each file ensuring full usability with safe content. This means that files are dissected and anything that has the potential to be dangerous is removed—and then the file is reassembled.

CDR 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 malware, VMware detection, obfuscation and many others.

How does CDR work?

CDR follows a three-step process:



1	Verify file type and identify all active embedded content in the file	2	Remove all potentially malicious content and reconstruct the file with only its legitimate components	3	Use regenerated threat-free file with full functionality and quarantine the original file

1. **Identify and Scan Files**

   Files are evaluated and verified as they enter the sanitization system to ensure file type and consistency, with identification of over 4,500 file types. Each file is scanned to identify all embedded active content in the file, such as macros, hyperlinks and OLE objects. File extensions are examined to prevent seemingly complex files from posing as simpler files, and red-flagged for malicious content, alerting organizations when they are under attack. OPSWAT Deep CDR supports sanitization for over 100 common file types, including PDF, Microsoft Office, HTML, many image file types, JTD, and HWP.

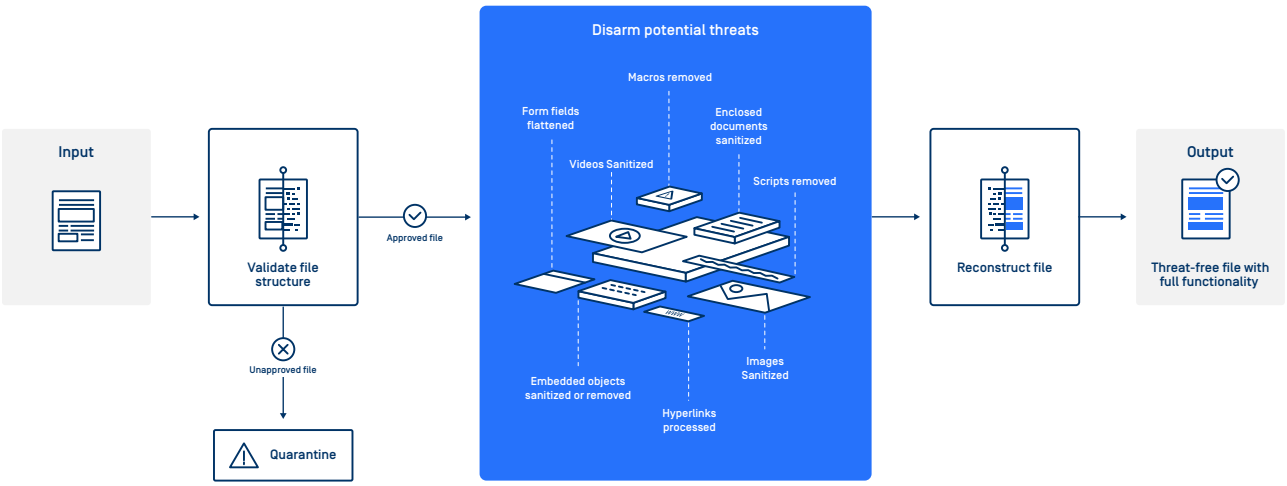
2. Sanitize Files

The files are rebuilt in a fast and secure process. File elements are separated into discrete components, malicious elements are removed, and metadata and all file characteristics are reconstructed. The new files are recompiled, renamed and delivered, preserving file structure integrity so that users can safely use the file without loss of usability.

3. Use Files

The newly regenerated files can now be used. Even complex files remain usable - for example, animations embedded in PowerPoint files remain intact after the CDR process is completed. Finally, the original files are quarantined for backup and further examination. By rendering fully usable files with safe content, the CDR engine protects organizations against the most sophisticated threats while maintaining user productivity.

An overview of how OPSWAT Deep CDR works is provided below. There is more information on this technology in Section 3.



Identify, Sanitize, Reconstruct: Overview of OPSWAT Deep CDR Workflow

Two common CDR use cases are summarized below.

Can CDR Prevent Threats Based on Software Vulnerabilities?

A software vulnerability refers to the weakness of an asset that can be exploited by cyber attackers. Both known vulnerabilities and unknown vulnerabilities can be the root cause of security incidents. Many vulnerabilities leverage files to compromise file containers.

