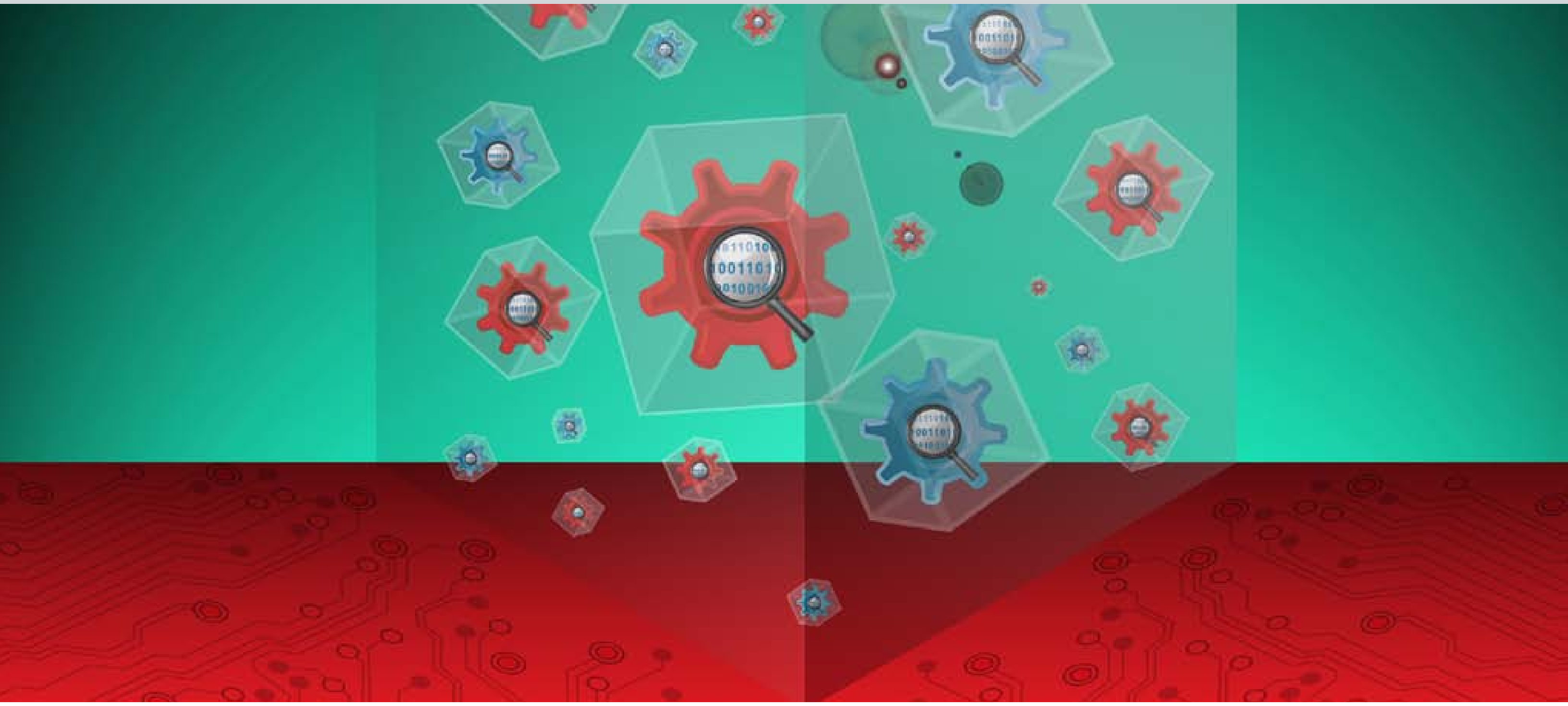
FORTINET

White Paper



FortiMail: Playing safely in the Sandbox

Email attacks are becoming more and more targeted

For years, cybercriminals have used email to personalize attacks, tricking victims as a means to increase success. The proliferation of Advanced Persistent Threats (APTs) and other forms of stealth malware have taken targeted attacks to a whole new level, and it's only going to get worse. Users can expect targeted phishing emails to become more personalized; targeted by organization, language, region, city or interest group as cybercriminals strive for greater return on their investments.

Cybercriminals have long been relying on email as a vehicle to deliver infected PDFs, .exe files and other malicious attachments. That's not going to change. What will likely change, however, is the technical sophistication of the attached malware. While numerous reports have noted that overall spam levels have decreased, the number of emails that come with malicious code attached are on the rise.

With the proliferation of these emails, it only stands to reason that attached APTs will not only become more common, but the norm.

