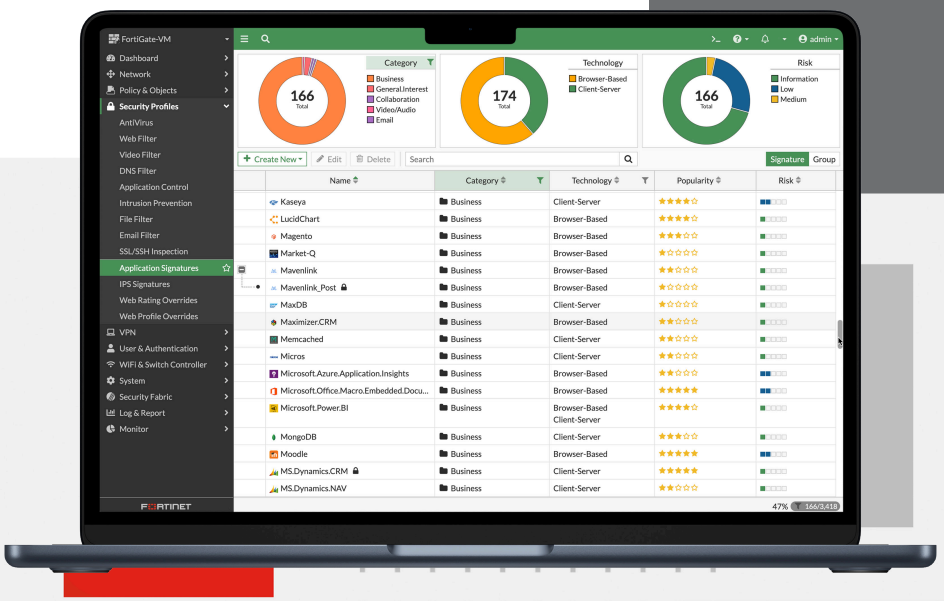
FortiGate® 虚拟防火墙



优势摘要

- 支持 FortiOS 操作系统提供的所有安全和网络服务，高效抵御各类威胁
- 提高虚拟基础设施监控的可见性
- 支持通过单一管理平台统一管理虚拟设备和物理设备
- 灵活的订阅模型可供选择，全方位满足任何基础设施需求

虚拟环境的安全整合

FortiGate虚拟防火墙是Fortinet特别针对软件定义数据中心和云环境设计，助力企业构建安全生态系统。为企业成功整合数据中心提供鼎力支持，支持FortiOS操作系统提供网络和安全性无缝融合的安全服务，高效抵御各类威胁。

Fortinet 有物理和虚拟两种设备模式可供选择，确保安全性的同时，为用户交付卓越的服务与性能体验。虚拟设备支持快速部署并通过单一管理平台进行统一管理，减少虚拟基础架构中的盲点。该生态系统提供灵活的订阅和使用模式，支持多种虚拟化和云平台部署。

FOS

广泛适用于：

硬件

虚拟设备

托管

云平台

容器

FortiOS 安全无处不达

Fortinet 高级操作系统 FortiOS

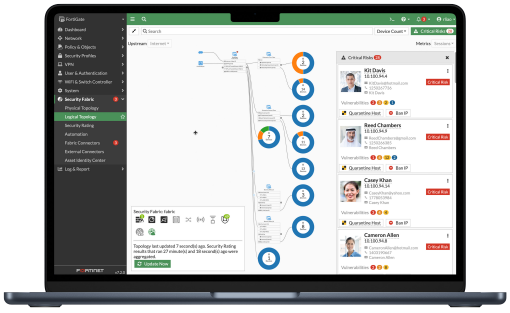
作为 Fortinet Security Fabric 安全平台的强劲支撑，FortiOS 助力用户打造网络和安全高效融合的高性能网络体系。该系统支持在任意位置部署，可跨网络、端点和多云环境提供一致且上下文感知的安全态势。

FortiOS 支持 FortiGate 的所有部署形式，无论是物理设备、虚拟设备、容器或是云环境。这种通用部署模型支持将多种技术和用例全面整合至单一简化的统一策略和管理框架中。其有机构建的最佳功能、统一的操作系统和超可扩展性，助力企业无需牺牲性能或安全性也可全面保护所有网络边缘，高效简化网络运营和业务运营。