For example, hackers can leverage the disclosed Adobe Acrobat and Adobe Reader vulnerability, CVE-2019-16451, to distribute backdoor malware capable of controlling an infected system - providing attackers with the ability to install programs; view, modify, and erase data; create new accounts with full user rights.

OPSWAT Deep CDR is effective for addressing file-based vulnerabilities since rebuilding the file removes malicious commands and exploits hidden in images, videos, and other innocent file formats.

Can CDR Protect Against the Risk of Increasingly Complex File Formats?

File formats are allowing increasingly complex functions through embedded scripts, macros, and programming designed to streamline workflows and boost productivity. For example, PDFs may contain elements including hyperlinks, media files, forms, Unicode characters, and encrypted data.

60%
of 2019 attacks were targeted

1,045
publicly disclosed vulnerabilities in 2019

59%
companies experienced malicious code attacks

This complexity allows users to be more productive, but also enables malicious actors to embed scripts and exploits that take advantage of the flaws in applications. OPSWAT Deep CDR protects against these file-based vulnerabilities as it rebuilds files and prevents malicious commands, scripts, and embedded objects.

SECTION 2

How to Select a CDR Technology Solution

There are many CDR solutions available on the market today. How do you know which solution is best for your organization? We have compiled a summary of 15 key questions to ask during the evaluation process for a Content Disarm and Reconstruction solution.

1. **What type of archive formats are supported?**

   Archives have become increasingly prevalent over the past couple of years to integrate and store multiple file types in a single volume. Ask to review the list of archives the CDR supports and check that you can control related features, such as the level of recursion. For example, if a PDF is embedded within a PowerPoint file, can the technology analyze and reconstruct both files?

2. **How many file types are supported?**

   There are more than 5,000 known file types. Ask how many file types the CDR supports; review evidence per file type; and compare the list of file types to the ones your organization uses.

3. **Is usability preserved?**

   When you deal with files such as PowerPoint that include animation builds, or Excel where you want to preserve macro functionality, you need to ensure the rebuilt file will retain these capabilities. One way to test this is by processing a sample file as part of your evaluation process.

4. **Does the CDR support comprehensive configurations to fit your use case?**

   Check to see if you can configure the embedded objects that should be removed/sanitized for each file type. Check that you can fine tune the sanitization process as well as image quality, hyperlink handling, etc.

5. **Can you create an audit trail?**

   For example, make sure the CDR records and logs which objects were removed, and which objects were sanitized? Also find out if you can verify the integrity of an archive.

6. **Can you deploy different policies for separate data channels?**

   For example, will the CDR allow you to retain an Excel macro for internal emails while removing it for external emails?

7. **Which operating systems does the CDR support?**

   If your organization supports both Windows and Linux, can the vendor support both?

8. **What is the performance per file type?**

   Different file types should have different performance. Deploy the CDR technology and run some sample files, including large files and multi-level archives to verify that the CDR performance meets your organization's requirements.

9. **How secure is the design?**

   Is a secure design pattern applied? How is the CDR engine protected? Is Secure SDLC (Software Development Lifecycle) implemented, enabling you to review a static analysis code review. Are third-party libraries used? Ask to review a CDR design architecture and challenge the design with questions about compromised CDR components.

10. **Is the technology sustainable?**

    How many engineers are actively working on the CDR technology? Ask to see an organization chart to validate the number of resources and their backgrounds. Ask to review their engineering QA procedures. Is the build process safe? Do they have a solution to prevent malware embedded into the build chain? What security certification does the vendor have?

11. **How is the CDR technology tested?**

    Is there any third-party validation by a government agency or other independent organizations? Ask to see their pen test results. How big is the test data set? Ask to see true malware samples and zero-day attack samples. Ask to manually verify test data sets. Do they test with recent threats? Request a data set.

12. **How easily does the CDR integrate with your current products?**

    Ask to review the REST API documentation.

13. **Is the technology continuously updated?**

    Ask to see the release history for the past two quarters. Ask to see the product roadmap.

14. **How quickly can they support a new file type?**

    There are 5,000 file formats – how many can they support? Ask about specific file types you use in your organization, including regional file types such as HWP or JTD.

15. **Is the IP properly protected?**

    If the technology leverages third-party libraries, are they properly licensed? Ask to see the EULAs for the list of libraries or other supporting documents. Ask about any technology patents.

