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 coinciding vendor solutions to those needs to choose from. Every year, Fortinet answers thousands of requests for proposal (RFPs) or information (RFIs) regarding security solutions and has collected hundreds of unique questions just for EPP and EDR solutions. Over the past seven years, ransomware has been top of mind, and with the COVID-19 pandemic, numerous concerns around working off-site are present in these questions.

FortiEDR is an endpoint protection platform (EPP) and endpoint detection and response (EDR) solution designed to stop attacks before, during, and after execution, along with multiple tools global organizations use to improve security operations. This paper covers how FortiEDR helps customers check some of the common boxes between a global distribution of organizations of all sizes and from all verticals.

> "FortiEDR helps us sleep better at night, no worries of waking up to malware outbreaks."
>
> – IT leader in retail on
> Gartner Peer Insights

Protection Efficacy

Let's start with the common denominator between all the EPP and EDR solutions, security. Outside of field tests in a proof of concept within your organization, one can look to the FortiEDR MITRE ATT&CK Enterprise Evaluation results. FortiEDR will block malware with the best of them and do it accurately without foreknowledge of the attack (for example, a new strain or zero-day attack). FortiEDR blocked all participating attacks for the second year, discovered 97% of the sub-steps, and had an analytical score of 94% (which one could state is within a top-five result out of 30 vendors).

While one could argue that these top vendors were better prepared for the independent evaluation than others, one could look to the results of the University of Piraeus's non-sponsored and unannounced research, *An Empirical Assessment of Endpoint Security Systems Against Advanced Persistent Threats Attack Vectors.*[1] In their first round, they performed four different attacks and were able to bypass each one of the limited numbers of EDR solutions they had access to at least once. In their second round, they added FortiEDR, which became the first solution out of the box, which could block all four of their attacks. Within the third and expanded version of the paper, FortiEDR was only one of two out of 31 types and versions of EPP/EDR solutions that could withstand their attacks. FortiEDR is designed from the ground up to be the best at attack-surface reduction.