Spear-phishing is standard in cybercrime

The significant spike in advanced malware coupled with targeted attack trends are equipping spear-phishers with increasingly sophisticated tools to add to their arsenal. That means stealthier and more effective spear-phishing campaigns. These days, cybercriminals are equipped with the ability to send specialized, highly targeted attacks to focused groups, as well as personalized emails to individuals, designed to trick even the most security-savvy of users.

Data is the new target

Once upon a time, phishers were intent on acquiring login credentials and credit card information. That hasn't changed, but these days, they're also targeting high-value Big Data that includes intellectual property, blueprints and source code. Malware that rides on malicious attachments increasingly possesses stealth capabilities aimed at evading detection, silently infiltrating classified systems and lifting an organization's most sensitive data. As in the past, the gateway to critical information is often via email, providing a direct pathway to an organization's crown jewels by exploiting the weakest link — the user.

While an invaluable communication tool, email remains one of the most attacked threat vectors around. The reason? Lack of user training and curiosity leads to exploits being executed.

Ahead of the game

FortiMail has always been at the forefront of email threat mitigation, Fortinet being the first vendor to combine cutting-edge anti-spam techniques with anti-virus detection, real-time behavioural analysis and malware URL detection. FortiMail, combined with the expert knowledge of the FortiGuard threat research team, has enabled customers to stay one step ahead of the threat.

FortiMail Proactive Signature Detection and Real-time Malware Analysis

Traditional malware signature detection is reactive; signatures are merely fingerprints of threats that have been spotted "in the wild". Fortinet's advantage is the patented Compact Pattern Recognition Language (CPRL), a proactive signature detection technology developed through years of research by FortiGuard Labs. A single CPRL signature can catch 50,000 or more disguises a piece of malware can be wrapped in.

Signature-based systems deliver the best performance but are not adept at detecting emerging APTs and Advanced Evasion Techniques (AET). This is where the multi-level malware detection features employed by FortiMail excel. On-appliance real-time sandboxing analyzes files for threats and can quickly identify candidates for further consideration. Previously this may have required manual inspection however, now this can be automated using FortiSandbox.

Advanced Threat Protection

FortiSandbox is an advanced threat protection detection solution designed to identify the highly targeted and tailored attacks that increasingly bypass traditional defenses and lurk within networks. It replicates and runs the malicious code as though it were running in the customer environment. Benefits of a multi-level email threat prevention system include:

Examines activity, rather than attributes

By executing objects within its secure virtual runtime environment, the sandbox can analyze activity — system changes, exploit efforts, site visits, subsequent downloads, botnet communications and more — to expose sophisticated threats.

Inspects across all operating environments

Code emulation examines and runs instruction sets to assess intended activity independent of operating environment for broader security coverage.

Pre-filters to reduce load and latency

Leverage Fortinet's top-rated, proactive antimalware and other threat intelligence to detect some previously unknown threats without the time and effort of full "sandboxing".

Provides rich threat intelligence

Uncover information related to the full threat lifecycle, not just initial code, to speed remediation. Optionally submit information to FortiGuard Labs for automated prevention updates.

