COMPREHENSIVE SECURITY WITH THE FORTIGATE ENTERPRISE PROTECTION BUNDLE

Security Services Bolster Production Against Current and Future Threats

EXECUTIVE SUMMARY

Organizations of all sizes face growing complexity in both networking and the threat landscape. Multi-cloud deployments and Internet-of-Things (IoT) devices expand the attack surface, and disparate point solutions deployed to address new threat vectors often do not integrate with existing infrastructure. This results in both business inefficiency and increased risk.

The FortiGate Enterprise Protection bundle addresses both of these problems by providing the most comprehensive package of security services available in the market today. It covers the areas of protection needed to effectively address the complex and evolving threat landscape—and every cyberattack channel, from the endpoint to the cloud. The Enterprise Protection bundle provides a centralized way to deal with complex risk, compliance, management, and visibility concerns. In sum, the FortiGate Enterprise Protection bundle delivers critical services to protect organizations from current and future cyber threats.

Digital transformation (DX) can bring great benefits to organizations, but it also brings increased complexity to the corporate network—and to network security. DX has exponentially expanded the attack surface. For example, enterprises now use an average of 61 different cloud apps,[1] and a million new IoT devices come online every day.[2] At the same time, the convergence of IT with operational technology (OT) is accelerating,[3] and compliance and risk management are an increasing concern at many enterprises.[4]

Add that threats are becoming more sophisticated, making the challenges facing security leaders even more daunting. For example, in the third quarter of 2018, FortiGuard Labs detected almost 34,000 new malware variants—a 43% increase over the second quarter and a 129% increase over the first quarter.[5] Zero-day attacks are becoming more common, and 75% of unknown malware detected by FortiSandbox was not found on the VirusTotal tool—which aggregates information from 50 different antivirus vendors.[6]

In the third quarter of 2018, FortiGuard Labs detected almost **34,000 new malware variants**—a 43% increase over the second quarter and a 129% increase over the first quarter.[5]

COMPLEXITY BRINGS CHALLENGES

The results of these complexities are concerning. In one survey, the typical organization experienced 20 breaches in the past 24 months—four of which resulted in outages, data loss, or compliance events.[7] 48% of all data breaches are now caused by the hacking of web applications.[8] And 90% of companies with connected OT environments have experienced a security incident.[9]

As organizations respond to these trends, they often unwittingly exacerbate this complexity from a security operations perspective. The average enterprise now manages 75 different security solutions,[10] many of which operate in silos. This increases management overhead and requires a lot of manual work on the part of overstretched cybersecurity staff. Team members find themselves needing to prioritize which threat feeds and logs to review, inevitably enabling vulnerabilities to fall through the cracks. And since 68% of breaches are not discovered for months or longer,[11] cleaning up the damage can often be a major undertaking that distracts cybersecurity personnel from their core responsibilities.

While these challenges are daunting, many of the gaps that enable intrusions and other security incidents involve basic security hygiene. As computer networking becomes more complex, organizations find that keeping up with basic configuration issues is difficult with a disaggregated security architecture. The Online Trust Association finds that 93% of successful cyberattacks could have been prevented if routine scans and patches were implemented.[12] And according to Gartner, "Through 2022, at least 95% of cloud security failures will be the customer's fault."[13]

Clearly, today's widely distributed networks need protection across a broad attack surface—from the endpoint to the cloud, across OT and critical infrastructures, to IoT products and platforms. At the same time, organizations need to consolidate their security tools and services in a manner that delivers real-time updates and proactive protection at machine speed and scale—and with extreme accuracy.

FORTIGATE ENTERPRISE PROTECTION BUNDLE PROVIDES A HOLISTIC SOLUTION

The **FortiGate Enterprise Protection bundle** is a comprehensive, cost-effective solution that consolidates the elements of comprehensive protection needed to address the complex threat landscape, today and in the future. It includes a complete set of foundational security services, plus three critical services not available with other bundles in the market:

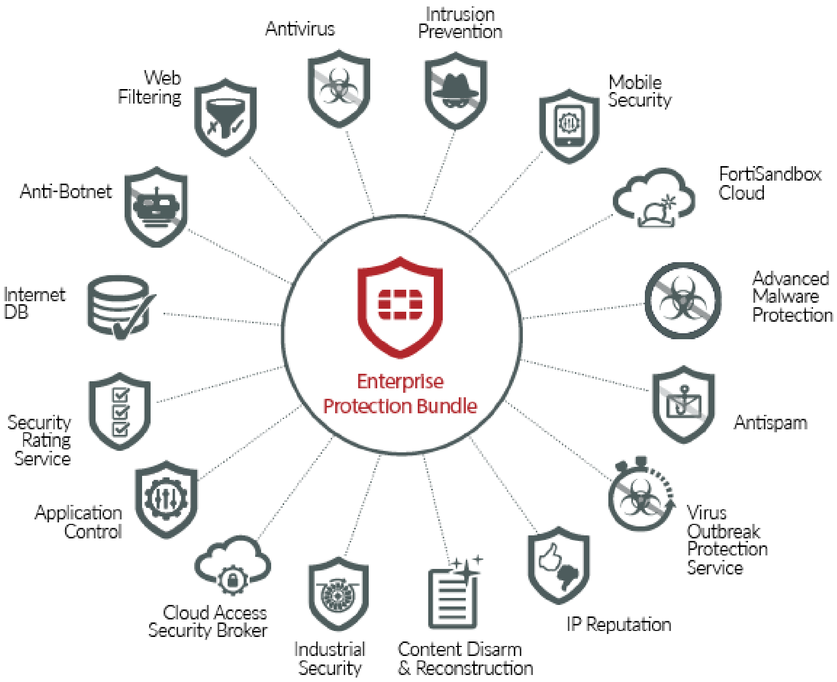
- The **FortiCASB** cloud access security broker service helps organizations establish and maintain consistent policies and governance across multi-cloud environments and common compliance and audit tools. This ensures smoother operations, better compliance, and enhanced security.
- The **FortiGuard Security Rating Service** helps organizations evaluate their current security posture against relevant benchmarks—including security standards, results from peer organizations, and the goals of the business. It provides actionable information used to prioritize patch management, improve processes, and adjust configurations over time.
- The **Fortinet Industrial Security Service** enables organizations to deal with the security risks presented by the convergence of IT and OT. It continuously updates signatures to identify and police most of the common industrial control system (ICS) and supervisory control and data acquisition (SCADA) protocols for granular visibility and control. Additional vulnerability protection is provided for applications and devices from the major ICS manufacturers.

These services build upon the foundation of the comprehensive advanced malware protection capabilities included in the Enterprise Protection bundle, providing the core security needed to address the threat landscape and to keep cyber criminals at bay. Some of these capabilities are critical differentiators. The following are not offered by other security providers:

- **Antivirus paired with cloud-based sandbox analysis** helps organizations protect against both known and unknown threats.
- **Virus Outbreak Protection Service (VOS)** detects malware between signature updates by checking the Fortinet Global Threat Intelligence Database for files not in the signature database.

- **Content Disarm and Reconstruction (CDR)** strips the active content from incoming files in real time, creating a sterile flat file and removing all malicious content.

The Enterprise Protection bundle also includes essential services such as an intrusion prevention system (IPS), web filtering, antispam, application control, and IP reputation services. All Fortinet offerings are backed by comprehensive threat intelligence from FortiGuard Labs, leveraging a very mature artificial intelligence (AI) and machine learning (ML) program that analyzes well over 100 billion files every day. The sheer volume of data processed by FortiGuard Labs every day provides an unparalleled and unique perspective on the threat landscape.



THE FORTIGATE ENTERPRISE BUNDLE OFFERS THE MOST COMPREHENSIVE, ADVANCED PACKAGE OF SECURITY SERVICES ON THE MARKET TODAY.

WHO NEEDS THE ENTERPRISE PROTECTION BUNDLE?

The Enterprise Protection bundle is designed to address security needs and challenges that impact almost every organization. The following user profiles are solved by the different capabilities in the Enterprise Protection bundle:

- **Cloud-based platforms.** Almost every organization operates multiple cloud-based services. An increasing number look to the cloud for most or all new services that are added. Even more traditional enterprises now need to coordinate their security strategy across multiple clouds and on-premises infrastructure. The FortiCASB service gives these organizations full visibility and centralized control of cloud security policies and practices.
- **IoT proliferation.** Most organizations are deploying IoT devices, and many of them are critical to the business. This dramatically increases the number of endpoints they manage, and the bulk of these devices do not have adequate security controls. The advanced malware protection capabilities in the Enterprise Bundle help protect these endpoints against known and unknown threats, and the Security Rating Service helps security leaders to understand how to optimize their defenses along this new attack surface.
- **Connected OT.** More and more OT systems are being connected to the internet or a company's IT network via IoT devices and through cloud platforms, exposing them to cybersecurity risk for the first time. The Fortinet Industrial Security Service continually monitors ICS and SCADA systems for vulnerabilities to their most common protocols.
- **Compliance and risk management.** Every organization has more compliance requirements than a decade ago, and many industries and organizations have unique compliance needs. Beyond satisfying auditors, the business risks posed by cybersecurity gaps are now a crucial topic of interest in boardrooms and C-suites. The Security Rating Service provides enterprises with a real-time, objective view of their security posture and associated IT risks. It also provides recommendations on how to improve that posture.

WHAT CHALLENGES CAN THE ENTERPRISE SECURITY BUNDLE HELP ADDRESS?

The FortiGate Enterprise Protection bundle helps organizations address many of the challenges posed by the complexity of IT networks and the ever-evolving threat landscape. Some of the more prevalent challenges it helps solve include:

- **Complex threat landscape.** Today's advanced threats require a thorough, real-time response. The Fortinet Enterprise Protection bundle provides comprehensive protection from known and unknown threats while eliminating silos that reduce efficiency and increase risk.
- **Vulnerability management.** Whether in the DevOps environment or with cloud-based applications, many organizations are unaware of vulnerabilities in their systems. The Security Rating Service helps identify vulnerabilities before they can cause problems, and prioritize patches according to business risk.
- **Cybersecurity skills shortage.** Given the difficulties of adding new staff, realizing the maximum value from existing team members will most certainly continue to grow as a business imperative. Consolidating security services into a single bundle reduces overhead and eliminates hours of manual work for cybersecurity personnel.

WHAT BENEFITS DOES THE ENTERPRISE PROTECTION BUNDLE BRING?

Deploying the FortiGate Enterprise Protection bundle provides organizations with the broad, integrated, and automated protection of the Fortinet Security Fabric in a format that reduces cost and administrative complexity. Customers realize these specific benefits:

1. **Robust, real-time threat intelligence.** There are many subscription-based threat-intelligence feeds, but FortiGuard Labs has one of the world's most robust threat-intelligence networks, providing complete and real-time information about known and unknown threats.
2. **Advanced threat protection.** Unlike many subscription bundles, FortiGate bundles provide not only detection but also protection and remediation against advanced threats.
3. **Operational efficiency.** The FortiGate Enterprise Security bundle enables threat intelligence to be integrated across a broader set of security elements, enabling automation of manual tasks like reporting and log pulls. Purchasing a consolidated offering from a single vendor greatly reduces administrative overhead.
4. **Cost efficiency.** The FortiGate Enterprise Protection bundle is designed with cost efficiency in mind, delivering broad protection at significantly lower cost than buying the services individually.

To recap, as threats become more complex, move faster, and attack an organization on multiple fronts, a more strategic and holistic approach to security is a necessity. The FortiGate Enterprise Protection bundle provides a comprehensive, integrated approach to protecting every part of the attack surface—from IoT devices to OT systems to multiple clouds.

[1] "Threat Landscape Report Q3 2017," Fortinet, accessed April 5, 2018.

[2] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed September 6, 2018.

[3] "IT and OT convergence—two worlds converging in Industrial IoT," i-SCOOP, accessed January 10, 2019.

[4] Mark McGregor, "Modern Compliance Management in Times of Constant Change," BPTrends, June 4, 2018.

[5] "Threat Landscape Report Q3 2018," Fortinet, accessed November 13, 2018.

[6] Based on internal data from FortiGuard Labs.

[7] "2018 Security Implications of Digital Transformation Report," Fortinet, July 26, 2018.

[8] "2018 Data Breach Investigations Report," Verizon, March 2018.

[9] John Maddison, "Resolving the Challenges of IT-OT Convergence," Fortinet, June 21, 2018.

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

[11] "2018 Data Breach Investigations Report," Verizon, March 2018.

[12] "Online Trust Alliance Reports Doubling of Cyber Incidents in 2017," Online Trust Alliance, January 25, 2018.

[13] Kasey Panetta, "Is the Cloud Secure?", Gartner, March 27, 2018.

FORTINET

www.fortinet.com