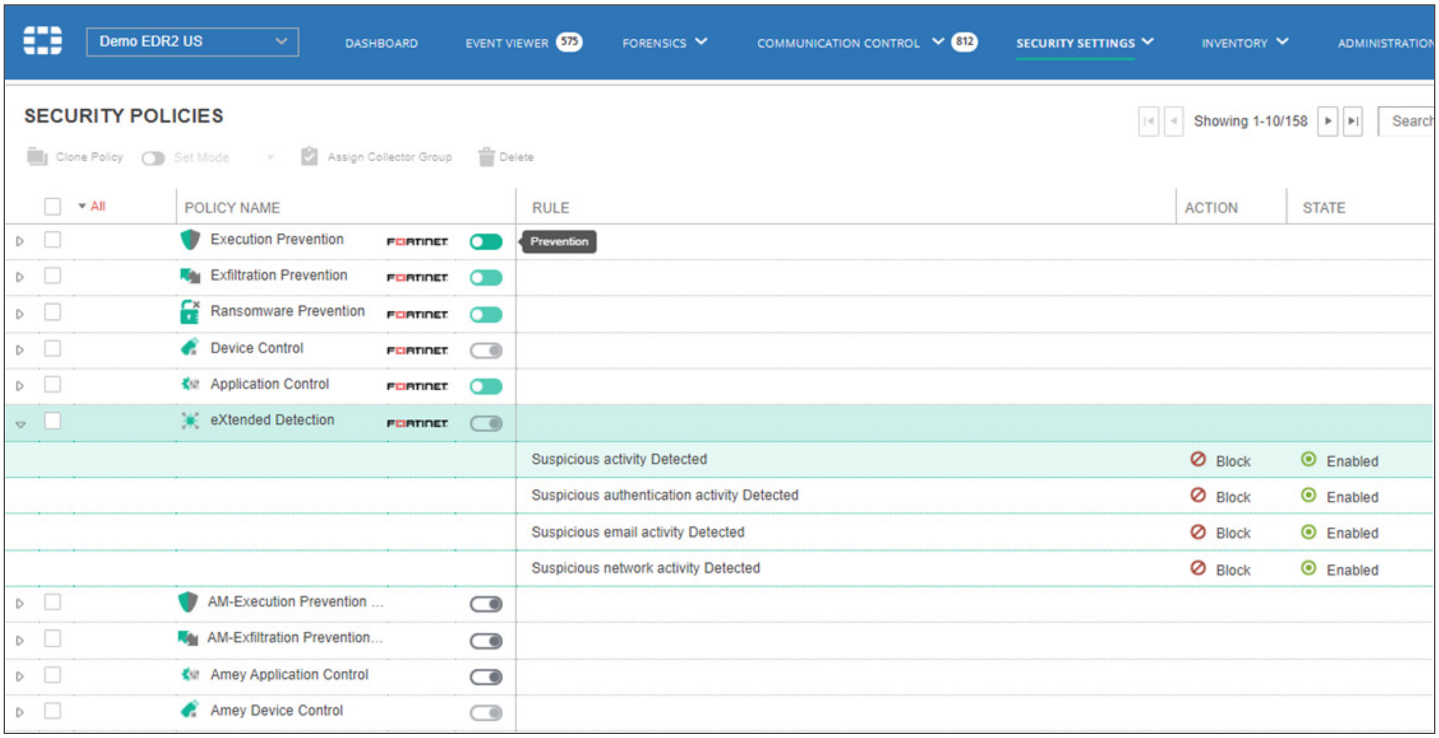
Living With Vulnerabilities

Vulnerabilities exist across every ecosystem, and despite the best intentions to have everything updated all the time, it is nearly impossible to do so. FortiEDR catalogs the applications that organizations have and the vulnerabilities with ratings. It also provides virtual patching. It allows the user to create granular controls based on the application's reputation and the severity of any vulnerability it may have. These controls can do various things, such as move endpoints to a higher security collector group or just allow the application to work but don't allow for it to communicate with the internet. More information can be found in our Admin Guide on Vulnerabilities.

Ransomware Defense and Recovery

One of the reasons for the excellent FortiEDR MITRE ATT&CK Evaluation results, which focused on two types of Russian nation-state ransomware, is its dedicated ransomware policy designed to stop this attack strain instantly. Customers with the dedicated ransomware policy active have never been infected by it.

In the case of a ransomware infection, FortiEDR can roll back the device to a previously known clean state, not just for Windows but for macOS and Linux too. Customers may choose not to activate the policy to allow FortiEDR to monitor their environment before a mass deployment. More information can be found in our admin guide.



SECURITY POLICIES

□ All	POLICY NAME			RULE	ACTION	STATE
□	Execution Prevention	FORTINET	●	Prevention		
□	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 nearly 47% of people working away from the office part- or full-time,[2] many are away from traditional corporate network defenses such as firewalls (which are used to eliminate attacks in the initial phases) and can often operate offline. Because of this, organizations look to EDR solutions for 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 (to access cloud-based definitions), it may falter in offline tests. FortiEDR provides behavior-based protection against threats and doesn't need online features to protect the device. Online connectivity does have benefits, but they are not required.

Anti-tampering Capabilities

Malware will often try to implement a malicious bootloader (also known as a bootlocker) to stop the operating system from loading when infected with ransomware for an additional layer of pain (to demand payment). FortiEDR exists as a firewall for the kernel level, which makes it adept at detecting fileless threats and others that try to initiate within the memory of a system. Furthermore, it contains security controls to protect itself and can detect tampering, making it impossible for malware to turn off.

Operating System Support

FortiEDR has one of the broadest coverage models for operating systems on the market. Including all current operating systems, it covers Windows XP SP2+, Windows server 2003 SP2+, macOS El Capitan+, 15-year-old Linux systems and beyond, various VDI environments, and Google Cloud computer environments.

