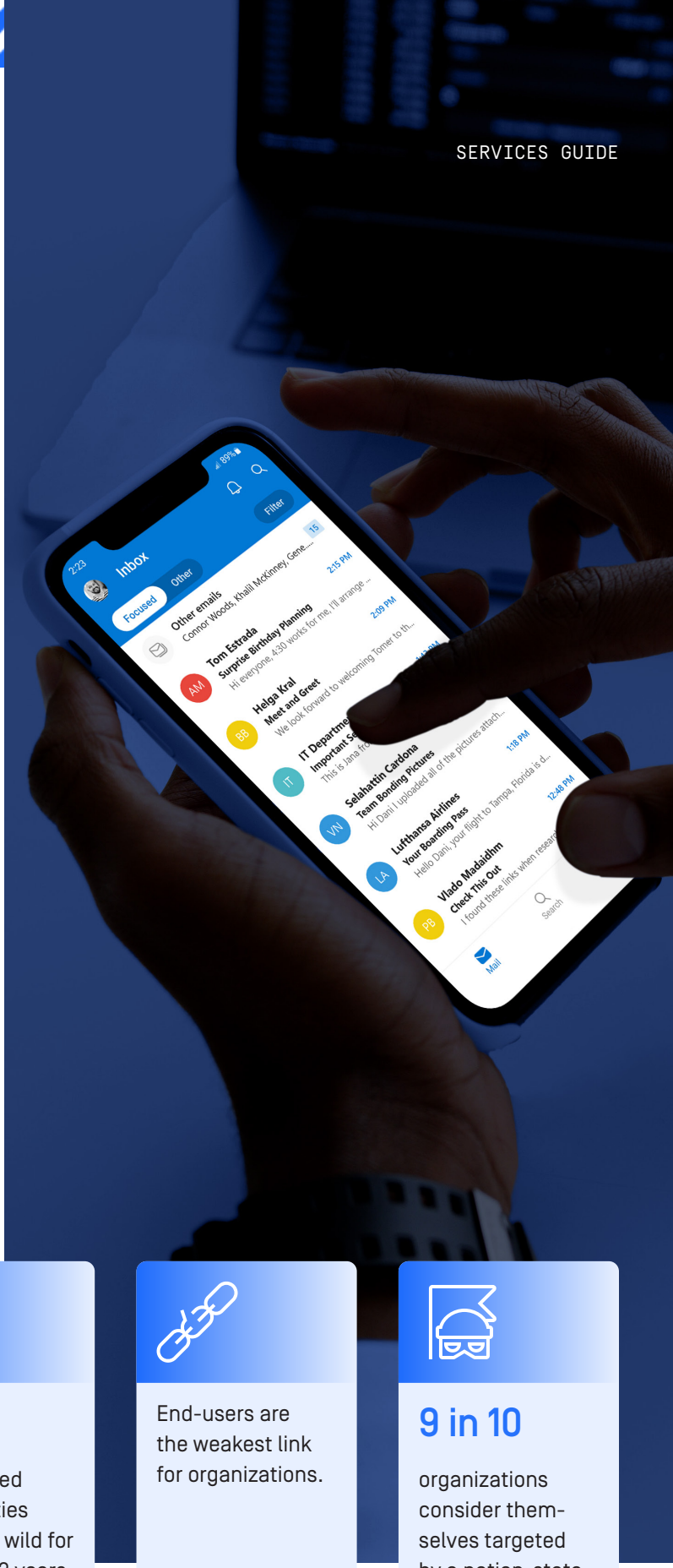
OPSWAT.

Email Risk Assessment

Evaluate Your Email Security Posture to Ensure Maximum Protection



OPSWAT is a leading critical infrastructure protection (CIP) cybersecurity company, winner of the "Overall Enterprise Email Security Solution of the Year" award at the CyberSecurity Breakthrough Awards.

With a mission to protect the world's critical infrastructure, OPSWAT helps organizations identify and prevent cybersecurity vulnerabilities across industries.

Why Perform an Email Risk Assessment?

Cybercriminals' number one attack vector is email-based exploits. OPSWAT Email Risk Assessment determines whether or not you're doing what's necessary to stay protected.

Stay Focused on Email Security

86%

of malware is delivered by email.

Attackers lure users into executing malicious code and exploiting vulnerabilities.

57%

of discovered vulnerabilities were in the wild for more than 2 years.

End-users are the weakest link for organizations.

9 in 10

organizations consider themselves targeted by a nation-state threat actor.

OPSWAT.

Services Guide

What Does an OPSWAT Email Risk Assessment Involve?

1.

We help your email administrator connect the OPSWAT Email Risk Assessment Tool to one or more high-profile email boxes in your email system (for example: sales@your-company.com, marketing@your-company.com, ceo@your-company.com, etc.).

