SOLUTION BRIEF

Stop Email-based Ransomware Attacks With FortiMail

Executive Summary

According to the Verizon 2021 Data Breach Investigations Report, ransomware's involvement in successful breaches increased to 10%, more than doubling from the prior year.[1] Our own FortiGuard Labs reported a 10.7x increase in ransomware detections across our sensors from June 2020 to June 2021.[2]

Threat vectors for ransomware can be attributed to three main pathways: email, Remote Desktop Protocol (RDP) tools, and software vulnerabilities exploits. Because email enables a direct communications line between an attacker and employees in an organization, email-based ransomware threats pose a particular danger initiated at the click of a link or opening of an attachment.

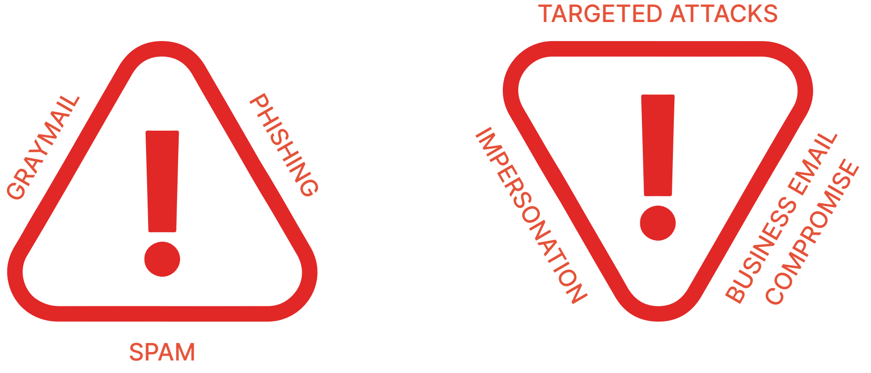
1 of every 3 ransomware attacks involves email as a threat vector.

FortiMail

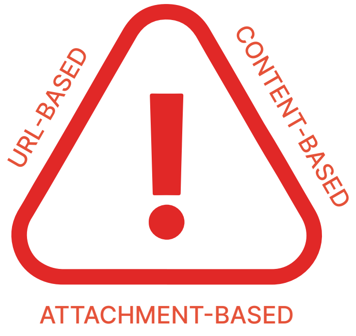
Because email is involved in more than one out of every three ransomware attacks, Fortinet FortiMail is a critical step to protecting organizations from ransomware.

FortiMail is powered by FortiGuard Labs threat intelligence and integrated into the Fortinet Security Fabric, providing powerful capabilities to help organizations combat ransomware. FortiMail provides best-in-class performance validated by independent testing firms to deliver advanced multilayered protection against the full spectrum of email-borne threats. This protection works to stop a malicious email during the Initial Access MITRE ATT@CK stage of a ransomware attack, eliminating or minimizing any impact to organizations. Meanwhile, integrated data loss prevention (DLP) also works to block the exfiltration of sensitive data through the exfiltration phase of ransomware attacks.

Types of Email-borne Threats and Risks



Building Blocks



FortiMail is designed to help organizations stop ransomware threats with integrated capabilities that seek to detect both the tactics threat actors use and the underlying payloads associated with those tactics.

FortiMail provides best-in-class performance against email-based ransomware threats by:

- Detecting phishing, spear phishing, and impersonation attacks
- Applying URL inspection techniques to detect ransomware-related threats at the end of a click
- Performing advanced analysis and detonation of suspect file attachments