SECTION 3

How OPSWAT Can Help

OPSWAT developed CDR technology to address zero-day cyber threats that are not detected by traditional anti-malware and dynamic analysis solutions like sandboxes.

Traditional anti-malware and dynamic analysis solutions like sandboxes are missing threats because they were built to detect an anomaly in a file or in a file's behavior.

OPSWAT CDR technology, called Deep CDR, assumes all files are malicious. It ingests files and then regenerates these files in a way that ensures the regenerated file is both usable and harmless. Hence, our CDR technology provides protection without needing to know whether a suspected file is "good" or "bad".

OPSWAT introduced Deep CDR in 2012 and our solution is widely deployed globally, particularly by customers in Critical Infrastructure Industries.

Deep CDR further enhances the security effectiveness of CDR by diving "deep" into nested layers of compression and embedded objects—such as an Excel chart inside of a Word document that is embedded in a PDF that was delivered to your inbox zipped up into a single file.

Vulnerabilities in Acrobat and Reader can allow a specially crafted PDF to run malicious code that anti-malware products will not detect.

Deep CDR removes the malicious content without relying on detection. A good analogy is like taking a gun and removing anything in its chambers. It doesn't matter if it was a bullet, a blank, or a speck of dust—what matters is that if someone accidentally uses the gun, nobody gets hurt.

So why dig deeper into the files?

According to the Verizon Data Breach Investigations Report, many PDF files are vehicles for delivering macro-enabled Office documents that are embedded within the PDF.

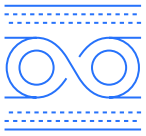
According to the Symantec Internet Security Threat Report, in 2019 48% of malicious attachments were Office files. That's a huge jump up from 5% in 2017.

Deep CDR dissects a PDF, removes the document, dissects the document, removes any potentially harmful active content, and then reconstructs every object in every nested layer before Acrobat, Word, or any of the dozens of other supported applications access or touch the files.

OPSWAT Deep CDR Features and Benefits

100+ Supported File Types

Sanitize and reconstruct 100+ common file types, ensuring each file is completely usable with safe content. Supported file types include PDF, Microsoft Office, HTML, and many image files. JTD and HWP files are also supported.



200+ File Conversion Options

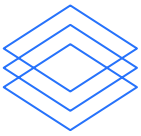
Customizable file conversion enables you to change files into different formats (e.g., convert a .jpg file into a .bmp file, then to a .pdf file, then back to a .jpg). Multiple conversions prevent document-based threats from entering highly secure networks.

4,500+ File Type Verifications

Verify 4,500+ file types to combat spoofed file attacks and detect seemingly complex files from posing as simpler files.

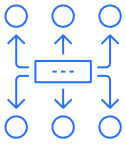
30X Performance

For fast, efficient prevention, Deep CDR is on average 30 times faster than sandbox analysis and prevents malware (including zero-day) that has been built to evade sandbox detection.



30+ Engine Multiscanning Integration

Integrates with OPSWAT Multiscanning, alerting users if they are under attack. Provides visibility across different channels and file entry points, including email attachments, files on portable media devices, and browser downloads—enhancing the security of the entire organization.



Customizable Workflow

Customize the order of Multiscanning and Deep CDR steps for different file entry points. Depending on which channels files originate from, you can first sanitize external files, deliver the sanitized version to users, and then multiscan the original files for complete visibility of the attack matrix.

OPSWAT Critical Infrastructure Protection Solutions

OPSWAT provides advanced threat prevention solutions to solve multiple critical infrastructure challenges, including:

- **Cross-Domain –** Govern and secure data or device transfer for your segmented and air-gapped network environments.
- **Email Security –** Protect your organization against advanced email attacks.
- **File Upload Security –** Prevent malicious file uploads that can compromise your networks.
- **Malware Analysis –** Analyze suspicious files or devices with our platform - on-prem or in the cloud.

- **Network Access Control –** Prevent risky devices including BYOD and IoT from accessing your networks with full endpoint visibility.
- **Secure Access –** Secure local or remote access to your cloud applications, internal networks, and resources.
- **Storage Security –** Protect your on-prem or cloud storage services and maintain regulatory compliance.