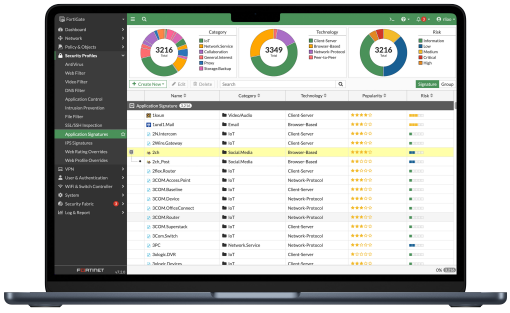
FortiOS 极大地扩展了 Fortinet Security Fabric 无缝集成的AI/ML、内联沙箱检测、ZTNA 策略等高级技术和服务的能力。此外，凭借 SASE 解决方案，可跨混合部署模式为硬件、软件和软件即服务提供高效保护。

FortiOS 扩展了可见性和控制能力，支持跨大规模网络的集中管理，可确保安全策略的一致部署和执行，并具有以下关键属性：

- 交互式向下钻探和拓扑查看器，可显示网络的实时状态
- 一键式修复功能，提供准确、快速的安全保护，防止威胁入侵和漏洞滥用
- 独特的威胁评分系统将加权威胁与用户紧密关联，精准研判威胁调查的优先级



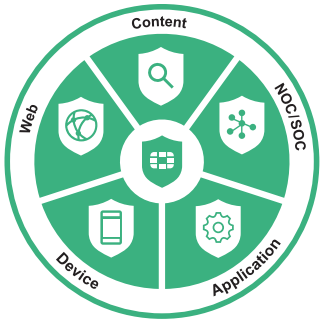
直观易用的网络和端点漏洞视图



通过 FOS 应用程序签名实现安全风险的可见性

FortiConverter 迁移和配置服务

FortiConverter 可提供一站式迁移和配置服务，助力企业快速、轻松地从各种传统防火墙配置顺畅迁移至 FortiGate 下一代防火墙。该服务采用高级方法和自动化流程最佳实践，消除配置错误和冗余。企业还可搭配部署全新 FortiOS 技术加速网络保护。



FortiGuard 安全服务

FortiGuard AI 驱动的安全防护

Fortinet 丰富的 FortiGuard Security Services 安全服务套件由 FortiGuard Labs 倾力支持，由 FortiGuard Labs 安全威胁研究人员、工程师和取证专家精心打造的高性能 AI 驱动威胁情报和支持服务，助力企业实时提前预防已知和未知等各类威胁。

Web 安全

高级云交付 URL、DNS（域名系统）和视频过滤服务，帮助企业从容应对网络钓鱼及其他基于 Web 传播的攻击等各类安全威胁，同时满足合规性要求。

此外，其动态内联 CASB（云访问安全代理）服务专注于保护 SaaS 业务数据，而内联 ZTNA 流量检查和 ZTNA 态势检查则提供针对应用程序的每会话访问控制。此外，该专属服务还支持无缝集成 FortiClient Fabric Agent，将安全性覆盖至远程和移动办公用户。

内容安全

最新且最具创新的内容安全技术可实时检测和预防基于文件的攻击策略及已知和未知等各类威胁。凭借 CPRL（紧凑型模式识别语言）、AV、内联沙箱及威胁横向蔓延保护等优势功能，为企业提供高效应对勒索软件、恶意软件和基于凭据攻击的完整解决方案。

设备安全

经优化的先进安全技术，可持续监控并有效保护 IT、IIoT 和 OT（运营技术）设备免遭漏洞利用和基于设备等各类威胁攻击。其经验证的近实时 IPS 威胁情报，可有效检测和拦截已知威胁和零日威胁，具备对 ICS/OT/SCADA 协议的深入可见性和控制能力，并可提供自动发现、网络隔离和基于模式的身份识别等策略。

