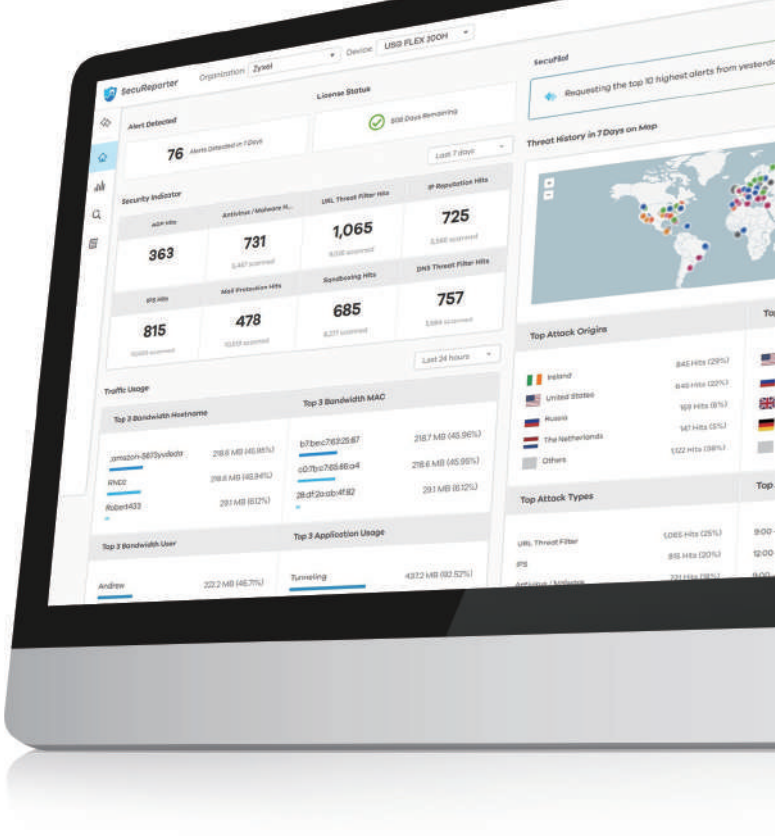
ZYXEL
NETWORKS



SecuReporter

Cloud Analytics Service

The Zyxel CNM SecuReporter is a cloud-based intelligent analytics and report service with collection and correlation features designed for Zyxel firewalls & Nebula product lines. It provides network administrators with centralized view of network activities.

When it comes to the cyber security, the analytics is the last piece of the puzzle, and it is needed more than ever. We brought the best minds in the IT industry together to create an all new SecuReporter. It provides intuitive working interface for IT professionals. SecuReporter supports nebula networking products, enabling it to get a fast response to security events that occur in your access points and network switches.

Benefits

A 360 Degree Analysis of Your Cybersecurity

The number of cybersecurity threats and their complexities are growing, which drives the need for 360-degree visibility for monitoring network. SecuReporter offers multiple dimensions of analytics on abnormal behaviors across your business. Analyze the time trend, threat type, signature, and email subject leads for precise detection. Monitor malicious activity from source IP and destination IP for bidirectional analysis.

- Cloud-based “Software as a Service” (SaaS)
- Centralized insights on user and client behavior
- Multidimensional cloud-based firewall analytics on abnormal behaviors
- Custom and preconfigured-reporting
- Seamless setup and monitoring with Nebula management ecosystem
- Advanced Analytics include Sandboxing, IP Reputation, URL Threat and DNS Filter
- SecuReporter AI-driven insights for seamless network visibility and control

