Lumen® SASE Solutions with Fortinet FortiAnalyzer

FortiAnalyzer is a powerful log management, analytics, and reporting platform, providing organizations with single-pane orchestration, automation, and response for simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack surface.

Integrated with the Fortinet Security Fabric, advanced threat detection capabilities, centralized security analytics, and complete end-to-end security posture awareness and control helps security teams identify and eliminate threats before a breach can occur.

Orchestrate security tools, people, and process for streamlined execution of tasks and workflows, incident analysis and response, and rapidly expedite threat detection, case creation and investigation, and mitigation and response.

Automate workflows and trigger actions with fabric connectors, playbooks, and event handlers to accelerate your network security team's ability to respond to critical alerts and events, plus service level agreement (SLA) for regulation and compliance.

Respond in real-time to network security attacks, vulnerabilities, and warnings of potential compromises, with threat intelligence, event correlation, monitoring, alerts and reporting for immediate tactical response and remediation.

Key Features

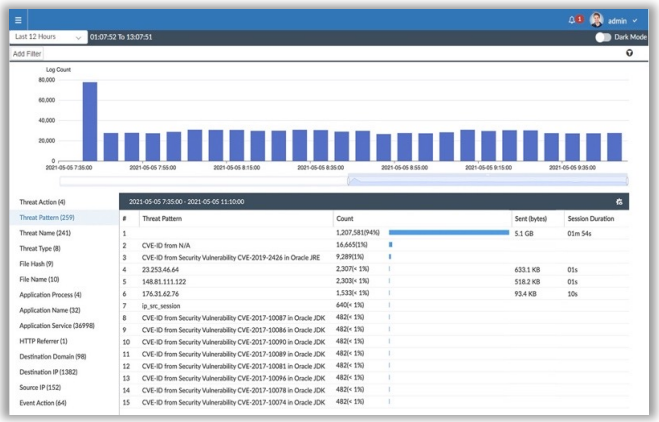
- Security Fabric Analytics with event correlation and real-time detection across all logs, with Indicators of Compromise (IOC) service and detection of advanced threats
- Fortinet Security Fabric integration with FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail, and others for deeper visibility and critical network insights
- Enterprise-grade high availability to automatically back-up FortiAnalyzer databases (up to four node cluster), which can be geographically dispersed for disaster recovery
- Security Automation to reduce complexity, leveraging REST API, scripts, connectors, and automation stitches to expedite security response and reduce time-to-detect
- Multi-Tenancy solution with quota management, leveraging (ADOMs) to separate customer data and manage domains for operational effectiveness and compliance
- Flexible deployment options as appliance, VM, hosted, or public cloud. Use AWS, Azure, or Google for cloud secondary archival storage

Feature highlights

Incident detection and response

Centralized NOC/SOC visibility for the attack surface

The FortiSOC view helps teams in the security operations center (SOC) and network operations center (NOC) protect networks with access to real-time log and threat data in the form of actionable views with deep drill-down capabilities, notifications and reports, and predefined or customized dashboards for single-pane visibility and awareness. Analysts can utilize FortiAnalyzer workflow automation for simplified orchestration of security operations, management of threats and vulnerabilities, responding to security incidents, or investigate proactively by looking for anomalies and threats in SIEM normalized logs in the Threat Hunting view.

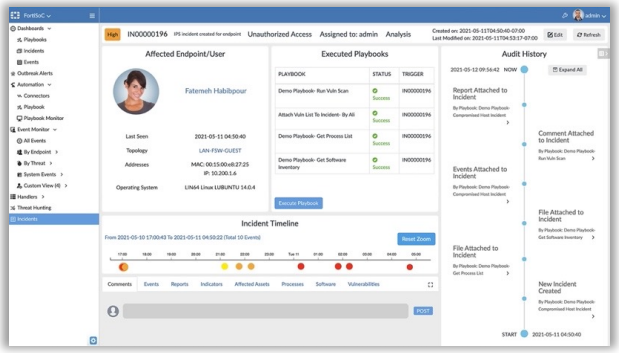


Event management

FortiAnalyzer Event Monitor enables security teams to monitor and manage alerts and events from logs. Events are processed and correlated in an easily readable format that analysts can understand for immediate response. Analysts can use the Event Monitor for investigative searches into alerts and use the predefined or custom event handlers for NOC and SOC, with customizable filters to generate real- time notifications for around-the-clock monitoring, including handlers for SD-WAN, VPN SSL, wireless, network operations, FortiClient, and more.