SOC/NOC 高级管理工具

附加至 NGFW 的NOC（网络运营中心）和 SOC（安全运营中心）高级管理工具，助力企业简化运营并实现快速激活。

SOC 即服务

包括第一层威胁搜索和自动化、日志定位、24x7 全天候 SOC 专家分析、托管防火墙和端点功能及警报分类。

最佳安全实践的架构评分

包括供应链虚拟补丁修复、前沿风险和漏洞数据共享以及针对数据泄露后的及时补救措施，助力企业高效制定最佳的业务决策。

安全守护任意规模的任意网络边缘

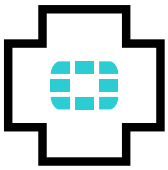
高级虚拟安全处理单元（vSPU）

通常，虚拟防火墙旨在用于保护软件定义的数据中心和多云环境中的虚拟环境，因其经济且易于部署等优势，有助于用户轻松实现虚拟防火墙在云和云之间的迁移。与物理防火墙相比，多数虚拟防火墙的缺点在于，其网络吞吐量明显较低，极易在整个网络中造成性能瓶颈并降低业务敏捷性。

FortiGate 虚拟防火墙（FortiGate-VM）搭载高级虚拟安全处理单元（vSPU），突破吞吐量瓶颈，可在私有云和公有云中提供最佳防护效能。借助FortiGate-VM，企业可将任意应用程序安全地迁移至云中并支持云中高可用性大规模虚拟专用网络（VPN）等各种用例。

FortiGate-VM 提供高性价比 NGFW 解决方案，具备多项行业领先功能：

- 作为FortiGate-VM 搭载的一项独特技术，vSPU通过将部分数据包处理卸载至用户空间并在操作系统中使用内核旁路解决方案，大幅增强性能。凭借 vSPU 技术，FortiGate-VM可将用于 UDP 防火墙规则的吞吐量提高三倍以上。
- 支持Intel QuickAssist技术（Intel QAT），适用于最新的QuickAssist适配器，并通过site-to-site IPSec VPN加速流量处理。利用 QAT 技术，FortiGate-VM 可提升两到三倍的吞吐量，具体取决于数据包帧大小。
- 作为业内首家支持 AWS C5n 实例的下一代防火墙供应商，Fortinet助力企业通过FortiGate-VM高效保护云中计算密集型应用程序。



FortiCare 支持服务

Fortinet 致力于帮助用户获得最大投资回报率并赢得商业成功。FortiCare 支持服务每年会助力成千上万家企业部署的 Fortinet Security Fabric 解决方案以最佳状态运行。我们的生命周期产品组合提供设计、部署、运营、优化和升级服务。运营服务提供具有增强的 SLA 的设备级 FortiCare Elite 服务，以满足客户的运营和可用性需求。此外，我们的定制客户级支持服务可提供快速的事件解决和主动维护服务，以最大限度地发挥 Fortinet 产品的安全和性能。

