Fortinet Delivers Third Generation of Network Security with the Evolution of its Security Fabric

FortiOS 6.0 delivers more than 200 new capabilities across Security Fabric to automate security operations and protect the digital attack surface

Michael Xie, founder, president and chief technology officer at Fortinet
"Digital transformation is creating new operating and service delivery models that provide undeniable value to users through technologies such as IoT, mobile computing and cloud-based services, generating a vast digital attack surface. As the speed and scale of cyber threats expands, security must take on its own transformation by integrating into all areas of digital technology and be able to translate user intent into automated business response. FortiOS 6.0 delivers hundreds of new features and capabilities that were designed to provide the broad visibility, integrated threat intelligence and automated response required for digital business."

News Summary
Fortinet (NASDAQ: FTNT), a global leader in broad, integrated and automated cybersecurity solutions, today announced at its global partner and user conference, Accelerate 18, the evolution of its Security Fabric architecture with the release of FortiOS 6.0, the world's most deployed network security operating system. With more than 200 new features and capabilities, enterprises will benefit from new levels of security operations automation and advanced protections for their expanding digital attack surfaces.

- Fortinet introduces new security capabilities across the key solution areas within its Security Fabric architecture, including management and analytics, multi-cloud, network, advanced threat protection, unified access, web applications, email, IoT and endpoint security.
- Industry-leading secure SD-WAN functionality, threat detection services, and expanded visibility from IoT to multi-cloud networks protect the vast attack surface resulting from digital transformation (DX) strategies.
- New automated lifecycle workflows, attack surface hardening services, with customized ranking and industry benchmarking, deliver the next level of NOC/SOC management.
- Business, network and entity level tagging functionality enable business precise segmentation, providing the critical building blocks for intent-based network security.

Broad Visibility, Integrated Detection and Automated Response
According to a Gartner survey, in EMEA, 47 percent of the CIO respondents have a dedicated digital business team. It also revealed that few of these teams (16 percent) are made up of IT associates only. "While IT delivery is still a responsibility of the CIO, achieving revenue growth and developing digital transformation were identified most often as top business priorities for organizations in 2018," according to Gartner.*

As companies look to transform everything from their business operating models to service delivery methods, they are adopting technologies such as mobile computing, IoT and multi-cloud networks to achieve business agility, automation and scale. The increasing digital connectedness of organizations is driving the requirement for a security transformation, where security is integrated into applications, devices, and cloud networks to protect business data spread across these complex environments.

The Fortinet Security Fabric is an integrated and automated security framework designed to protect today's dynamic networks. It provides the broad visibility, integrated detection of advanced threats, and automated response, combined with the continuous trust assessment required to secure today's digital business.

Available in Q1 2018, the FortiOS 6.0 release provides critical capabilities required to secure the digital attack surface spurred by digital transformation. Some key new features and capabilities across the Security Fabric solution areas include:

Network Security:

- Enhanced SD-WAN path controller measures application transactions for business-critical applications. These granular transactions are key in achieving better application performance for SaaS, VoIP and other business applications with built-in automated fail-over capabilities. New one-touch VPN and zero-touch deployment further reduce complexity and rapidly enable enterprise branches.

Multi-Cloud Security:

- Expanded Cloud Connectors within the Security Fabric now include visibility of multiple clouds, spanning private cloud connectors (support for VMware NSX, Cisco ACI and Nokia Nuage), public cloud connectors (support for AWS, Microsoft Azure, Google Cloud Platform, and Oracle Cloud), and SaaS clouds with CASB connectors (support for Salesforce.com, Office 365, Dropbox, Box, AWS and more). These Cloud Connectors enable organizations to have complete visibility of their security posture across all cloud networks to correlate both on and off network traffic through a unified security management console.
- FortiCASB 1.2 delivers Fabric integration with AV and ForitCloud Sandbox, extended protection and detection capabilities, as well as shadow IT discovery reporting. Additionally, FortiCASB offers expanded support for AWS to provide advanced compliance, reporting and analysis tools for enhanced visibility and control for AWS users.

IoT Endpoint Security:

- FortiClient 6.0 will include expanded operating system support for Linux, sharing actionable insight about these systems with the Security Fabric. FortiClient will also provide richer intelligence about all types of endpoints, including the application inventory on each device.
- A new Fabric Agent can send telemetry data from the endpoint to the Security Fabric for deeper insight on what is running on a network's endpoint devices and quickly identify vulnerabilities. It is also certified compatible to work with a range of Fabric-Ready endpoint security partners.