Incident management

The Incidents component in FortiSOC enables security operations teams to manage incident handling and life cycle with incidents created from events to show affected assets, endpoints, and users. Analysts can assign incidents, view and drill down on event details, incident timelines, add analysis comments, attach reports and artifacts, and review playbook execution details for complete audit history.



Integrate with FortiSOAR for further incident investigation and threat eradication including support to export incident data to FortiSOAR through the FortiAnalyzer fabric connector (enabled on FortiSOAR with API admin setup).

Playbook Automation

FortiAnalyzer Playbooks boost an organization's security team's abilities to simplify investigation efforts through automated incident response, freeing up resources and allowing analysts to focus on tasks that are more critical.

Out-of-the-box playbook templates enable SOC analysts to quickly customize their use cases, including playbooks for investigation of compromised hosts, infections and critical incidents, data enrichment for Fabric View Assets & Identity views, blocking of malware, C&C IPs, and more. Security teams can define custom processes, edit playbooks and tasks in the visual playbook editor, utilize the Playbook monitor to review task execution details, import or export playbooks, and use built-in connectors for allowing playbooks to interact with other Security Fabric devices like FortiOS and EMS. The new connector health check provides an indicator for verifying that connectors are always up and working.

Security services

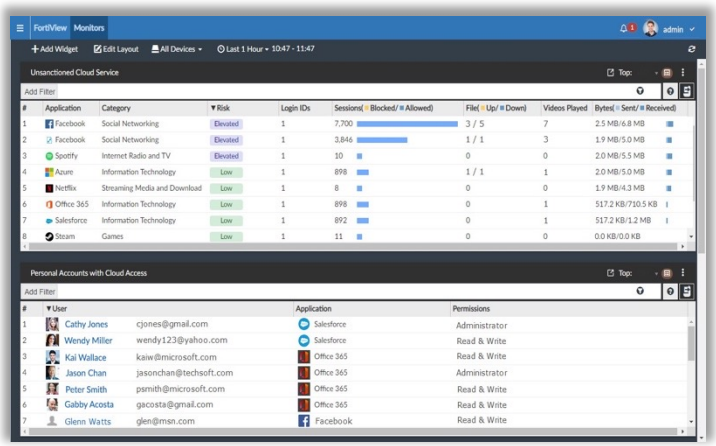
Include the FortiSOC subscription to enable further automation for incident response with enhanced alert monitoring and escalation, built-in incident management workflows, connectors, and many more FortiSOC playbooks.

The FortiGuard Indicators of Compromise subscription empowers security teams with forensic data from 500,000 IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system, that have been determined with high confidence to be malicious infections or intrusions, and historical rescan of logs for threat hunting.

Feature highlights

The Shadow IT monitoring service provides continuous monitoring usage of unapproved devices and resources, and unsanctioned accounts and unauthorized use of SaaS and IaaS, API integration, third party apps, and rogue users using personal accounts for managing company assets.

The FortiGuard Outbreak alert service provides an automatic download of content packages with resources for detecting the latest malware and threats, including views for summary of outbreaks, kill chain mapping for how the malware works. FortiGate coverage explains what FortiGate NGFW components and services will block the threats, and Fabric Coverage for leveraging the full Fabric security protection.



Security fabric analytics

Analytics and reporting

Security teams are empowered with FortiAnalyzer automation driven analytics and reports providing full visibility of network devices, systems, and users.

FortiAnalyzer delivers correlated log data with threat intelligence for analysis of real-time and historical events, providing context and meaning to network activity, risks, and vulnerabilities, attack attempts, operational anomalies, and continuous monitoring of sanctioned and unsanctioned user activity and investigation of Shadow IT.