SecuReporter

nebula

Enhanced Security with SecuReporter and Nebula

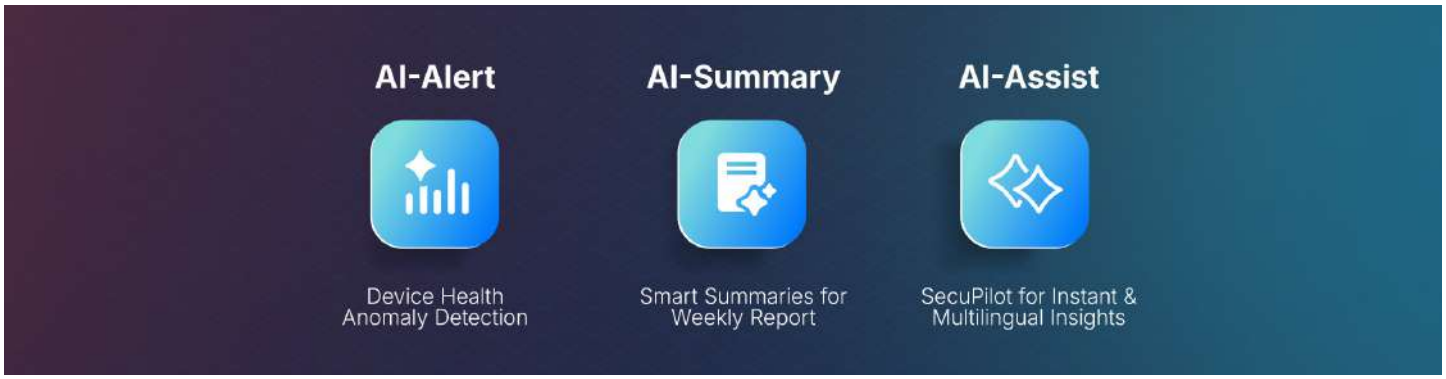
SecuReporter boosts your cloud firewall with a comprehensive view of Nebula network activities, offering swift security responses. It streamlines analytics and compliance, now featuring real-time push notifications and alerts within the Nebula app.

Scale capacity and save cost with cloud computing

Cloud-based "Software as a Service" (SaaS) is easy to scale up cloud capacity, drawing on the service's remote servers, allowing to cut out the high cost of hardware.

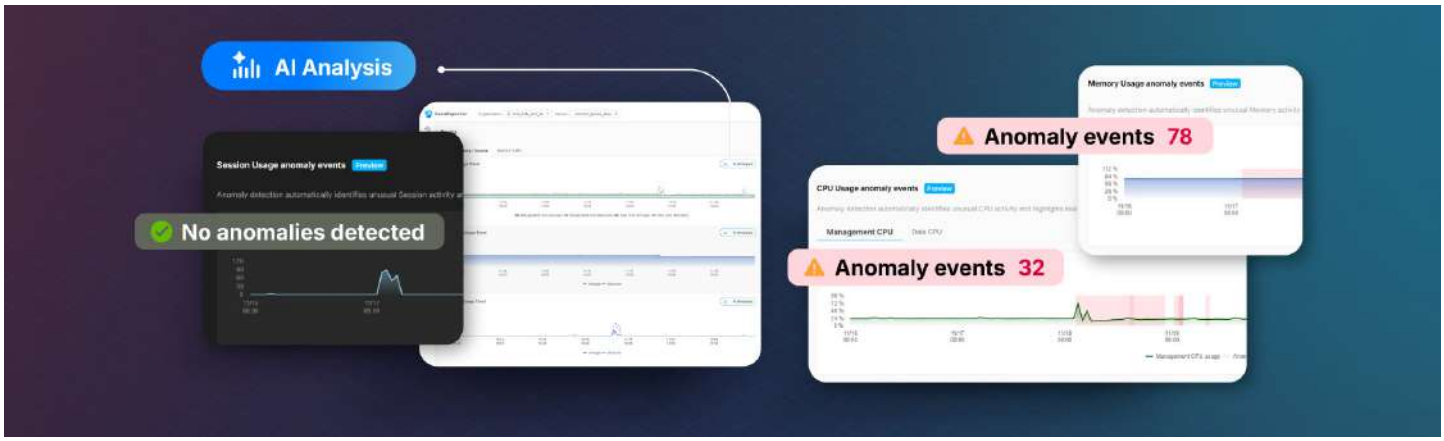
AI-driven insights for seamless network visibility and control

SecuReporter AI processes massive volumes of log data to organize and highlight the most critical insights. By turning raw information into clear, prioritized, and actionable intelligence with features like Device Health Anomaly Detection, Smart Report Summaries, and SecuPilot, it enables administrators to swiftly assess their security posture. This functionality significantly reduces alert fatigue and allows them to make confident, data-backed decisions with AI guidance, ultimately driving greater operational efficiency and cultivating a stronger, more intelligent security defense.



Proactive Device Health Anomaly Detection*

Introducing Device Health Anomaly Detection, an AI-driven feature that monitors how your devices behave, learns their patterns, and alerts you when something doesn't look right. Leveraging advanced machine learning, the AI continuously monitors CPU, memory, and session usage to construct a unique, dynamic behavioral baseline for every network device. This intelligent mechanism flags subtle deviations that traditional static thresholds miss, enabling administrators to identify issues early—from performance degradation and hardware stress to covert threats like crypto-mining and botnets. Empower your administrators with clear, actionable summaries to instantly trace root causes and secure network integrity before damage occurs.



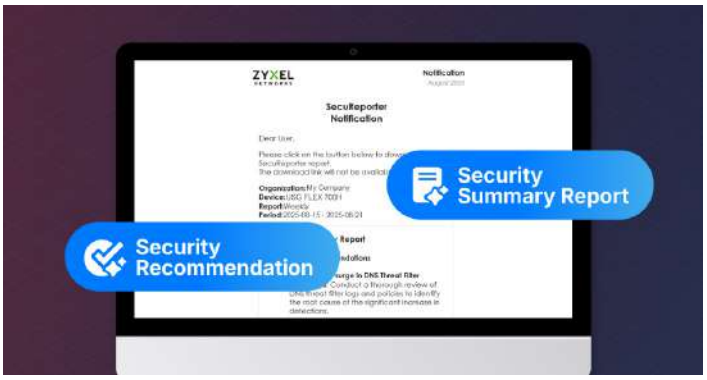
*: USG FLEX 500H/700H only.

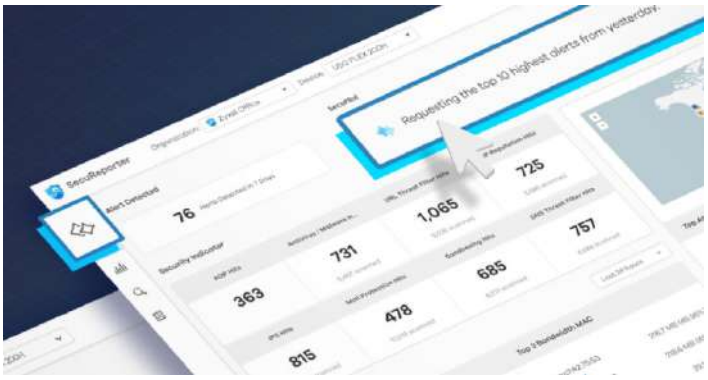
Smart Report Summaries

Automatically delivers AI-generated summaries that highlight key security insights with clear, easy-to-read visuals. Instead of going through lengthy raw data, users receive focused recommendations and contextual explanations—such as identifying unusual changes in security event detections—so they can take action quickly and confidently.

SecuPilot for Instant, Multilingual Insights

Instantly access essential device information, security data, traffic logs, and alerts, keeping you ahead of potential threats with various chart options, including bar, column, pie, donut, trend, and grid formats. Generate comprehensive summaries with ease. Powered by the cutting-edge LLM model, SecuPilot supports over 40 languages. Simply ask, and the AI remembers your questions.





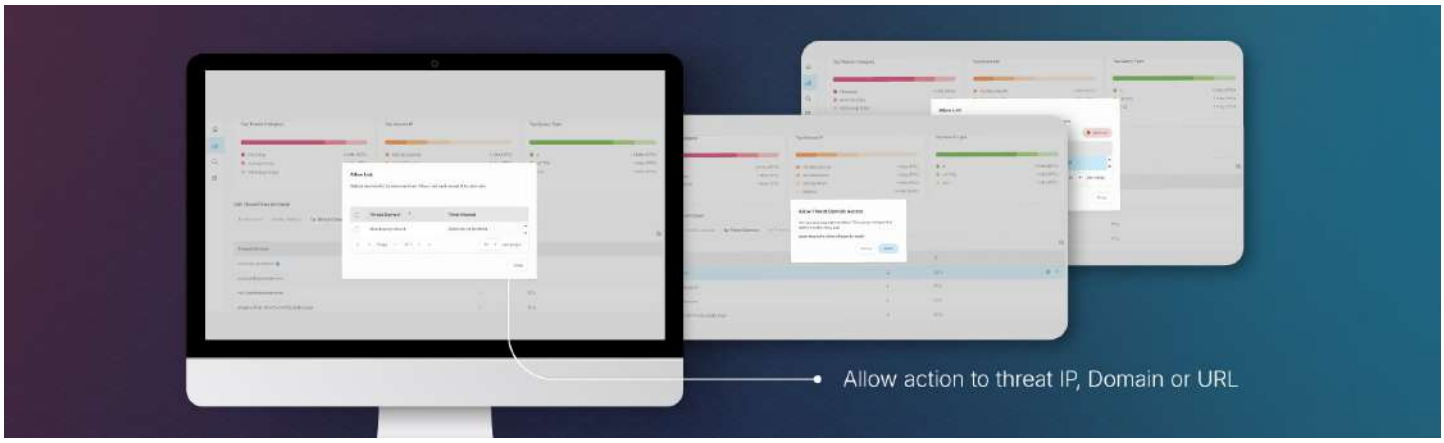
MSP Threat Report*

Designed to help MSP admins quickly identify security risks across customers and gain clear visibility into threat activity from a single, centralized view. The flexible profiles allow you to create customized reports while aligning time zones for consistent data. You can quickly pinpoint which organizations or devices face the greatest increases in threat. By providing detailed attack type insights, it enables administrators to prioritize their responses and efficiently strengthen their protection policies seamlessly.