In addition to Deep CDR, OPSWAT deploys several other market leading technologies including Multiscanning, Proactive DLP, and Threat Intelligence to deliver a superior threat prevention solution. Our MetaDefender platform integrates these technologies into a comprehensive, modular solution that can grow with your organization and be deployed across a wide range of use cases.

OPSWAT MetaDefender Platform Overview

Additional Resources

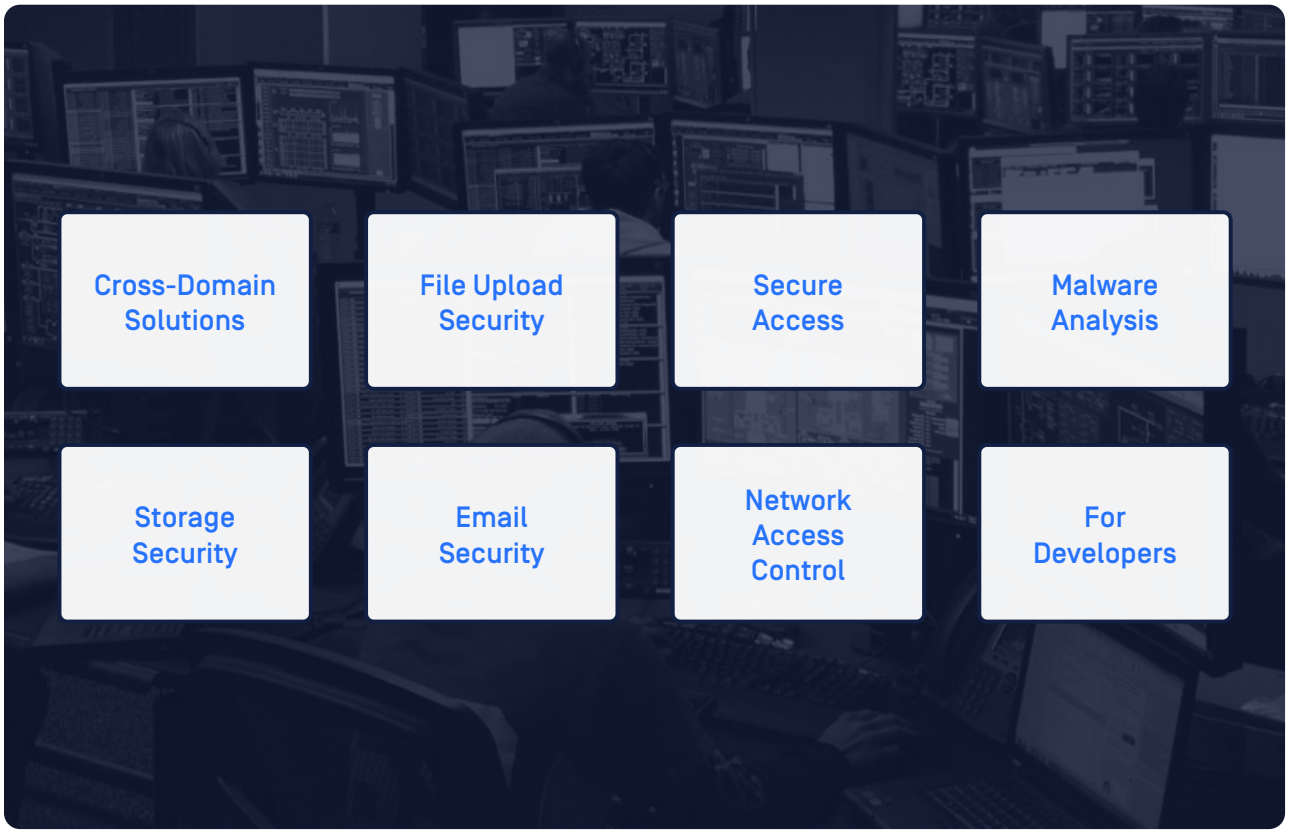
To learn more about how CDR can help enhance your cybersecurity protection, contact us to speak with one of our cybersecurity experts.

You can also access additional CDR resources by visiting OPSWAT CDR.