Assets and identity

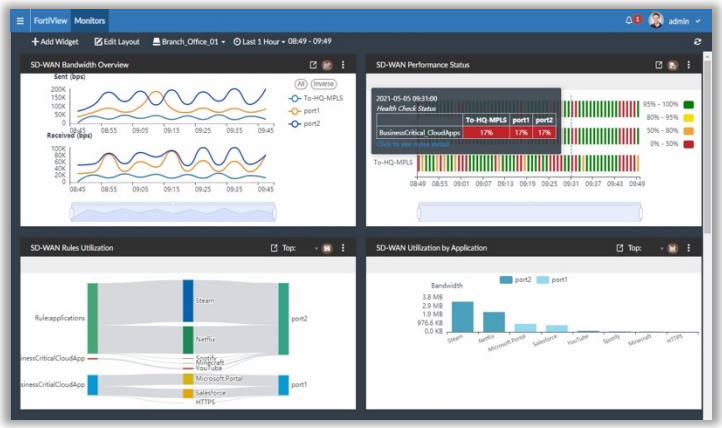
FortiAnalyzer Fabric View with Asset and Identity monitoring provides full SOC visibility of users and devices, including analytics of the attack surface and enables analysts to view and manage detailed UEBA information collected from logs and fabric devices, with filters and custom views for refining results.

The Assets & Identity views provide security teams with elevated visibility into an organization's endpoints and users with correlated user and device information, vulnerability detections, and EMS tagging and asset classifications through telemetry with EMS, NAC, and Fortinet Fabric Agent.

FortiView is a comprehensive monitoring solution that provides multilevel views and summaries of real-time critical alerts and information such as top threats and IOCs to your network including Botnet and C&C, top sources/destinations of network traffic, top applications, websites and SaaS, VPN and System information, and other Fabric device intelligence.

Monitors view provides operations teams with customizable NOC and SOC dashboards and widgets designed for display across multiple screens in the Operations Center. Monitor events in real-time through the pre-defined dashboard views for SD-WAN, VPN, Wi-Fi, Incoming/Outgoing Traffic, Applications and Websites, FortiSandbox Detections,

Endpoint Vulnerabilities, Software Inventory, Threats, Shadow IT (monitoring service), Fabric State, and many more.



Analysts can expand their investigation in Log View, with easy navigation of managed device logs using search filters, log drill down, formatted or raw logs, log import/export, plus define custom views and create log groups.

With a FortiSOC license, a SIEM database is automatically created to store normalized logs for devices in Fabric ADOMs.

Feature highlights

FortiAnalyzer reports

FortiAnalyzer provides over 60 report templates, 800+ datasets, and 750+ charts that are ready-to-use with sample reports, including reports for Secure SD-WAN, VPN monitoring, threat assessments, 360 Security Reviews, situational awareness, self-harm and risk indicators, bandwidth and applications, FortiClient, FortiMail, FortiSandbox, FortiDeceptor, compliance, and many others.

Analysts can easily customize, clone, and modify reports to their needs with filters by device, subnets, and type to deliver specific business metrics to target stakeholders. Schedule reports to run at non-peak hours or run on demand, define output profiles for notifications, and deliver reports in flexible viewing formats including PDF, HTML, CSV, and XML.

Deployments

Deploying FortiAnalyzer

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

Multi-Tenancy with flexible quota management

FortiAnalyzer provides the ability to manage multiple sub-accounts with each account having its own administrators and users. The time-based archive/analytic log data policy, per Administrative Domain (ADOM), allows automated quota management based on the defined policy, with trending graphs to guide policy configuration and usage monitoring.

Analyzer-Collector Mode

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

Log forwarding for third-party integration

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

Trusted Platform Module (TPM) encryption

FortiAnalyzer G Series features a dedicated micro-controller module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys in TPM, with hardware-based security mechanisms that protect against malicious software and phishing attacks.