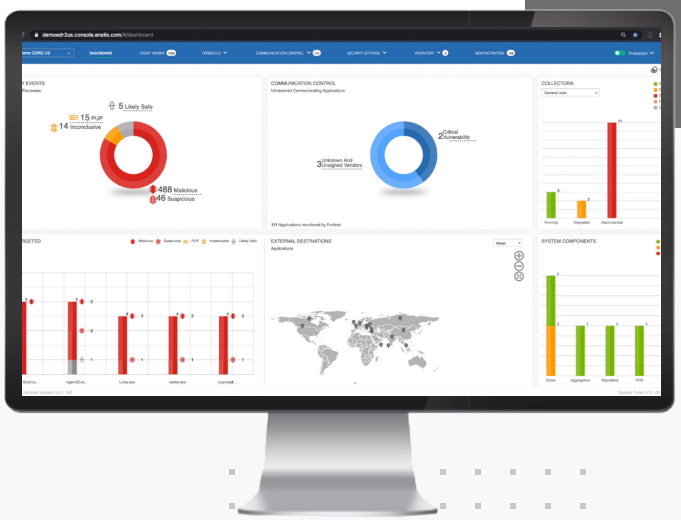
FortiXDR™



Telemetry

- Cloud Security
- Web App Security
- Email Security
- Network Security
- LAN/ WAN/ WLAN
- Identity Services
- Endpoint Security
- IoT Security
- Security Incident Event Managment (SIEM)

Automated Incident Identification, Investigation, and Remediation

FortiXDR brings security orchestration to the Fortinet Security Fabric and third-party solutions with eXtended Detection and Response (XDR). Specifically, it analyzes security and audit related information feeds from your data lakes without need of replication to identify potential security incidents. These cross-platform feeds are correlated into incidents investigated by artificial intelligence. Based on the classification returned, organizations can pre-define an automated cross-platform response. FortiXDR customers can identify more threats, contain them faster and ease the alert burden on security teams.

MITRE ENGENUITY | ATT&CK® Evaluations

PCI DSS COMPLIANT

HIPAA COMPLIANT

AICPA SOC aicpa.org/soc4so

Highlights

Extended Detection

Applies Fortinet curated analytics to the correlated telemetry natively shared across the Security Fabric to correlate low-fidelity alerts into single high fidelity events.

AI-Powered Investigation

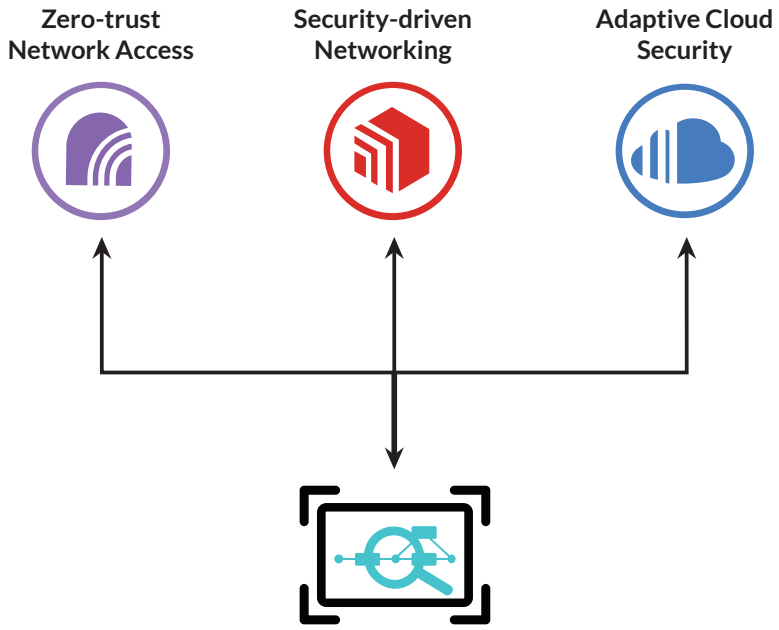
Leverages a Fortinet deep learning engine, dynamically selected enriching, and microservices to replicate the investigation of security incidents typically handled by security experts.

