WHAT'S NEW IN FORTIOS 6.0?

With over 200 new features, the FortiOS 6.0 release is a massive step forward in security, and as the world's most deployed network security operating system, is sure to make the world a safer place.

More than a firewall operating system, FortiOS enables broad connectivity and awareness among security components, both within the network and from other disciplines, such as endpoint, management, and analytics. This security ecosystem made possible by FortiOS is the Fortinet Security Fabric. The Security Fabric is the cornerstone of third-generation network security, realizing the vision today of a broad, integrated, and automated security ecosystem. FortiOS 6.0 goes a long way to further enable this vision.

SECURITY FABRIC

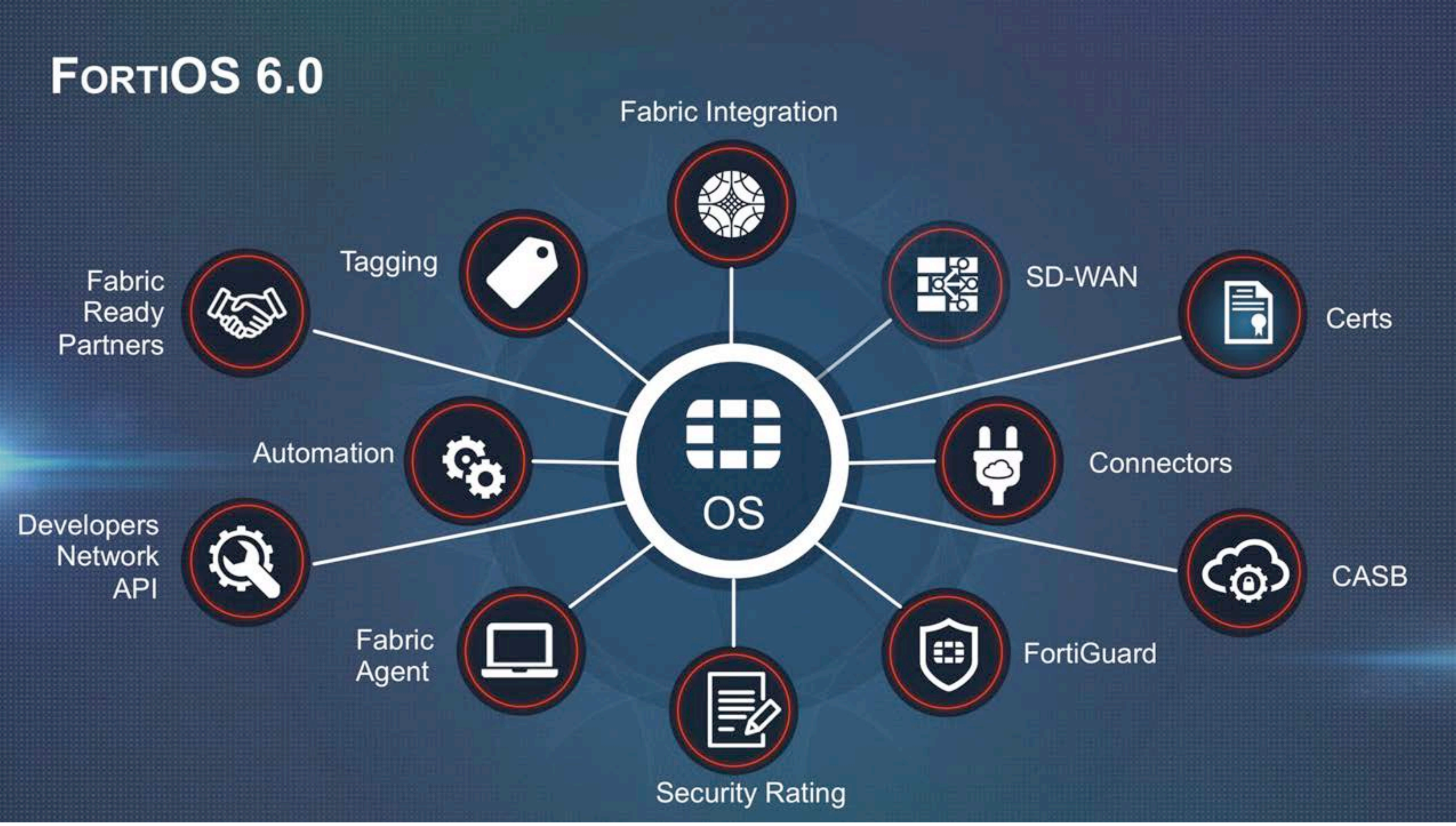
The Fortinet Security Fabric is broad because it extends beyond the boundaries of firewalls and even network security. Already marshalling the resources of switches and wireless access points to further extend control possible with network security, FortiOS 6.0 improves that footprint, extending into email gateway security, WAN optimization, and web content caching, coordinating and enhancing both awareness and control.

Working hand-in-hand with a broad reach, the ability to interact and control is made possible through integration. Unlike primitive integrations that can only copy and display data available in other places, the Security Fabric enables adjustment and reconfiguration. It is a deeper level of integration that makes extending security control a reality.

With that deep level of integration, the Security Fabric unlocks authentic automation across a broad infrastructure. More than pre-programmed reactions within a single product, Security Fabric automation crosses both product and vendor boundaries, such as raising incidents and processing change requests from the same third-party service management systems.

