FORTINET

SOLUTION BRIEF

FortiEDR Integration with Google Cloud Security Command Center and Amazon GuardDuty

Executive Summary

According to a 2022 research report from Enterprise Strategy Group (ESG), 52% of survey respondents say that security operations are more difficult today than they were two years ago.[1] When asked why it was so difficult, respondents pointed to the changing threat landscape and attack surface as the top reason.[2] A third of IT security peers said that the "increased use of public cloud services" was also a source of their difficulties.[3] Other notable challenges were the expansion of data collected, too many unscalable manual processes, gaps in security monitoring, and the inability to automate complex tasks among many others.[4]

When asked to respond to statements regarding their organization's security operations environment, 89% of participants felt their organization would benefit from collecting, processing, and analyzing more data.[5]

The Role of Extended Detection and Response (XDR) in Your Security Program

The concept of XDR is built on the foundation of endpoint detection and response (EDR), both of which solve similar problems. While EDR specifically covers endpoints with additional integrations, the "X" in XDR indicates that the solution can normalize and correlate data from other security products to detect attacks and automate a response.

With XDR solutions increasingly gaining adoption, the mission today for security vendors is to build their solution to ingest multiple data lakes of security data to come closer to the concept of a self-healing ecosystem. Outside of the trifecta of network, email, and endpoint, cloud-based workloads are a growing part of the attack surface and represent an attractive target for attackers to exploit. By ingesting multiple data streams, teams can more effectively correlate incidents to automate the detection, response, and even some remediation tasks related to an incident across protected endpoints, servers, and cloud instances.

Why Integrate FortiEDR with Your Preferred Cloud Provider

FortiEDR is the first solution on the market that not only integrates with the Fortinet Security Fabric and hundreds of third-party solutions but also with Google Cloud Security Command Center and Amazon GuardDuty. FortiEDR is able to correlate the data from security incidents from multiple sources without the need to duplicate data lakes, which reduces the overall total cost of ownership of the solution. Operating from a single pane of glass, the solution can accomplish tasks such as automating the resolution of security incidents from the firewall to the endpoint to your Google Cloud and Amazon Web Services (AWS) instances.

Here are two common use cases for the technology:

- Imagine that a domain within your Google Cloud or AWS instance is compromised. Thanks to the integration between FortiEDR and the security controls of your cloud instances, your endpoint will block access to the domain until it is repaired. FortiEDR will correlate that data within the threat hunting feature with any additional outbound data to see how it may have been compromised, exploring it to identify any additional potential compromises.

- A second similar use case pertains to cryptominers, which often attack servers and cloud instances. Google Cloud and AWS will share threat data related to affected hosts, hashes, and the associated network characteristics of an attack with FortiEDR. The EDR solution will then correlate this data with any files and network characteristics with its threat hunting module and flag it as a form of retroactive threat intelligence to resurface potential affected hosts. With the added benefit of automated playbooks, FortiEDR can remove files, block IP addresses on your firewall to stop follow-on attacks, or move impacted hosts to a remediation virtual local area network (VLAN) with solutions like FortiNAC.

Why Choose FortiEDR to Integrate with Your Environment

FortiEDR integrates with Fortinet products, third-party security solutions, and cloud platforms by identifying potential security incidents and correlating related security data to be investigated by artificial intelligence (AI). FortiEDR customers can identify more threats using AI that has been trained on the broadest set of telemetry originating from the most independently certified controls and covering the most cyber kill chain stages available in the industry. As a result, incidents are contained faster due to preconfigured, automatable responses coordinated across both Fortinet and third-party products. Additionally, FortiEDR is easy to deploy and configure.

Learn more about FortiEDR through demo videos, documentation, and more on our website.

[1] Jon Oltsik, "ESG Research Report: SOC Modernization and the Role of XDR," Enterprise Strategy Group, October 24, 2022.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

December 20, 2022 9:12 PM