Extended Response

Utilizes a granular, automatable framework to pre-define remediation actions across multiple security infrastructure controls like firewalls, email security, identity, and more.

Fully Automatable Extended Detection and Response (XDR)

As an extension of the Fortinet Security Fabric, FortiXDR benefits from the broadest set of telemetry originating from the most independently certified controls and covering the most cyber kill chain stages available in the industry. FortiXDR supports pre-configured automatable response coordinated across both Fortinet and third-party products. Most importantly, FortiXDR is the only XDR solution that includes patent-pending artificial intelligence trained to dynamically conduct incident investigation by leveraging microservices that emulate different aspects of the process just like an expert security professional. Built on the cloud-native foundation of FortiEDR, it is easy to deploy and continually curated by Fortinet experts.



Available in

Virtual

Hosted

Benefits

Reduce Alert Volume

FortiXDR applies analytics to the correlated telemetry of the Security Fabric- reducing cross-platform security information and alerts by 75% and converting them to high fidelity incident detections.

Speed Mean Time to Detection

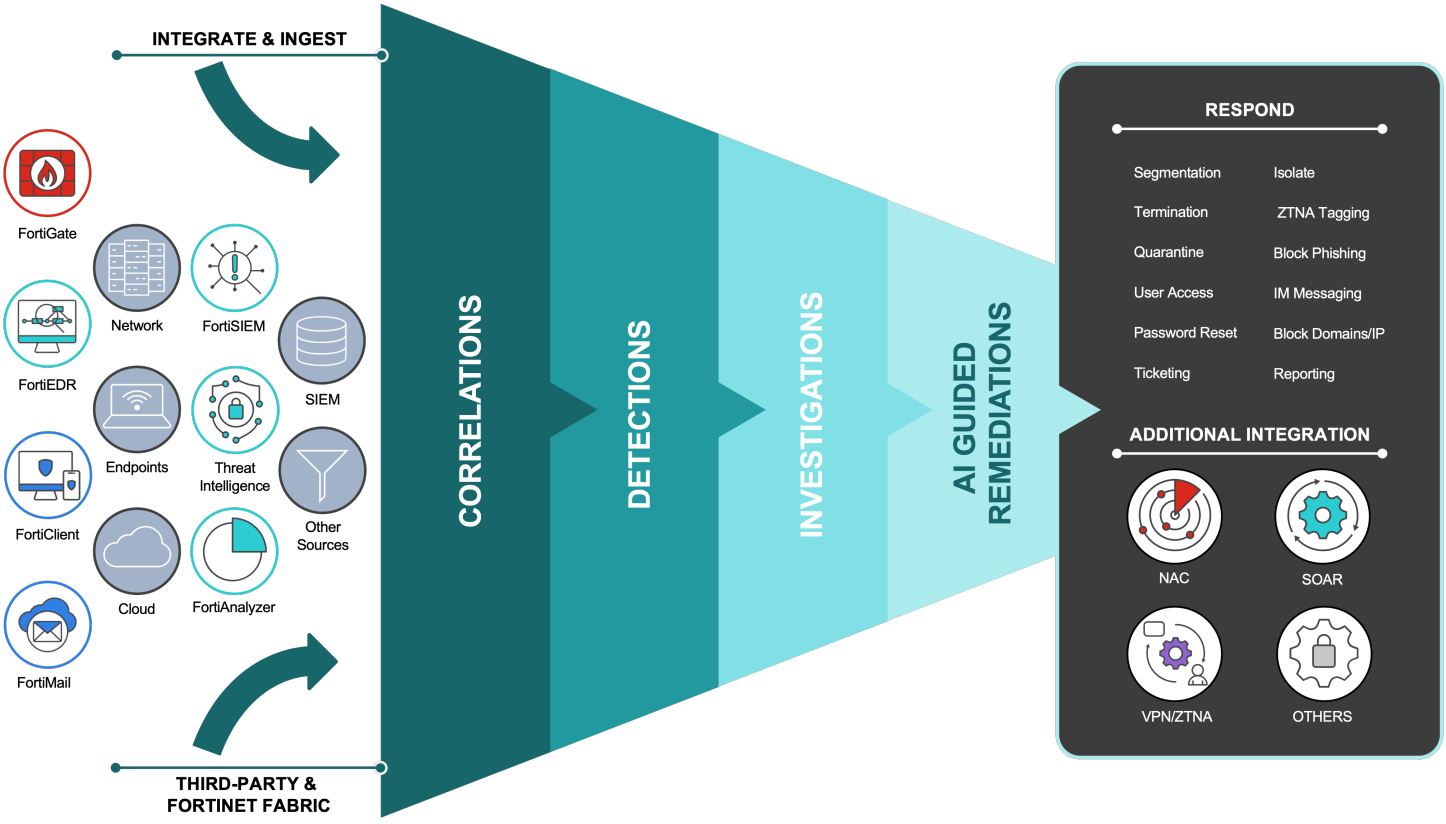
FortiXDR uses deep learning artificial intelligence to automate the investigation process and classify security incidents in 30 seconds or less.

