OPSWAT.

DATASHEET

MetaDefender® Cloud Email Security

Advance Your Email Security Posture

Email continues to be the primary attack vector. Organizations are facing increasingly sophisticated social engineering tactics that lure users to execute malicious code - exploiting unknown application vulnerabilities, resulting in a breach of their network. The challenges are compounded by slow and often inefficient protection against zero-day threats.

OPSWAT MetaDefender Cloud Email Security has introduced some key capabilities to move email protection to a higher level of effectiveness, to the advanced security posture.

Key Features

Anti-Phishing and Anti-Spam:
Our solution applies an advanced multi-step anti-phishing approach to avoid human error. By combining multiple detection technologies, emails are sent through a series of blacklists and content-filtering technologies to identify spam, social engineering, blackmail scams, and malicious phishing attacks. The hyperlinks in the emails are rewritten to redirect the user toward MetaDefender Cloud which verifies the URL's reputation in real-time via 30 online sources.

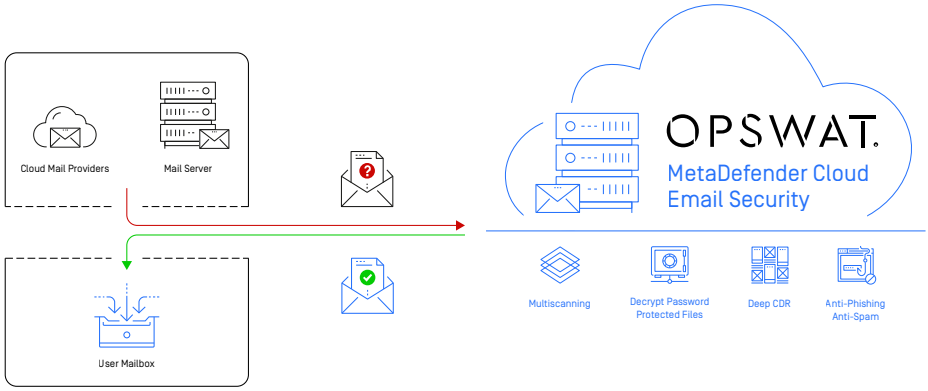
Manage Password Protected Attachments:
Password-protected attachments are no exception, as a decryption password must be provided so that Deep CDR and Multiscanning are applied.

Zero-Day Malware Prevention:
Deep CDR is an advanced threat prevention technology that enables organizations to protect themselves against attackers using undisclosed and zero-day threats by sanitizing more than 120 file types and emails from malicious active content. Our approach is 30 times faster than detection-based security.

Advanced Threat Protection:
The Multiscanning technology improves the detection rates of malware and advanced threats. It also reduces the vulnerability time to virtually zero. Beyond the traditional signature detection, Multiscanning leverages heuristics and machine learning engines to address unknown threats.

OPSWAT.

MetaDefender Cloud Email Security



Capabilities

Increase Detection of Advanced Threats
The Multiscanning technology analyzes each email with signatures, heuristics, and machine-learning technologies by using up to 35 anti-malware engines*.

Reduce Window of Exposure
The Multiscanning technology combines multiple AV engine update windows, reducing the window of vulnerability (WoV) for companies. MetaDefender Core packages can significantly reduce exposure time to less than 7 minutes.

Prevent Zero-day Attacks
Deep CDR disarms every email's content and attachments by removing potentially malicious content. Only the reconstructed, fully usable files will be delivered. Our solution sanitizes over 120 common file types, including password-protected attachments.

Leverage Dynamic Anti-phishing
The Dynamic Anti-Phishing technology addresses phishing attacks on multiple stages. It applies advanced heuristics, neural networks, and spear-phishing filters as well as IP/sender and content reputation checks to prevent phishing attacks.

Benefits

- Reducing human error by uncovering potential phishing attacks on multiple stages
- Protecting users from social engineering attacks, ensuring IT can rely less on user awareness
- Providing flexibility with cloud-based email service so you can quickly scale your email security resources and functionality to meet business needs
- Increasing the effectiveness of malware detection to provide advanced email protection.
- Reducing the Window of Vulnerability (WoV) against malware, thus effectively preventing malware outbreaks
- Protecting business productivity files by removing document-based threats from attachments
- Effectively eliminating zero-day targeted attacks by relying on prevention rather than detection

Summary

OPSWAT MetaDefender Cloud Email Security introduces some key capabilities to fill security gaps, reducing the cybersecurity risk of emails and eliminating potential human errors to move email security to an advanced level. By applying OPSWAT technologies, our solution enables organizations to better protect themselves against sophisticated attacks, including undisclosed and zero-day threats which are commonly used today. Our solution is available as a service and on-premises.

Contact us

Detection rates of top 10,000 threats with OPSWAT Multiscanning