DATA SHEET

FortiEDR™

Real-Time Endpoint Protection, Detection and Automated Response

FortiEDR delivers real-time, automated endpoint protection with the orchestrated incident response across any communication device — including workstations and servers with current and legacy operating systems as well as manufacturing and OT systems — all in a single integrated platform, with flexible deployment options and a predictable operating cost.

Real-Time Proactive Risk Mitigation & IoT Security

Enables proactive reduction of the attack surface, including vulnerability assessment and proactive risk mitigation-based policies that enable communication controls of any discovered application with vulnerabilities.

Pre-Infection Protection

Provides the first layer of defense via a custom- built, kernel-level Next Generation machine-learning-based Anti-Virus (NGAV) engine that prevents infection from file-based malware.

Post-Infection Protection

FortiEDR is the only solution that detects and stops advanced attacks in real-time, even when the endpoint has been compromised. No breaches, no data loss, no problem. FortiEDR eliminates dwell time and provides a suite of automated Endpoint Detection and Response (EDR) features to detect, defuse, investigate, respond and remediate incidents.

Supported Platforms

- Windows XP SP2/SP3,7, 8.x and 10.x, Windows Server 2003 R2, 2008 R1, 2008 R2, 2012, 2012 R2, 2016, 2019
- macOS Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15)
- VDI Environments: VMware Horizons 6 and Citrix XenDesktop/ XenApp
- Red Hat Enterprise Linux 6.8, 6.9, 6.10 and 7.x
- CentOS 6.8, 6.9, 6.10 and 7.x
- Ubuntu 16.04, 18.04

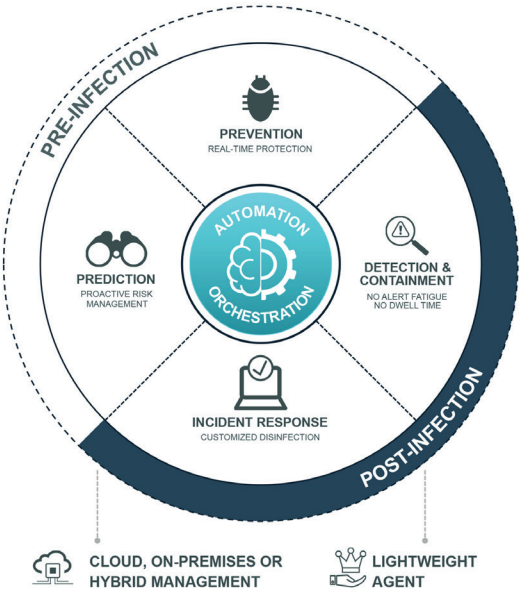
HIPAA COMPLIANT

PCI DSS COMPLIANT

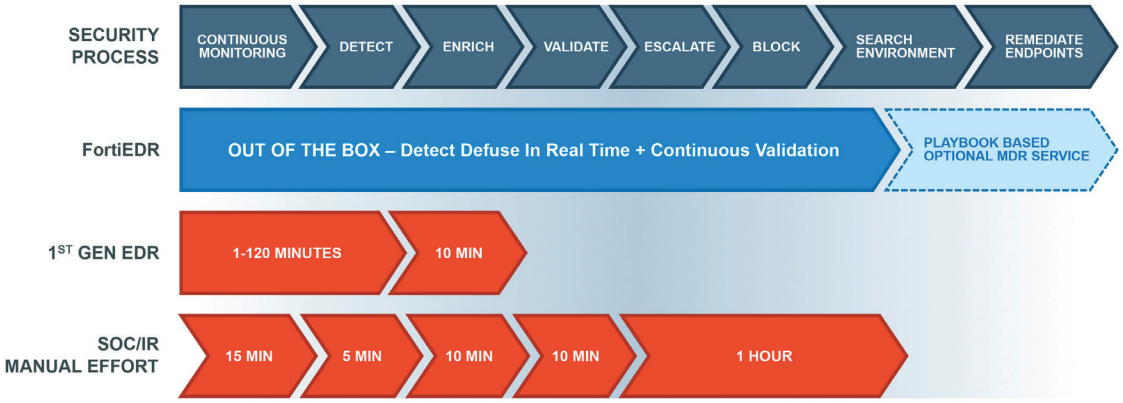
Highlights

Comprehensive Endpoint Security Platform

FortiEDR is the only endpoint security solution built from the ground up to detect advanced threats and stop breaches and ransomware damage in real-time even on an already compromised device, allowing you to respond and remediate incidents automatically to protect data, ensure system uptime, and preserve business continuity. FortiEDR defends everything from workstations and servers with current and legacy operating systems to POS and manufacturing controllers. Build with native cloud infrastructure, FortiEDR can be deployed in the cloud, on-premise in an air-gapped environment and as a hybrid deployment.