部署

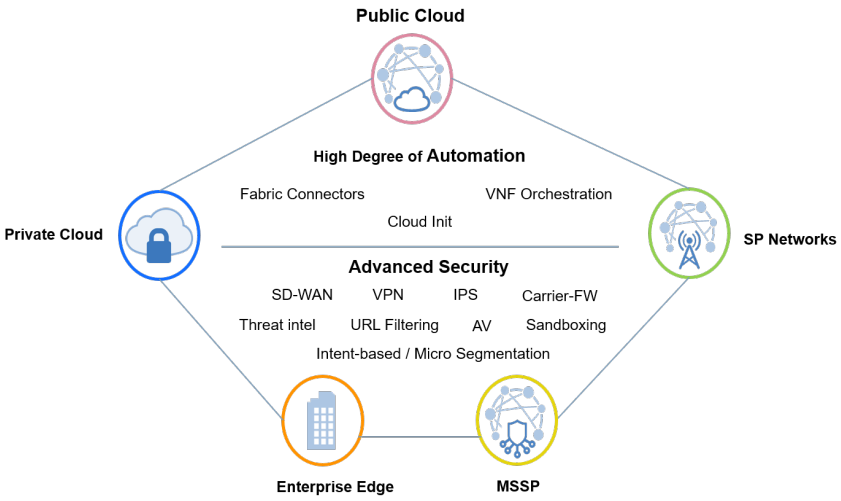
下一代防火墙（NGFW）

- 将威胁防护安全功能全面整合至单一高性能网络安全设备，以降低复杂性
- 利用强大的入侵防御技术，有效识别并拦截接口和协议中潜藏的网络威胁，实时检测网络流量中的实际应用程序
- 利用行业规定的密码密钥组合，提供业内无与伦比的 SSL 检测性能，实现最大化投资回报率
- 凭借高级威胁防护功能，实时主动拦截各类新兴恶意复杂攻击

VPN 网关

- 直接连接FortiGate防火墙，以检测进出AWS VPC的SSL和IPsec VPN流量
- 多个VPC 之间的VGW（虚拟专用网关）至 FortiGate VPN
- 混合云site to site IPsec VPN
- 远程访问VPN

获得全面的可见性并应用一致的控制策略



部署

灵活的部署模式可供选择

如今，企业的IT 基础架构中，鲜少会采用 100% 硬件设备或 100% 虚拟设备的单一部署模式。因此，您的安全策略部署既需要硬件设备也需要虚拟设备。Fortinet 助力企业同时采用硬件和虚拟设备构建适合企业环境需求的安全解决方案，以保护核心及边缘网络并提高在虚拟基础架构内通信的可见性和控制能力。凭借 FortiManager 虚拟设备或物理设备，助力企业通过单一管理平台轻松管理和更新硬件和虚拟设备等所有 Fortinet 安全资产。

多重威胁防护体系

凭借先进操作系统 FortiOS™ 的强劲支撑，FortiGate 虚拟设备可有效消除虚拟环境所面临的各种安全威胁。无论作为云边界安全网关，或是在虚拟基础架构内部作为区域间的安全防御部署 FortiGate 虚拟设备均采用当下最高效的安全管理措施，满足企业所需的安全功能，全方位保护您的基础架构。

规格参数

	VM-01/01V/01S	VM-02/02V/02S	VM-04/04V/04S	VM-08/08V/08S	VM-16/16V/16S	VM-32/32V/32S	VM-UL/ULV/ULS
技术参数							
vCPU支持数量（最小/最大）	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / 无限
存储支持（最小/最大）	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
无线接入点控制（隧道/全局）	32 / 64	512 / 1024	512 / 1024	1024 / 4096	1024 / 4096	1024 / 4096	1024 / 4096
虚拟域 (默认/最大)*	10 / 10	10 / 25	10 / 50	10 / 500	10 / 500	10 / 500	10 / 500
防火墙策略	10 000	10 000	10 000	200 000	200 000	200 000	200 000
已注册端点最大数量	2000	2000	8000	20 000	20 000	20 000	20 000
无限用户许可	是	是	是	是	是	是	是

注：所有性能值均为“最高”值显示，实际性能可能因网络和系统配置而异。

网络接口支持

FortiGate 6.4.0 及以上版本，FortiGate 实例可使用的最大网络接口数为 24。旧版可使用的接口数为 18，最小数量为 1。可连接至实例的网络接口的实际数量会因云平台和实例类型而异。即便 FortiGate 最多允许 24 个接口，但也无法支持您将超过最大限制的接口数量连接至实例。

* 默认情况下，FG-VMxxV 和 FG-VMxxS 系列不支持多 VDOM 功能。您可通过单独订阅 VDOM永久许可证进行添加。请参阅 VDOM SKU 的订购信息。

云提供商
私有云（Hypervisors）
VMware ESXi v5.5 / v6.0 / v6.5 / v6.7 / v7.0
VMware NSX-T* v2.3 / v2.4 / v2.5
Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019**
Microsoft AzureStack
Citrix Xen XenServer v5.6 sp2、v6.0、v6.2 及更高版本
开源 Xen v3.4.3，v4.1 及更高版本
适用于Red Hat Enterprise Linux系统的KVM qemu 0.12.1 & libvirt 0.10.2 及更高版本/ CentOS 6.4及更高版本/ Ubuntu 16.04 LTS（通用内核）
KVM qemu 2.3.1 for SuSE Linux Enterprise Server 12 SP1 LTSS
Nutanix AHV (AOS 5.10, Prism Central 5.10)***
Cisco Cloud Services Platform 2100***
Cisco ENCS (NFVIS 3.12.3)****

