November 19, 2013

Fortinet(R) Introduces New Advanced Threat Detection & Mitigation Sandbox to Strengthen Enterprise Edge

New Appliance Extends Fortinet's Next Generation Firewalls and Email Gateways to Address Advanced Persistent Threats

SUNNYVALE, CA -- (Marketwired) -- 11/19/13 -- Fortinet® (NASDAQ: FTNT) -- a global leader in high-performance network security -- today announced the FortiSandbox-3000D, an advanced threat prevention appliance that provides enterprises with a powerful tool to help combat Advanced Persistent Threats (APTs). The new offering combines a unique dual-level sandbox, dynamic threat intelligence, real-time dashboard and rich reporting in a single device that integrates with Fortinet's FortiGate next generation firewalls (NGFW) and FortiMail email gateway appliances.

Fortinet NGFWs act as a first line of defense by scanning and mitigating threats. When used with FortiSandbox, the appliances together are able to identify and apply advanced inspection to suspicious or high risk files and then update protections based on the full threat lifecycle of attacks uncovered. And with the new FortiMail version 5.1, Fortinet email gateways can now similarly identify suspicious or high risk files in email and pass them to FortiSandbox for advanced inspection.

FortiSandbox At-a-Glance
The FortiSandbox-3000D can be deployed on-premise on its own without changing any network configurations. Or, as mentioned, it can also be integrated with and extend Fortinet's FortiGate and FortiMail platforms for improved detection and mitigation.

Consistent with Fortinet's product development approach, the FortiSandbox consolidates specialized threat detection and intelligence services across protocols and functions into a single, high-performance and highly affordable appliance. At the heart of the appliance is a dual-level sandbox to effectively deal with increasing virtual machine (VM) evasion techniques and the increasing sophistication of attacks that require more advanced inspection.

"Today's most sophisticated attackers are increasingly bypassing traditional anti-malware solutions and establishing a persistent presence within organizations' networks," said John Grady, Research Manager, Security Products at IDC. "These highly targeted attacks evade signature-based defenses by leveraging compression, encryption, and polymorphism among other methods. Some malware variants are even able to detect virtual environments and utilize sleep techniques to make identification much more difficult. Combating today's attacks requires a comprehensive and integrated approach that goes beyond anti-malware, virtual sandboxes and separate monitoring systems. The FortiSandbox appliance is a step in this direction."

Key features of FortiSandbox include:

- ***Dynamic Antimalware and Updates/Cloud Query:*** Receives updates from FortiGuard Labs and can send queries back to the Labs in real time, helping to intelligently and immediately detect existing and emerging threats
- ***Code Emulation:*** Performs lightweight sandbox inspection in real time, including certain malware that uses sandbox evasion techniques and/or only executes with specific software versions
- ***Full Virtual Environment:*** Provides a contained runtime environment to analyze high risk or suspicious code and explore the full threat lifecycle
- ***Advanced Visibility:*** Delivers comprehensive views into a wide range of network, system and file activity, categorized by risk, to help speed incident response
- ***Callback Detection:*** Inspects network traffic for requests to visit malicious sites, establish communications with C&C servers and other activity indicative of a compromise
- ***Manual Analysis:*** Allows security administrators to manually upload malware samples to perform virtual sandboxing without the need for a separate appliance
- ***Optional Submission to FortiGuard:*** Tracer reports, malicious files and other information may be submitted to FortiGuard Labs in order to receive remediation recommendations and updated in line protections

"The introduction of the FortiSandbox appliance is in direct response to APTs that are using highly sophisticated evasion techniques to avoid security detection," said John Maddison, vice president of Marketing for Fortinet. "Given our many years of threat research and development, we're finding that inspection of file activity, as a complement to inspection based on attributes, is a necessary means of combating APTs. Our customers now have the opportunity to easily and cost-effectively perform detailed analysis of specific threats traversing their networks with the added benefit of integrating with our FortiGate and FortiMail appliances to perform in line, real-time threat mitigation."

Availability
The FortiSandbox-3000D is available now.

Follow Fortinet Online:
Twitter at: www.twitter.com/fortinet
Facebook at: www.facebook.com/fortinet
YouTube at: http://www.youtube.com/user/SecureNetworks
LinkedIn at: http://www.linkedin.com/company/fortinet
G+ at: https://plus.google.com/+fortinet

About Fortinet
Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com.

FTNT-O

Media Contact:
Rick Popko
Fortinet, Inc.
408-486-7853
rpopko@fortinet.com

Investor Contact:
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Source: Fortinet

News Provided by Acquire Media