*: The MSP Threat Report requires the Nebula MSP Pack license; only on-cloud firewalls are supported.

Streamline your security with real-time alerts and actionable insights

SecuReporter enhances real-time alerts and response by allowing users to manage mistakenly blocked websites directly within the platform, eliminating the need to access the Zyxel device Web GUI. This feature enables administrators to quickly set allow lists from both the firewall and SecuReporter, increasing flexibility and saving valuable time.



Client Identity

SecuReporter gives you more visibility of your networks including wired, wireless, BYOD, and IoT devices. Helps identify abnormal behavior, then pinpoints with detailed information of the client device including IP address, MAC address and hostname, users email of Astra endpoint service. SecuReporter also provides full detailed client information on analytics reports and event logs, helping SMB(s) reduce investigation time.

Centralized insights and client insights

SecuReporter offers centralized visibility of network activities and potential threats within entire network environment. It allows administrators to proactively monitor network status. Users can quickly and easily activate SecuReporter on the cloud.

Complies with national personal data protection regulations

We are committed to following the latest national data protection regulations, such as the GDPR and OECD Privacy Principles. SecuReporter offers three options you can choose: Partially anonymous, Fully Anonymous, Non-Anonymous to protect personal data.

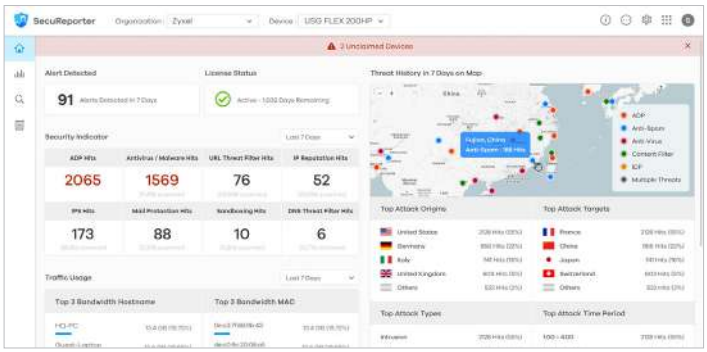
Improved customization and log downloads via API

Zyxel SecuReporter offers customizable PDF reports with personalized logos, titles, and comments. Generate reports instantly or schedule them daily, weekly, or monthly. The SecuReporter OpenAPI allows easy access to device logs from the past 31 days via HTTP requests using any programming language or cURL commands.

Interface Overview

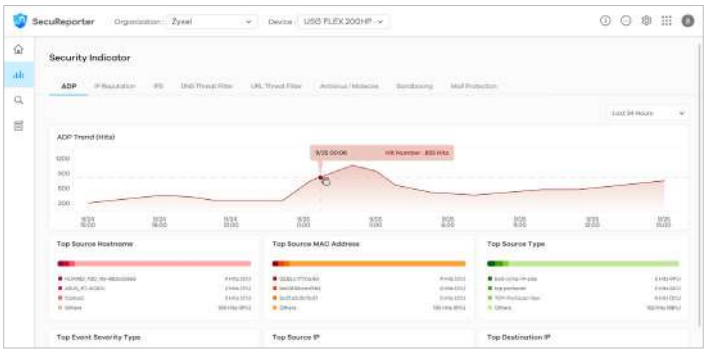
Dashboard

Turn massive data of network activity into clear data points in the dashboard. Show your devices with a city-level location. The pins on the map show the threats' origin and targets. The pin color indicates the frequency of these attacks. You can also find what kind of attacks are detected, where the threats are coming from, how they impact traffic usage, when attack occurs, and more indicators. You can get individual indicator log data that reveals key details.



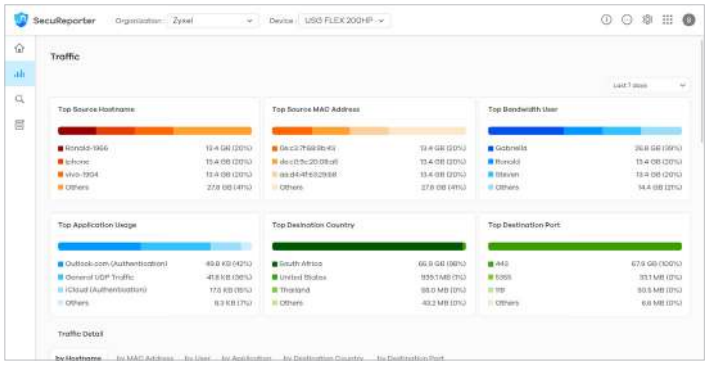
Indicator

Get deep insights into all activities that are happening in the network security environment. Get precise detection with intuitive graphic, indicator that analyzes time trend, threat type, signature, and client device information leads for precise detection. Monitor malicious activities from source IP and destination IP for bidirectional analysis to perform deep investigative analysis.



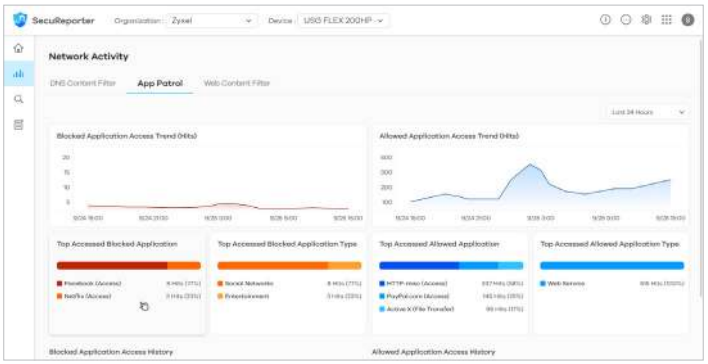
Traffic

Get a high-level view of network activity that pinpoints top source hostname, top MAC address, top bandwidth user, top application usage, and top destination countries.



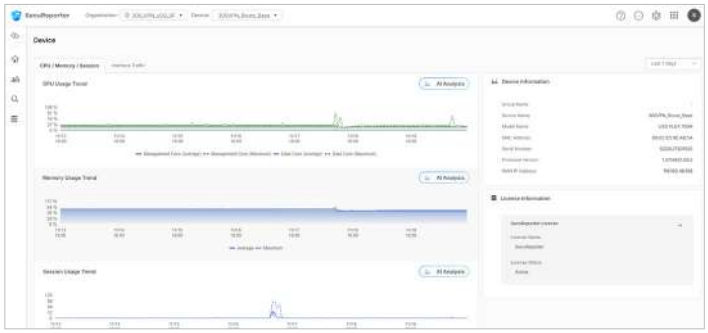
Application

Shows real-time access application history reports of what applications and website are being accessed, blocked, and allowed.



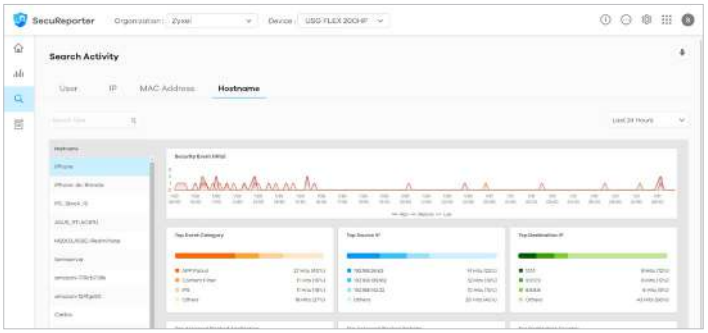
Device*

Gain deeper visibility into device behavior with AI-driven insights. Monitor CPU, memory, and session usage trends, analyze performance over time, and quickly identify anomalies. You can also view information and status about license key activations.



Search

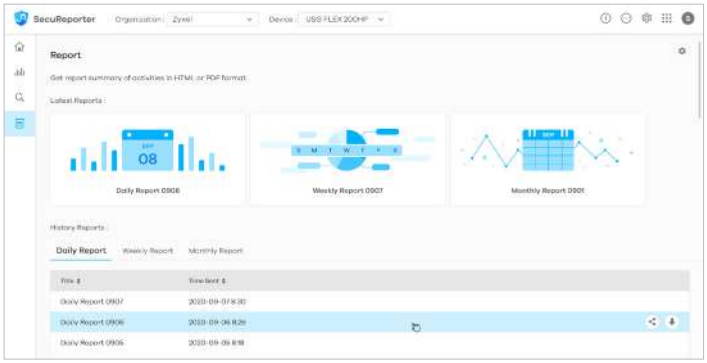
Zyxel security firewall series send logs to SecuReporter cloud-based platform for long-term retention without storage limitation. Search Log makes it easy to search your log data by filtering along with a specific time period, IP, MAC address and hostname.



