SOLUTION BRIEF

How FortiEDR Checks Buyers’ Boxes

Executive Summary

As organizations begin to evaluate new endpoint security platforms, they have various needs to fulfill and a variety of vendors from which to choose. Every year, Fortinet answers thousands of requests for proposal (RFPs) and requests for information (RFIs) regarding security solutions. As a result, we have collected numerous unique questions and responses focused on endpoint protection platform (EPP) and endpoint detection and response (EDR) solutions. Over the past few years, business leaders have voiced specific concerns about protecting their enterprises from ransomware and their organization’s employees as they increasingly work from anywhere.

FortiEDR is an EPP and EDR solution designed to stop attacks before, during, and after execution, offering organizations the opportunity to improve security operations. Based on the “must haves” many leaders are looking for in EPP and EDR solutions, below is a closer look at how FortiEDR helps customers check those boxes.

What is FortiEDR? According to this customer, a “Solid EDR product delivered by a solid and secure market leader.”[1]

Protection Efficacy

Aside from conducting a proof of concept with a potential vendor, one of the best tools to use to evaluate vendor capabilities is third-party, non-sponsored testing reports. FortiEDR fields superior protection results thanks to its kernel-based anti-malware engine, receiving a 100% protection score in SE Labs’ Endpoint Security: Enterprise 2022 Q4 evaluation when tested against 100 malware strains.[2] Additionally, in the fifth round of the MITRE ATT&CK Evaluations, FortiEDR received high marks for superior visibility by discovering 98% of the sub-steps and received an analytical score of 95%.[3]

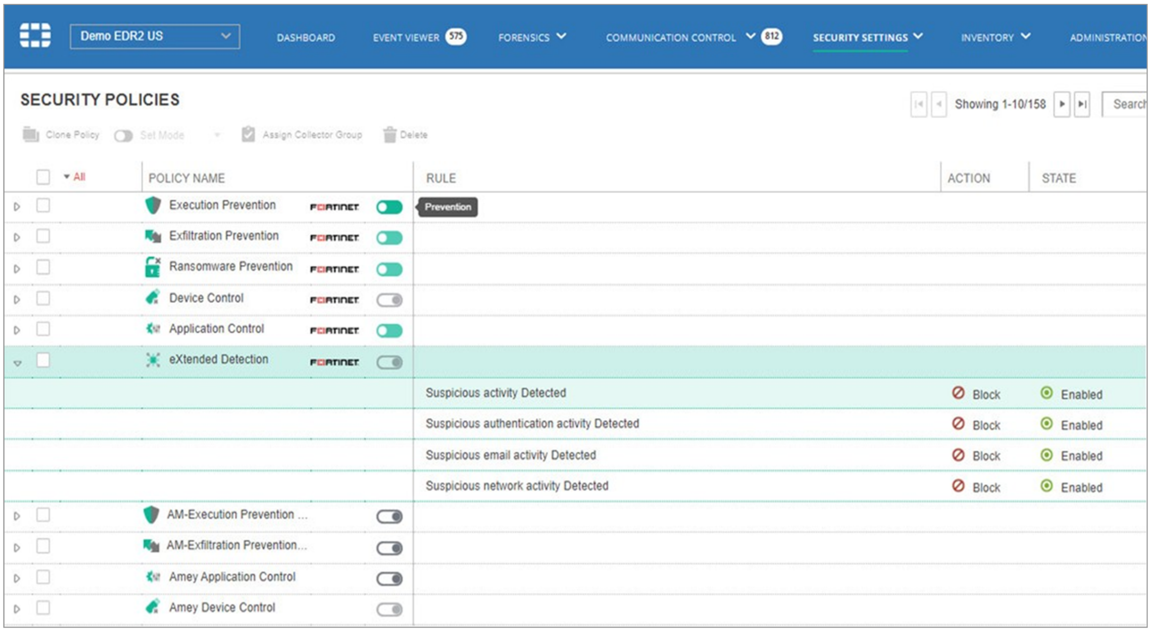
Vulnerability Ratings

Vulnerabilities exist across every ecosystem, yet timely patch management is a challenge for even the most well-staffed organizations. To help security teams update devices and applications faster, FortiEDR catalogs the applications that organizations have and rates potential vulnerabilities. The solution also provides virtual patching, allowing the user to create granular controls for each user group based on the application’s reputation and the severity of an associated vulnerability. Security practitioners can use these controls to perform various functions, such as moving endpoints to a higher security collector group or allowing the application to work while halting any communication with the internet. More information can be found in our Admin Guide on Vulnerabilities.