Benefits



FortiEDR automates security processes and provides real-time protection post-infection without alert fatigue or dwell time.

Protection

With FortiEDR, you get proactive, real-time, automated endpoint protection with the orchestrated incident response across platforms. It stops the breach with real-time post-infection blocking to protect data from exfiltration and ransomware encryption.

Management

FortiEDR delivers a single unified console with an intuitive interface. The cloud-managed platform closes the loop and automates mundane endpoint security tasks so your people do not have to.

Scalability

With a native cloud infrastructure and a small footprint, FortiEDR can be deployed quickly and scale up to protect hundreds of thousand endpoints.

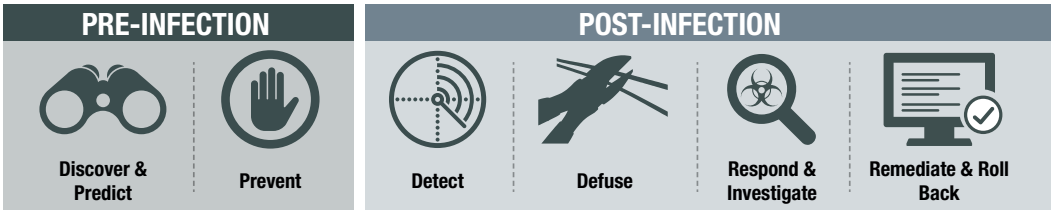
Flexibility

FortiEDR can address an array of enterprise use cases. The cloud management platform can be deployed on-premise in an air-gapped environment, or on a secure cloud instance. Endpoints are protected both on- and off-line.

Cost

Eliminate post-breach operational expenses and breach damage to the organization, all for a low, predictable cost and capped TCO.

Features



Discover and Predict

FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to:

- Discover and control rogue devices (e.g., unprotected or unmanaged devices) and IoT devices
- Track applications and ratings
- Discover and mitigate system and application vulnerabilities with virtual patching
- Reduce the attack surface with risk-based proactive policies

Prevent

FortiEDR uses a machine learning antivirus engine to stop malware pre-execution. This cross-OS NGAV capability is configurable and comes built into the single, lightweight agent, allowing users to assign anti-malware protection to any endpoint group without requiring additional installation.

- Enable machine learning, kernel-based NGAV
- Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database
- Protect disconnected endpoints with offline protection
- USB device control

Detect and Defuse

FortiEDR detects and defuses file-less malware and other advanced attacks in real-time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C&C) communications, file tampering, and ransomware encryption. At the same time FortiEDR backend continues to gather additional evidence, enrich event data and classify the incidents for a potential automated incident response playbook policy to apply. FortiEDR surgically stops data breach and ransomware damage in real-time, automatically allowing business continuity even on already compromised devices.

- Leverage OS-centric detection, highly accurate in detecting stealthy infiltrated attacks, including memory-based and “living off the land” attacks
- Stop breaches in real-time and eliminate threat dwell time
- Achieve analysis of entire log history
- Prevent ransomware encryption, and file/registry tempering
- Continuously validate the classification of threats
- Enhance signal to noise ratio and eliminate alert fatigue

Respond and Remediate

Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes, manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment.

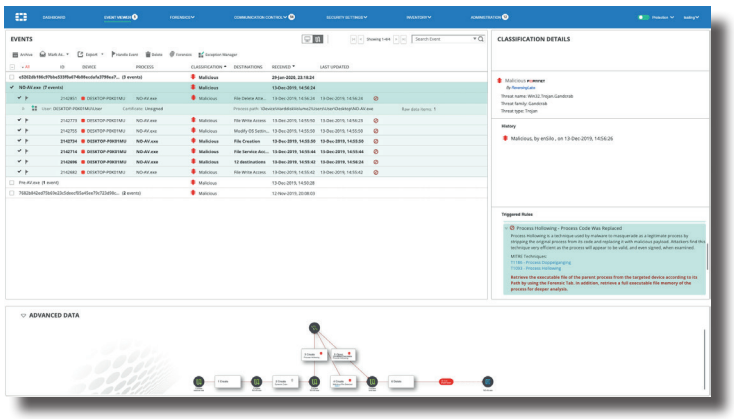
- Automate incident classification and enhance the signal-to-alert ratio
- Standardize incident response procedures with playbook automation
- Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Optional managed detection and response (MDR) service

