Guardicore

Guardicore + Fortinet
SOLUTION BRIEF

Host-Based Isolation for Compromised Endpoints
Using Guardicore Centra with FortiSOAR

Isolate non-compliant or compromised endpoints from your broader IT environment

FORTINET

Preventing lateral movement in east-west traffic can dramatically reduce the impact of a security incident such as ransomware. If bad actors can't exploit attack paths inside the perimeter to compromise additional assets or access sensitive data, it will reduce their capacity for damage. In addition, when limited to the initial point of breach, attackers can't make their way to more endpoints or business-critical applications and data.

Rapid detection and response are critical to stopping attacks early in the kill chain. Fortinet's FortiSOAR integration with Guardicore Centra enables SOC teams to flag potentially malicious activity and quickly address it with intelligent automation and orchestration capabilities.

How the integration works

If an activity on an endpoint, such as running malware or accessing a malicious website, triggers an intrusion prevention system (IPS) event, Fortigate automatically will block the traffic. It also will log the event details in FortiAnalyzer. The FortiSOAR platform will execute a playbook that can collect this information next time it polls FortiAnalyzer and present it for the SOC team to action or run automatically, all depending on the level of automation you'd like to implement for your Incident Response processes.

> ***Fortinet's FortiSOAR integration with Guardicore Centra enables SOC teams to flag potentially malicious activity and quickly address it with intelligent automation and orchestration capabilities.***

KEY BENEFITS

Improve response times

Empower analysts and responders with the ability to quarantine assets automatically.

Prevent lateral movement

Stop attackers from gaining a further foothold in your environment, reducing the impact of breaches.

Embrace agility

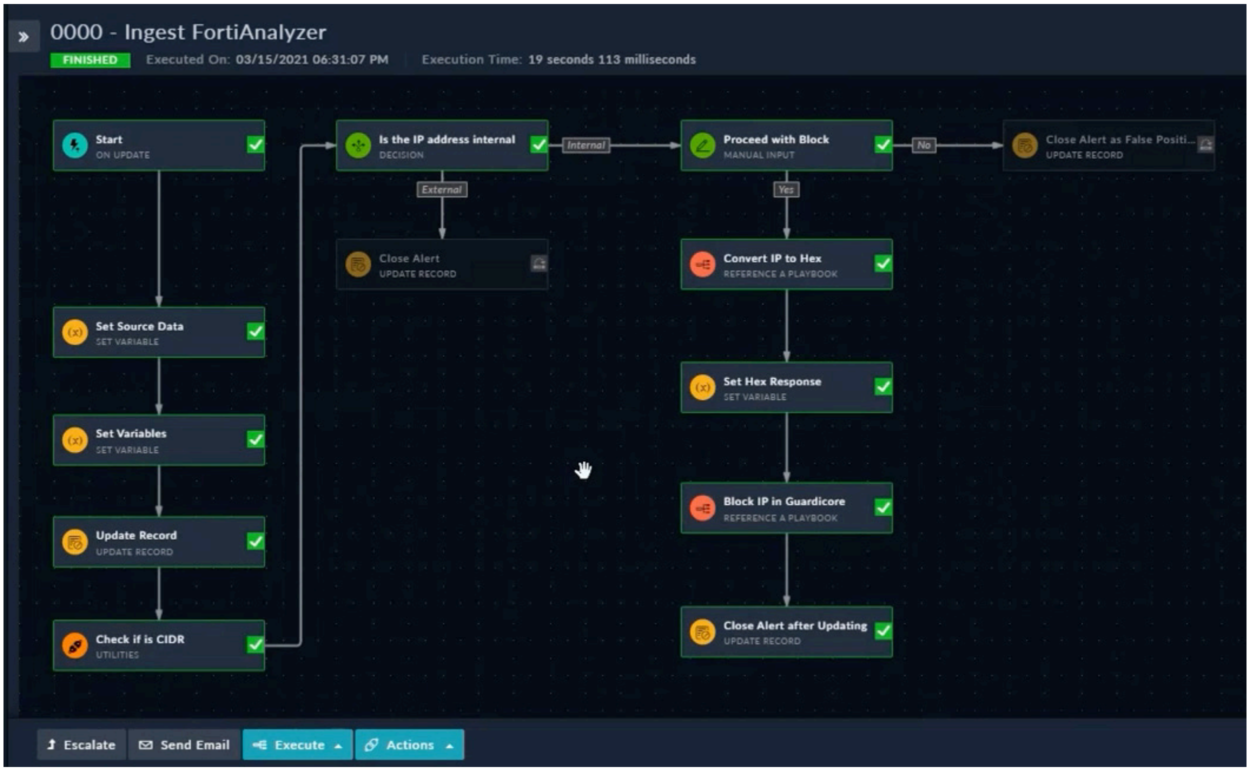
A software-based approach means that no network changes or downtime are required to create or change security policies.

Integrate east-west security and microsegmentation with your Fortinet firewalls and IPS

Guardicore provides distributed, identity-based microsegmentation integrated with Fortinet via a Security Fabric connector, allowing you to add policies inside your hybrid cloud immediately.

In addition to organizing the events in a centralized location, FortiAnalyzer will also perform several background tasks to further populate each with enriched data from historical information and threat feeds. If a relevant playbook is found for an event, the option to immediately isolate the affected asset will be presented to the SOC team.

After the segmentation platform applies a quarantine label to the IP address of the compromised endpoint, a Guardicore agent will enforce the quarantine policy at the workload level.



0000 - Ingest FortiAnalyzer

FINISHED Executed On: 03/15/2021 06:31:07 PM | Execution Time: 19 seconds 113 milliseconds

The joint solution provided by Guardicore and Fortinet gives responders the ability to quickly cut off potential attack paths in their environment as soon as an issue is detected. This significantly improves SOC teams' effectiveness and readiness against today's evolving threats.

Protection across any complex environment

www.guardicore.com

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint.