SOLUTION BRIEF

Simplify Operations with the Fortinet Security Fabric and FortiAnalyzer

Executive Summary

As digital transformation (DX) accelerates, network security management continues to pose significant challenges for organizations of all sizes. Misconfigurations and other human errors that contribute to breaches are often the result of network and security complexity, lack of visibility across the network, and inconsistent policy enforcement. In addition, as the network increasingly expands across on-premises data centers, edges, and the cloud due to DX initiatives, securing resources grows increasingly challenging. The array of disparate security products, each with individual management consoles, means visibility is limited and configurations tend to be inconsistent across the network.

FortiAnalyzer solves these challenges with consolidated network information and automated processes. Part of the Fortinet Security Fabric, FortiAnalyzer integrates with other Fortinet offerings and enables you to leverage security analytics and automation without the need for additional consoles or solutions.

75% of organizations are pursuing security vendor consolidation.[1]

Today’s Network Security Management Challenges

In an era marked by sophisticated cyberthreats and stringent regulatory standards, organizations in all sectors face the following:

Complex threat landscape: Rapidly evolving cyberthreats require swift detection and response, but legacy systems cannot keep pace.

Time-consuming compliance and audit management: Meeting global and industry-specific regulatory standards can be complex and drain IT resources.

Fragmented security infrastructure: Managing multiple security solutions can lead to operational inefficiencies and gaps in threat detection and response.

Inefficient manual processes: Time-consuming manual processes for threat detection, response, and reporting can delay reaction times and put undue burden on security teams.

Data overload: High volumes of network logs and security data can be challenging to manage and analyze effectively.

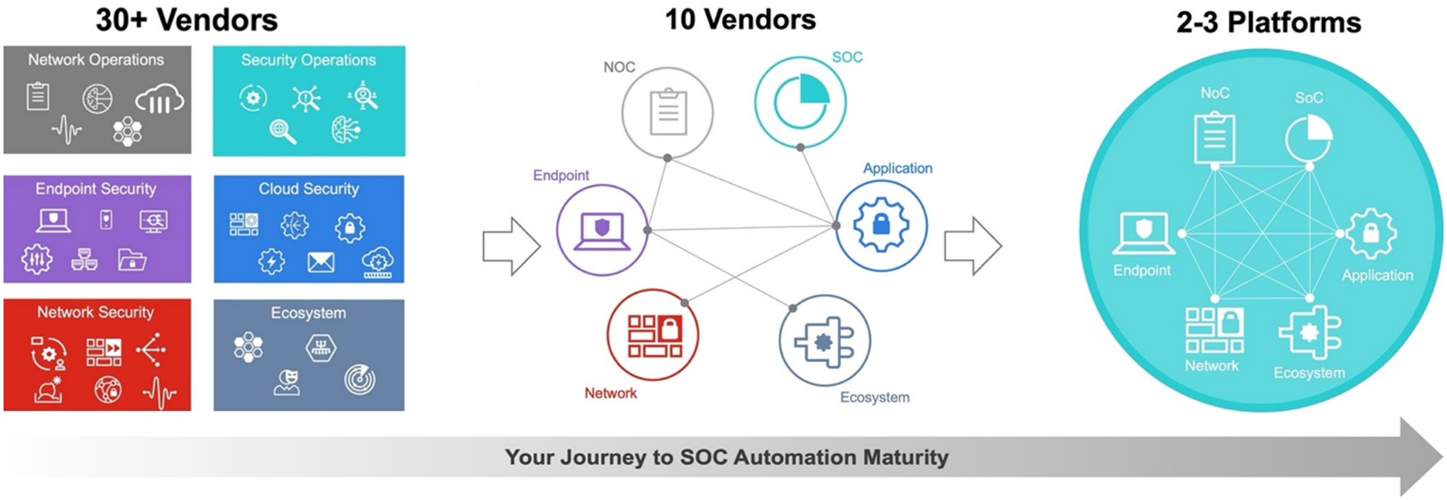
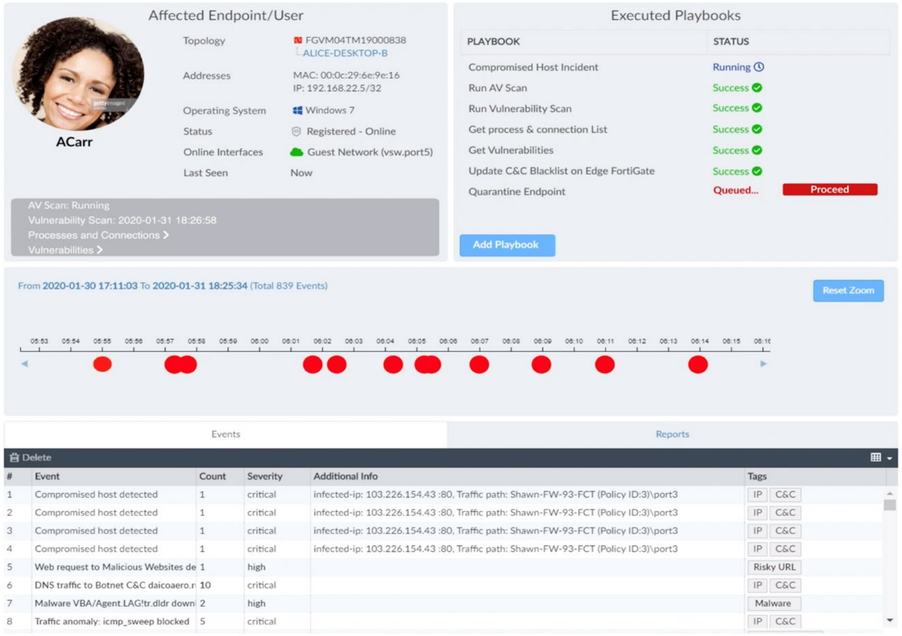


Figure 1: Vendor consolidation enables efficient, synchronized, and automated operations.



Affected Endpoint/User

ACarr

Topology	FGVM04TM19000838 ALICE-DESKTOP-B
Addresses	MAC: 00:0c:29:6e:9e:16 IP: 192.168.22.5/32
Operating System	Windows 7
Status	Registered - Online
Online Interfaces	Guest Network (vsw.port5)
Last Seen	Now

AV Scan: Running
Vulnerability Scan: 2020-01-31 18:26:58
Processes and Connections >
Vulnerabilities >

Executed Playbooks

PLAYBOOK	STATUS
Compromised Host Incident	Running
Run AV Scan	Success ✓
Run Vulnerability Scan	Success ✓
Get process & connection List	Success ✓
Get Vulnerabilities	Success ✓
Update C&C Blacklist on Edge FortiGate	Success ✓
Quarantine Endpoint	Queued...

From 2020-01-30 17:11:03 To 2020-01-31 18:25:34 (Total 839 Events)

#	Event	Count	Severity	Additional Info	Tags
1	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3)\port3	IP C&C
2	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3)\port3	IP C&C
3	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3)\port3	IP C&C
4	Compromised host detected	1	critical	infected-ip: 103.226.154.43 :80, Traffic path: Shawn-FW-93-FCT (Policy ID:3)\port3	IP C&C
5	Web request to Malicious Websites de	1	high		Risky URL
6	DNS traffic to Botnet C&C daicoaero.r	10	critical		IP C&C
7	Malware VBA/Agent.LAG!tr.dldr down	2	high		Malware
8	Traffic anomaly: icmp_sweep blocked	5	critical		IP C&C

Figure 2: FortiAnalyzer shows insights into security operations.

51% of analysts reported improved threat detection using automated workflows.[2]

Leverage Advanced Analytics and Automation

Navigating the complexities of today's constantly evolving network landscape requires a unified solution. FortiAnalyzer, with its advanced network security analytics, ensures extensive visibility, advanced threat detection, and comprehensive reporting across various deployment locations. Automation capabilities simplify policy management and system configurations, plus offer timely threat response.

FortiAnalyzer works seamlessly with the Fortinet Security Fabric, leveraging a collaborative ecosystem of security solutions working in concert. This integration enables unified policies, coordinated threat response, and consolidated operations, enhancing the overall efficacy of your security setup. Key capabilities include:

Interoperability: FortiAnalyzer is part of the Fortinet Security Fabric, enabling seamless communication with your security components, enabling quicker identification, isolation, and remediation of threats across the network.

