SOLUTION BRIEF

Fortinet and Guardicore Security Solution

Broad, Integrated, and Automated Security With the Fortinet Security Fabric and Guardicore Centra

Executive Summary

Guardicore Centra integration with Fortinet improves security visibility and enables policy automation and rapid incident response, greatly enhancing overall security effectiveness and readiness against today's fast-moving cyber threats.

Security Challenges

Organizations face multiple major challenges today, including coping with rapidly growing attack surfaces, advanced cybersecurity threats, increased infrastructure complexity, and an expanding regulatory landscape.

Overseeing security operations has become increasingly time-consuming as today's enterprise networks and services grow in complexity and scale. Organizations face a dire need for automation, especially given the growing shortage of skills and personnel in the cybersecurity area. Ensuring security tools are in lockstep via automation and dynamic synchronization can significantly reduce risk, errors, and inconsistencies that may introduce gaps in protection. Preventing lateral movement of threats in east-west traffic can also dramatically reduce the impact of a security incident such as ransomware. Rapid detection and response are critical to stopping attacks early in the kill chain. There is a critical need for an integrated and automated approach to security.

Benefits

- Provide unified and consistent security that is always up to date in modern hybrid environments,via dynamic object synchronization
- Implement a zero-trust architecture without expensive tools or resources
- Easily deploy in minutes with turnkey integration
- Automate security to ensure protection keeps pace with DevOps and business innovation

FORTINET FABRIC-READY

Joint Solutions

Fortinet Fabric Connector and Guardicore Centra

Fortinet Fabric Connectors deliver turnkey, open, and deep integration into partner technologies and platforms, enabling security automation and simplified management. The deep integration between Guardicore Centra and Fortinet FortiManager via the Fortinet Fabric Connector provides enterprises with a unified and consistent security layer that's always up to date. This improves security posture and advances zero-trust network security—even in the face of today's fast-paced operational changes.

The joint solution enables organizations to synchronize protection with dynamic operational changes in their environments, extending visibility from on-premises to the cloud and enforcing granular L4–L7 segmentation policies.

It also can apply policy-based firewall controls using east-west traffic inspection, leveraging unified labeling and asset management solutions for internal applications. This combination ensures consistent access controls apply to north-south traffic at the perimeter in addition to internal traffic moving laterally.

Security administrators can deploy the integration between Guardicore and Fortinet in minutes without the need for hardware or software modifications to the underlying infrastructure.

The Fabric Connector integration features a Universal Connector Management Extension Application (MEA) that enables policy automation and provides dynamic object updates between Guardicore Centra and devices managed by FortiManager. Once configured, you can also retrieve label and asset information from FortiManager and create objects for use in FortiGate policies.

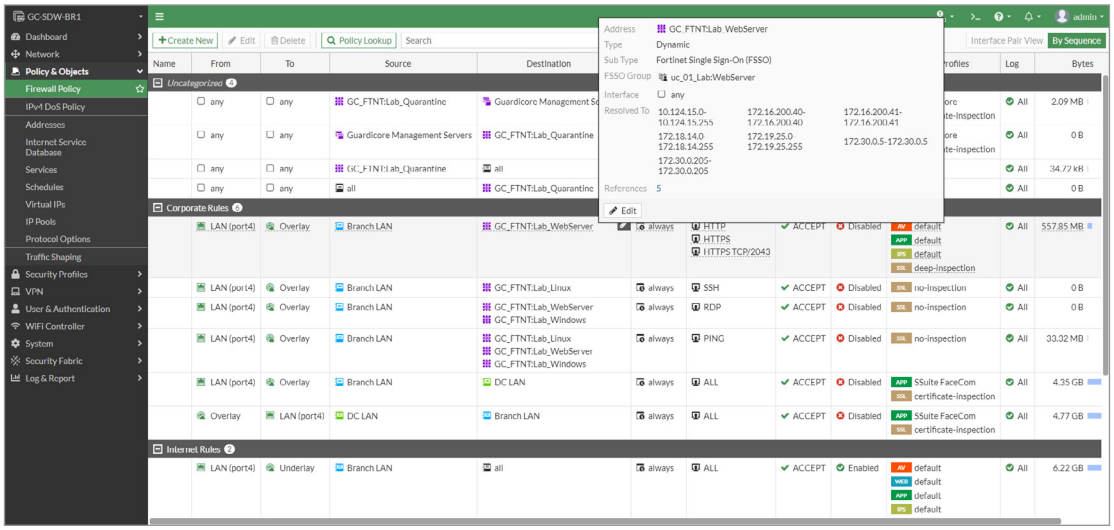

Figure 1: Integration of Guardicore labels with Fortinet policies and objects.

