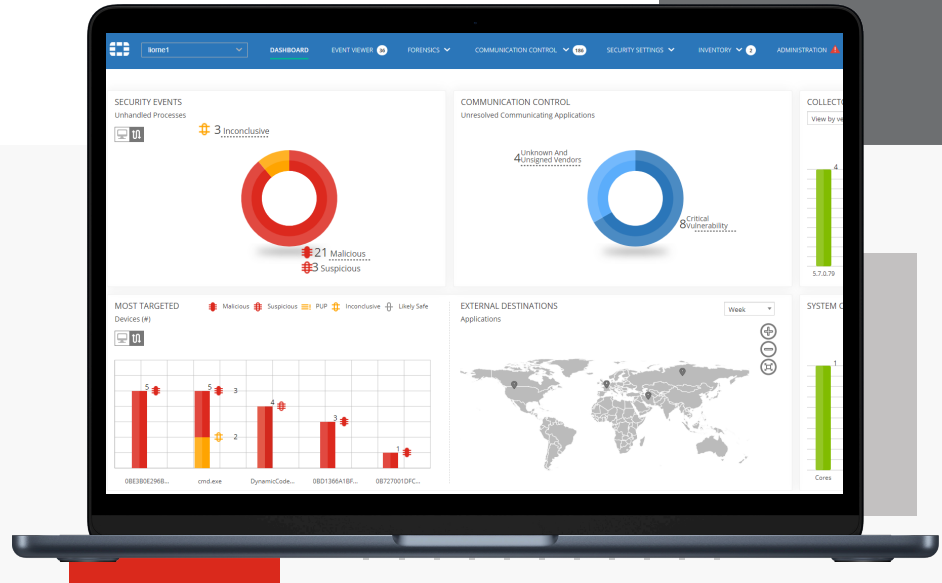


FortiEDR™



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 mobile devices, workstations, servers, and cloud workloads for current and legacy operating systems, as well as manufacturing and OT systems with full feature parity. FortiEDR features native integrations with the Fortinet Security Fabric along with numerous third-party solutions and is the base for FortiXDR, which is enabled with an additional license.



Supported Platforms

- Windows XP SP2, 7, 8, 8.1, 10, and 11 (32-bit and 64-bit versions)
- Windows Server 2003 SP2, R2 SP2, 2008 SP1, 2008 R2 SP2, 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), Monterey (12), Ventura (13), and Sonoma (14)
- Linux Versions: RedHat Enterprise Linux and CentOS 6.8+, 7.2+, 8+, and 9+
Ubuntu LTS 16.04.5+, 18.04/ 20.04/and 22.04 server, 64-bit only
Oracle Linux 6.10, 7.7+, and 8.2+
Amazon Linux AMI 2 2018
Open SUSE Leap 15.2
SUSE Linux Enterprise Server SLES v12 SP5 and v15
RedHat 9
- VDI Environments: VMware Horizons 6 and 7 and Citrix XenDesktop 7
- Google Cloud Marketplace enablement for all supported OSes
- Mobiles: Android 8.1+ and iOS 15+

Features



Real Time Proactive Risk Mitigation and IoT Security

Greatly reduces the attack surface through vulnerability assessments and risk mitigation policies like virtual patching, device discovery, 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 in real time.



Post-Infection Protection

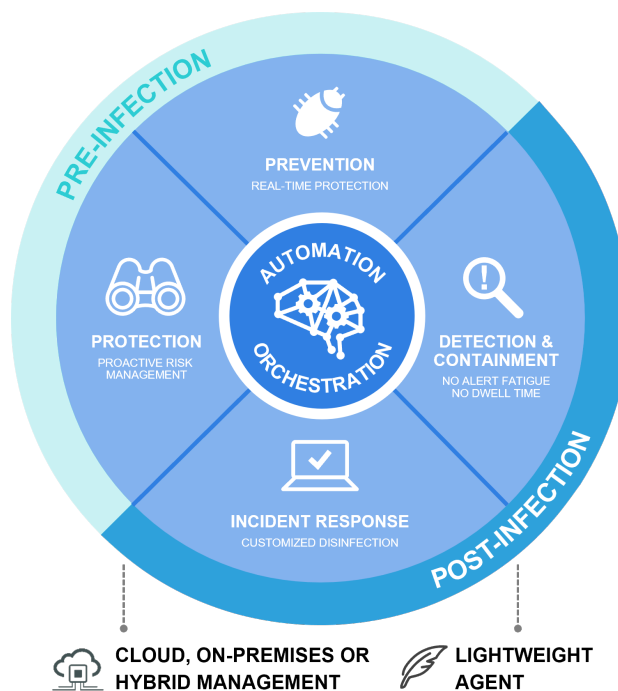
FortiEDR is the only solution that detects and stops advanced attacks in real time, even when the endpoint has been compromised. No breaches, no data loss, no problem. FortiEDR eliminates dwell time and provides a suite of automated endpoint detection and response (EDR) features to detect, defuse, investigate,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