*: Device health anomaly detection is available on USG FLEX 500H/700H only.

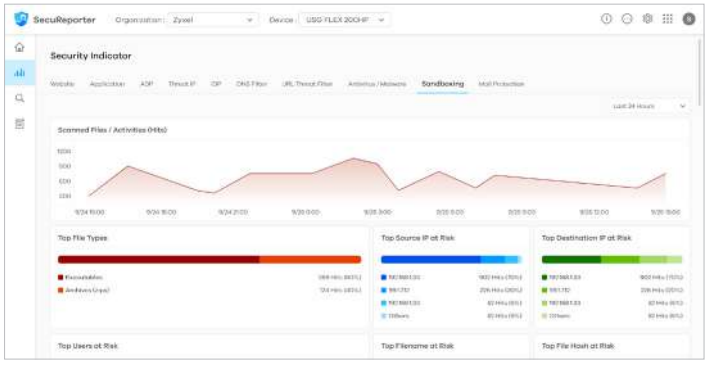
Customizable Reports

Easily create and customize reports with your own branding, and schedule them by choosing the weekday that best fits your workflow for delivery to clients or managers. Select from various cover designs, add your custom logo, and preview the report format with your preferences. The redesigned content highlights key analysis results for quick and easy review.



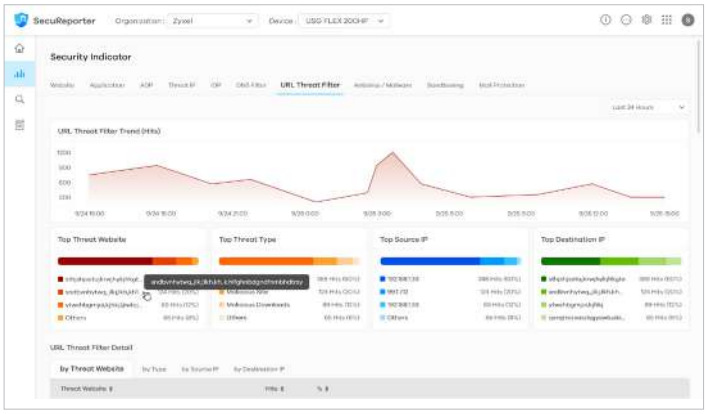
Sandboxing Analytics*

The Sandboxing report includes data for all sandboxing scanning activities like source IP, destination IP, file type, file hash, and scan results (safe, suspicious, or malicious). Alert email will be sent for every submitted file that is found to be malicious.



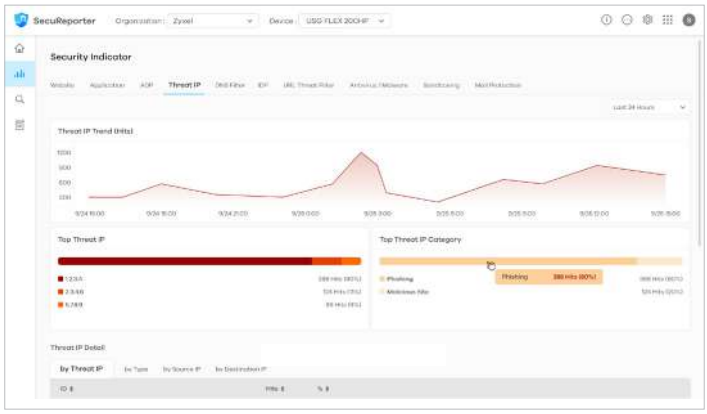
URL Threat Analytics*

Botnet Filtering provides the list of malicious web to do a quick check and automatically block malicious URL. Users can have a view of the Top Botnet block URL and identify its type with Botnet Filter report. Easily find out the user who has been compromised.



