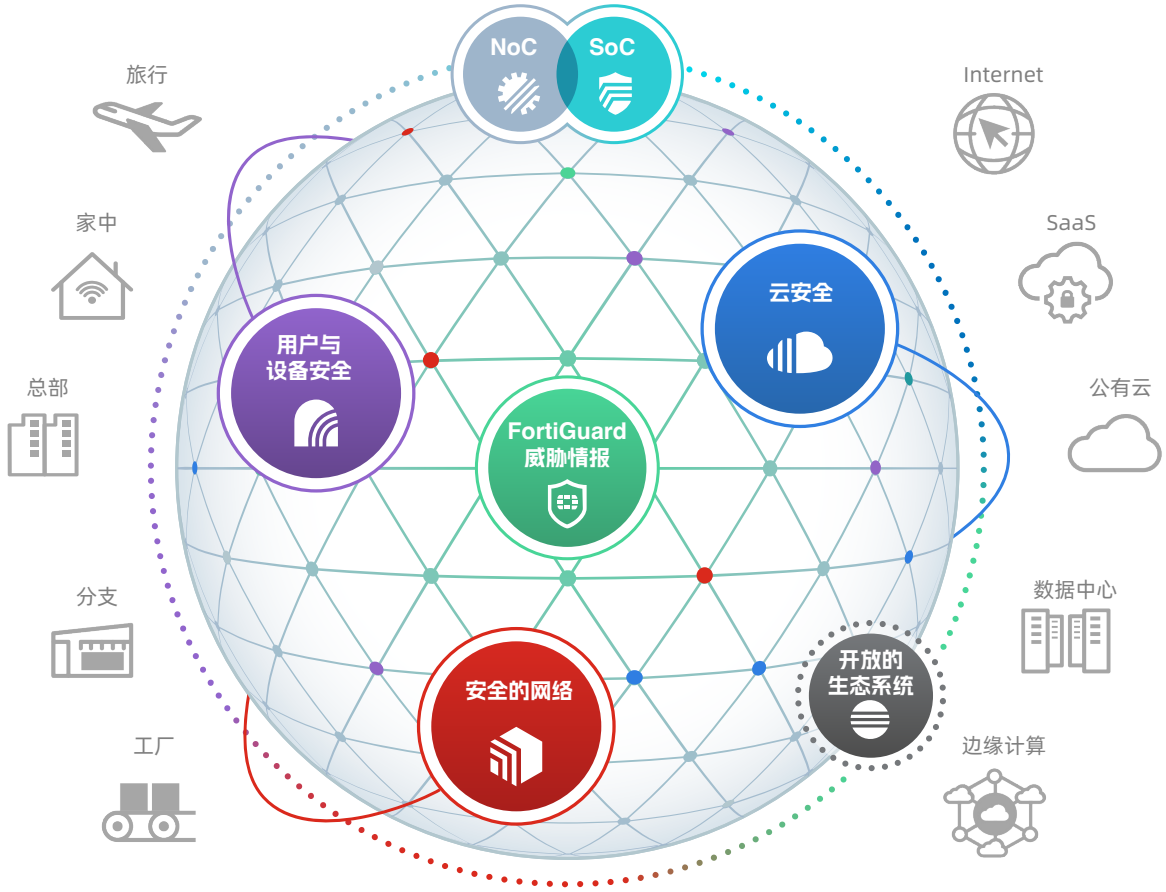
FortiGuard 全球威胁研究与响应实验室及安全服务介绍

Fortinet FortiGuard 全球威胁研究与响应实验室

新的网络威胁每时每刻都在出现。无论是勒索软件、网络钓鱼活动，还是系统漏洞，企业都必须时刻准备好防御新的威胁。对威胁形势的广泛了解，以及在多个层面快速做出反应的能力，是提供有效安全的基础。

FortiGuard实验室由数百名研究专家组成，平均拥有超过16年的威研究和应对经验。通过夜以继日的威胁研究及特征库更新，为FortinetSecurity Fabric解决方案提供全面的安全更新，从而对客户提供最先进的保护，增强客户的网络安全防御。

FortiGuard订阅服务可为Fortinet产品线提供多种安全服务的更新。



FortiCare服务

Fortinet的FortiCare服务包括技术支持，硬件保修和系统软件升级服务。另外，FortiCare服务还包含了一些FortiGuard订阅服务。当需要任何技术服务时，用户可以根据自己需求来选择Email或电话支持服务，技术服务邮箱:**support_cn@fortinet.com**;技术服务电话:**400-600-5255**。

用户购买产品后，需要到**https://support.fortinet.com**进行产品注册以得到标准的服务支持，同样，购买的订阅服务也需要在support上进行注册激活。产品及服务注册指南请参阅http://support.fortinet.com.cn网站中“注册指南“部分。