* 请参见《VMware 上的 NSX-T 兼容性指南》，了解最新支持平台。

** FortiGate-VM 6.2.3+ 支持 Microsoft Hyper-V 2019。

*** FortiGate-VM 6.0.3+ 支持 Nutanix AHV 和 Cisco CSP 2100。

**** FortiGate-VM 6.2.3+ 支持 Cisco NFVIS 3.12.3。

云提供商
公有云（Marketplaces）
亚马逊 AWS（包括 GovCloud 和 AWS 中国）
AWS 上的 VMware Cloud*
Dell EMC上的VMware Cloud**
微软 Azure（包括区域 Azure：美国政府、德国和中国）及AzureStack联合
Google GCP（Google云平台）
Oracle OCI
阿里云（AliCLOUD）
IBM云 (Gen1 / Gen2)

虚拟化/云平台支持因型号和FortiOS构建而异。请参考相应的发行说明。 FG-VMxxV 系列需要 FortiOS 5.4.8+ / 5.6.1+ / 6.0.0+

* FortiGate-VM 6.0.4+ 支持VMware Cloud on AWS

** FortiGate-VM 6.2.3+ 支持VMware Cloud on Dell EMC*

订购信息

以下 SKU 针对永久许可方案：适用于已在Marketplace推出的产品系列。

产品	SKU	描述
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM ‘虚拟设备’ 1x vCPU。默认情况下，FG-VM01V 型号不支持 VDOM。
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM ‘虚拟设备’ 2x vCPU。默认情况下，FG-VM02V 型号不支持 VDOM。
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM ‘虚拟设备’ 4x vCPU 。默认情况下，FG-VM04V 型号不支持 VDOM。
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM ‘虚拟设备’ 8x vCPU 。默认情况下，FG-VM08V 型号不支持 VDOM。
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM ‘虚拟设备’16x vCPU。默认情况下，FG-VM016V 型号不支持 VDOM。
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM ‘虚拟设备’32x vCPU。默认情况下，FG-VM032V 型号不支持 VDOM。
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM ‘虚拟设备’无限 vCPU。默认情况下，FG-VMULV 型号不支持 VDOM。
可选配件/备件	**SKU**	**描述**
虚拟域 (VDOM) 许可证添加 5	FG-VDOM-5-UG	用于将 5个 VDOM 添加到 FortiOS 5.4 及更高版本的升级许可证，受平台最大 VDOM 容量的限制。
虚拟域 (VDOM) 许可证添加 25	FG-VDOM-15-UG	用于将 15个 VDOM 添加到 FortiOS 5.4 及更高版本的升级许可证，受平台最大 VDOM 容量的限制。
虚拟域 (VDOM) 许可证添加 25	FG-VDOM-25-UG	用于将 25个 VDOM 添加到 FortiOS 5.4 及更高版本的升级许可证，受平台最大 VDOM 容量的限制。
虚拟域 (VDOM) 许可证添加 50	FG-VDOM-50-UG	用于将 50个 VDOM 添加到 FortiOS 5.4 及更高版本的升级许可证，受平台最大 VDOM 容量的限制。
虚拟域 (VDOM) 许可证添加 240	FG-VDOM-240-UG	用于将 240个 VDOM 添加到 FortiOS 5.4 及更高版本的升级许可证，受平台最大 VDOM 容量的限制。

旧版仍对每个vCPU型号的RAM大小有所限制，而FortiGate-VM 6.2.2版所有vCPU型号已无RAM限制。旧版有必要升级至6.2.2版本才能消除RAM限制。

