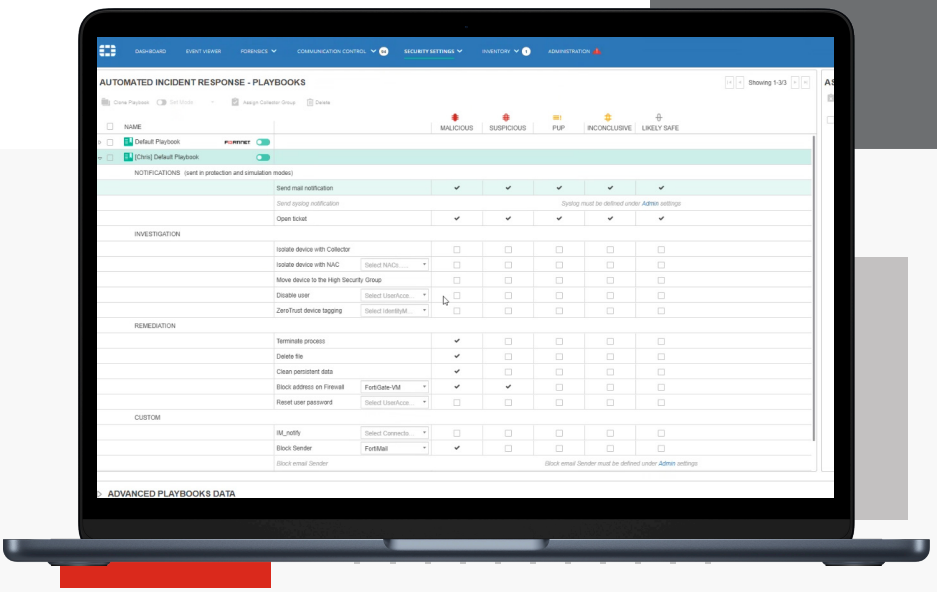
FortiEDR™



Highlights

- Real time proactive risk mitigation and IoT Security
- Pre-infection Protection
- Post-infection protection

Real Time Endpoint Protection, Detection, and Automated Response

FortiEDR delivers real-time, automated endpoint protection with orchestrated incident response across any protected device. This protection includes workstations, servers, and cloud workloads with current and legacy operating systems, as well as manufacturing and OT systems. FortiEDR features native integrations with the Fortinet Security Fabric along with numerous third-party solutions.

Available in

Software

Supported Platforms

- Windows XP SP2/SP3, 7, 8, 8.1, 10, and 11 (32-bit and 64-bit versions)
- Windows Server 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, and 2022
- MacOS Versions: El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x), and Monterey (12.x), and Ventura (13.x)
- Linux Versions: RedHat Enterprise Linux and CentOS 6.x, 7.x, 8.x, and 9.x,
  Ubuntu LTS 16.04.x, 18.04.x, 20.04.x, and 22.04x server, 64-bit only
  Oracle Linux 6.x+, 7.7+, and 8.2+,
  Amazon Linux AMI 2
  SuSE SLES 15.1
- VDI Environments: VMware Horizons 6 and 7 and Citrix XenDesktop 7
- Google Cloud Marketplace enablement for all supported OSes

Features

Real Time Proactive Risk Mitigation and IoT Security

Greatly reduces the attack surface through vulnerability assessments and risk mitigation policies like virtual patching and application control.

Pre-Infection Protection

Provides a proven first layer of defense via a custom-built, kernel-level next-generation machine-learning-based antivirus (NGAV) engine that prevents infection from advanced attacks like ransomware.