Highlights

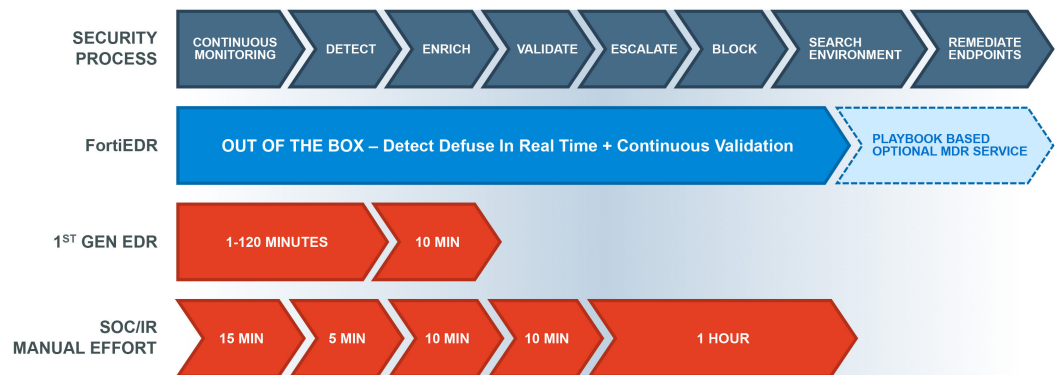
Comprehensive Endpoint Security Platform

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 your pocket to the cloud with current and legacy operating systems to POS and manufacturing controllers with a flat per-device licensing cost. Built with native cloud infrastructure, FortiEDR can be deployed in the cloud, on-premises, and as a hybrid deployment.



Benefits



How FortiEDR reduces the meantime to detect and repair events compared to legacy solutions and methods



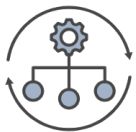
Protection

As proven with MITRE ATT&CK Enterprise Evaluation results and SE Labs Endpoint Security Enterprise 2023 Q4 tests, FortiEDR enables proactive, real-time, automated endpoint protection with orchestrated incident response across platforms. Using AI and machine learning at the kernel level (on Windows and Linux), 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, ZTNA, NDR, SOAR, and more to improve security and automated 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 that continually monitors system behavior for policy violations.



Cost

Eliminate post-breach operational expenses and breach damage to the organization, all for a low, predictable cost and capped TCO with flexible purchasing options like FortiFlex.



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 (such as unprotected or unmanaged devices) and IoT devices
- Track applications and their CVE status
- 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 via FortiGuard Threat Intelligence
- Protect disconnected endpoints with offline protection
- Leverage application control to easily add allowed or blocked applications to pre-defined lists and also provide granular management of applications
- 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 with FortiGuard Threat Intelligence and multi-engine sandboxing, both within Fortinet Cloud Services
- 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 (without reliance on VSS images which are targeted by ransomware), 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 the FortiEDR 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

The screenshot displays the FortiEDR interface with the following components:

- EVENTS Table:**

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
hobgoblin (7 events)						
50671	hobgoblin	wemgr.exe	Malicious		16-Mar-2023, 16:50:26	16-Mar-2023, 16:57:46
50593	hobgoblin	explorer.exe	Inconclusive	File Creation	16-Mar-2023, 16:50:26	16-Mar-2023, 16:50:26
50593	hobgoblin	explorer.exe	Suspicious	2 destinations	16-Mar-2023, 16:49:53	16-Mar-2023, 16:56:59
50580	hobgoblin	msi_installer.exe	Suspicious	File Execution At...	16-Mar-2023, 16:49:43	16-Mar-2023, 16:57:46
50662	hobgoblin	svchost.exe	Malicious	Modify OS Sett...	16-Mar-2023, 16:50:21	16-Mar-2023, 16:50:21
50647	hobgoblin	net.exe	Malicious	10.20.10.9	16-Mar-2023, 16:50:08	16-Mar-2023, 16:50:08
50634	hobgoblin	MSSVCCFG.dll	Malicious	Network Access	16-Mar-2023, 16:50:03	16-Mar-2023, 16:50:03
50612	hobgoblin	msedge.exe	Malicious	Network Access	16-Mar-2023, 16:49:58	16-Mar-2023, 16:49:58
- CLASSIFICATION DETAILS:**
 - Malicious **runner**
 - Threat name: Unknown
 - Threat family: Unknown
 - Threat type: Unknown
 - Automated analysis steps completed by Fortinet Details
 - History: Malicious, by Fortinet, on 16-Mar-2023, 16:50:03
- ADVANCED DATA:**
 - Event Graph: Automated Analysis
 - Analysis View
 - Graph showing process flow: 1 Create (Process explorer.exe) → 2 Create (Process explorer.exe) → 3 Inject (Malicious File Created, Process explorer.exe) → 4 Create (Injected Executable, Process msedge.exe) → 5 Connect (Injected Executable, Process msedge.exe) → 6 Block (Process msedge.exe) → 7 Connect (Process msedge.exe).