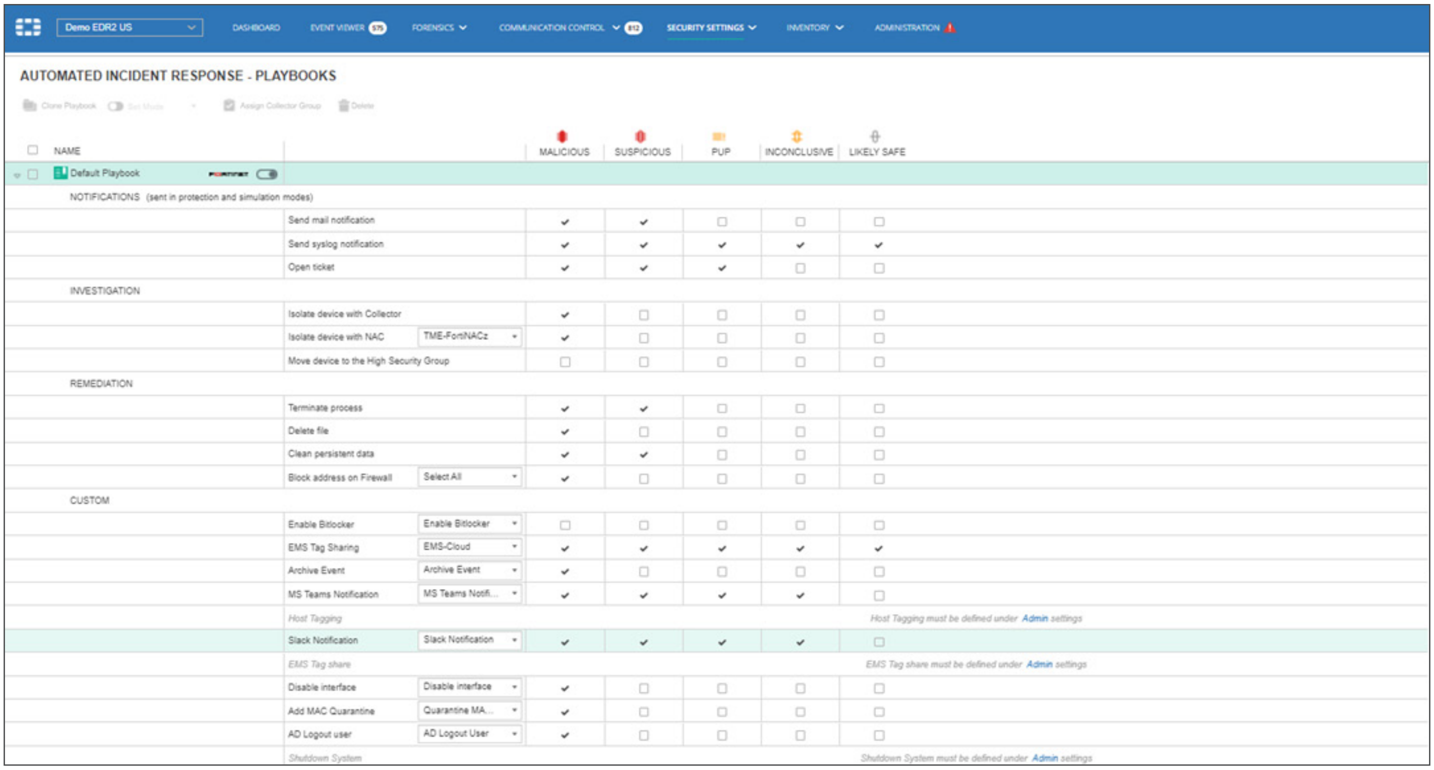
Agent Weight

One of the main motivators for the industry to move away from antivirus-based endpoint protection platforms was 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 over that, even though it continually monitors for malicious changes and doesn't require routine system scans (although that can be done). We believe this review on Gartner® Peer Insights™ confirms this.

> "FortiEDR [is] The Best Endpoint Security For Bank And MFI."
>
> – CTO of large K-12 school district on Gartner Peer Insights

EDR Automation

This is where FortiEDR really demonstrates the difference between many other solutions on the market. FortiEDR helps overburdened security operations center (SOC) and security staff by automating many tasks based on how it is set up to run. The automated playbooks in FortiEDR allows one to create many granular options for multiple custom user groups, tenants, connections to the Fortinet Security Fabric, and over 300 pre-built third-party connectors, such as email security, firewalls, and identity providers. Our Admin Guide on Custom Integration provides more information.



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 (XDR) Capabilities

FortiXDR springs from 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 steam, but many vendors’ marketing efforts are creating confusion as they attempt to define a security concept that Gartner is better solidifying. Following Gartner guidance, organizations should look to a mature security company that has its own security information and event management (SIEM); security orchestration, automation, and response (SOAR); and other back- and front-end components like firewalls and email security.[3]

Managed Service Options

Fortinet Managed Detection and Response (MDR) and incident response teams offer a managed EDR solution called FortiResponder. This solution takes the burden off of SOC teams by acting as a senior SOC analyst and providing quarterly security environment reviews. Our MDR team will provide 24/7 threat monitoring, alert triage, and guided remediation instructions with remote remediation and rollback options as part of the service. Our web page has more information about incident response and readiness services.

Total Cost of Ownership (TCO)

FortiEDR provides simplified pricing with three base styles of EDR with MDR options. The cost per endpoint is the same regardless of being a server or an endpoint. Customers find that FortiEDR has one of the best TCOs on the market due to a rich base of entitlements, including a native 30 days of data storage, which most vendors will charge extra for just to get to this standard.

Operational Technology (OT) Support

CISOs face several challenges when securing 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, FortiEDR brings protection to systems that may not have been updated or even rebooted in years and are rife with vulnerabilities. It also comes out of the box with a simulation mode to monitor the environment first before deploying and possibly blocking a false positive (and shutdown the OT system from producing), so one 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 in real time automatically and efficiently, without overwhelming security teams with a slew of false alarms or disrupting business operations. There are stellar results with the University of Piraeus and the MITRE ATT&CK Evaluations.

Seventy-six reviewers on Gartner Peer Insights also give it 4.7 out of 5 stars, with 96% of them recommending the solution, as of June 8, 2022.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Reviews have been edited to account for errors and readability.

[1] George Karantzas and Constantinos Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors," January 11, 2022.

[2] Alison Auginbaugh and Donna S. Rothstein, "How did employment change during the COVID-19 pandemic? Evidence from a new BLS survey supplement," U.S. Bureau of Labor Statistics, January 2022.

[3] Market Guide for Extended Detection and Response, Gartner Research, November 2021.

June 17, 2022 11:24 AM
1637475-0-0-EN