Speed Time to Response

FortiXDR enables customers to predefine response flows — based on incident type, severity and scope as well as impacted users and groups — to automate a coordinated response.

Free Up Security Teams

The reduction of alert volume, use of AI for investigation and automation of response actions allows expert security professionals to move towards more proactive tasks; assessing cyber threats, organizational risk exposure and opportunities to improve security posture.



Features

Extended Detection

FortiXDR includes a curated and expanding set of analytics to make accurate detection of high-risk incidents along with convicting metadata across the Security Fabric.

- Network / Port Scanning / ARP Spoofing
- Brute Force / C2C
- Data Exfiltration / Lateral Movement
- Compromised Credentials / Account
- Potential Phishing

AI-Powered Investigation

FortiXDR uses a Deep Learning engine to dynamically replicate a range of investigation processes with the aid of microservices that replicate the actions of expert analysts and return cross-platform remediation recipes by:

- Pulling Telemetry and Threat Intel
- Performing Static and Dynamic File Analysis
- Comparing Community and Other Reputations
- Building and Comparing UEBA and Other Baselines
- Utilizing additional microservices like Fortinet Cloud Services

Extended, Automatable Response

FortiXDR includes an intuitive framework for customers to pre-define granular, and coordinated response actions based on:

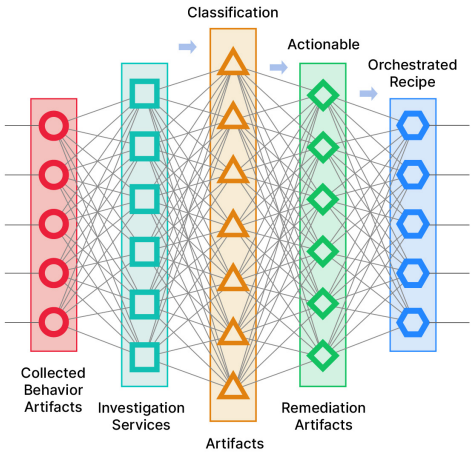
- Users and Groups
- Type, Severity, and Scope of Incident
- Device Isolation and Remediation
- Credential Expiration
- New Threat Intelligence

Features

Third-Party Support

In addition to integration with a range of Fortinet products including FortiGate, FortiNAC, FortiSandbox, FortiEMS, FortiSIEM, FortiAnalyzer, and more, FortXDR also supports integration with non-Fortinet, API supporting products via connectors including:

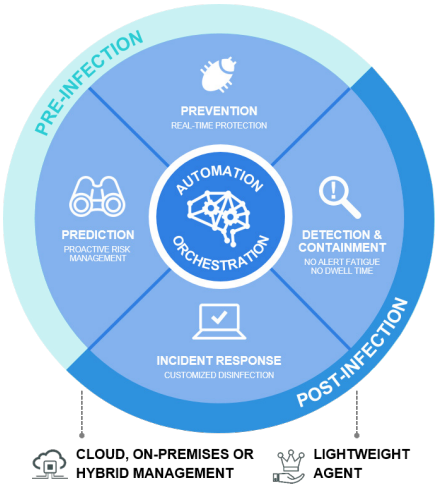
- Firewalls
- Identity Services
- Ticketing Platforms
- Cloud Access Security Brokers (CASB)
- Cloud Workload Protection Platforms
- Network Sandboxes
- Data Lakes



Pre- and Post- Execution Protection

FortiXDR is built on the cloud-native foundation of FEDR and includes an ability to stop breaches and ransomware damage in real-time:

- Pre- and post-execution behavior-based protection
- Unique ability to detect and defuse attacks without stopping system operation
- Patented ransomware protection intercepts file write activity in real-time to evaluate commands and prevent encryption
- Defends everything from workstations and servers with current and legacy operating systems to POS and OT controllers
- Deploys in the cloud, on premise, in an air-gapped environment, and hybrid



Features

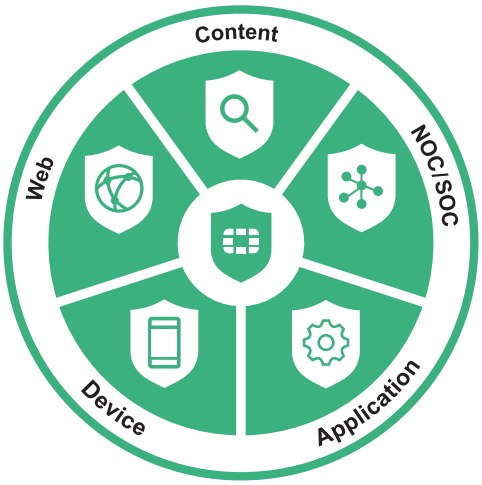
Security Fabric Integration

FortiXDR leverages the Fortinet Security Fabric architecture and integrates with many Security Fabric components:

- FortiGate: instruct enhanced response actions such as suspending or blocking an IP address following an infiltration attack
- FortiNAC: instruct enhanced response actions such as isolating a device
- FortiSandbox: real-time event analysis and classification, threat intelligence sharing
- FortiSIEM: sends events and alerts for unified monitoring and reporting
- FortiGuard Labs: enrich incidents to aid investigation
- FortiMail: Block malicious emails

Fortinet Services

FortiGuard experts deliver upfront deployment services and expert assistance to ensure a successful deployment—including architecture and planning, configuration, installation, playbook set up, environment tuning, and training. They also provide ongoing Managed eXtended Detection and Response (MxDR) service for 24×7 continuous expert monitoring.



Features

Management Architecture

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

Native Cloud Infrastructure
FortiXDR 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 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).

Offline Protection
Protection and detection happen on the endpoint, protecting disconnected endpoints.

Platform Support

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

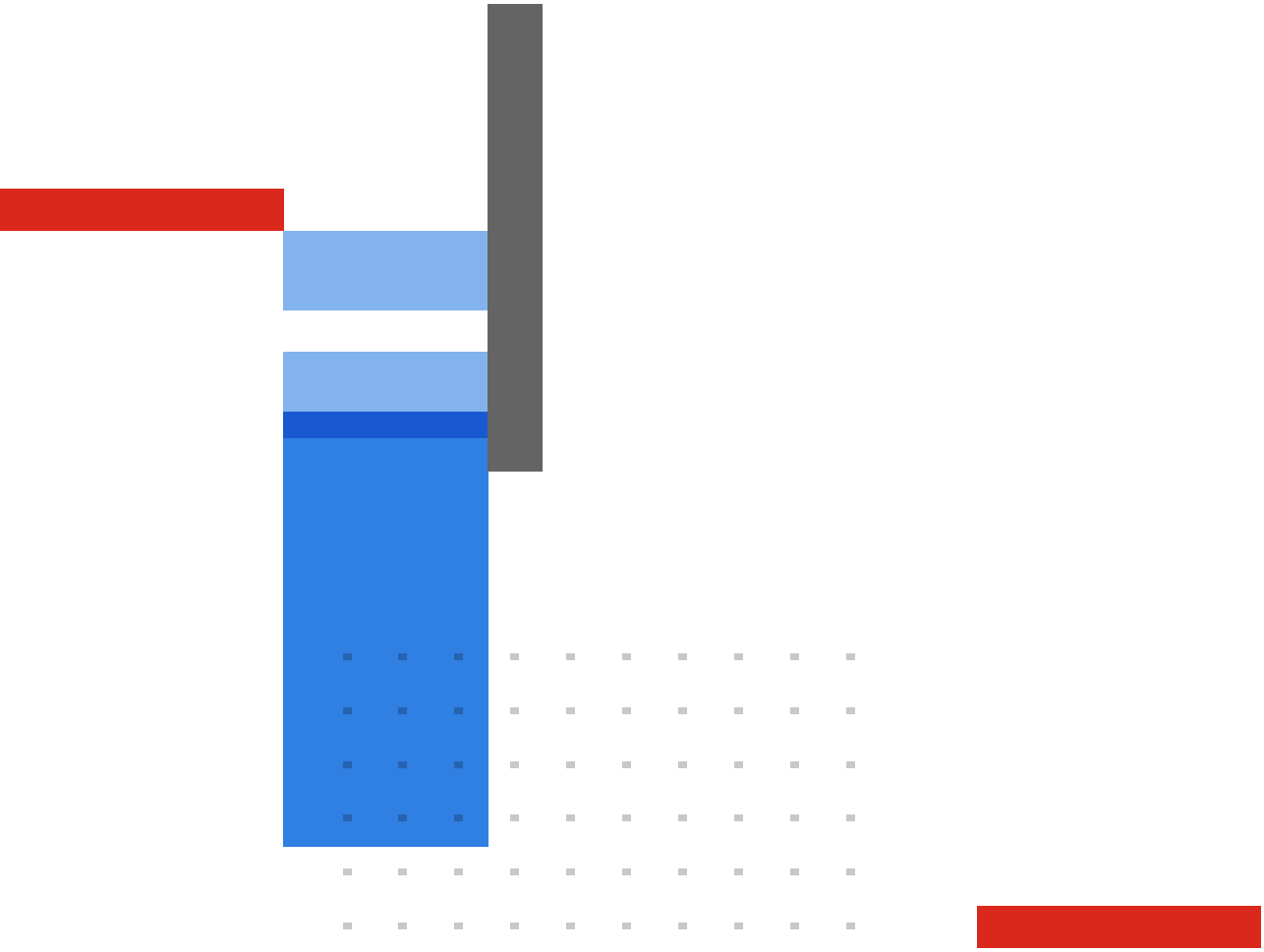
- Windows XP SP2, 7, 8, 8.1, 10, and 11 (32-bit and 64-bit versions)
- Windows Server 2003 SP2, R2 SP2, 2008 SP1, 2008 R2 SP2, 2012, 2012 R2, 2016, 2019, and 2022
- MacOS Versions: El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11), and Monterey (12), and Ventura (13)
- 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 OS

Ordering Information

Product	SKU	Description
Option 1	FCx-10-FEDR1-393-01-DD	FortiEDR Protect & Respond and XDR Cloud Subscription and FortiCare Premium
Option 2	FCx-10-FEDR1-596-01-DD	FortiEDR Protect & Respond and Managed XDR Cloud Subscription and FortiCare Premium
Option 3	FCx-10-FEDR1-394-01-DD	FortiEDR Discover, Protect & Respond and XDR Cloud Subscription and FortiCare Premium
Option 4	FCx-10-FEDR1-597-01-DD	FortiEDR Discover, Protect & Respond and Managed XDR Cloud Subscription and FortiCare Premium

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

April 12, 2024

FXDR-DAT-R05-20240412