Post-Infection Protection

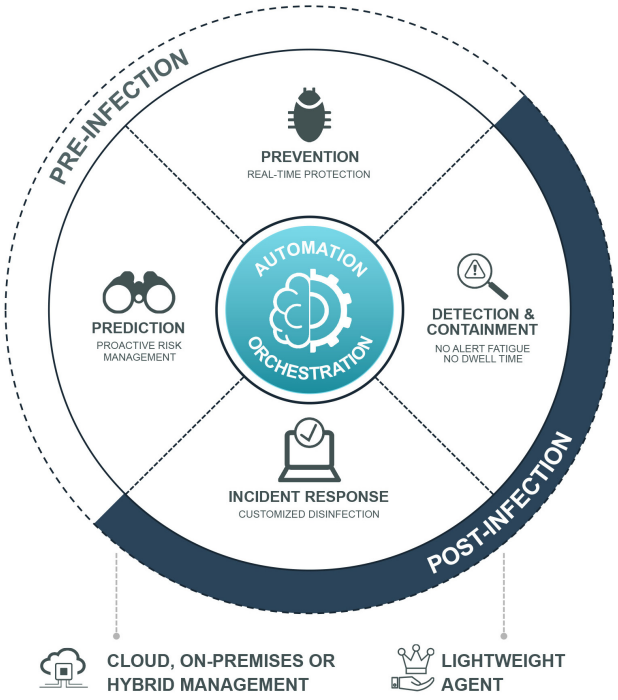
FortiEDR is the only solution that detects and stops advanced attacks in real time, even when the endpoint has been compromised. No breaches, no data loss, no problem. FortiEDR eliminates dwell time and provides a suite of automated endpoint detection and response (EDR) features to detect, defuse, investigate,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

Highlights

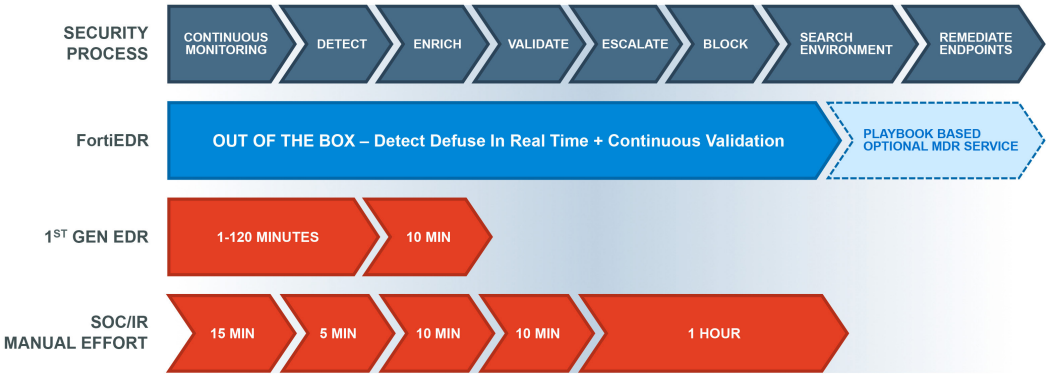
Comprehensive Endpoint Security Platform

Listed as a visionary in the Gartner Magic Quadrant for Endpoint Protection Platforms, 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. This solution allows 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. Built with native cloud infrastructure, FortiEDR can be deployed in the cloud, on-premises, and as a hybrid deployment.



Benefits



Protection

As proven with MITRE ATT&CK Evaluation results and SE Labs, FortiEDR enables proactive, real-time, automated endpoint protection with orchestrated incident response across platforms. Using AI and machine learning at the kernel level, it stops breaches with real time blocking to protect data from exfiltration and ransomware encryption.

Management

FortiEDR delivers a unified and intuitive cloud-managed platform. It closes the loop by automating routine endpoint security tasks to reduce strain on your staff. It also supports RBAC and secure remote shell.

Integration

Integrate with Fortinet and third-party solutions like NGFW, NAC, SIEM and more to improve security and orchestration.

Scalability

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

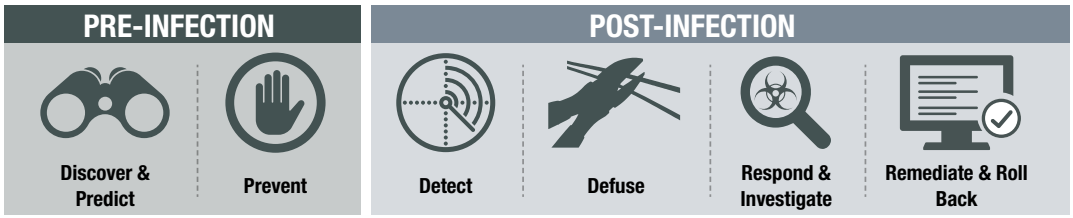
Flexibility

FortiEDR can address an array of enterprise use cases. The cloud management platform can be deployed on-premises, or on a secure cloud instance. Endpoints are protected both on- and off-line through onboard AI.

Cost

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

Feature Highlights



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 the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies

Prevent

FortiEDR uses a machine learning anti-malware engine to stop attacks before 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
- Leverage application control to easily add allowed or blocked applications to pre-defined lists. This feature is useful for locking down sensitive systems like POS devices
- 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 (C2) communications, file tampering, and ransomware encryption. At the same time, Fortinet Cloud Services (FCS), FortiEDR's back end, continues to gather additional evidence, enrich event data, and classify the incidents for a potential automated incident response playbook policy to activate.

Feature Highlights (continued)

FortiEDR surgically stops data breaches 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 on Windows, macOS, and Linux.

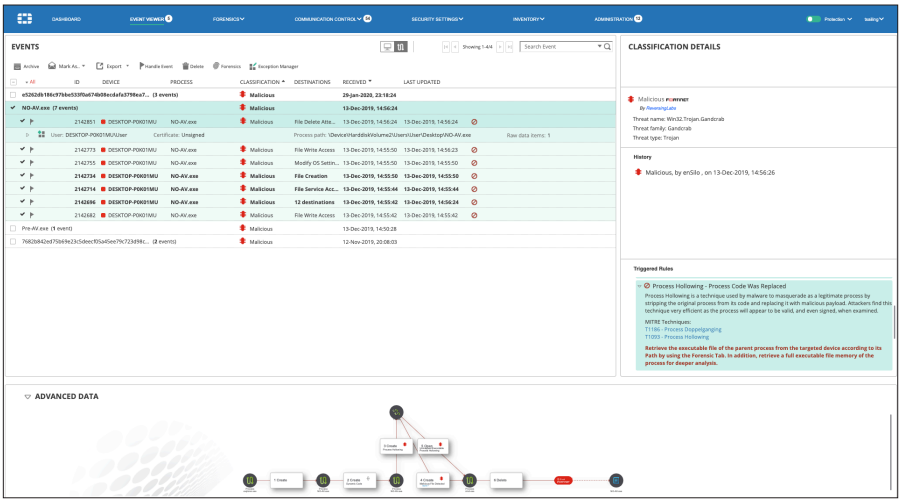
- Automate incident classification to improve incident response and ease of resolution
- Recommends response actions to security analysts
- Standardize incident response procedures across the Fortinet Security Fabric and third-party security and IT tools with playbook automation
- Optimize security resources 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
- Get additional help with the optional managed detection and response (MDR) service

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 interface provides helpful guidance, best practices, and suggests the next logical steps for security analysts. Threat hunting is made easier through the consumption of third-party queries by translating common IoC syntax such as TAXII into FortiEDR's Lucene syntax.

Features

- 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 maps attacks, corresponding to the MITRE ATT&CK framework, as well as logical next step for forensic investigation



Guide interface displays clear explanations why the event is flagged as suspicious or malicious maps attacks corresponding to the MITRE ATT&CK 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 to a remediation VLAN.

FortiSandbox

FortiEDR's native integration with FortiSandbox automatically submits suspicious files to the sandbox in the cloud, supporting real-time event analysis and classification. Additionally, it 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 out of the box 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.

FortiClient/EMS

Ingest the endpoint status from FortiEDR for a Zero-Trust Network Access (ZTNA) posture check.

Services

FortiEDR Deployment Best Practices Services (BPS)

The deployment services deliver expert assistance to ensure a successful deployment. These services include 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 24×7 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.