HEART OF THE FORTIOS 6.0 RELEASE

FortiOS has been the heart of FortiGate next-generation firewalls for years now, serving thousands of customers in every industry across the globe. The needs of this diverse customer base are widespread and not every one of the more than 200 new features and capabilities will be interesting to all customers; however, there are a few clear themes that organize most of the 6.0 development. Beyond its mission of enabling the Fortinet Security Fabric, FortiOS 6.0 makes significant gains in three areas: third-generation network security, SD-WAN, and Fabric integration that unlocks automation.



THIRD-GENERATION NETWORK SECURITY

With most people using multiple devices, the attack surface continues to grow and become increasingly complex. This alone is sufficient to require new approaches and new solutions, but on top of this, resources are constrained and security talent is running short. The visibility and detection capabilities of traditional network security are being stretched beyond their abilities, and that is exactly where FortiOS 6.0 comes in.

The third generation of network security is a connected and aware architecture. The Security Fabric forms the base of this architecture, but a deliberate focus on security visibility is a big component of FortiOS 6.0. The complexity of the modern attack surface is greatly tempered with the third generation of visibility and context now available from Fortinet.

Asset tagging is one of the new ways to cross silos and cut through the noise. FortiOS 6.0 now allows you to tag devices, interfaces, and objects with business context, so you can logically manage the traffic, despite the tempest of change at the physical layer. Additionally, new services are available to simplify security assessment, such as a list of compromised hosts from the Indicators of Compromise (IOC) service, automatic removal of malicious scripts in files from the Content Disarm & Reconstruction service, near-instantaneous intelligence updates to protect against emerging malware in seconds, and assessment of your security posture against similar organizations.

THIRD-GENERATION NETWORK SECURITY FEATURES

- Tagging
- Security Rating
- FortiGuard Services
  - Virus Outbreak Service
  - Content Disarm & Reconstruction Service
  - IOC service evolution
  - Audit DB

SD-WAN

Software-Defined Wide Area Networks (SD-WAN) in branch sites is one of the fastest growing areas in networking and with the FortiOS 6.0 release, Fortinet has a world-class SD-WAN solution, delivering on the promise of broad-reaching solutions.

Branch offices continue to demand more network capacity, but the backhaul links that ensure performance, control, and security of branch office traffic are becoming cost prohibitive. Looking for alternative networking solutions, organizations are adopting multiple less expensive Internet links per site, positioning SD-WAN to ensure application performance across these multiple, less reliable links. The problem is that much of the security capability for the branch was served up through the backhaul and cutting the proverbial backhaul strings has also circumvented this protection.

Fortunately, Fortinet brings back world-class network security to the branch office. FortiGate SD-WAN was born in security and offers the same capability and sophistication available in the data center and other sensitive sites. FortiOS 6.0 includes an enhanced SD-WAN path controller with SLA controls to measure application transactions, ensuring critical applications travel on the best of the multiple branch links at every instance. While familiar FortiGate capabilities secure branch traffic, these new SD-WAN features, with automated fail-over capabilities, ensure performance for SaaS, VoIP, and critical business applications. Zero-touch deployment and one-touch VPN further reduce complexity in branch setup and support.

SD-WAN FEATURES

- World-class security
- Multi-path intelligence
- Application SLAs
- One-click VPN
- SD-WAN traffic shaping

FABRIC INTEGRATION UNLOCKS AUTOMATION

While digital transformation seems to greatly benefit most organizations' businesses, it also tends to shift more of the business and more of the risk to IT. This means a larger and more complex network to manage, more infrastructure to architect, and more assets to protect – more work for everyone. However, budgets do not seem to grow at the same pace as the new work proliferates. FortiOS 6.0 tackles this challenge by automating processes that are tightly integrated together.

Without meaning integration – integration on the control plane – automation is not a scalable possibility. FortiOS 6.0 employs deep integration to unlock meaningful automation. Automating processes saves time, frees up precious resources, and improves security posture.

FortiOS 6.0 includes some new integrations, including Fabric inclusion of FortiMail (email gateway), expanding local caching capacity seamlessly with FortiCache and a new CASB product. However, meaningful automation comes from a new User-Defined Automation feature, where threat alerts, system events, user or device status, and other external inputs form triggers. When these triggers are activated, immediate action takes place in the form of quarantines, configuration changes, reports, or other notifications. In this way, security processes are automated, saving time, freeing up resources, and greatly improving security posture.

INTEGRATION AND AUTOMATION FEATURES

- User-Defined Automation
- FortiCASB
- FortiMail
- Fabric Agent
- Caching storage (FortiCache)

OTHER NOTABLE FORTIOS 6.0 FEATURES

Details on each of the following features is available in the FortiOS 6.0 release notes	
Additional Security Rating tests and rules	SD-WAN IPv6 support
Automated daily reports	SD-WAN DSCP match
Automated on-demand reports	SDN connectors
Security Rating widget	Cloud-init on Azure
FortiClient is compliant when managed by EMS	IPv6 enhancements
Wireless user quarantine	NAT improvements
Audit DB service	EMAC-VLAN support
Specialized C-level and auditor reports (FortiAnalyzer)	Application group policy objects
Additional monitoring widgets (FortiAnalyzer)	Application control rule sequencing
Historical FortiView (FortiCloud)	External web filter blacklists
Device detection through FortiSwitch	Improved VM utilization of CPU cores
Destination name resolution	VM configurable interrupt affinity and packet distribution
SD-WAN dynamic routing	Improved API for Developers Network