

## **Fortinet FortiSandbox Catches Zero-Day and Advanced Threats Hidden in IE, MS Office Files, PDFs, Web Page URLs, Zip files and Network File Share Locations**

*Further Strengthens FortiGate and FortiMail with New Integrated Capabilities as part of Fortinet's broader Advanced Threat Protection Framework*

Fortinet® – a global leader in high-performance cyber security – recently announced the launch of FortiSandbox 2.0, delivering enhanced features to their top-rated FortiSandbox Advanced Threat Detection Appliances and FortiSandbox Cloud solutions with the power to discover and isolate more advanced threats from more places than ever before. Integrated with FortiGate, FortiSandbox Cloud offers the ability to quarantine compromised users and end points with one-click, delivering additional mitigation against zero-day and advanced threats. When used together with FortiMail, previously unknown email threats are proactively and automatically blocked. FortiSandbox 2.0 combined with Fortinet's Advanced Threat Protection (ATP) Framework ensures a new level of protection from sophisticated cyber threats.

### **Protection from Advanced Threats**

In today's cybersecurity landscape, what you can't detect can hurt you; with highly targeted and tailored attacks increasingly bypassing traditional security defences disguised as innocuous files constantly exchanged in an organization's day-to-day workflow.

Combating these advanced threats, Fortinet's FortiSandbox enhances its independently rated and NSS Labs Recommended 99% breach detection rating with new features that scan more file types including Microsoft Office, PDFs, Internet Explorer, web URLs, shared file repositories and can even unzip and scan archived files so IT departments have confidence that they are protected from malicious code no matter where it tries to hide.

"The number one most exploited vector for attacks within an enterprise has consistently been through an organizational emails."

Said John Maddison, Vice President, Marketing Products at Fortinet. “Our updated FortiSandbox 2.0 and overhauled Advanced Threat Protection Framework were engineered to shine a light on the dark places, like emails and attached documents, where many other security solutions just can’t see. This provides Fortinet customers with the piece of mind that they are protected from the most nefarious threats out there.”

At the same time, procurement and legal departments are assured of license compliance based on Genuine Microsoft Windows and Office licenses that ship with every appliance. FortiSandbox with FortiGate or FortiMail reports the who, when, and where on malicious and suspicious files and makes it easy to block or quarantine any incursion, taking advanced threat protection a step further than just threat detection.

### **Flexible Deployment**

FortiSandbox advanced threat protection is available as physical, virtual and new add-on cloud solutions so customers have the flexibility to select a deployment mix that fits their needs, while seamlessly integrating with existing FortiGate and FortiMail infrastructure to deliver an advanced integrated security solution without the complexity and cost.

### **A Constantly Evolving Framework of Protection**

Part of Fortinet’s newly enhanced Advanced Threat Protection (ATP) Framework, FortiSandbox seamlessly integrates with Fortinet’s FortiGate firewall appliances and FortiMail email security platforms, all backed by the industry-leading FortiGuard threat research lab; delivering continuous and automatic updates with immediate protection against the latest threats whenever they arise. The combination of Fortinet’s Prevent, Detect and Mitigate approach to advanced threats enables organizations to stop known threats before they infect the infrastructure, discover new threats and then learns to continually evolve and deliver enhanced threat prevention.

### **Breaking The Kill Chain**

Say a malicious email is sent to someone in the network that protected by Fortinet ATP framework featuring FortiGate firewalls, FortiMail email security and FortiSandbox. FortiGate reroutes file elements within the email to FortiSandbox for analysis, while FortiMail automatically holds the offending mail until it can be confirmed clear of malicious intent. If that email is found to contain nefarious elements, FortiMail will block the email and FortiSandbox uploads the data from its analysis to FortiGuard, which then triggers an automatic update to the entire Fortinet security ecosystem across the globe.

That is just one example. Fortinet's integrated approach to Zero-day and advanced threat protection delivers seamless security designed to break the kill chain in a way that individual standalone solutions never could.