Specifications

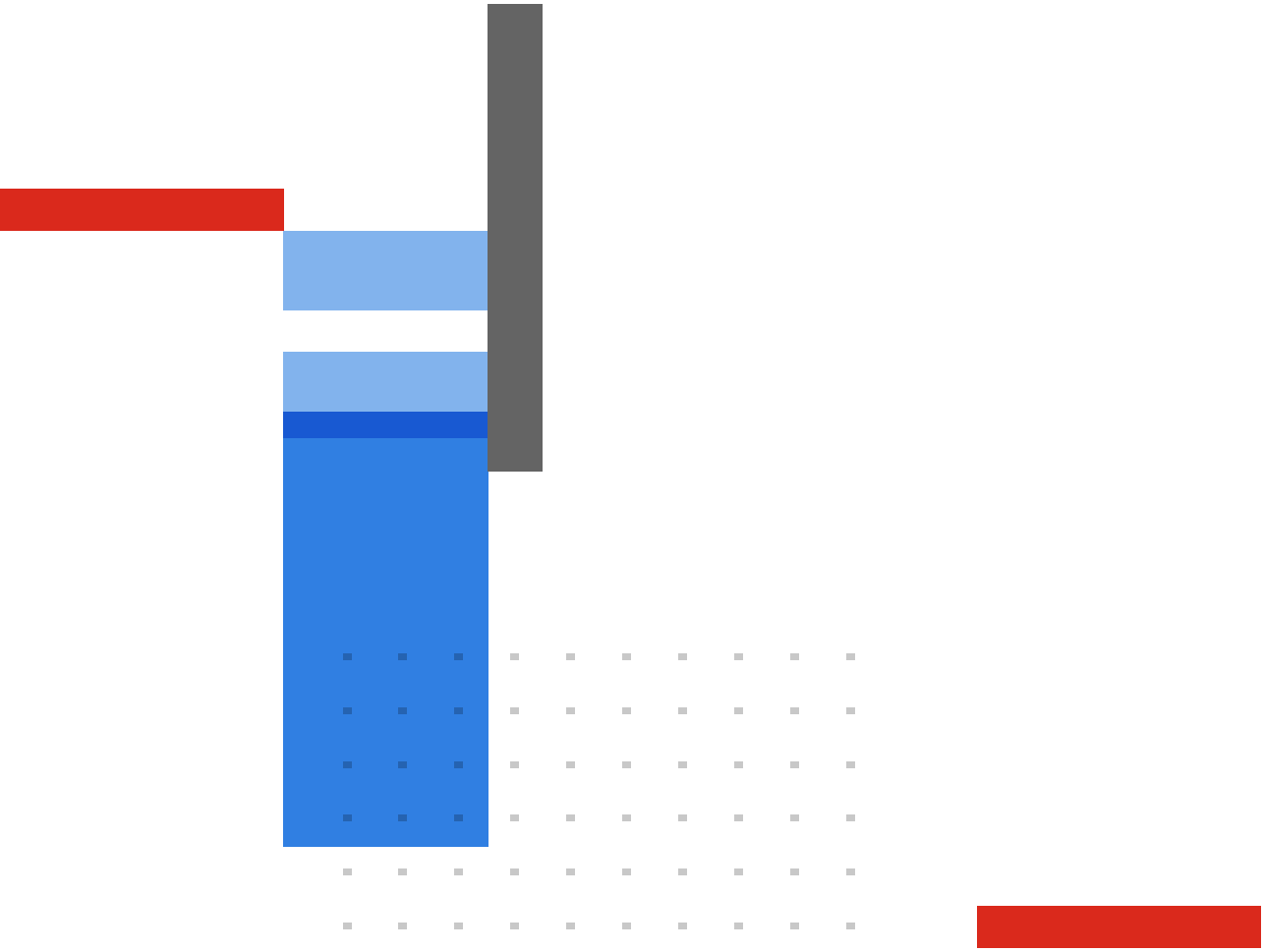
Management and Architecture

A single, integrated management console provides prevention, detection, and incident response capabilities in English and Japanese. Extended REST APIs are available to support any console action and beyond. Avoid risking misconfiguration of security settings with granular role-based access control (RBAC) for administrators and users of the management console. Secure remote shell grants administrators remote troubleshooting capabilities for their work-from-anywhere workforce with a suite of security utilities including timed certificates to mitigate exploitation.

- **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
- **Lightweight Endpoint Agent** - FortiEDR solution utilizes less than 1% CPU, up to 120 MB of RAM, 20 MB of disk space, and generates minimal network traffic
- **Cloud Deployable** - Deployable from Google Cloud Marketplace with automated endpoint deployment orchestration for Google Compute Engine

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

October 3, 2023

FEDR-DAT-R15-20231003