Ransomware Defense and Recovery

One of the reasons that FortiEDR performed so well in the fourth round of the MITRE ATT&CK Evaluations in 2022—which focused on two types of Russian nation-state ransomware—is its dedicated ransomware policy designed to stop specific attack strains.[4] FortiEDR monitors for malicious file changes within a safe, nonproduction part of the memory of a system. Once the solution spots malicious behavior, the change is not allowed to happen in production and the cause of the change is automatically eliminated and the administrator is notified.

In the case of a ransomware infection, FortiEDR can roll back the device to a previously known clean state for a variety of operating systems, including Windows, macOS, and Linux. Customers can also choose not to activate the policy to allow FortiEDR to monitor their environment before a mass deployment.



SECURITY POLICIES

POLICY NAME	RULE	ACTION	STATE
Execution Prevention FORTINET			
Exfiltration Prevention FORTINET			
Ransomware Prevention FORTINET			
Device Control FORTINET			
Application Control FORTINET			
eXtended Detection FORTINET			
	Suspicious activity Detected	Block	Enabled
	Suspicious authentication activity Detected	Block	Enabled
	Suspicious email activity Detected	Block	Enabled
	Suspicious network activity Detected	Block	Enabled
AM-Execution Prevention ...			
AM-Exfiltration Prevention...			
Amey Application Control			
Amey Device Control			

Figure 1: FortiEDR dedicated policies

Offline Protection

With an increasing number of organizations embracing work-from-anywhere strategies, many corporate users are away from traditional network defenses such as firewalls, which are used to eliminate attacks in the initial phases. Because of this shift, organizations look to EDR solutions to serve as the first and last lines of defense for employee endpoints. While some EPP solutions rely on signatures to stop an attack, even if nearly perfect in tests where the device is online, the technology may falter in offline tests. FortiEDR provides behavior-based protection against threats and doesn’t need online features to protect the device. Although not required, online connectivity adds the benefit of accessing Fortinet Cloud Services (FCS), an included microservice in all bundles. FCS incorporates threat intelligence and multiple sandboxes to assist FortiEDR in assigning the correct verdicts to policy violations, aiding in event management, and automating actions according to incident response playbooks.

Anti-Tampering Capabilities

FortiEDR contains security controls to detect tampering, making it impossible for malware to turn off the solution. Because FortiEDR is kernel-based, the technology is immune to the documented evasion tactics that affect common EDR solutions. You won’t find FortiEDR evasion tactics sold on malware marketplaces.

Operating System Support

FortiEDR has one of the broadest coverage models for operating systems on the market. In addition to current operating systems, it covers Windows XP SP2+, Windows Server 2003 SP2+, macOS El Capitan+, old and new Linux variations, various VDI environments, and Google Cloud computer environments.