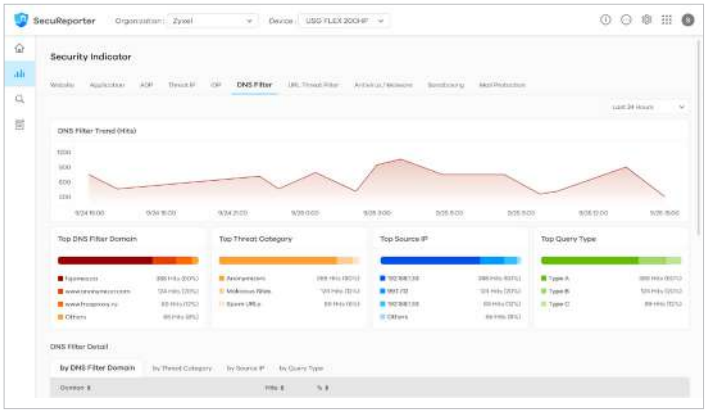
IP Reputation Analytics*

IP reputation provides malicious IP records to do a quick check. Filter increases threat visibility in SecuReporter which assists in tracing cyber threat sources. The report shows the blocking record details, Top attacking IP, attack type, and the level of risk.



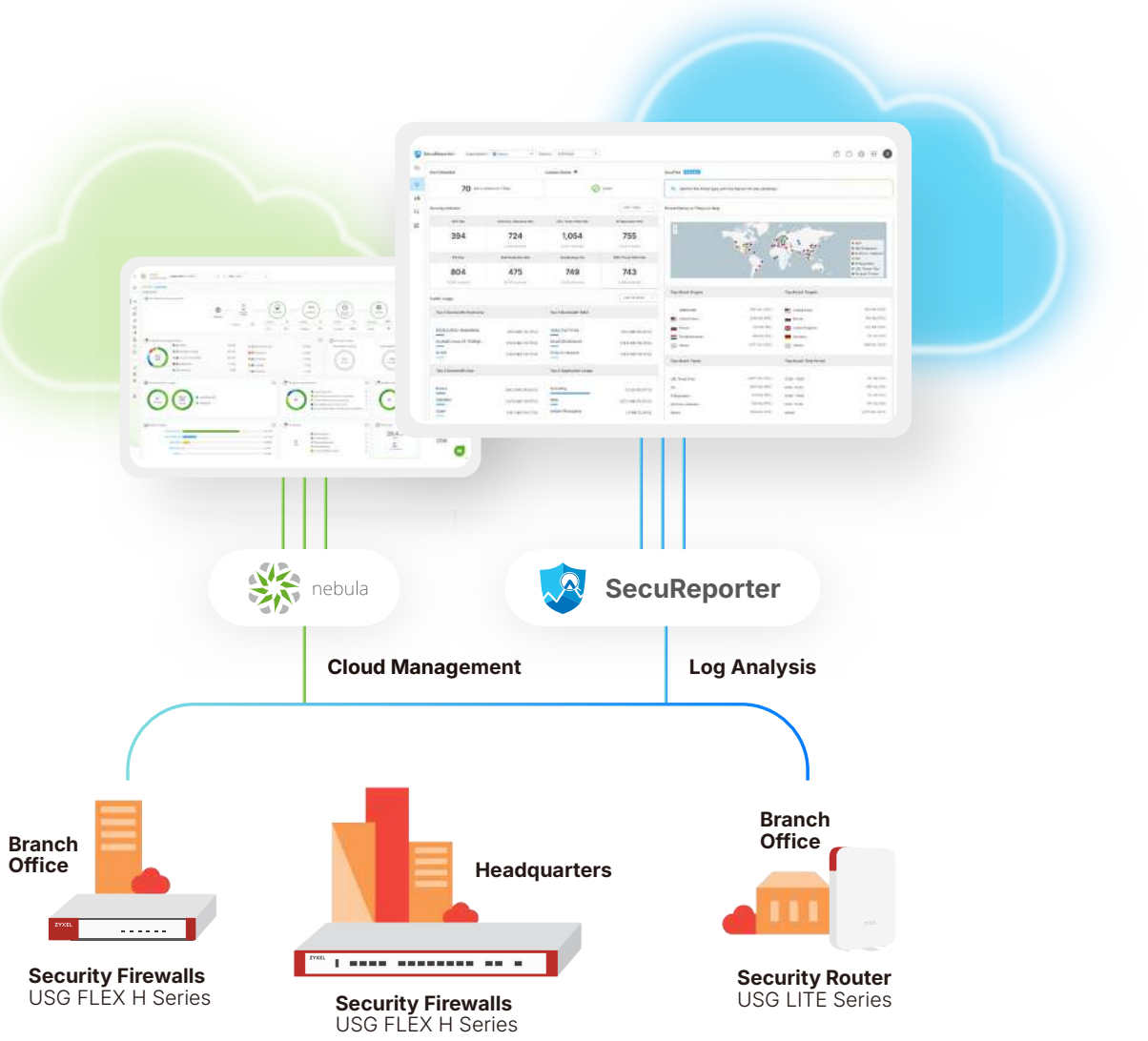
DNS Filter Analytics*

The DNS report includes detection trend, Top domains, Top threat categories and query types. Based on the report, IT can fully customize blocklist to ban access to any unwanted domains.



