USE CASE BRIEF

AppLogic NETWORKS

Enterprise Network Security

Identify and Eliminate Network Security Threats to Close Security Gaps

KEY BENEFITS

- Creates an additional layer on top of basic device protection offered by OS/applications
- Detects evolving behavior of complex malware through known communication pattern/protocol between devices and abnormal traffic patterns
- Monitors and observes the infectious communication where attacks involve multiple devices
- Perform actions (block) on infected traffic, and can apply rules on in-line traffic upon detection of malicious activity

INTRODUCTION

Cyber threats continue to evolve in sophistication and rise in frequency, making it increasingly challenging for enterprises to protect the network from malicious and organized cyber criminals. Owning large infrastructure and holding highly sensitive data, enterprises are seeing attacks targeting their networks and applications growing in volume and complexity year over year.

The proliferation of smart devices (including IoT), the globalization and cloud migration of business critical applications, and expansive enterprise networks have create more network entry points for cyber-threats to exploit. An enterprise security infrastructure needs to close their security gaps, in particular, account for and eliminate network-based threats.

Firewalls and end-point security are extremely valuable components of an enterprise security portfolio. But these alone do not provide complete security coverage. In a 2023 Poneman Institute report, 68% of organizations reported that a significant attack circumvented their firewall or other defenses. In addition, various studies have suggested that next generation firewalls may not detect anywhere from 30-70% of advanced threats.

Enterprises are highly vulnerable to cyberattacks on their enterprise network. Once threats have penetrated end-point security they become free to roam networks to identify and attack vulnerable assets and data. Visibility into these threats is imperative if organizations want to ensure the highest level of security coverage, reduce their exposure risk, and eliminate the possibility of breaches and hefty fines.

In some cases, cybersecurity teams see some form of possible issues due to anomalous activity, but don't specifically know if this is a real attack nor have any details of the attack. Most security solutions used for identifying and quantifying cyber activity lack the necessary network visibility and contextual awareness, which is arguably the biggest challenge facing security professionals in managing their last security theater – the network.

SOLUTION OVERVIEW

AppLogic Networks Enterprise Network Security solution, part of our Enterprise Solution Portfolio, provides the additional threat detection and elimination coverage that enterprises require to close security gaps. Our Enterprise Network Security solution detects and eliminates threats on your enterprise network and within your network traffic to further expand your security coverage and reduce your risk.

The AppLogic Networks Enterprise Network Security allows enterprises to manage and control the security of their enterprise network with an eye towards three objectives:

- Identifying and eliminating threats before the attackers reach valuable and sensitive assets,
- Delivering deep forensic information that helps an organization put a fingerprint on their attacks, and
- Maintaining a high network QoE for users not directly impacted but suffering due to network resource limitations from the attack

The Enterprise Network Security solution delivers two key components in building actionable cyber threat intelligence: it collects near real-time information from the network, and provides trends and analytics with crucial insights that enable NetOps teams and security specialists to choose the best approach in defining long term strategies. Using AppLogic Networks' real-time data and analytics reporting interfaces, security teams can monitor and analyze malicious traffic, and the sources threatening network users and resources, such as botnet traffic, and active connections related to phishing scams and malware infections.

Positioned in the network protection domain, the Enterprise Network Security solution adds to these enterprise security capabilities the ability to execute real time mitigation policies to block malicious threats, and therefore protect users and data from a range of network threats and malicious traffic that can compromise equipment and data. The Enterprise Network Security solution analyzes and solves security challenges across all devices and systems on the network. The Enterprise Network Security solution works with the Network Optimization solution – both integrated components of the AppLogic Networks' Enterprise portfolio – to identify and act on malicious activity, applying network policies in real time to protect users and networks.