以下 SKU 适用于年度订阅许可方案：

产品	SKU	描述
FortiGate-VM01-S	FC1-10-FGVVS-<技术支持服务包>-02-DD	FortiGate-VM 订阅许可证（1个虚拟核心 CPU）
FortiGate-VM02-S	FC2-10-FGVVS-<技术支持服务包>-02-DD	FortiGate-VM 订阅许可证（2个虚拟核心 CPU）
FortiGate-VM04-S	FC3-10-FGVVS-<技术支持服务包>-02-DD	FortiGate-VM 订阅许可证（4个虚拟核心 CPU）
FortiGate-VM08-S	FC4-10-FGVVS-<技术支持服务包>-02-DD	FortiGate-VM 订阅许可证（8个虚拟核心 CPU）
FortiGate-VM16-S	FC5-10-FGVVS-<技术支持服务包>-02-DD	FortiGate-VM 订阅许可证（16个虚拟核心 CPU）
FortiGate-VM32-S	FC6-10-FGVVS-<技术支持服务包>-02-DD	FortiGate-VM 订阅许可证（32个虚拟核心 CPU）
FortiGate-VMUL-S	FC7-10-FGVVS-<技术支持服务包>-02-DD	FortiGate-VM 订阅许可证（无限虚拟核心 CPU）

FortiOS 6.2.3及6.4.0以上版本均支持FortiGate-VM S系列。FortiGate-VM S 系列对所有级别的vCPU 均没有 RAM 限制。
FortiManager 6.2.3及6.4.0 以上版本适用于FortiGate-VM S 系列设备的管理。

订阅信息

服务类别	服务产品	单选项目	服务包		
			企业级防护	统一威胁防护	高级威胁防护
安全服务	FortiGuard IPS 服务	•	•	•	•
	FortiGuard 高级恶意软件保护（AMP）— 防病毒防移动恶意软件、防僵尸网络、CDR、防病毒爆发及 FortiSandbox 云服务	•	•	•	•
	FortiGuard Web 安全 — URL和网页内容、视频和安全DNS过滤	•	•	•	
	FortiGuard 反垃圾邮件服务		•	•	
	FortiGuard IoT 检测服务	•	•		
	FortiGuard 工业安全服务	•	•		
	FortiCloud 于 AI 驱动的内联沙箱服务 [1]	•			
NOC 服务	FortiGate Cloud（SMB 日志记录 + 云管理）	•			
	FortiGuard Security Fabric 评分和合规监控服务	•	•		
	FortiConverter 迁移和配置服务	•	•		
	FortiGuard SD-WAN Underlay 带宽和质量监控服务	•			
SOC 服务	FortiAnalyzer 云服务	•			
	FortiAnalyzer SOCaaS 云服务	•			
硬件和软件支持	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
基础服务	FortiGuard 应用程序控制	包含 FortiCare 订阅服务			
	FortiCloud ZTNA 内联 CASB 服务 [1]				
	互联网服务 (SaaS) 国家 IP 库升级				
	GeoIP DB 升级				
	设备/OS 签名检测				
	可信的证书数据库更新				
	DDNS (v4/v6) 服务				