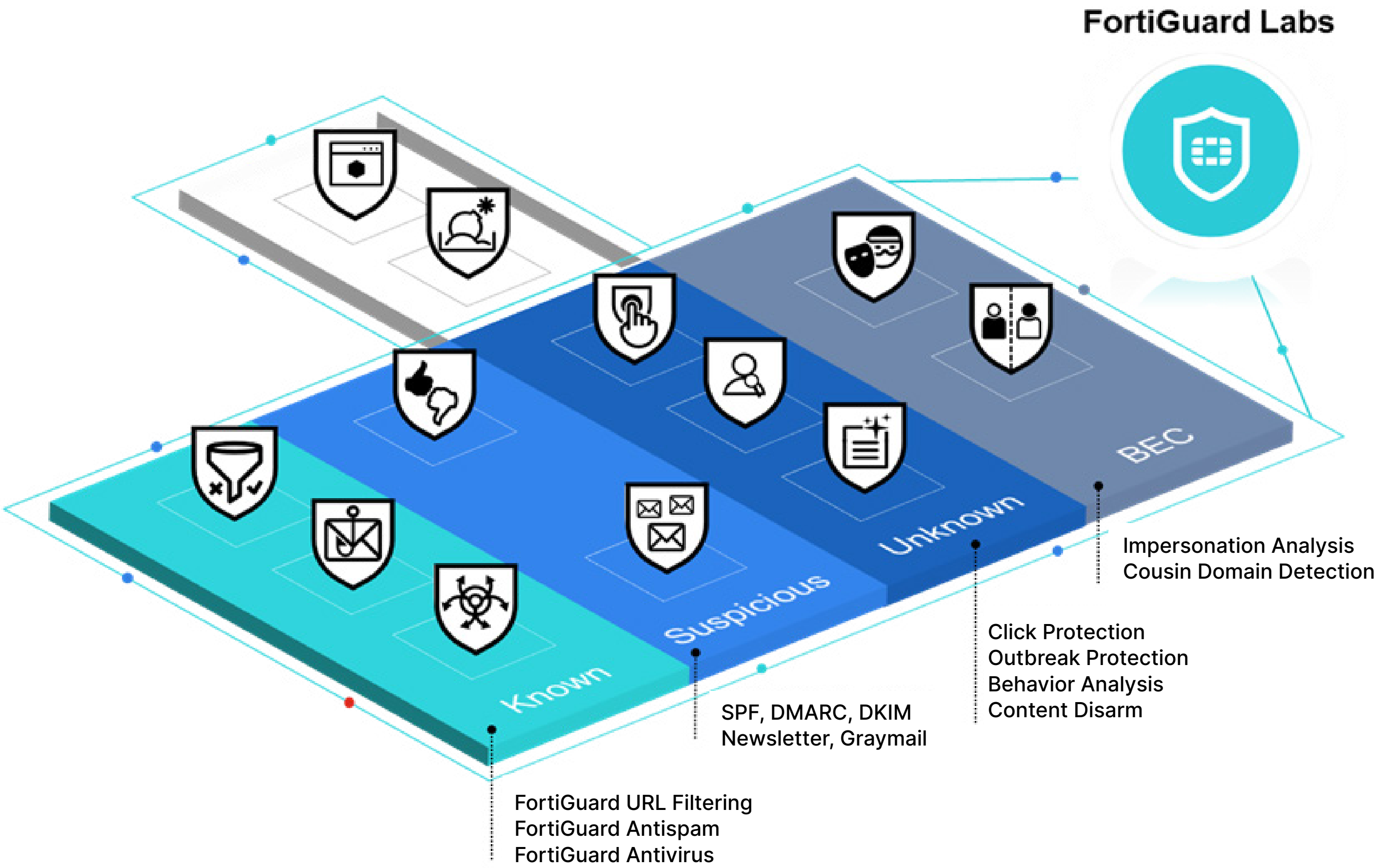


Figure 1: Inbound email security protections through FortiMail.

Protection against email-borne threats

Advanced techniques such as outbreak protection, content disarm and reconstruction, sandbox analysis, impersonation detection, and other technologies work together to detect malicious threats at scale.

Validated performance

Fortinet is one of the only email security vendors to consistently prove the high efficacy of FortiMail solutions through independent testing conducted by SE Labs, ICSA Labs, and Virus Bulletin.

Fabric-enabled email security

Integrations with the Fortinet Security Fabric enable advanced capabilities such as sandboxing and browser isolation for use with FortiMail. In addition, fabric integration allows organizations to expand coverage against ransomware through capabilities such as endpoint detection and response (EDR). Logs can also be sent to FortiSIEM for further analysis and correlation. Last, FortiSOAR can be used to automate workflows and response actions involving email.

Powered by FortiGuard Labs

FortiMail is powered by threat intelligence from FortiGuard Labs. With visibility across 500,000 customer environments worldwide, FortiGuard Labs actively monitors ransomware developments and trends and drives insights into new protections in FortiMail for combating ransomware.

