SOLUTION BRIEF

# Integrating FortiEDR and FortiXDR with the Fortinet Security Fabric

## Executive Summary

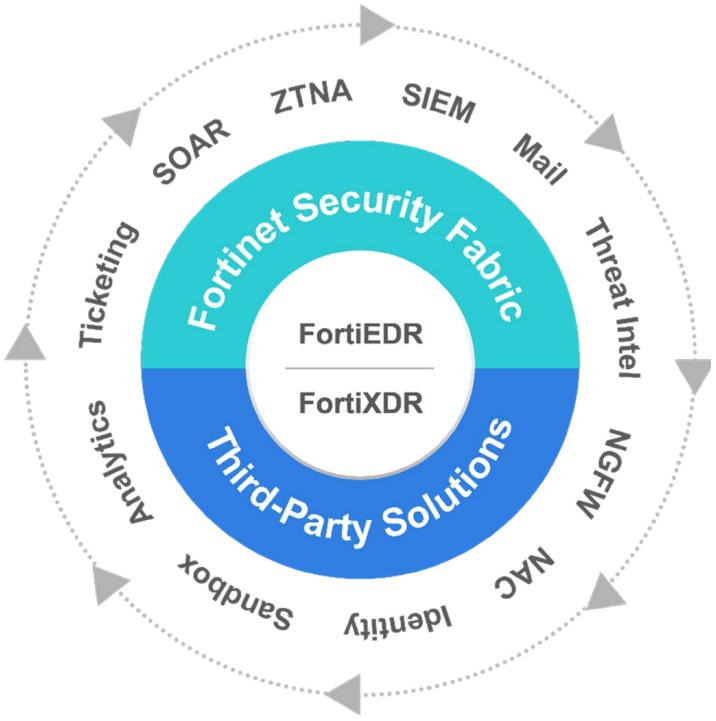
The evolving threat landscape poses significant challenges for security teams as they work to effectively protect their organizations. Limited visibility across endpoints and the entire security fabric often hinders a team's ability to promptly detect and respond to potential threats, resulting in inefficient security operations and inconsistent policy enforcement. Rapid containment of confirmed threats is also critical, as delayed actions may lead to extensive damage because of an attack. Further, many organizations use non-integrated, disparate security solutions, introducing complexities, potential security gaps, and increased acquisition costs.

Businesses need a comprehensive solution to address these issues, one that enhances threat visibility, automates security orchestration, enables rapid threat containment, and eliminates security gaps. Integrating FortiEDR endpoint detection and response and FortiXDR extended detection and response with the Fortinet Security Fabric helps security teams overcome these challenges, empowering enterprises with an effective and unified cybersecurity approach.

## Why Organizations Choose FortiEDR and FortiXDR

Fortinet FortiEDR is a robust cybersecurity solution designed to provide advanced threat detection, response, and protection for one of the broadest OS coverage models for servers and workstations across hybrid deployments. When combined with the Fortinet Security Fabric, FortiEDR becomes an integral part of a holistic cybersecurity ecosystem that offers end-to-end protection against ransomware by bringing kernel-based prevention and remediation capabilities to the endpoint.

FortiXDR builds on FortiEDR to offer cross-platform protection, analyzing and correlating event data from cloud, network, endpoint, and other security products to detect threats across the entire Fortinet and multivendor security fabric. This enables security teams to conduct threat investigation and automated remediation on all Fortinet and many multivendor components of the security ecosystem.




## Key Benefits of the Fortinet Security Fabric Integration

### Enhanced threat visibility

Integration with the Fortinet Security Fabric provides real-time, AI-driven, continuous monitoring of endpoints and infrastructure-wide activities. This monitoring enables security teams to detect threats across the entire attack surface, facilitating faster response times, especially when leveraging XDR capabilities.

### Automated security orchestration

The integration also supports automated security orchestration, allowing the customized enforcement of security policies and responses across collector groups and integrated elements, resulting in more efficient security operations.

### Rapid threat containment

In the event of a confirmed threat, FortiEDR and FortiXDR can instantly take automated actions, such as isolating affected endpoints from the network or executing incident response actions to remediate and block the scope of an attack. FortiXDR helps organizations correlate normalized data from across the Fortinet Security Fabric and third-party solutions to detect threats across the ecosystem for automatic or guided incident response.

### Eliminate security gaps

Integration with the Fortinet Security Fabric eliminates security gaps, as all Fortinet solutions are designed to work together. In contrast, using an array of point solutions from various vendors introduces complexity, increases costs, and often leaves "cracks" in the security posture that become attractive targets for threat actors.

