PROTECT DIGITAL BUSINESS WITH A UNIQUE EMAIL SECURITY APPROACH

INTRODUCTION

Digitalization of today's businesses is creating new opportunities, but also opening new avenues of attack. Ever the entrepreneurs, many cyber criminals are quick to exploit new portions of the attack surface like IoT, cloud surfaces, and more.

However, they also stick with proven methods until they are no longer profitable. In fact, in the 2018 Data Breach Investigations Report,[1] Verizon found that 49% of all malware was actually installed via an age-old avenue: email. So it's not surprising that leading analyst firm Gartner asserts, "Advanced threats (such as ransomware and business email compromise) are easily bypassing the signature-based and reputation-based prevention mechanisms that a secure email gateway (SEG) has traditionally used."[2]

That's why Fortinet Email Security provides the latest security technologies to deal with an evolving set of email attack classes: spear phishing, ransomware, business email compromise, and more. But, stopping only incoming attacks leaves organizations constantly on the defensive. Fortinet Email Security goes further to uncover the full threat life cycle (and supporting cyber-criminal ecosystem) intended to follow the initial attack.

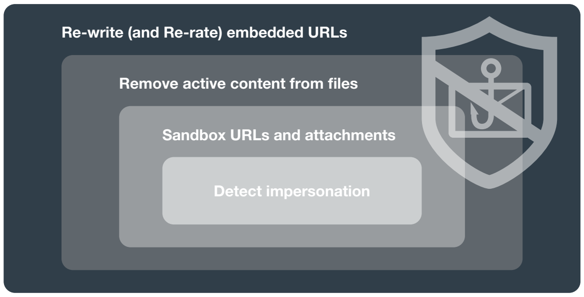
This unique approach enables organizations to proactively secure their digital businesses. And it's available in a range of easy-to-use form factors, for organizations short on specialized cybersecurity skills and staff.

ADVANCED EMAIL SECURITY FOR ADVANCED THREATS

New capabilities from FortiGuard Labs (more than 230 threat researchers across more than 10 disciplines) help Fortinet Email Security keep pace with the very latest email attack techniques.

These include:

- Click Protect to identify websites that are weaponized after email delivery.
- Content Disarm & Reconstruction that removes embedded active code to deliver safe files.
- FortiSandbox to identify brand-new malicious attacks, attachments, and websites.
- Impersonation Analysis to detect spoofing and other indicators of email fraud.


Re-write (and Re-rate) embedded URLs
Remove active content from files
Sandbox URLs and attachments
Detect impersonation

These techniques complement the established features of our full-featured secure email gateway solution.

Verizon found that **49% of all malware was actually installed via** an age-old avenue: **email.**[1]

Fortinet Email Security consistently earns top ratings in independent testing like ICSA Labs, NSS Labs, and Virus Bulletin.

ICSAlabs CERTIFIED ADVANCED THREAT DEFENSE

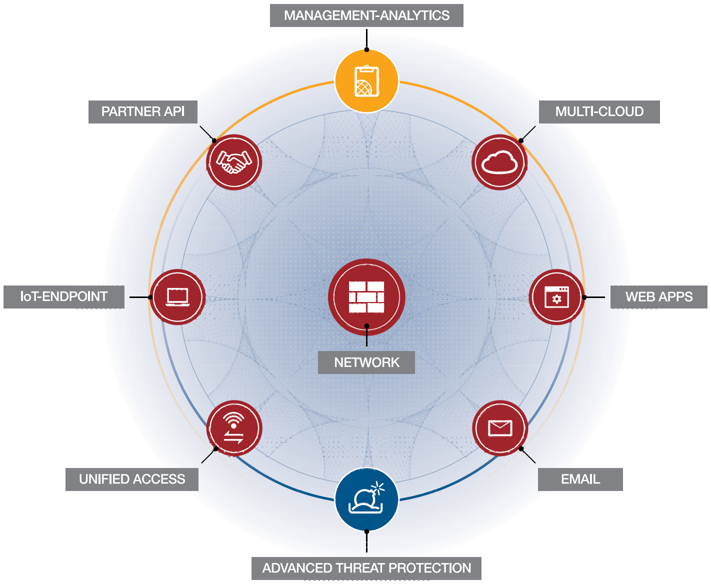
NSS LABS RECOMMENDED

vb 100 VIRUS Oct 2011 virusbtn.com

MOVING TO A PROACTIVE SECURITY APPROACH

That said, incoming email is often only the first stage in a multistage attack that may include communication to other websites, download of additional components, and more. With the help of FortiSandbox (as well as FortiGuard Labs), organizations are able to uncover the stages, components, and associated cyber-criminal infrastructure that extends beyond what is seen and blocked by your email security.

Further, new threat intelligence can be automatically generated and distributed throughout your security infrastructure, creating a security fabric.



This enables organizations to move from reactive to proactive security, across multiple avenues of attack.

EASING THE BURDEN ON SECURITY TEAMS

This proactive approach through automated intelligence generation and sharing is critical for organizations impeded by a shortage of skilled cybersecurity professionals and too many other business-enabling projects clamoring for time and attention. Fortinet Email Security is offered in flexible form factors.

Organizations have the option to:

- Outsource email security systems to a managed security provider or Fortinet.
- Move email security systems to public or private cloud environments.
- Deploy plug-and-play appliances in their own data center.

ADVANCED PROTECTION WITH FORTINET EMAIL SECURITY

Fortinet Email Security can help address the latest email threats and reduce the time required for security administration, incident investigation, and response. These make the business case for advanced protection from costly email threats—like business email compromise, ransomware, targeted attacks, and more—even stronger.

Fortinet is the only vendor with email security as part of an integrated and automated fabric architecture, enabling it to automatically generate and share intelligence to address advanced threats across all major attack vectors. This intelligence sharing is a critical component that helps organizations move from a reactive to more proactive security posture, enabling protection across multiple avenues of attack.

[1] "Verizon 2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[2] Neil Wynne, "Market Guide for Secure Email Gateways," Gartner, May 3, 2017.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990