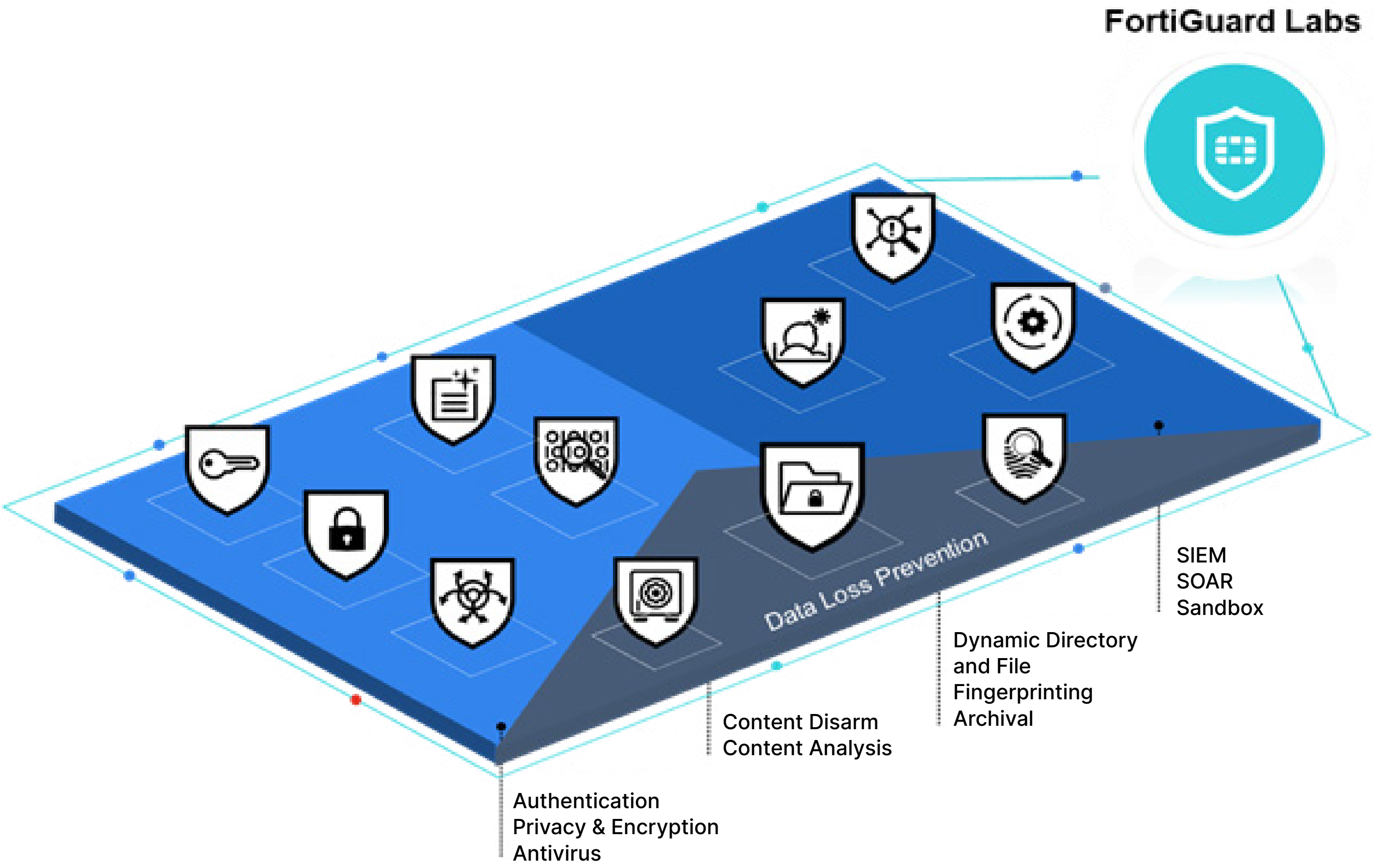


Figure 2: Outbound email security protections through FortiMail.

Protection Against Email-based Ransomware Threats

Ransomware has gone beyond media hype to having a very real impact on organizations around the world. Reducing the risk of email-based ransomware threats starts with highly effective email security tools with advanced capabilities that identify the characteristics of email content and sender/received reputation while also inspecting URLs and attachments.

Fortinet FortiMail delivers advanced integrated capabilities that address the complexities of email-based ransomware threats to prevent, detect, and respond to ransomware attacks at the earliest stages of the MITRE ATT&CK framework. In addition, integrated DLP capabilities work to block the exfiltration of sensitive data sent via outgoing email.

FortiMail provides proven email security performance validated by independent testers SE Labs, ICSA Labs, and Virus Bulletin.

[1] "2021 Data Breach Investigations Report," Verizon, 2021.

[2] "Global Threat Landscape Report," Fortinet, August 2021.

FORTINET

www.fortinet.com

October 26, 2021 7:40 AM
1324994-0-0-EN