Features

Investigate and Hunt

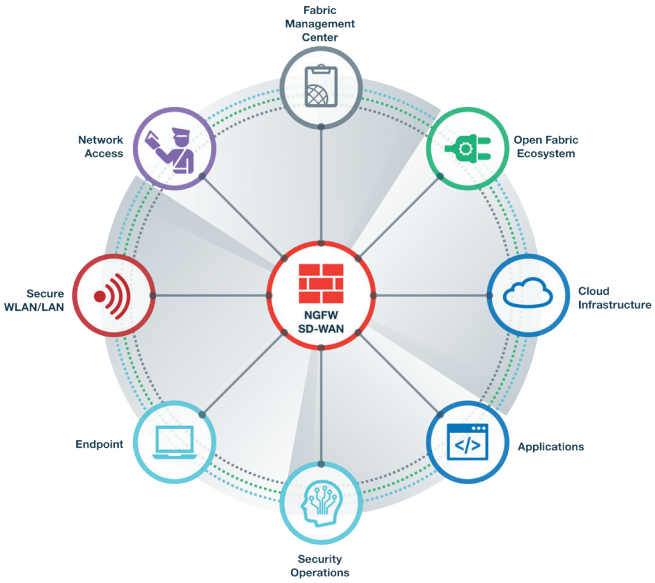
FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. Its unique guided interface provides helpful guidance, best practices and suggests the next logical steps for security analysts.

- Automate investigation with minimal interruption to end-users
- Automatically defuse and block threats, allowing security analysts to hunt on their own time
- Patented Code-tracing technology delivers full attack chain and stack visibility which points to the smoking gun even if the device is offline
- Preserve memory snapshots of in-memory attacks for memory-based threat hunting
- Guide interface displays clear explanations why the event is flagged as suspicious or malicious, lists corresponding MITRE attack framework, as well as logical next step for forensic investigation



Guide interface displays clear explanations why the event is flagged as suspicious or malicious, lists corresponding MITRE attack framework, as well as logical next step for forensic investigation

Security Fabric Integration



FortiEDR leverages the Fortinet Security Fabric architecture and integrates with many Security Fabric components including FortiGate, FortiNAC, FortiSandbox, and FortiSIEM.

FortiGate

The FortiEDR connector enables the sharing of endpoint threat intelligence and application information with FortiGate. FortiEDR management can instruct enhanced response actions for FortiGate, such as suspending or blocking an IP address following an infiltration attack.

FortiNAC

FortiEDR shares endpoint threat intelligence and discovered assets with FortiNAC. With Syslog sharing, FortiEDR management can instruct enhanced response actions for FortiNAC, such as isolating a device.

FortiSandbox

FortiEDR native integration with FortiSandbox automatically submits files to the sandbox in the cloud, supporting real-time event analysis and classification. Additionally, it also shares threat intelligence with FortiSandbox.

FortiSIEM

FortiEDR sends events and alerts to FortiSIEM for threat analysis and forensic investigation. FortiSIEM includes a designated parser for FortiEDR OOTB and can also utilize JSON and REST APIs to further integrate with FortiEDR.

FortiGuard Labs

FortiEDR native integration with FortiGuard Labs allows up-to-date intelligence, supporting real-time incident classification to enable accurate incident response playbook activation.

Services

FortiEDR Deployment Services

The deployment services deliver expert assistance to ensure a successful deployment. Including architecture and planning, configuration, installation, playbook set up, environment tuning, and training.

FortiResponder Managed Detection (MDR) and Response Service

The FortiResponder Managed Detection and Response (MDR) Service provides customers with 24x7 continuous threat monitoring, alert triage, and incident handling by experienced analysts and the platform. Customers gain peace of mind knowing that highly trained experts review and analyze every alert, take actions to keep customers secure, and provide detailed recommendations on remediation and next steps for incident responders and IT administrators. The FortiResponder MDR Service helps scale existing operations and further enhances SOC maturity.

Specification

Management, architecture, and platform support

A single, integrated management console provides prevention, detection, and incident response capabilities. Extended REST APIs are available to support any console action and beyond.

- **Offline protection** - Protection and detection happen on the endpoint, protecting disconnected endpoints.
- **Native cloud infrastructure** - FortiEDR features multi-tenant management in the cloud. The solution can be deployed as a cloud-native, hybrid, or on-premises. It also supports air-gapped environments.
- **Lightweight endpoint agent** - FortiEDR utilizes less than 1% CPU, up to 120 MB of RAM, 20 MB of disk space, and generates minimal network traffic.

