FORTINET

360 Protection Bundle

Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support

Executive Summary

The growth of technologies such as public and private clouds, software-defined wide-area networks (SD-WAN), and DevOps have resulted in increasingly complex IT networks at almost every organization. At the same time, cybersecurity threats have become more sophisticated and fast-moving. The Fortinet 360 Protection Bundle helps companies of all sizes address these challenges by providing a comprehensive set of security and operational services through a cloud platform.

The 360 Protection Bundle addresses three key use cases for network and security teams: (1) cloud-based, single-pane-of-glass management; (2) risk-based analytics, orchestration, and automation; (3) comprehensive FortiCare ASE Support. Organizations leveraging the 360 Protection Bundle have the network and security tools to fully implement Fortinet recommended best practices, regardless of the size of the company or security staff. They also see reduced risk, increased efficiency and productivity, and lower total cost of ownership (TCO).

> 90% of organizations experienced disclosures of sensitive data in the past year, with 41% reporting 5 or more.[4]

Organizations of all sizes are delivering greater business agility, improved performance, increased efficiency, and cost savings through the strategic use of cutting-edge technology. For example, public and private clouds, SD-WAN, and DevOps processes are transforming the marketplace and promoting business growth across many industries.

While their benefits are undeniable, such innovations also bring greatly increased network complexity, which in turn introduces new security issues. An organization's data, applications, and network traffic are no longer confined to the corporate data center, where a perimeter-based approach could provide protection. Instead, the attack surface has dramatically expanded to the edges of the network. This makes it more difficult to protect against malicious threats.

At the same time, the threat landscape is becoming more complex, with increasingly sophisticated attacks occurring more frequently and moving at machine speed. One example: in the fourth quarter of 2018, FortiGuard Labs detected nearly 34,000 new malware variants—a 128% increase over the first quarter of the same year.[1] Part of this problem is tied to zero-day attacks, which are becoming more common—75% of unknown malware detected by FortiSandbox was not found on the VirusTotal tool, which aggregates information from 50 different antivirus vendors.[2] And these attacks affect organizations of all sizes, with small and midsize businesses now comprising 58% of data breach victims.[3]
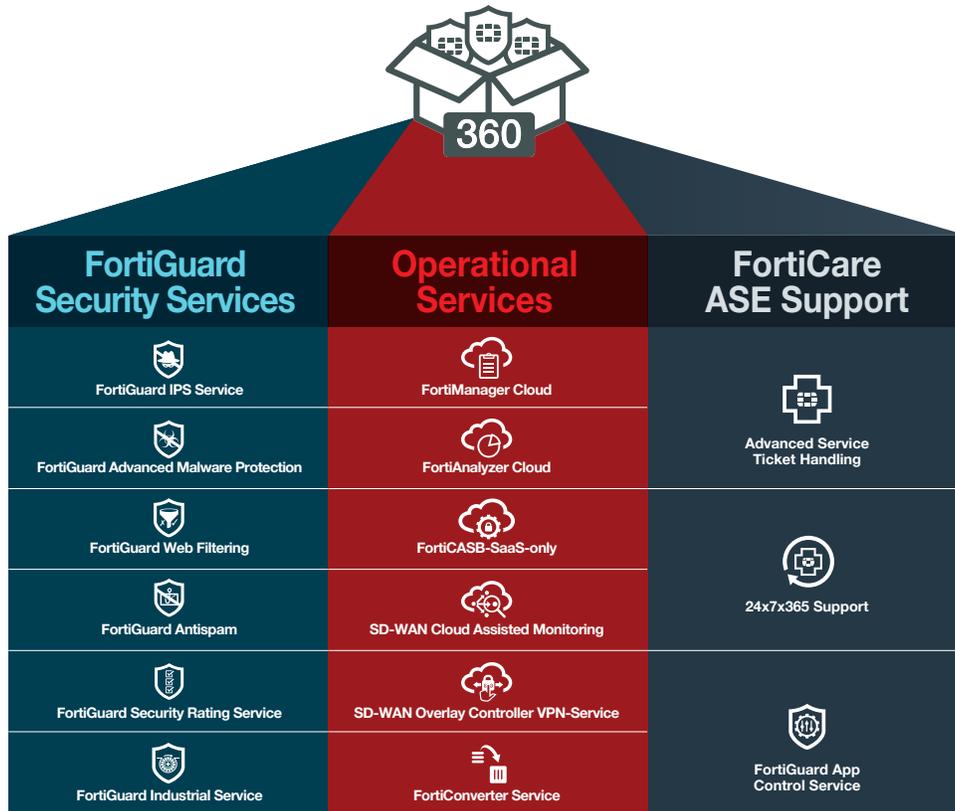
Optimizing Network Management with the 360 Protection Bundle

The 360 Protection Bundle from Fortinet includes operational services via cloud-based, real-time, single-pane-of-glass management and analytics.

