Introducing FortiOS™ 6.0

Driving Security Transformation to Integrate Across All Areas of Digital Technology

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.

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.

Broad Visibility

Visibility and protection need to extend across the entire digital attack surface to encompass and unify physical networks, IoT, mobile devices and users, and increasingly complex multi-cloud environments. The Fortinet Security Farbic provides IT teams a holistic view into devices, traffic, applications, and events and the ability to stop a threat anywhere along its attack chain.

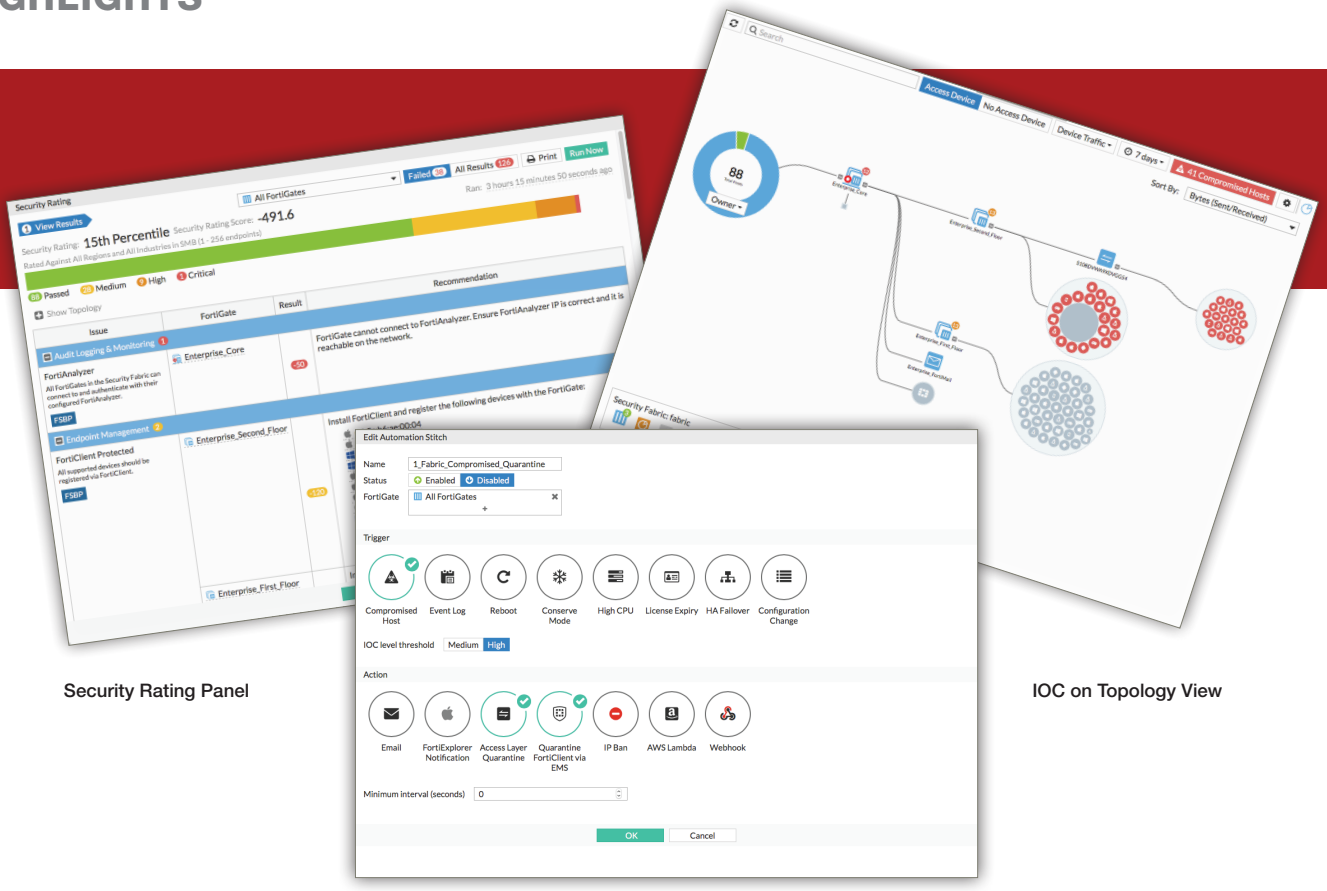
Integrated Threat Intelligence

The integration of devices using open standards, common operating systems, and unified management platforms enables the sharing and correlation of real-time threat intelligence. The Fortinet Security Fabric also supports the coordinated detection of advanced threats through sophisticated, centralized analytics that are difficult or impossible to achieve using traditionally isolated security deployments.

Automated Response

Like today's digital business, cyber crime happens at digital speeds. The latest Fortinet Security Fabric automatically provides continuous trust assessment and then provides an immediate, coordinated response to detected threats. And because these network environments are highly elastic, it is also able to dynamically adapt as requirements and configurations change.

HIGHLIGHTS



Security Rating Panel

IOC on Topology View

Configuring Automation

What's New - Key Features

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:

- Multi-path intelligence for SD-WAN
- Asset tagging
- FortiCASB integration
- Multi-cloud support with SDN connectors
- FortiClient Support For Linux
- New FortiGuard services
- Indicator of compromise (IOC) quarantine and IP ban
- FortiMail and FortiWeb feature enhancements
- Administrator-defined automation
- Automated security audits and expanded audit rules

HIGHLIGHTS

Network Security

An 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 business applications with built-in automated failover capabilities. New one-touch VPN and zero-touch deployment further reduce complexity and rapidly enable new enterprise branches.

Fortinet also introduces business precise segmentation through tagging, delivering the building blocks enterprises need to move toward 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.

Multi-Cloud Security

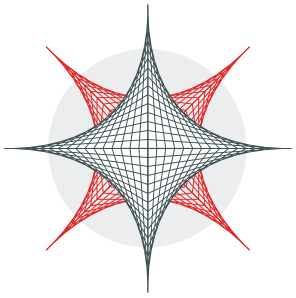