1.运行 FortiOS 7.2 时可用

FortiGuard 服务包

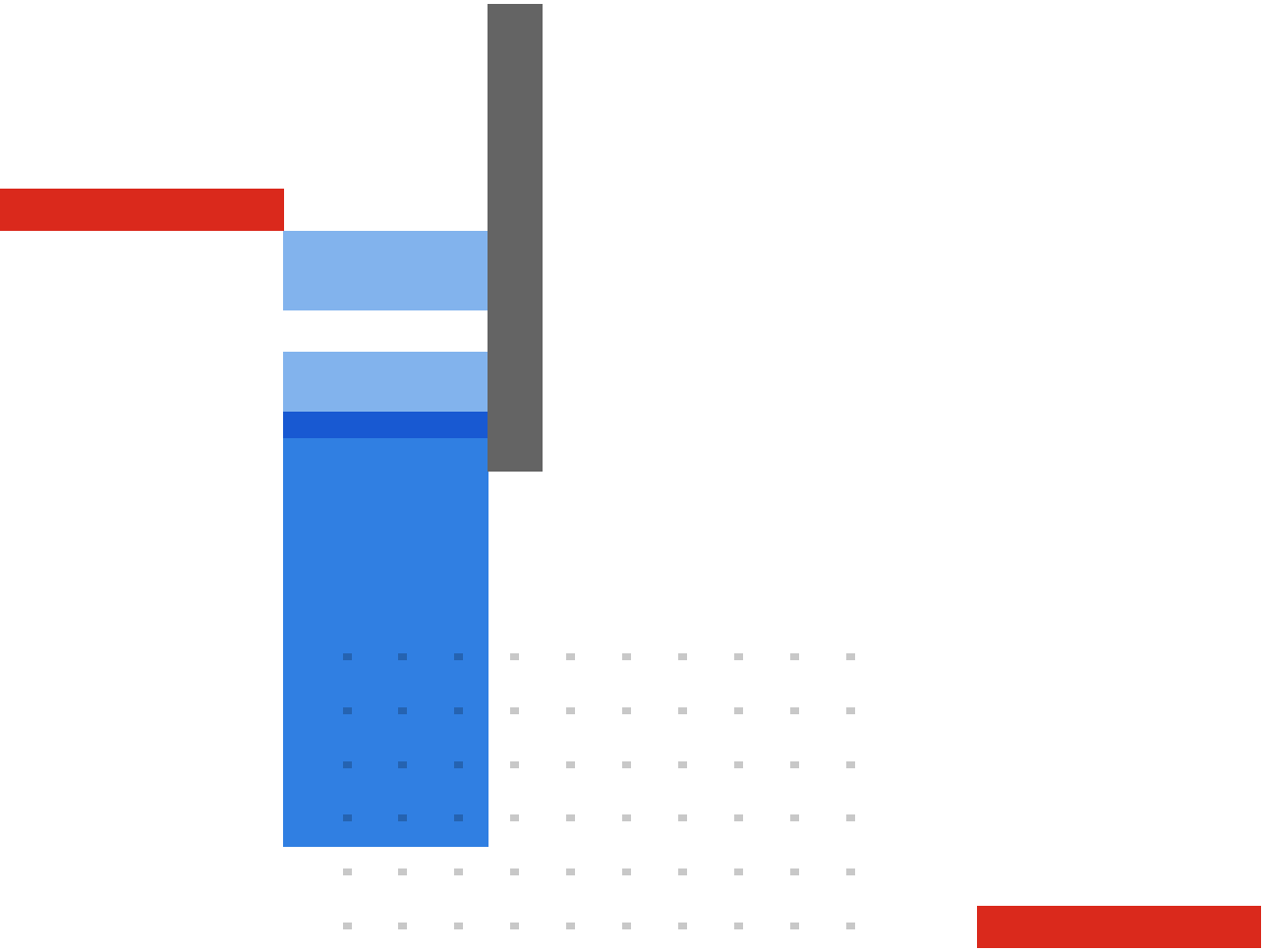
FortiGuard 全球威胁研究与响应实验室提供全面的安全情报服务，以增强 FortiGate防火墙平台的安全性能。您可选择其中一个 FortiGuard服务包轻松优化 FortiGate的防护性能。

FortiCare Elite

FortiCare Elite 服务提供增强的服务等级协议（SLA）以及加速问题解决的服务方案。此高级支持服务选项为用户提供专业支持团队的专属访问支持。一键ticket解决方案，简化专家技术团队响应问题的流程。此选项还为工程终止（EoE）提供 18 个月的支持服务，以增加灵活性，并支持访问全新 FortiCare Elite 管理门户。该直观门户为用户提供了设备和安全运行状况的一站式统一视图。

Fortinet CSR 政策

Fortinet 致力于通过网络安全推动人类的进步和可持续发展，尊重人权和道德商业惯例，为您构建始终可信赖的数字世界。请向 Fortinet 声明并保证，您不会使用 Fortinet 的产品和服务以任何方式参与或支持侵犯人权的行为，包括涉及非法审查、监视、拘留或过度使用武力等行为。使用 Fortinet 产品的用户需遵守Fortinet EULA并透过Fortinet举报人政策中概述的程序报告任何涉嫌违反 EULA 的行为。



FORTINET

www.fortinet.com

February 8, 2023

FG-VM-DAT-R54-20230208