By leveraging the Fortinet Fabric Connector integration with Guardicore, organizations can automate and synchronize their security controls in conjunction with dynamic operational changes, simplifying overall security management and ensuring that protection doesn't get in the way of DevOps processes or rapidly bringing innovations to market.

Guardicore Centra and FortiAnalyzer

Fortinet FortiAnalyzer offers advanced logging and reporting capabilities, centralized security analytics across the Fortinet Security Fabric, and security automation via application programming interfaces (APIs).

Through integration with Guardicore Centra, organizations can now ensure FortiAnalyzer also has access to additional segmentation—and threat detection-related data from Guardicore. This helps teams better track threat activity, assess risk, and detect potential issues or problems to reduce a breach's impact on your organization.

FortiAnalyzer's unified logging and reporting capabilities can also leverage the rich data the integration provides when generating security and compliance reports for stakeholders and auditors. Through the integration, FortiAnalyzer can ingest data from Guardicore through syslog, and information pertaining to incidents, system alerts, agent logs, audit logs, and label change logs can all be exported to FortiAnalyzer.

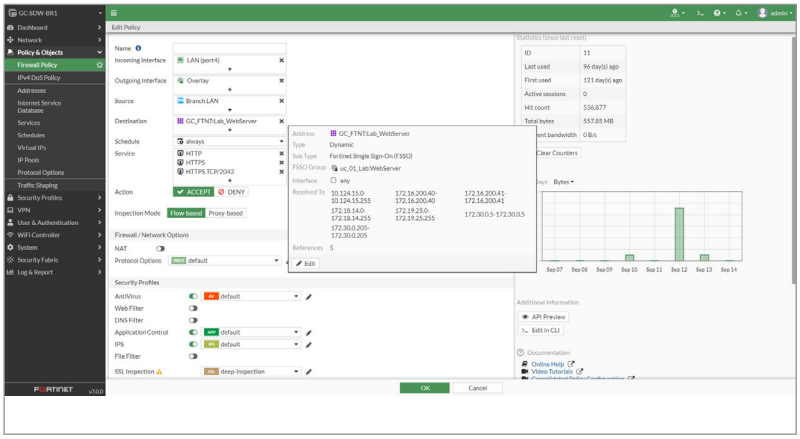

Figure 2: Guardicore Centra and FortiAnalyzer integration.

Benefits

- Reduce risk: See noncompliant activity, outdated segmentation policies, or other data that enables your organization to reduce risk
- Simplify operations: See alerts and potential issues in a centralized location for quick follow-up
- Increase visibility: Leverage Guardicore-generated data, such as audit logs in FortiAnalyzer reports

Guardicore Centra and FortiSOAR

Fortinet FortiSOAR security orchestration, automation, and response (SOAR) provides innovative case management, automation, and orchestration. It pulls together all of an organization's tools, helps unify operations, and reduces alert fatigue, context switching, and the mean time to respond to incidents.

Fortinet FortiSOAR integration with Guardicore Centra enables security operations center (SOC) teams to flag potentially malicious activity and quickly address it with intelligent automation and orchestration capabilities.

If a suspicious activity on an endpoint, such as running malware or accessing a malicious website, triggers an intrusion prevention system (IPS) event, the Fortinet FortiGate Next-Generation Firewall (NGFW) will automatically block the traffic. It also will log the event details in FortiAnalyzer. The FortiSOAR platform will execute a playbook that can collect this information from FortiAnalyzer periodically, and present it to the SOC team to take action or run automatically, all depending on the level of automation you'd like to implement for your incident response processes.

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.