Expanded cloud connectors within the Security Fabric now provide visibility of multiple clouds, spanning private, Infrastructure-as-a-Service (IaaS), and native cloud controls. Enhanced FortiCASB (cloud access security broker) integration offers visibility and advanced threat protection of Software-as-a-Service (SaaS) applications. This enables organizations to have a complete view of their security posture across all cloud networks to correlate both on- and off-network traffic through a unified security management console.

FortiCASB delivers Security Fabric integration with AV and FortiCloud Sandbox, expanded shadow IT discovery reporting, support for AWS to provide advanced compliance, reporting and analysis tools for enhanced visibility and control for AWS users.

IoT-Endpoint Security

Continuous endpoint visibility, compliance, and control strengthen organizations' overall security posture. FortiClient Fabric Agent sends telemetry from endpoints to the Security Fabric, providing deep insight on what is running on the devices, user ID, compliance status, and vulnerabilities. It is certified compatible to work with a range of Fabric-Ready endpoint security solutions.

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.



FORTINET SECURITY FABRIC

HIGHLIGHTS

Advanced Threat Protection (ATP)

GDPR regulations in May 2018 will further increase 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 Protection 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.

Secure Unified Access

Integrated security in Fortinet switches and wireless access points enables automation of security response to events. These automated responses enable a quick response, such as quarantine, when an infected device connects to a switch or access point.

Email & Web Applications Security

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.

Management & Analytics

New automated workflow capabilities with continuous risk assessment across the Security Fabric allow users to set responses based on predefined triggers, such as system events, threat alerts, user and device status. Response methods such as quarantine, notifications, configuration adjustments, and custom reports provide organizations with real-time control of their workflow environments.

The automated auditing feature provides trending data on a business' security compliance posture with benchmarking that ranks organizations against similar firms in terms of size and industry.

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: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-PB-FOS6

FOS6-PB-R1-201802