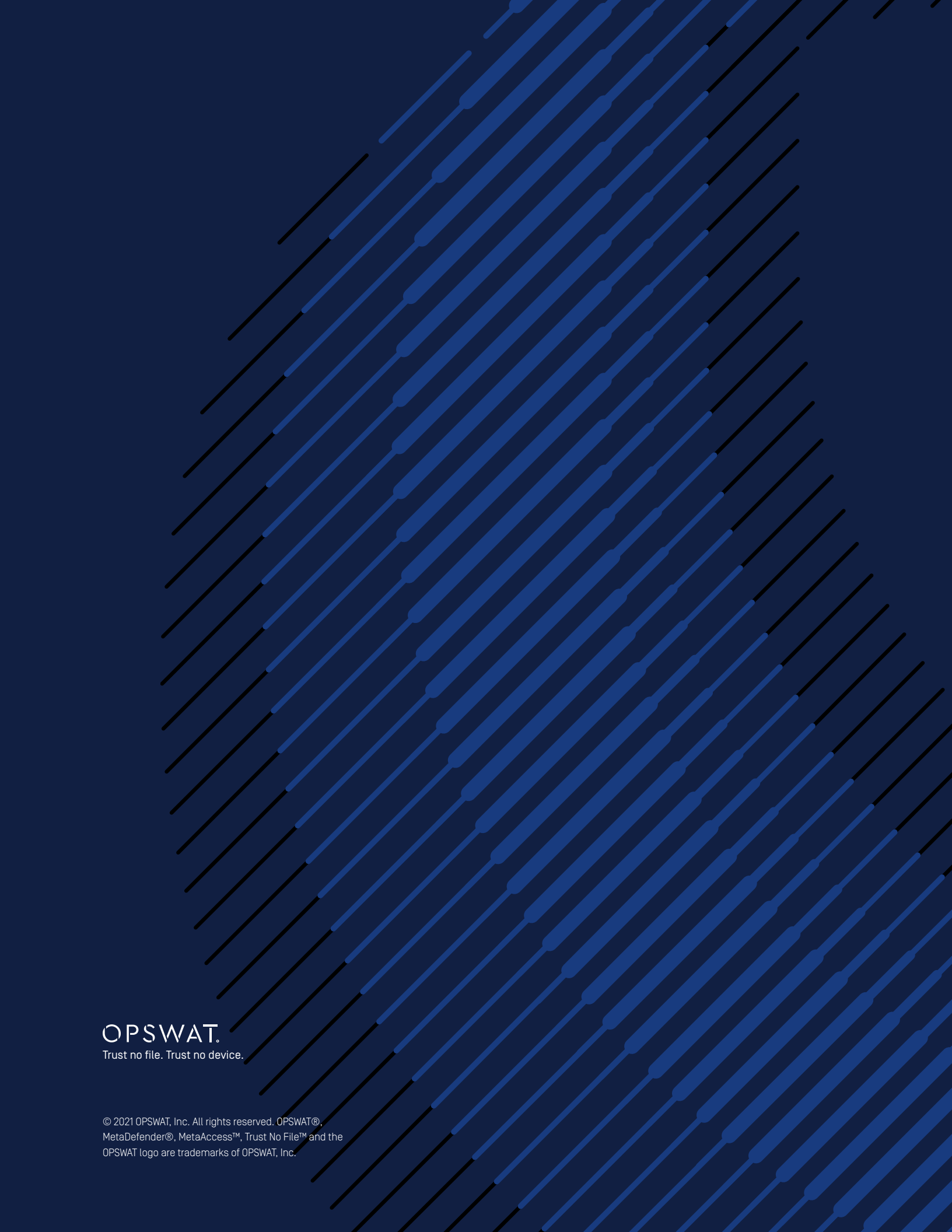
About OPSWAT

OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organizations from malware and zero-day attacks. To minimize the risk of compromise, OPSWAT Critical Infrastructure Protection (CIP) solutions enable both public and private organizations to implement processes that ensure the secure transfer of files and devices to and from critical networks.

More than 1,000 organizations worldwide spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations; and to protect their reputation, customers, partners, and employees from cyber-driven disruption.



Visit us on LinkedIn, Twitter, Facebook, and YouTube.



OPSWAT.

Trust no file. Trust no device.

© 2021 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess™, Trust No File™ and the OPSWAT logo are trademarks of OPSWAT, Inc.