UNIQUE FLOW THREAT IDENTIFICATION

Cyber-threats continue to become more sophisticated and there are now very unique network-based threats. Key specific challenges for enterprises include:

- High-Value Targets: Enterprises are prime targets for attackers, as disruptions impact users, critical business, and infrastructure.
- Scale and Impact of DDoS: DDoS attacks are growing in scale, overwhelming bandwidth and session capacity, directly degrading subscriber experience and network availability.
- IoT Vulnerabilities: With many organizations using IoT devices, many lacking basic security, enterprise with such devices face expanded attack surfaces and limited control over endpoint behavior.
- Perimeter Limitations: Traditional perimeter-based defenses (e.g., firewalls, IDS/IPS) are insufficient in cloud-native, virtualized, and edge-computing environments where threats bypass central chokepoints.
- Lack of Contextual Visibility: Most security tools lack awareness beyond IP addresses, making it difficult to associate threats with specific devices, users, or geolocations for effective mitigation.
- ROI and Deployment Gaps: Demonstrating ROI on security investments is challenging, especially when proactive defenses avoid visible damage. Additionally, most mitigation tools lack agility for on-demand deployment during live attacks.
- Asymmetric Traffic Blind Spots: Asymmetric routing hinders session correlation across sites, limiting threat tracing and analysis.

Through traffic inspection and analysis, Enterprise Network Security can uniquely identify network traffic threats such as:

- Flow masquerading
- Phishing websites and traffic – unsafe web browsing
- Communication and traffic exchanged between infected devices – botnet and C&C
- Spyware and fraud protection
- DDoS attacks
- Malware embedded in encrypted traffic
- Address and Port scanning
- Flow and SYN flooding

KEY CAPABILITIES

Enterprise Network Security is built on AppLogic Networks' industry-leading deep packet inspection (DPI), application identification and traffic analysis to inspect all network traffic regardless of the network scale, and augmenting it with industry-best databases for security-specific categorization of malicious traffic. The use case is further enriched by the industry's most trusted IP geolocation database so that NetOps teams can correlate local users with the source of malicious attacks to feed mitigation decisions.

Traffic Identification and Analysis

AppLogic Networks industry-leading deep packet inspection and traffic identification and analysis technology help track and analyze your network traffic. . For Enterprise Network Security, the analysis identifies abnormal or unidentifiable traffic patterns and match these with the integrated, industry-leading CrowdStrike threat signature database to detect and mitigate threats at network speeds and scale.

AppLogic Networks' application intelligence is powered by a state-of-the-art traffic identification engine. Backed by the most granular and comprehensive signature database, the engine utilizes a finite state machine to minimize false positives and fingerprint guessing. A major reason why threats may sneak past firewalls is their limitations in working with encrypted traffic, which now makes up over 90% of all internet traffic. The AppLogic network intelligence has unmatched low-latency inspection to analyze encrypted application traffic (using obfuscation, TLS, etc.) with a number of different techniques (SNI and Common Name extraction, heuristic analysis, behavioral metrics, ML/AI, ARR).

Threat Detection and Classification

The AppLogic Networks ContentLogic Cyber Security Intelligence (CSI) Database provides a continuously updated stream of high-confidence indicators of compromise (IoC). The solution integrates one of the industry's most trusted threat intelligence providers – CrowdStrike – who was named a leader in Managed Detection and Response (MDR) by Forrester Wave, Q1 2025.

Using the ContentLogic Cyber Security Intelligence Database (CrowdStrike), the solution can detect more than 40 threat types and enrichment with classification metadata for:

- Real-time matching of flow performed against multiple parameters including: URL, hostname, TCP/UDP port, protocol type and subnet,
- Historical usage, measurements, and dimensions, including threat category, devices involved, location, and QoE
- Real-time activity monitoring
- Asymmetric traffic threat detection

Integrated Databases

AppLogic Networks supports multiple 3rd party URL databases through its ContentLogic product, including the CSI database for Cyber Security. The ContentLogic product enables clearly defined categorization of internet sites, which in turn enables sophisticated policy enforcement based on, for example, specific site categories, URLs, threat types, etc.