Advanced Threat Protection (ATP):

- GDPR regulations in May 2018 will further increase regulatory mandates on global businesses, making automated audit best practices across an enterprise's security network critical. The new FortiGuard Security Rating Service provides expanded audit rules, customized auditing based on network environments, and on-demand regulatory and compliance reports.
- New FortiGuard Virus Outbreak Service (VOS) closes the gap between antivirus updates with FortiCloud Sandbox analysis to detect and stop malware threats discovered between signature updates before they can spread throughout an organization.
- New FortiGuard Content Disarm and Reconstruction Service (CDR) proactively strips potentially malicious content embedded in Microsoft Office and Adobe files to sanitize the most common file formats used to spread malware and help close the opportunity for infection from social engineering or human error.
- New FortiGuard Indicators of Compromise (IOC) Service uses a continuously updated list of known bad elements and scans devices connected to the Security Fabric to identify compromised devices for immediate action.
- FortiSandbox ATP for Amazon Web Services, available as on-demand and BYOL, allows organizations to defend against advanced threats natively in the cloud, working alongside network, email, endpoint and other security, or as an extension to their on-premises secure architecture.

Email & Web Applications:

- FortiMail now supports the new FortiGuard VOS and CDR Services. These new services prevent the spread of fast emerging attacks and extract active content to thwart attacks using embedded code execution.
- New widgets provide a comprehensive, centralized view of all email and web applications on a network, with advanced threat protection integrated into the apps within the Fabric.

Security Management & Analytics:

- New Incident Response (IR) lifecycle capabilities across the Security Fabric allow users to automate responses based either on predefined triggers (system events, threat alerts, user and device status) or through direct ITSM integration. Response methods such as quarantine, notifications, configuration adjustments, and custom reports provide organizations with real-time control of their workflow environments.
- Automated attack surface hardening feature provides recommendations and trending data on security compliance and best practice adoption, with benchmarking that ranks

organizations against similar firms in terms of size, industry and region.

Unified Access:

- With FortiOS 6.0, integrated security in Fortinet switches and wireless access points enables automation of security response to events, such as quarantine, segment or block, when an infected switch or access point is in violation of a configured policy.

Business Precise Segmentation Delivers Foundation for Intent-Based Network Security

Fortinet introduces business precise segmentation through tagging, delivering the building blocks enterprises need to move towards intent-based network security. Organizations can tag devices, interfaces and objects at the business, entity, and network level and set global policies for automatic enforcement when new objects are created on the network. This level of tagging is foundational to intent-based network security architecture as it enables business precise segmentation, automated management and control of all network elements.

Supporting Quotes

"We know our customers demand reliability, speed and a high level of service. We chose Fortinet in our move to an SD-WAN based network because of their combination of cutting-edge networking capabilities and world-class security, all through one management interface for both LAN access and SD-WAN. And most importantly, with Fortinet's Security Fabric, we know we'll stay protected against evolving security risks from the local area network to the cloud, thanks to proactive threat detection and mitigation. With Fortinet as our partner and its commitment to security innovation as demonstrated with its FortiOS 6.0 release, we know we'll have secure power for today and be powerful enough for tomorrow."
- Jonathan Merrell, chief information officer at Alorica

"Our customers' already find managing their IT environments a challenge. With deployment of multi-cloud environments, technologies like SD-WAN making waves in the industry, and the influx of IoT devices onto corporate networks, the task of management is only increasing in complexity. Ensuring consistent visibility, effective control, and seamless management across these ever-expanding environments has become a top priority for many IT leaders. Fortinet is a leader in the security space, and a trusted partner, who brings a high level of value to the equation with their unique Security Fabric Architecture approach; an architecture which allows for unification of management panes, and integration into not just Fortinet technology, but third party technologies as well. With their latest release of FortiOS 6.0, we can now more effectively meet the evolving demands of our customer base, by providing technologies that enable more advanced, integrated and certainly automated security capabilities into their dynamic environments."
- Josh King, director of Security Solutions at Carousel Industries

"Using a single partner for integrated protection across multiple threat vectors, from public cloud workloads to email SaaS applications, is a key priority for ShipServ. Fortinet is an all-in-one cyber security company with a common, intuitive security management interface across all the Fortinet Security Fabric solutions, making it much easier to support. Protecting a hybrid cloud and on-premise environment can be very complex and we couldn't achieve this level of integrated, automated security without the Fortinet Security Fabric solutions we've implemented."
- Dominic Aslan, vice president of IT operations at ShipServ

*Gartner Press Release, "Gartner Survey Shows Digital Business Is Turning CIOs Into Business Leaders," 7 November 2017. https://www.gartner.com/newsroom/id/3824763.