The 360 Protection Bundle also includes a complete set of security services from Fortinet, including robust and complete advanced malware protection, an intrusion prevention system (IPS), and a security rating service. Also included are services to help protect SD-WAN infrastructure, virtual private network (VPN) systems, and industrial control systems (ICS).

This, along with the FortiCare ASE Support included in the bundle, provides a comprehensive toolset that enables organizations of any size to follow the best practices for operations and security recommended by Fortinet—all without adding staff.

FortiGuard Security Services	Operational Services	FortiCare ASE Support
FortiGuard IPS Service	FortiManager Cloud	
FortiGuard Advanced Malware Protection	FortiAnalyzer Cloud	Advanced Service Ticket Handling
FortiGuard Web Filtering	FortiCASB-SaaS-only	
FortiGuard Antispam	SD-WAN Cloud Assisted Monitoring	24x7x365 Support
FortiGuard Security Rating Service	SD-WAN Overlay Controller VPN-Service	
FortiGuard Industrial Service	FortiConverter Service	FortiGuard App Control Service

The 360 Protection Bundle includes real-time network management, comprehensive security and operational services, and advanced support.

Fulfilling Key Use Cases

The 360 Protection Bundle helps organizations address the complexity of their distributed networks and the increasingly sophisticated nature of threats by supporting three critical use cases for network security teams:

1. **Cloud-based, single-pane-of-glass management.** As the attack surface has broadened, organizations have added a variety of point solutions to fill the resulting security gaps. In many instances, this has resulted in a siloed security architecture that makes it almost impossible to produce a single, enterprise view of an organization's security posture. Managing all these solutions is also difficult, especially given the cybersecurity skills shortage.[5]

The FortiGate 360 Protection Bundle includes FortiManager-Cloud and FortiAnalyzer-Cloud, which enables organizations to leverage centralized management and analytics tools for the entire Fortinet Security Fabric—all from a cloud-based platform. Fabric-enabled devices are visible from a single pane of glass—whether they are at headquarters, at branch locations around the world, or mobile.

2. **Risk-based analytics, orchestration, and automation.** Once adversaries have infiltrated a network, they often remain dormant for a long time to avoid detection before moving laterally within the network to exfiltrate sensitive data. New research pegs the cost of cyber crime in 2018 for the typical organization at $13 million—a 12% increase over 2017 and a 72% increase over five years.[6] The same research shows that employees are the most common cause of successful cyberattacks. While some of these attacks are malicious, most are caused by human error.

A fragmented security architecture results in inefficient manual processes that increase the likelihood of human error. This brings heightened risk for even the most common type of breach. The speed of today's advanced threats also means that manual processes are not timely enough to provide adequate protection, with exfiltration of corporate data now happening in minutes in some cases.[7]

Enterprises use an average of 75 security products to secure their networks.[8]

The 360 Protection Bundle supports an integrated security architecture—in the form of the Fortinet Security Fabric—with centralized logging, reporting, and analysis. This enables automation of security processes, comprehensive analysis from a single console, and minimized opportunity for human error.

3. **FortiCare ASE Support.** The cybersecurity skills shortage and increased compliance requirements have increased the demand for security services—whether purchasing solutions from security vendors as a subscription service or leveraging managed security service providers (MSSPs) to supplement in-house staff. Many companies are currently using a hybrid approach, leveraging MSSPs, subscription services, and in-house staff.

In numerous instances, these security services support business-critical infrastructure for which downtime or active cyberattacks could directly impact the bottom line. As a result, when security teams need support, they typically need it immediately. And they need assurance that issues will be resolved in a specific time frame.

This is where FortiCare ASE Support in the 360 Protection Bundle can help. This package provides prioritized, world-class support from trained agents located around the globe—24×7×365. Aggressive service-level agreements (SLAs) ensure that issues are resolved in a timely manner. And in today's world of hybrid security services, FortiCare ASE Support is available to both end-users and MSSPs.

> **60% of cybersecurity and IT professionals say their organizations are at moderate or extreme risk of cybersecurity attacks as a result of the cybersecurity skills shortage.[9]**

Conclusion

To recap, the 360 Protection Bundle supports an integrated security architecture with centralized visibility and control and risk-based analytics. This brings a number of benefits to an organization:

- Risk reduction through automated threat response, improved configurations, and better operations management

- Efficiency and productivity gains through elimination of manual processes and centralized control and analysis

- Lower TCO due to reduced operational glitches and fewer security incidents requiring manual response

The 360 Protection Bundle also provides a comprehensive suite of security services, support for secure SD-WAN networking, and advanced support. This complete protection helps organizations of all sizes manage complexity in their networks and deliver full protection across the entire attack surface.

[1] "Threat Landscape Report Q4 2018," Fortinet, accessed March 12, 2019.

[2] Based on internal data from FortiGuard Labs.

[3] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[4] "The future of cyber survey 2019," Deloitte, accessed March 20, 2019.

[5] "2016 Cybersecurity Skills Gap," ISACA, January 2016.

[6] "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, accessed March 12, 2019.

[7] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[8] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

[9] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

FÜRTINET®