## Available Integrations

FortiEDR and FortiXDR integrate seamlessly with other Fortinet products and third-party security solutions. This integration creates a unified and powerful security infrastructure that can defend against evolving cyberthreats. Security practitioners can integrate FortiEDR and FortiXDR with:

- **FortiGate:** Both solutions integrate seamlessly with FortiGate Next-Generation Firewalls and third-party firewalls. This enables real-time threat intelligence sharing, so the firewall can enforce dynamic security policies based on the endpoint's threat posture. For example, if an attack is recorded on a protected endpoint, the IP address where it originated can be instantly blocked on all integrated Fortinet and many non-Fortinet firewalls.

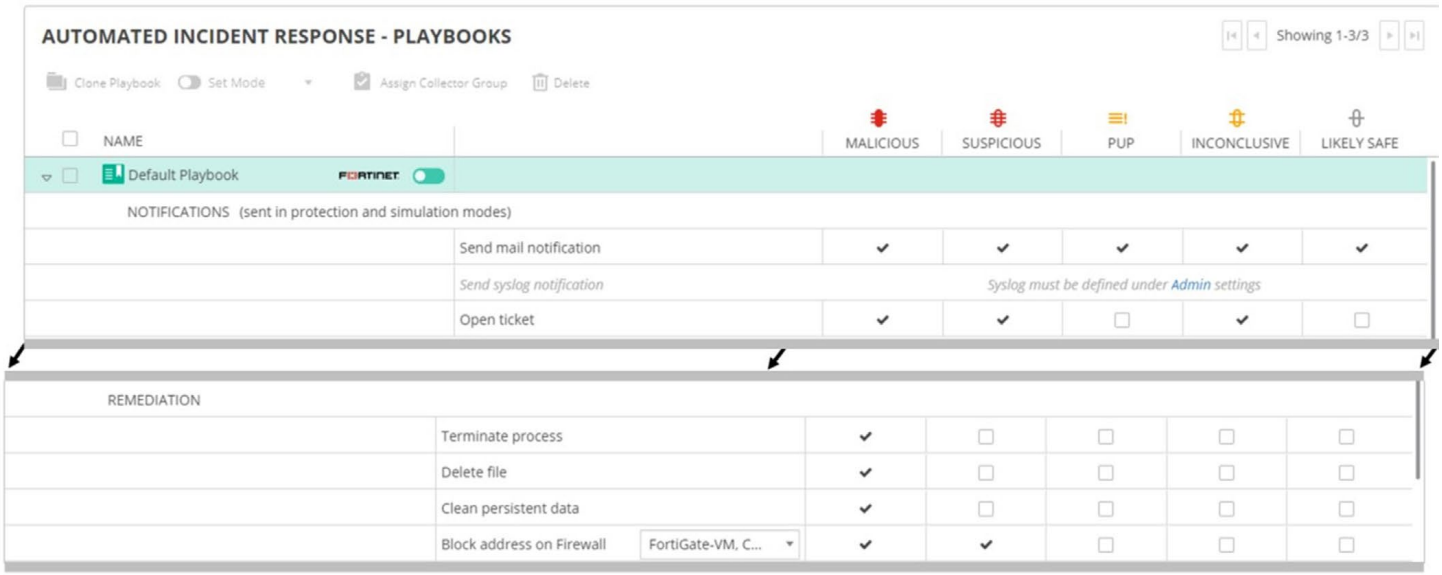



Figure 1: In the remediation section of the default playbook setup screen, this administrator chose to block addresses for malicious and suspicious verdicts on selected firewalls.

- **FortiNAC:** Assimilating with a network access control (NAC) solution like FortiNAC enables security policy enforcement based on the endpoint's compliance status and network context. A core use case is to have the NAC solution push endpoints with malicious or suspicious policy violations to a virtual local area network (VLAN) for remediation.

- **FortiSandbox:** This advanced threat analysis solution analyzes unknown files that meet several conditions. If a file is determined to be suspicious or malicious, then the event is classified as non-safe, and the pre-execution policy blocks any future execution attempt of the file in the environment. Combining these two actions reduces false positives and the risk of unknown or suspicious files from executing. It offers real-time verdicts for proactive protection against potential exploits and sleeping threats.
- **FortiAnalyzer:** Connecting with Fortinet's centralized logging and reporting solution enables security teams to gain deeper insights into endpoint activities and threats through comprehensive log analysis and detailed reporting from sources like firewalls, Active Directory, and more. FortiAnalyzer collects, aggregates, and analyzes endpoint security data, providing valuable context for FortiXDR threat detection, incident investigation, and threat hunting.
- **FortiSIEM:** The Fortinet security information and event management solution provides advanced threat detection and correlation of security events across the network and endpoints. By exporting events to FortiSIEM, the FortiEDR and FortiXDR solutions contribute up to 30 types of metadata for FortiSIEM threat correlation and compliance reporting.
- **FortiSOAR**: Integration with FortiSOAR security orchestration and automation centralizes and automates FortiEDR and FortiXDR incident investigation and automated response actions. With 500 connectors and 800 prebuilt playbooks, analysts can rapidly respond to incidents across the entire Fortinet and multi-vendor security fabric.
- **FortiClient Endpoint Management Server:** This integration enables FortiClient to ingest the endpoint status data for a zero-trust network access (ZTNA) posture check to ensure that only healthy and compliant devices gain access to the network and applications. FortiEDR and FortiXDR also provide ZTNA device tagging for infected devices and can live side by side with FortiClient.
- **FortiMail:** This integration allows FortiXDR detection and investigation scope to include email events and FortiXDR analyst response actions to immediately block any malicious email addresses associated with an incident.
- **Third-party solutions:** FortiEDR and FortiXDR support integration with various third-party security and IT solutions through prebuilt APIs and standardized interfaces. This capability allows organizations to leverage their existing security investments and create a comprehensive cybersecurity ecosystem. Integration with third-party solutions such as identity, messaging, cloud, and SIEM platforms, threat intelligence feeds, and orchestration tools enhances threat detection, incident response, and overall security operations. Fortinet also offers organizations the ability to build their own integrations using the REST API framework.

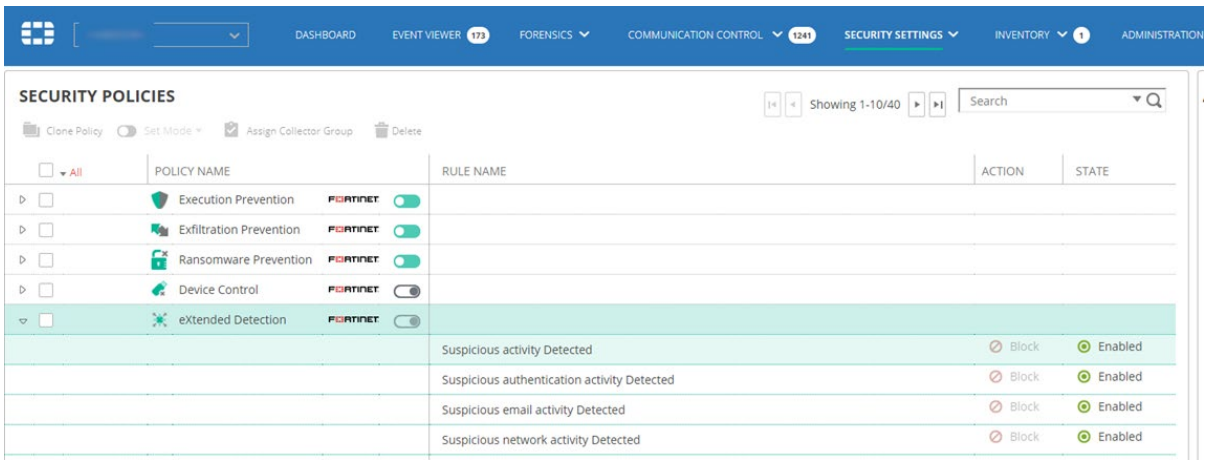



Figure 2: Getting started with FortiXDR

## Enhance Your Security Infrastructure Today

By integrating FortiEDR or FortiXDR with the Fortinet Security Fabric and third-party security solutions, organizations can extend the capabilities of endpoint security beyond traditional boundaries and create a unified, proactive, and adaptive security infrastructure. The combination of advanced endpoint protection, enterprise-wide threat detection, threat intelligence sharing, and automated incident response enhances an enterprise's ability to detect, respond to, and mitigate common and advanced cyberthreats. Flexible and scalable integration options allow organizations to tailor their security ecosystems to meet the unique challenges of their IT environments, ultimately bolstering cybersecurity posture.

For more information:

- Review the FortiEDR data sheet
- Review the FortiXDR data sheet
- Book a demo now

FORTINET

www.fortinet.com



September 12, 2023 10:45 AM

2300026-0-0-EN