FortiEDR supports Windows, macOS, and Linux operating systems, and offers offline protection.

- Windows (both 32-bit and 64-bit versions) XP SP2/SP3, 7, 8, 8.1 and 10
- Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 and 2019
- macOS Versions: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) and Catalina (10.15)
- Linux Versions: RedHat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7 and Ubuntu LTS 16.04.5, 16.04.6,
- 18.04.1 and 18.04.2 server, 64-bit
- Virtual Desktop Infrastructure (VDI) environments in VMware and Citrix. VDI Environments: VMware Horizons 6 and 7, and Citrix XenDesktop 7

FORTINET

Fortinet Product Matrix

產品	效能	Description	作業版本
Fortinet 標準版資安防護系統 一年授權	防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN，SSL VPN, SLB(主機負載平衡）及 無線網路控制器（Wireless Controller）	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 標準版資安防護系統 防護升級模組 一年授權	防護升級模組 一年授權		
Fortinet 高階版資安防護系統 一年授權	高階版防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN，SSL VPN, SLB(主機負載平衡）， 無線網路控制器（Wireless Controller），入侵防禦，應用程式控管，防毒，不當網頁過濾，防垃圾郵件	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 高階版資安防護系統 防護升級模組 一年授權	高階版資安防護系統 防護升級模組 一年授權		
FMG-VM-Base Fortinet 集中管理系統	集中管理系統 10 台設備	Fortinet 防火牆管理，設定和集中派送（政策，資安防禦資料庫）的中央管理系統 r, 支援 10 台設備	Vmware Hyper-V AWS
FMG-VM-10-UG Fortinet 集中管理系統	集中管理平台設備 數量升級 - 10 台設備		
FAZ-VM-BASEFortinet 集中日誌報表系統	集中日誌報表系統	Fortinet 防火牆的集中日誌報表管理系統	Vmware Hyper-V AWS
FAZ-VM-GB1 Fortinet 集中日誌報表系統 紀錄數量升級 - 1 GB/Day	集中日誌報表系統 紀錄數量升級 - 1 GB/Day		
FSA-VM Fortinet 先進威脅防護系統 (ATP)	先進威脅防護系統 (ATP)	即時執行沙箱檢測，提供虛擬的運行環境來分析高風險或可疑的程式，研判威脅完整的生命周期，協助用戶智慧地立即偵測出既存與新興的 網路威脅。	VMware
FWB-Base Fortinet 網站應用程式防火牆(WAF) 25Mbps	網站應用程式防火牆(WAF) 25Mbps	提供網站應用程式防火牆功能（WAF）， 網頁防置換，網頁自動備份及回復等功能	Vmware Hyper-V Citrix Xen Open Xen AWS
FWB-100-UG Fortinet 網站應用程式防火牆(WAF) 頻寬升級 100Mbps	網站應用程式防火牆(WAF) 頻寬升級 100Mbps		

FWB-VM01/VM02/VM04/VM08 Fortinet 網站應用程式防火牆(WAF) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網站應用程式防火牆(WAF) 支援 1 CPU		
FAD-Base Fortinet 主機負載平衡系統 (SLB) 1Gbps	主機負載平衡系統(SLB) 1Gbps	支援網路的主機負載平衡，全球服務負載平衡（GSLB）及線路負載平衡（LLB）等功能	VMware
FAD-1000-UG Fortinet 主機負載平衡系統 (SLB) 頻寬升級 1Gbps	主機負載平衡系統(SLB) 頻寬升級 1Gbps		
FAD-VM01/VM02/VM04/VM08 Fortinet 主機負載平衡系統(SLB) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	主機負載平衡系統(SLB) 支援 1 CPU		
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡 400Mbps	網路負載平衡系統(WAN) 400Mbps	提供網路線路負載平衡，整合不同 ISP 的線路同時並存，提供進出 Internet 的資料流量	VMware ESXi / ESX 5.5, 6.0
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡頻寬升級 400Mbps	網路負載平衡頻寬升級(WAN) 400Mbps		
FC-10-FWV02-851-02-12 Fortinet 網路線路負載平衡 一年續約授權	網路負載平衡系統(WAN) 一年續約授權		
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡系統(SLB) (授權方式：依照 CPU 數量 2/4 二個授權方式出貨)	網路負載平衡系統(WAN) 支援 2 CPU		
FSM-AIO-BASE Fortinet 稽核管理系統 50 台設備一年授權	稽核管理系統 50 台設備一年授權	SIEM 應用解決方案，提供收集和整合各種網路和安全資訊，匯整之後進行統一分析和統計，藉以收集、監視和報告企業中的網路設備和資安產品發生的行為，持續進行企業內全面的安全風險評估。	Vmware ESX, Microsoft HyperV, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure
FSM-AIO-100-UG Fortinet 稽核管理系統升級 100 台設備一年授權	稽核管理系統升級 100 台設備一年授權		
FSM-WIN-ADV-50-UG Fortinet 稽核管理系統 Windows Agent 50 台設備一年授權	稽核管理系統 Windows Agent 50 台設備一年授權		