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 can send 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.



FortiNDR

This integration combines real-time AI-enabled network threat detection with endpoint data to provide early, enriched threat intel and decrease incident analysis and response time, helping SOC analysts be more efficient in detecting known/unknown threats and expediting response across any environment (on-premise, hybrid, multi-cloud).

Services

FortiEDR Deployment Best Practices Services (BPS)

This deployment service delivers expert assistance to ensure a successful deployment. These services include architecture and planning, configuration, installation, playbook set up, environment tuning, and training.

FortiGuard Managed Detection (MDR) and Response Service

The [FortiGuard 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

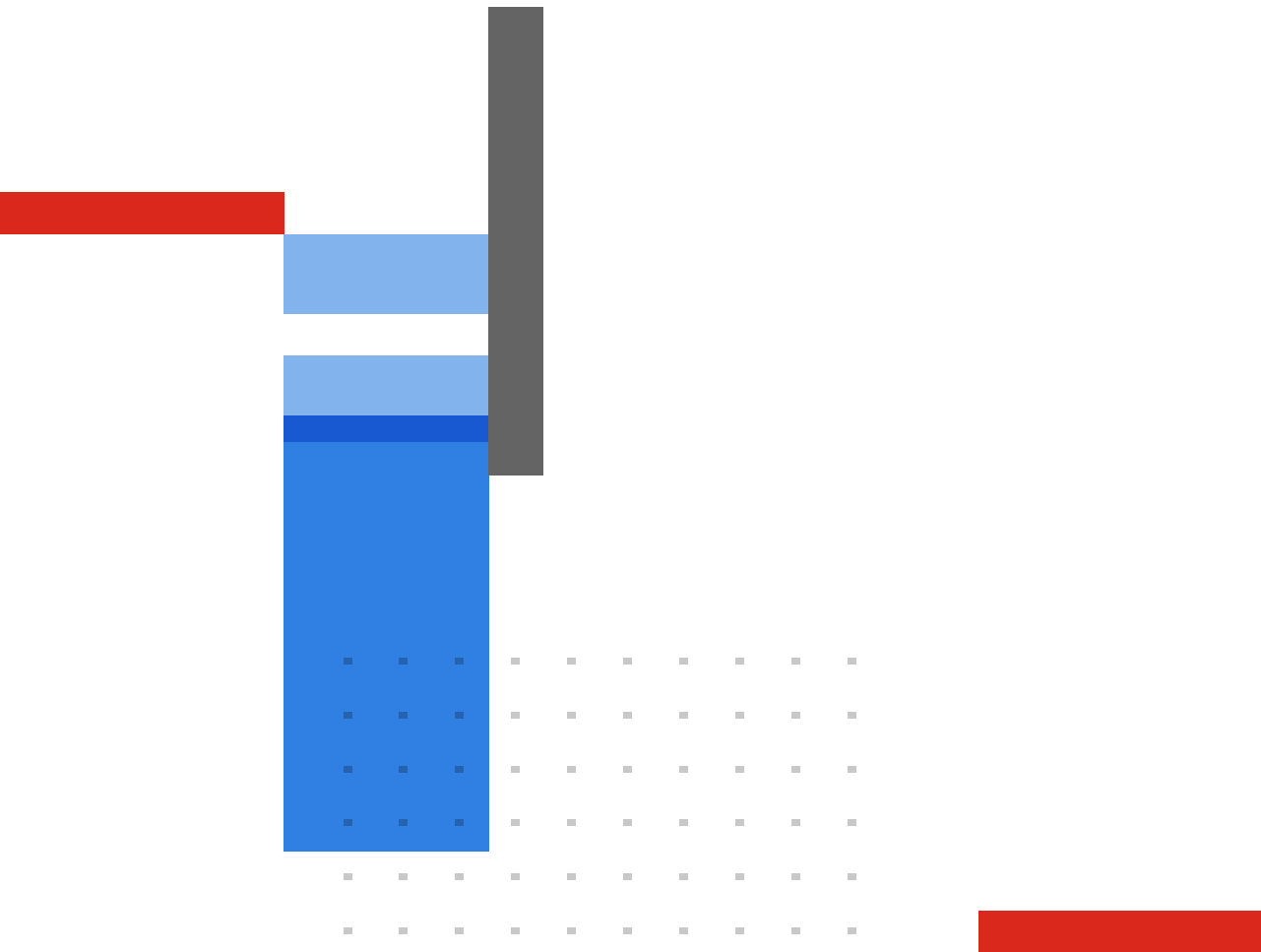
A single, integrated management console provides prevention, detection, and incident response capabilities in English, traditional Chinese, and Japanese. Extended REST APIs are available to support any console action and beyond. Avoid risking misconfiguration of security settings with granular role-based 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% to 2% CPU, 200 MB to 350 MB of memory usage, 750 MB to 1 GB of disk space, and generates minimal network traffic (Upper limits of memory usage and disk space are related to the threat hunting [response license] capability)
- **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](#).



www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.