Consolidation of operations: FortiAnalyzer offers centralized logging, analytics, and reporting to reduce the complexity of security operations. Consolidating disparate tasks into a single platform reduces operational overhead and ensures consistency in security policy application and enforcement.

Log management: FortiAnalyzer collects, stores, and analyzes log data from all Fortinet security devices, including FortiGate Next-Generation Firewalls, VPNs, and intrusion detection and prevention systems. With FortiAnalyzer, you can manage large volumes of logs and search for specific events using various search criteria, such as time range, source or destination IP, and protocol.

Actionable insights: FortiAnalyzer delivers advanced security analytics that convert raw network data into actionable insights. You can leverage these insights to fine-tune your organization's security posture, identify potential vulnerabilities, and ensure ongoing compliance with regulatory standards.

Automation: FortiAnalyzer automates routine tasks. This includes automating responses to security incidents, generating reports, and adjusting security policies based on network behavior.

Incident response: FortiAnalyzer provides real-time detection and response capabilities for incidents. It provides comprehensive visibility into network traffic and security events and correlates and analyzes events generated from all Fortinet devices. This consolidates visibility to provide an accurate picture of security threats. FortiAnalyzer generates alerts when security events occur, such as when a user attempts to access a restricted website.

Advanced threat detection: FortiAnalyzer integrates with FortiGuard Labs to provide real-time information on emerging threats and vulnerabilities. It analyzes and correlates threat data from multiple sources, including third-party threat feeds.

Achieve Key Security and Business Benefits with FortiAnalyzer

The solution ensures that IT leaders are equipped with data-driven insights, fostering swift and accurate business decisions that align with company objectives and market dynamics.

Boost visibility and threat detection

FortiAnalyzer amplifies visibility across network traffic, user activities, and system configurations. It combines sophisticated event correlation, network traffic analysis, and advanced AI techniques with an intuitive rules editor mapped to MITRE ATT&CK® use cases. FortiAnalzyer enables you to preemptively set if-this-then-that criteria, spot anomalies, identify potential breaches, and understand user behavior. Integrated machine learning allows for predictive analysis and trend spotting. Ultimately, you can dramatically reduce your attack surface and stop previously hidden threats before they escalate.

Increase operational efficiency and enhance security posture

A single dashboard offers a unified, real-time view of data across the Fortinet Security Fabric and other integrated systems. With FortiAnalyzer, you'll see a sharp reduction in threat response times, increased operational efficiency, and a stronger security posture. This fusion of data and analytics into one comprehensive viewpoint simplifies network management tasks and offers faster, actionable insights. With quicker decision-making, analysts reduce the risk of oversight errors and gain an agile response mechanism ready to tackle emerging threats.

Simplify compliance and auditing

FortiAnalyzer helps you comply with numerous global and industry-specific regulations with prepackaged compliance reports and customizable report options. Predefined compliance reports tailored to standards such as GDPR, HIPAA, and PCI-DSS make it simpler for organizations to maintain a steady compliance posture. Beyond reporting, FortiAnalyzer offers real-time tracking of user activities and network configurations against compliance benchmarks. Having this data easily accessible is critical in the event of an audit. FortiAnalyzer frees up resources, reduces potential penalties, and, most importantly, reinforces an organization's reputation as a trustworthy data custodian by simplifying compliance processes.

Summary

FortiAnalyzer brings unparalleled value to modern network security management. Advanced security analytics, superior logging and correlation capabilities, and intelligent automation stitches offer organizations a streamlined, efficient, and secure network management solution. FortiAnalyzer addresses the complex challenges of network security management, delivering enhanced visibility, robust threat protection, and simplified compliance management across the entire network infrastructure.

[1] "Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022," Gartner, September 13, 2022.

[2] Aviv Kaufmann, "The Quantified Benefits of Fortinet Security Operations Solutions," Enterprise Strategy Group, July 2023.

August 31, 2023 2:43 PM

2309122-0-0-EN