DATA SHEET

FortiXDR™

Available in:

Virtual Machine

Hosted

Fully automated incident identification, investigation, and remediation

FortiXDR enhances the Fortinet Security Fabric with eXtended Detection and Response (XDR). Specifically, it analyzes security and audit related information feeds from your Fortinet products 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.

Extended Detection

Applies Fortinet curated analytics to the correlated telemetry natively shared across the Security Fabric in order to identify high fidelity incidents.

AI-Powered Investigation

Leverages a Fortinet trained 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.

Telemetry

- Cloud Security
- Web App Security
- Email Security
- Network Security
- LAN/ WAN/ WLAN
- Identity Services
- Endpoint Security
- IoT Security

MITRE ENGENUITY | ATT&CK Evaluations

PCI DSS COMPLIANT

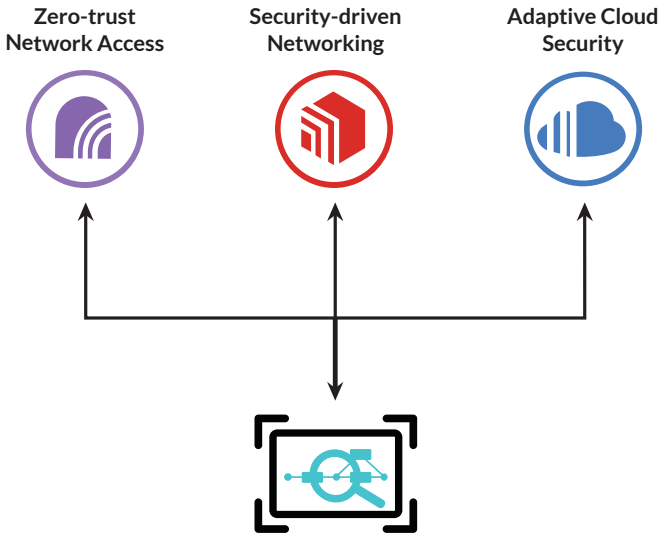
HIPAA COMPLIANT

AV comparatives

HIGHLIGHTS

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. Further, it supports pre-configured automatable response coordinated across both Fortinet and third party products. But most importantly, FortiXDR is the only XDR solution that includes patent-pending artificial intelligence trained to dynamically conduct incident investigation- leveraging microservices that emulate different aspects of the process- like expert security professional. Built on the cloud-native foundation of FortiEDR, it is easy to deploy and continually curated by Fortinet experts.



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 into more strategic roles; assessing cyber threats, organizational risk exposure and opportunities to improve security posture.

Incremental Investment

With high value detections from the combination of network and endpoint telemetry, FortiXDR adds value to any FortiGate customer. Over time, customers can continue to expand their Fortinet Security Fabric- covering email, web applications, cloud and more for an even greater return on their Fortinet investment.

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.

- Pull Telemetry and Threat Intel
- Perform Static and Dynamic File Analysis
- Compare Community and Other Reputations
- Build and Compare UEBA and Other Baselines
- More microservices

Extended, Automatable Response

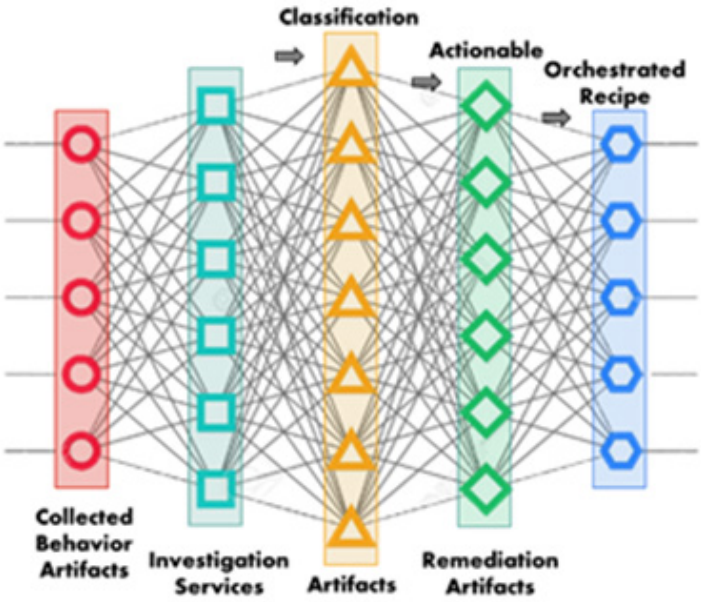
FortiXDR includes an intuitive framework for customers to pre-define granular, coordinate response actions based on:

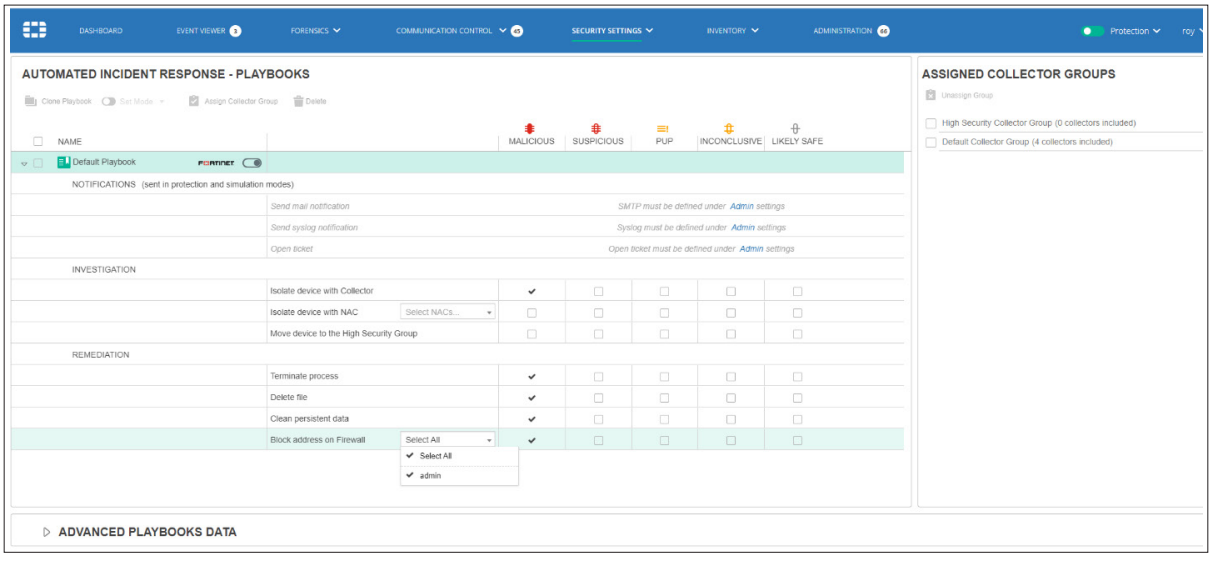
- Users and Groups
- Type, Severity, and Scope of Incident
- Device Isolation and Remediation
- Credential Expiration
- New Threat Intelligence

Third Party Support

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

- Firewalls
- Identity Services
- Ticketing platforms
- Cloud Access Security Brokers
- Cloud Workload Protection Platforms



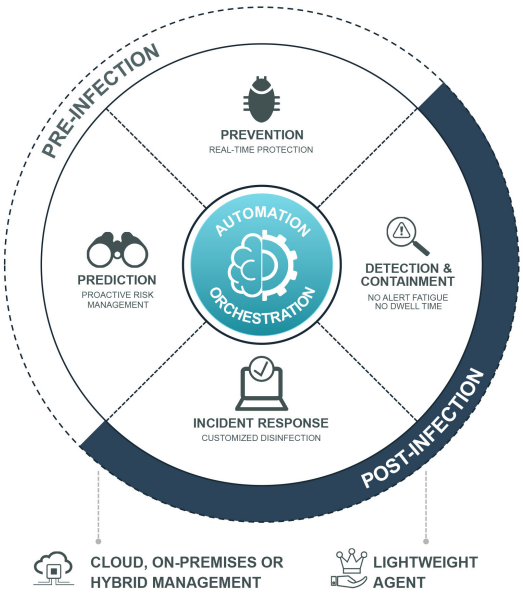


FEATURES

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



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

Third Party Support

In addition to integration with a range of Fortinet products FortXDR also supports integration with non-Fortinet products via connectors including:

- Firewalls
- Identity Services
- Network Sandboxes
- Data Lakes

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 utilizes less than 1% CPU, up to 120 MB of RAM, 20 MB of disk space, and generates minimal network traffic.

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 (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), Catalina (10.15), and Big Sur (11.0)
- Linux Versions: RedHat Enterprise Linux and CentOS 6.8-10, 7.2-9, 8.0-3; Ubuntu LTS 16.04.5-7, 18.04.1-5, 20.04.1 server, 64-bit; and Oracle Linux 8.2-3 (supported), SuSE SLES 11.1-4, 12.1-12.5 ,15.01-1 (6/30), Amazon Linux AMI 1-2 (6/30)
- Virtual Desktop Infrastructure (VDI) environments in VMware and Citrix. VDI Environments: VMware Horizons 6 and 7, and Citrix XenDesktop 7

ORDER INFORMATION

Product	SKU*	Description
Option 1	FCx-10-FEDR1-376-01-DD	FortiEDR Protect & Respond and XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.
Option 2	FCx-10-FEDR1-378-01-DD	FortiEDR Protect & Respond and Managed XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.
Option 3	FCx-10-FEDR1-377-01-DD	FortiEDR Discover, Protect & Respond and XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.
Option 4	FCx-10-FEDR1-379-01-DD	FortiEDR Discover, Protect & Respond and Managed XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.

*Minimum Order Quantity of 500.

FORTINET

www.fortinet.com