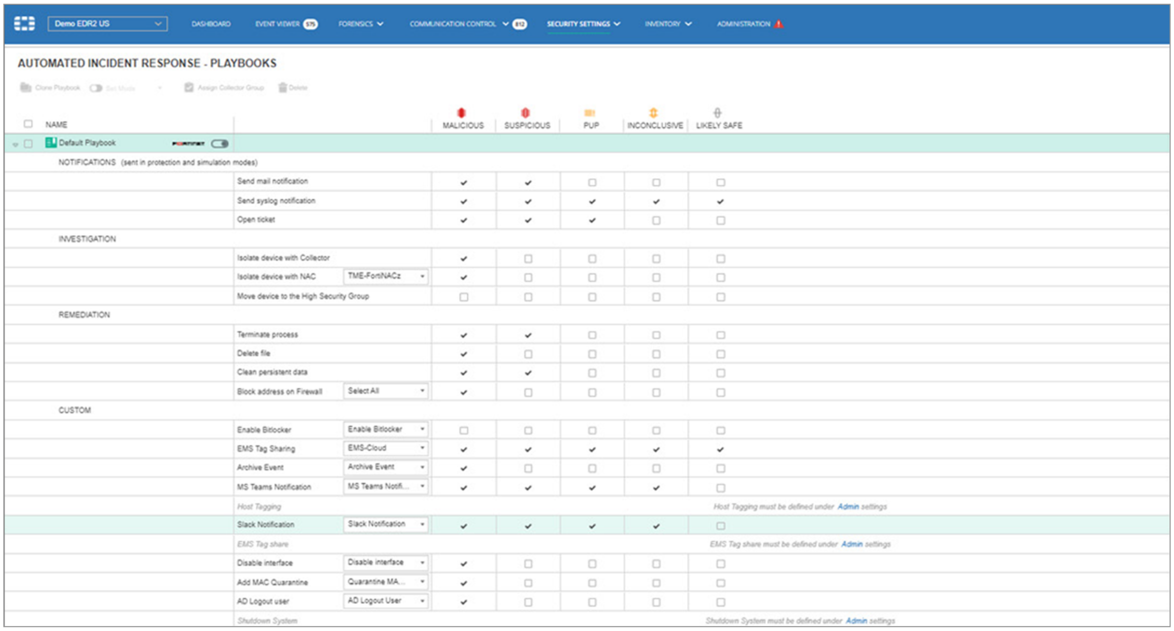
Agent Weight

One of the main motivations for the industry to move away from antivirus-based EPPs is the weight of the agent on the device. Downloading a large swath of new signatures, checking every file being written to disk, and running routine scans started to make endpoint security more of an inhibitor than an enabler. FortiEDR takes up less than 1% of system resources on average and rarely spikes higher, even though it continually monitors for malicious activities and doesn’t require routine system scans.

EDR Automation

FortiEDR helps overburdened security operations center (SOC) analysts and other security practitioners by automating many tasks based on how the tool is configured. The automated playbooks in FortiEDR allow you to create granular options for multiple custom user groups, tenants, and connections to the Fortinet Security Fabric. The solution also offers over 300 prebuilt third-party connectors, such as ticket, security information and event management (SIEM), email, firewall, and identity providers. Our Admin Guide on Custom Integration provides more information.

"FortiEDR is a good product, easy to use and light in resource-consumption."[5]



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

NAME			MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
Default Playbook							
NOTIFICATIONS (sent in protection and simulation modes)							
	Send mail notification		✓	✓	□	□	□
	Send syslog notification		✓	✓	✓	✓	✓
	Open ticket		✓	✓	✓	□	□
INVESTIGATION							
	Isolate device with Collector		✓	□	□	□	□
	Isolate device with NAC	TME-FortiNACz	✓	□	□	□	□
	Move device to the High Security Group		□	□	□	□	□
REMEDIATION							
	Terminate process		✓	✓	□	□	□
	Delete file		✓	□	□	□	□
	Clean persistent data		✓	✓	□	□	□
	Block address on Firewall	Select All	✓	□	□	□	□
CUSTOM							
	Enable Bitlocker	Enable Bitlocker	□	□	□	□	□
	EMS Tag Sharing	EMS-Cloud	✓	✓	✓	✓	✓
	Archive Event	Archive Event	✓	□	□	□	□
	MS Teams Notification	MS Teams Notifi...	✓	✓	✓	✓	□
	Host Tagging						Host Tagging must be defined under Admin settings
	Slack Notification	Slack Notification	✓	✓	✓	✓	□
	EMS Tag share						EMS Tag share must be defined under Admin settings
	Disable interface	Disable interface	✓	□	□	□	□
	Add MAC Quarantine	Quarantine MA...	✓	□	□	□	□
	AD Logout user	AD Logout User	✓	□	□	□	□
	Shutdown System						Shutdown System must be defined under Admin settings