FC1-15-EMS01-158-02-12 Fortinet 端點(End Point)資安防護 200 Clients 一年授權	端點(End Point)資安防護 200 Clients 一年授權	提供防病毒與惡意軟體檢測、雙因子認證、VPN 等功能，強化企業資安建置。FortiClient 主動防禦高級攻擊。它與 Security Fabric 的緊密集成使基於策略的自動化能夠控制威脅並控制爆發。FortiClient 與 Fabric-Ready 合作夥伴兼容，進一步加強企業的安全態勢。	Microsoft Windows, Windows Server
Fortinet 物聯網安全管理系統 100 台終端設備 一年授權	物聯網安全管理系統 100 台終端設備 一年授權	提供物聯網上每個終端設備的詳細分析以增強其可視性，控管設備之物聯網存取以保障資訊安全，並具備資料分析與報表功能。	VMware, Hyper-V
Fortinet 物聯網安全管理系統升級 100 台終端設備 一年授權	物聯網安全管理系統升級 100 台終端設備 一年授權		
FML-Base Fortinet 反垃圾郵件及郵件保全系統 100 人版	反垃圾郵件及郵件保全系統 100 人版	提供電子郵件主機功能、過濾並攔截垃圾郵件	VMware Hyper-V Citrix Xen KVM
FML-300-UG Fortinet 反垃圾郵件及郵件保全系統使用者數量升級 300 人	反垃圾郵件及郵件保全系統使用者數量升級 300 人		
FML-VM01/VM02/VM04/VM08 Fortinet 反垃圾郵件及郵件保全系統(授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	反垃圾郵件及郵件保全系統支援 1 CPU		
FAC-VM-Base Fortinet 身份認證系統 (Authenticator) 100 人版	身份認證系統(Authenticator) 100 人版	整合 RADIUS、LDAP 伺服器，提供標準及安全的雙因子認證	VMWare Hyper-V
FAC-VM-100-UGFortinet 身份認證系統 (Authenticator) 使用者數量升級 100 人	身份認證系統(Authenticator) 使用者數量升級 100 人		
FortiEDR Fortinet 端點偵測、保護與回應系統(雲端版)	Fortinet 端點偵測、保護與回應系統(雲端版)	FortiEDR 提供即時，自動化的端點保護 通信設備-包括工作站和所有伺服器 OT 系統-全部集中集成平台 具有靈活部署和一個可節省的運營成本	無
FortiEDR Fortinet 端點偵測、保護與回應系統(雲端版) 擴充 25 個端點資產	Fortinet 端點偵測、保護與回應系統(雲端版) 擴充 25 個端點資產		
FortiEDR Fortinet 端點偵測、保護與回應系統(本地自建版)	Fortinet 端點偵測、保護與回應系統(本地自建版)		*Windows (both 32-bit and 64-bit versions) XP SP2/SP3, 7, 8, 8.1 and 10 * Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 and 2019 * macOS Versions: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) and Catalina (10.15) * Linux Versions: RedHat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7 and Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 and 18.04.2 server, 64-bit *Virtual Desktop Infrastructure (VDI) environments in VMware and Citrix. VDI Environments: VMware Horizons 6 and 7, and Citrix，XenDesktop 7"
FortiEDR Fortinet 端點偵測、保護與回應系統(本地自建版) 擴充 25 個端點資產	Fortinet 端點偵測、保護與回應系統(本地自建版) 擴充 25 個端點資產		

FortiProxy Fortinet 上網行為控管系統 1CPU (依照 CPU 數量授權方式出貨)	Fortinet 上網行為控管系統 防護升級模組	FortiProxy 是一種安全的 Web 代理，可保護員工免受互聯網傳播的攻擊，結合了多種檢測技術， 例如：如網絡過濾，DNS 過濾，防止數據丟失，防病毒，入侵防禦和高級威脅保護	VMware ESX/ESXi, KVM Platform
FortiProxy Fortinet 上網行為控管系統 防護升級模組	Fortinet 上網行為控管系統 防護升級模組		