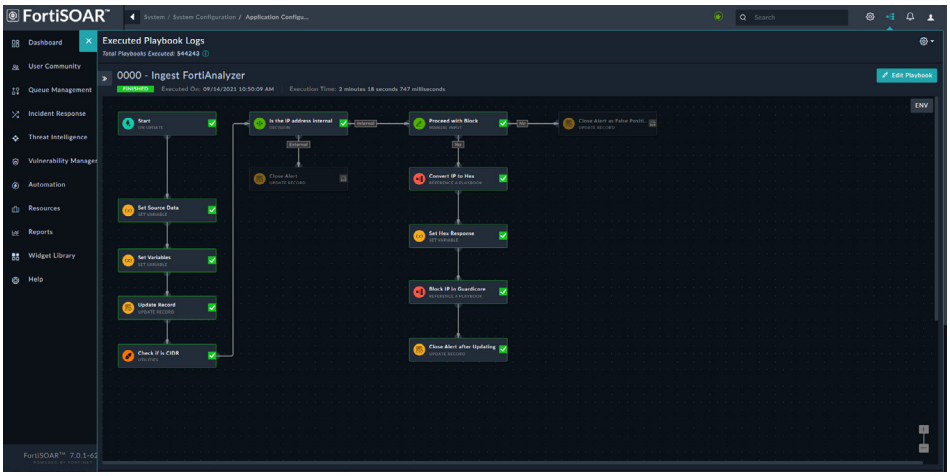

Figure 3: Guardicore Centra and FortiSOAR integration.

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

In summary, Fortinet FortiSOAR integration with Guardicore Centra enables SOC teams to flag potentially malicious activity and quickly address it with intelligent automation and orchestration capabilities. 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 rapidly evolving threats.

Guardicore Centra and FortiAuthenticator

Fortinet FortiAuthenticator is an identity and access management solution that protects against unauthorized access to corporate resources by providing centralized authentication services, including single sign-on (SSO) services, certificate management, and guest access management. Using FortiAuthenticator, IT/security practitioners can extend secure, conditional access to Guardicore Centra with an improved user experience, increased security, and platform neutrality.

Using multiple security tools, organizations are required to maintain access rights for administrators in order to protect corporate governance as well as ensure best practices for security. Guardicore Centra provides application owners the ability to define policies for their environment. Thus, it is required to extend access authorization to the Centra management console to a large number of individuals, each with a different role and set of permissions for actions, as well as assets that should be visible to them.

Benefits

- Integrated authentication for security administration
- Single and unified user management
- Centralized user access management
- Preserves and leverages the organization's previous investments in Active Directory (AD) and role-based access control (RBAC)

The integration of Guardicore Centra and Fortinet FortiAuthenticator, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers SSO, simplified management, and easy-to-use security, enabling Guardicore Centra users to be defined and authenticated by FortiAuthenticator.

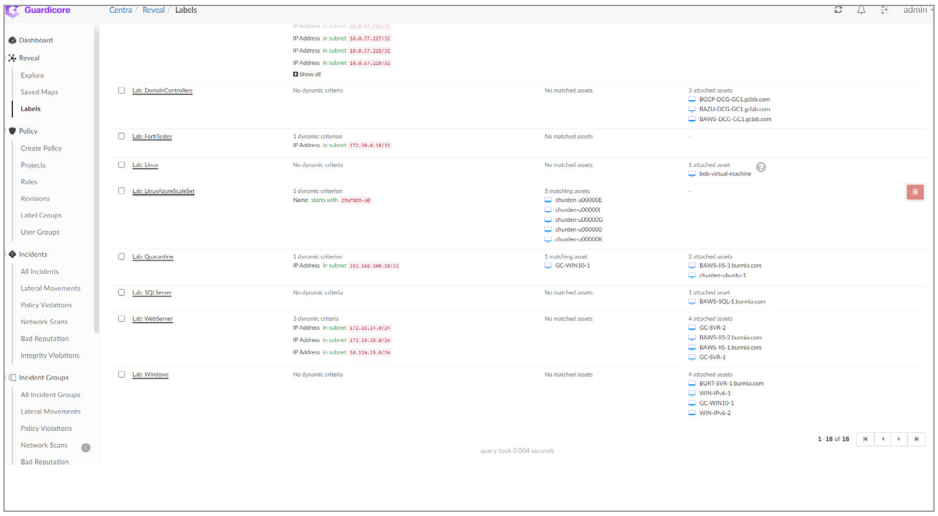

Figure 4: Guardicore Centra user interface.

About Guardicore

Guardicore is a data center and cloud security company that protects your organization's core assets using flexible, quickly deployed, and easy to understand microsegmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security — for any application, in any IT environment.

Our mission goes beyond creating great technology. We continuously engage with our customers as a trusted partner, ensuring they maximize the value of their security investments beyond their original goals and expectations.

Visit www.guardicore.com

Social media: Twitter | LinkedIn

FORTINET

www.fortinet.com

September 14, 2021 3:48 AM
1274560-0-0-EN