Figure 2: FortiEDR automated incident response playbook template

Extended Detection and Response Capabilities

FortiXDR extended detection and response is an evolution of the FortiEDR client and leverages many internal solutions that don't require a specific third-party solution or API to simulate the look of a real XDR solution. The XDR concept is gaining popularity among organizations. However, many vendors' marketing efforts are creating confusion as they attempt to define a security concept that analysts like Gartner are better at describing. Following guidance from Gartner analysts, organizations should look to a mature security company that has its own SIEM; security orchestration, automation, and response (SOAR); and other back- and front-end components like firewalls and email security.[6]

Managed Service Options

Our Fortinet Managed Detection and Response (MDR) and incident response teams offer a managed EDR solution called FortiResponder. This solution takes the burden off security teams by acting as a senior SOC analyst to conduct 24×7 threat detection, hunting, and analysis and perform containment and remediation actions. The team also informs you when there is a malicious or suspicious notification and provides routine reporting. The Fortinet website has more information about managed services and additional incident response and readiness services.

Total Cost of Ownership

FortiEDR provides simplified pricing through EDR and XDR bundles that can be paired with managed services. The cost per endpoint is the same regardless of whether it is a server or an endpoint. Customers find that FortiEDR has one of the best total costs of ownership (TCOs) on the market due to a rich base of entitlements, including a native 30 days of data storage, which many vendors only offer as an upcharge. Our XDR solution taps into existing data lakes, which reduces costs and complexities for our customers.

Operational Technology Support

CISOs face many challenges when securing operational technology (OT) endpoints. FortiEDR provides a robust solution for OT endpoint security by offering real-time threat protection, both pre- and post-infection. Organizations that deploy FortiEDR on their OT endpoints benefit from faster threat responses, automated actions, and fewer disruptions to production activities. With broad OS coverage that includes macOS, FortiEDR brings protection to a deep bench of Windows and Linux systems that may not have been updated in years and are rife with vulnerabilities. It also comes with a simulation mode to monitor the environment first before deploying so that teams can fine-tune their environment before full deployment.

Summary

FortiEDR delivers real-time visibility, analysis, protection, and remediation for endpoints as one of the most innovative endpoint security solutions. It proactively reduces the attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks. FortiEDR helps organizations identify and stop breaches automatically and efficiently, without overwhelming security teams with a slew of false alarms or disrupting business operations.

For more information, check out Gartner Peer Insights™ regarding FortiEDR, in which 127 reviewers give it an average of 4.6 out of 5 stars, with 94% recommending the solution.[7] These marks helped the solution take home the 2023 Gartner Voice of the Customer award for endpoint protection platforms. Gartner also recognized Fortinet as a Visionary in its Magic Quadrant for Endpoint Protection Platforms.[8] Gartner also awarded FortiEDR a 4.28 out of 5 stars for Type A organizations in its Critical Capabilities for Endpoint Protection Platforms report.[9]

[1] "Peer Review for FortiEDR," Gartner Peer Insights, May 22, 2023.

[2] "Endpoint Security (EPS): Enterprise 2022 Q4," SE Labs, accessed October 6, 2023.

[3] "ATT&CK Evaluations," MITRE Engenuity, 2023.

[4] Ibid.

[5] "Peer Review for FortiEDR," Gartner Peer Insights, May 31, 2023.

[6] "Market Guide for Extended Detection and Response," Gartner, August 2023.

[7] "FortiEDR Reviews," Gartner Peer Insights, accessed October 6, 2023.

[8] "Magic Quadrant for Endpoint Protection Platforms," Gartner, December 31, 2022.

[9] "Critical Capabilities for Endpoint Protection Platforms," Gartner, December 31, 2022.

FORTINET

www.fortinet.com

Reviews have been edited to account for errors and readability.

October 13, 2023 10:42 AM
1637475-B-0-EN