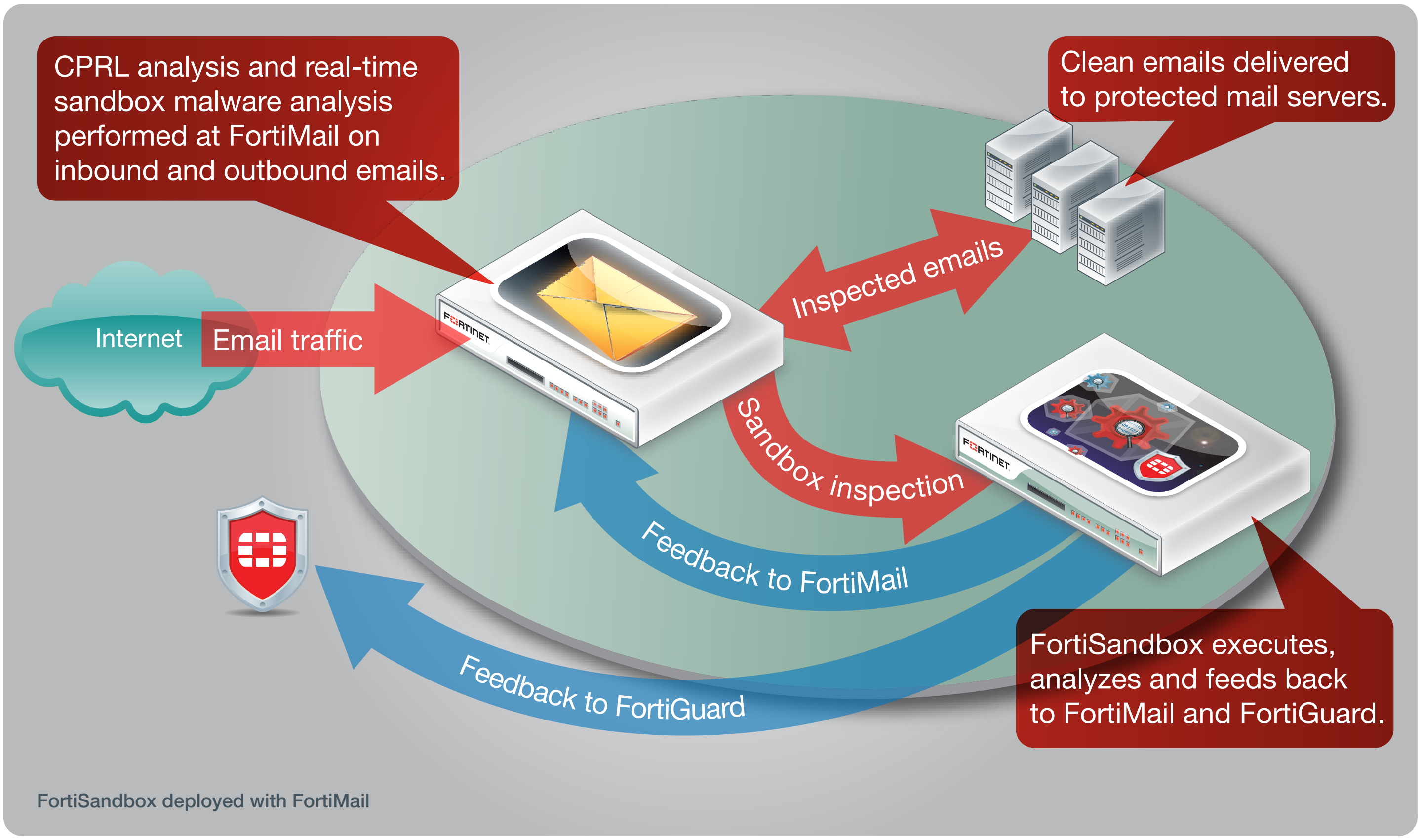
FortiMail/FortiSandbox Integration

Fortinet is at the forefront of threat research and protection, and email security is core to that research. FortiMail has been fully integrated into the FortiSandbox advanced threat protection solution to protect users from targeted attack. FortiMail inspects attachments, looking for unusual files that may have not triggered malware signatures and submits them for behavioural analysis by FortiSandbox. In the latest FortiMail release (5.2), emails are queued while they are evaluated by FortiSandbox, which makes the decision whether they should be quarantined or released.

FortiSandbox is integrated with the FortiGuard Threat Intelligence and Research Network. Threat details are fed back to the threat research team so that detection signatures can be created, allowing threats to be mitigated against rapidly at the first line of defence, reducing the load on the FortiSandbox infrastructure.

Conclusion

Email will be a popular threat vector for many years to come. This is because there is a wide range of skill levels of email users, and many can be tricked into executing malicious code. In order to make their attacks successful, malware


CPRL analysis and real-time sandbox malware analysis performed at FortiMail on inbound and outbound emails.
Clean emails delivered to protected mail servers.
Internet
Email traffic
Inspected emails
Sandbox inspection
Feedback to FortiMail
Feedback to FortiGuard
FortiSandbox executes, analyzes and feeds back to FortiMail and FortiGuard.

FortiSandbox deployed with FortiMail

writers are using custom-developed, targeted attacks or APTs. They can evade straightforward detection, using previously unseen (or "zero-day") malware, exploit vulnerabilities (unpatched security holes) and come from brand-new or seemingly innocent hosting URLs and IPs. Their goal is to compromise their target system with advanced code techniques that attempt to circumvent security barriers and stay under the radar as long as possible.

FortiSandbox complements your established FortiMail defenses with the cutting-edge capability to analyze files in a contained environment to identify previously unknown threats and uncover the full attack lifecycle. Rich threat intelligence, actionable insight and the option to share information with FortiGuard Labs in order to receive automated protection updates help organizations reduce the risk of compromise against targeted attack.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480