*: ATP/USG FLEX H/USG FLEX series only.

Application Diagram



Licensed Service

Customizable Report	Analytic History	Log Retention	Log Filtering Search	Product	Applicable
Daily Weekly Monthly	30 days (with customization)	1 Year	30 days (CSV file)	ATP Series	• Gold Security Pack
				USG FLEX H Series	• Gold Security Pack
				USG FLEX Series	• Default Bundle • Gold Security Pack • UTM Security Pack • Content Filter Pack • Single License
				USG Series	• Single License
				USG LITE Series	• Elite Pack (Traffic Log Archiving)

*: License subscription fee and permits may vary by country. For USG LITE series, SecuReporter support is limited to Traffic Log Archiving and requires the purchase of the Elite Pack license.

Specifications

Dashboard & Threat Map

Dashboard

- Events/Alarms notification symbol
- Top Users with Most Bandwidth
- Top Destination Countries
- Top Applications
- Top Destination Ports
- License status and remaining days
- Location is available by city level GeoIP
- Alerts Detected in 7 Days
- Total Counts of Malware/Virus Detected
- Spam Emails Detected
- Anomalies Detected
- Blocked Requests
- Threat Trend

Threat Map

- Statistics of attack packets in 7 days (detected in the device)
- Threat status when selecting a specific country
- Top Attack Origins / Top Attack Targets / Top Attack Types / Top Attack Time Period / Top Attackers IP Address / Top Attacked IP Address

Analysis

Security Indicator

Multidimensional analytics

- Anti Virus/Anti Malware
- IDP
- ADP
- Mail Protection
- Sandboxing*
- URL Threat Analytics*
- IP Reputation Analytics*
- DNS Filter Analytics*

Application & Website Activity

- Web Security
- Allowed websites
- Blocked websites Access trend
- Top Blocked Websites / Website Type
- Top Allowed Website / Website Type
- Top Source / Destination IP

Application Patrol

- Top Blocked Application / Application Type
- Top Allowed Application/ Application Type
- Top Blocked Destination Countries Blocked / Allowed Application Access History

Users aware search

- Security Events
- Application Usage
- Website Usage
- Top Destination Countries
- Traffic Upload/Download Usage Trend
- Login/Logout History

Client identity

- Search by User
- Search by IP Address
- Search by MAC address
- Search by Hostname
- Device Category identity
- Device OS identity
- User email of Astra endpoint service

Report

- User-defined Logo, title description, comments/suggestionn
- On-demand, by-schedule (daily, weekly, monthly) or send immediately
- Flexible report formats: PDF
- Provide multiple cover designs
- Report preview is available
- Smart report summaries
- Flexible time range selection
- MSP Threat Report*2

Event Alert

- Real-time alerts push notifications through Nebula app
- Alert events from Nebula app
- 15+ built-in event definitions; ready for use and highly customizable
- Automated mail alert
- Alert Trend
- Alert History
- Device health anomaly detection (preview)*1

Setting

- Create multi-tenant view
- Set Data Protection Policy, compliance for national general data protection rule
- Dark mode

Log Filtering Search

- Open API for device logs download
- Filter categories by Security, Event, or Traffic
- Specify history time of up to 30 days
- Exports result with CSV file

AI-powered SecuPilot

- Real-time, quick view of data in response to your questions
- Data scope includes device information, security data, traffic logs, and alerts
- Supports the cutting-edge LLM model and over 40 languages
- Customizable Reports: create stunning, tailored reports with various chart options, including bar, column, pie, donut, trend and grid formats

Account Management

Multi-Tenancy

- A unique logical entity structure to serve multiple tenants
- Multiple users with role-based access control

*: ATP/USG FLEX H/USG FLEX series only.
*1: USG FLEX 500H/700H only.
*2: The MSP Threat Report requires the Nebula MSP Pack license; only on-cloud firewalls are supported.

For more product information, visit us on the web at www.zyxel.com

Copyright © 2025 Zyxel and/or its affiliates. All rights reserved.
All specifications are subject to change without notice.