FORTINET

FortiGuard安全服务订阅

服务内容介绍			服务包种类				
类型	名称	内容简介	单项服务 (FortiGuard)	企业专业防护服务包（ENT）	统一威胁防护服务包（UTP）	高级威胁防护服务包 (ATP)	基础保障服务包（Premium）
FortiGuard	高级恶意软件防护服务 Advanced Malware Protection– AMP	**防病毒 (Antivirus):** FortiGate 内置可实时更新的病毒特征库，通过扫描网络中的传输文件，防御最新的病毒、间谍软件和其他内容级的威胁。	✓	✓	✓	✓	
		云沙盒 (FortiSandbox Cloud): 高级威胁防护解决方案，通过部署在云端的沙盒产品，实现对包括勒索软件在内的未知威胁进行识别后动态生成签名，并把签名下发到 FortiGate 进行阻挡。					
		僵尸网络防御 (Anti–botnet): FortiGate 内置可实时更新的僵尸网络域名数据库和 IP 数据库，当匹配到数据库内的域名和 IP 流量时，进行实时阻挡。					
		移动设备安全 (Mobile Security): 防御包括 Android、iOS 等的移动平台的最新威胁。					
		病毒爆发防护 (Virus Outbreak Protection): 实时在线查询最新爆发的病毒，消除最新发生的病毒威胁与病毒特征库更新之间的缺口，检测和阻止在 FortiGate 病毒特征库更新之前发现的恶意软件威胁，防止威胁在网络系统中传播。					
		内容解除及重建 (Content Disarm & Reconstruction): 实时从文件中剥离所有活动内容，创建无害的文件。活动内容是文件中一种交互式或动态的内容，被视为可疑活动内容将被删除。					
	入侵防御系统 IPS	FortiGate 内置可实时更新的攻击防护特征库，以深度过滤的方式，打开数据包扫描其中的内容，查找已知的与签名匹配的漏洞，防御基于网络的威胁。	✓	✓	✓	✓	
	Web 过滤 web filter	实时扫描用户访问的 URL，并在 FortiGuard 上查询 URL 的网址分类。FortiGuard 对全球数以亿计的网址进行分类，管理员只需要对不同分类进行阻止或监视的操作，就可以阻止用户访问与企业无关的网站或对用户的网站访问行为进行记录。	✓	✓	✓		
	垃圾邮件过滤 anti–spam	通过实时查询发件人的 IP 信誉数据库和垃圾邮件签名数据库，以及邮件中包含的钓鱼 URL，检测和阻止垃圾邮件信息。		✓	✓		
	基于 AI 的在线恶意软件防护 AI–based Inline Malware Prevention	也称为在线沙箱服务。下一代防火墙将未知文件阻断后送到在线沙箱，沙箱对可疑文件的静态和动态分析可实现亚秒级恶意软件检测和判决，如果文件是恶意的，将被实时阻止并隔离	✓	✓			
	数据泄漏防护 Data Loss Preventio	可以阻止信用卡和社会安全号码等敏感信息被发布到外部网络	✓	✓			
	工业安全 OT Security	通过不断更新工业安全特征库，识别和监控大多数通用的 ICS/SCADA(监控和数据采集) 协议，以实现粒度可见性和控制 , 并可对 OT 环境的漏洞利用进行阻止。	✓				
	攻击面安全 Attack Surface Security	包括 IoT 检测、安全评级服务。通过 IoT 检测，FortiGate 可以向 FortiGuard 发送终端设备信息，根据 FortiGuard 返回的结果获取关于该设备的详细信息；安全评级服务可以审计用户网络， 帮助用户了解网络安全态势， 指导用户设计、实现和持续维护适合其企业的安全架构。	✓	✓			
	配置转换服务 FortiConverter	配置转换服务，可以把第三方防火墙配置转换为 FortiGate 配置，或进行不同 OS 版本间的 FortiGate 配置转换。	✓	✓			
FortiCare	包含在 Forticare 内的 FortiGuard 订阅服务	**应用控制 (Application control):** FortiGate 内置的 4000+ 应用特征库，并分为 24 个分类。管理员可以快速创建允许、拒绝或限制对应用程序或应用程序分类的访问策略。		✓	✓	✓	✓
		Internet 服务数据库 (Internet Service DB): 数据库中收集了全球主要云服务、SaaS 服务的 IP 地址及服务类型。ISDB 可以在路由或防火墙策略中引用，快速实现 internet 服务的引流及访问控制。					
		设备和操作系统检测 (Device/OS Detection): 通过多种条件，实现客户端设备和操作系统类型的检测，并在图形界面上进行展示					
		IP 地理服务 (IP Geolocation Service): 基于国家的 IP 地址库，用于 Fortinet 设备配置基于地理位置的策略地址对象。					
		信任证书数据库 (Trusted Certificate Database): 内置的信任证书数据库，可以使 FortiGate 实现 SSL 流量检测时，识别服务器证书是否为安全的信任证书					
		动态 DNS(DDNS): 基于云的动态 DNS 服务					
		CASB 控制 (CASB SaaS Control): 云原生的云访问安全代理 (CASB) 服务，为云应用程序提供可见性、合规性、数据安全性和威胁防护，并支持对存储在 SaaS 和 IaaS 应用程序中的数据进行深度检查和策略管理。					
	硬件保修 Advanced HW （VM 产品无此项服务）	高级替换服务 : 硬件被 Fortinet 技术支持专家确认为无法远程解决需要将设备返厂维修的故障后，用户可以在发回设备前要求一台替换设备。我们将在 24 工作小时内将同型号或不低于原型号性能的替换机通过 Fortinet 付费的地面运输起运方式发送给客户。		✓	✓	✓	✓
	固件升级服务 Firmware & General Update	Fortinet 将为注册的产品不断地发布软件的中间版本，以及维护版本和大的版本。所发布的版本将提供新特性，增强功能和补丁。					
	技术支持服务 Enhanced Support	Fortinet 通过邮件、电话、远程等多种方式响应客户的技术请求，定位设备故障，通过提供临时解决方案和补丁来修复系统，必要时候安排硬件替换。					