2.

The tool retrieves copies of the last 60 days of correspondence within the identified boxes.

3.

We use OPSWAT's advanced cybersecurity technologies to identify malicious or suspicious data in emails and attachments for:

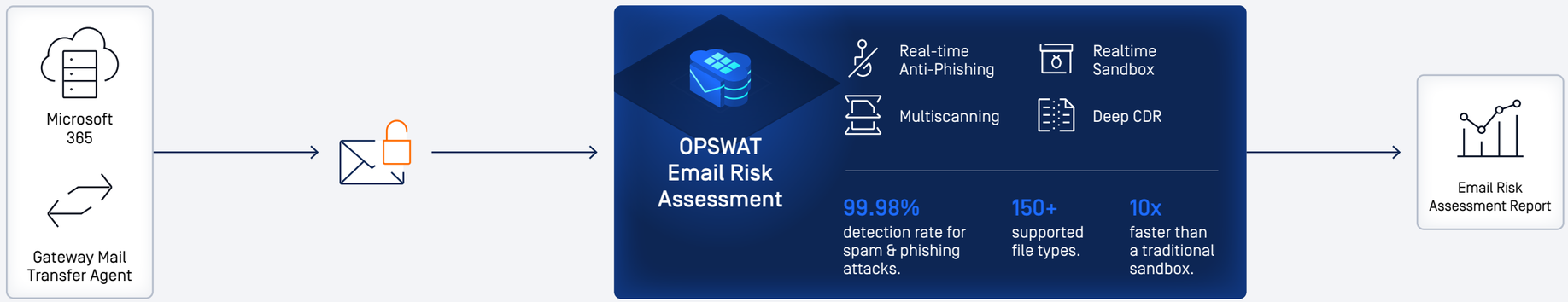
- Emails containing malicious active content that is often associated with unknown exploits or sophisticated zero-day threats
- Files purporting to be of a specific file type that are malformed and therefore suspicious
- Files flagged by at least one of the 30+ industry-leading anti-malware engines that may contain zero-day malware
- Emails containing phishing characteristics and social engineering tatics.

4.

At the end of the assessment, a comprehensive and actionable report is generated including your organization security scorecard and summary of the items identified.

5.

Following that, our Professional Services team can perform a deep dive into files of interest and make recommendations on addressing security gaps.



The Objective: Uncover phishing, malware, and exploits that bypass your M365 security and other solutions

OPSWAT.

Services Guide

Protection from Zero-Day Malware

Beyond traditional signature detection, OPSWAT's Multiscanning technology includes more than 30 industry-leading anti-malware engines. These engines improve the detection rates of recently introduced malware using heuristics and Machine Learning to address unknown malware.

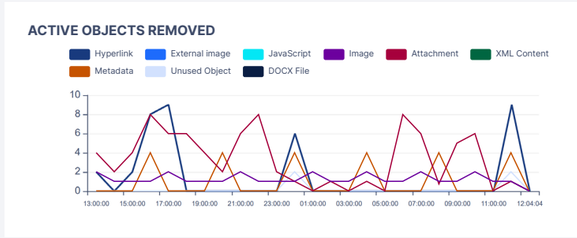
If malware is detected by the OPSWAT Email Risk Assessment, then you need to reconsider your current anti-malware scanning solution, as its security controls should have blocked these attacks.

Unknown Vulnerabilities and Zero-Day Exploit Prevention

OPSWAT's Deep Content Disarm and Reconstruction (Deep CDR) technology sanitizes files or file elements that are typically used for malware delivery to devices. OPSWAT's Email Risk Assessment Tool provides a comprehensive list of all such elements contained in the assessed set of email attachments.

ZERO-DAY MALWARE PREVENTION - CONTENT SANITIZED

File type	Sanitized	Objects removed	Blocked
Hypertext Markup Language	0	0	49
Portable Network Graphics	18	18	0



ACTIVE OBJECTS MITIGATED

Threat	Count
Trojan-Downloader.O97M.Dridex	27

Protection from Unknown Malware

OPSWAT's Sandbox provides a wide range of security benefits that strengthen the security posture of an organization against unknown risks. This will significantly increase malware detection rates.

The technology emulates a wide range of file formats, including Microsoft files, PowerShell, Jscript, and XSL to reveal sophisticated email threats. OPSWAT's Email Assessment Tool will provide Indicators of Compromise (IOCs) for unknown malware that is detected.

OPSWAT.

GET STARTED

Stop Threats Before They Stop You

An Email Risk Assessment is just one of the many ways OPSWAT's Professional Services team can help you get the most out of your cybersecurity solution.

Talk to an expert today to learn more.

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

OPSWAT.
Protecting the World's Critical Infrastructure

To explore how OPSWAT helps you protect your infrastructure, schedule a demo at opswat.com/contact