The following databases are available:

- IFD (Internet Filtering Database)
- CSI/Cyber Security Intelligence
- GeoLogic
- IWF (Internet Watch Foundation)
- IFD Lite
- OTT Microsoft
- DeviceLogic

Cyber Security Intelligence Database - CrowdStrike

The Cyber Security Intelligence (CSI) Database – CrowdStrike – provides a continuously updated stream of high-confidence indicators of compromise (IoC), including IP addresses, URLs, domains, and subnets sourced from one of the industry's most trusted threat intelligence providers. When integrated with an AppLogic, this feed enables:

- Proactive Defense: Enforce IOC-based policies directly in the data path, stopping known threats before they propagate.
- High Performance: Leverages ContentLogic's in-memory matching to ensure low-latency processing, preserving network throughput and service quality.
- Trusted Intelligence: Leverage CrowdStrike's proven reputation and global telemetry to stay ahead of emerging threats.

The database contains Indicators of Compromise (IoC), which defenders use to detect, track, and block known threats in real time or during forensic investigations. Each entry in the CSI databases includes metadata, which provides additional context. Not all fields are populated, but below are a few examples of the top-level categories. The CrowdStrike database is updated every 15 minutes through AppLogic Networks' iFeeds Distribution System.

Malware Classification and Threat Data

The ContentLogic Cyber Security Intelligence (CSI) Database can detected more than 40 threat types and adds additional metadata. Categorization and grouping are available in both use cases, providing visibility to the phases of an adversary attack lifecycle (cyber kill chain, MiTRE Attack) and adapting the responses accordingly. Malware classification includes:

- Malware family
- Malicious confidence
- MITRE and Kill Chain
- Target industries
- Threat actors
- Domain type
- IP address type

The threat metadata includes:

- Actor
- Domain Type
- IP Address Type
- Kill Chain
- Malicious Confidence
- Malware
- MITRE Attack
- Status
- Target
- Threat Type
- Vulnerability

GeoLogic Database Metadata

A GeoLogic database is included with Enterprise Network Security and is updated and distributed through the Intelligence Feeds (iFeeds) product. It's a subscription-based feature for the Enterprise Network Security solution.. GeoLogic adds Geo-IP location properties to each flow, indicating the location (Country, Region, City, Top Level Owner, and Lat/Long) of the remote hosts the subscribers are communicating with. Besides reporting in the dashboards, using Dynamic LiveView, the operator can create real-time views that use these new GeoLogic properties as filtering or distribution criteria to narrow down what traffic is displayed in LiveView surgically.

GeoLogic fields are also supported when creating IPFIX templates or TrafficObjects. Location properties for each flow, indicate the location (i.e., country, region, city, ISP, ASN, and latitude/longitude) of the remote hosts communicating with users (GeoLogic). The GeoLogic database update checks occur every 24 hours using the iFeeds database distribution framework.

Reporting and Visualization

In the AppLogic Networks' solution, security events and related data can be visualized by:

- Integrated purpose-built dashboards: Offers purpose-built dashboards for many of our use cases, including Cyber Threat. For details, see the next section.
- LiveView real-time traffic monitoring: This is the real-time monitoring and search tool in AppLogic Networks products that allows security and operations teams to deep-dive into individual subscriber activities and data connections in real-time.

Security Dashboards

The Enterprise Network Security solution offers a number of different dashboards integrated into Enterprise Insights for network operations and security operations teams to monitor, track, and analyze security threats. This includes the following.

Security Overview

The overview panel presents statistics on detected Low, Medium, and High subscriber threats. A threat location map. The information also includes data related to protected subscribers. Powered by GeoLogic, the threat location map panel displays a global map with threat locations identified by city, region, and country. The map panel allows users to zoom in/out to specific locations to display the total number of threats in a cluster.

The cluster size may differ between locations depending on the number of threats. The map cluster supports a tooltip feature, which displays the total threat count for a single or multiple locations in that cluster. The top threats data grid panel displays information about the current top threats on the network.

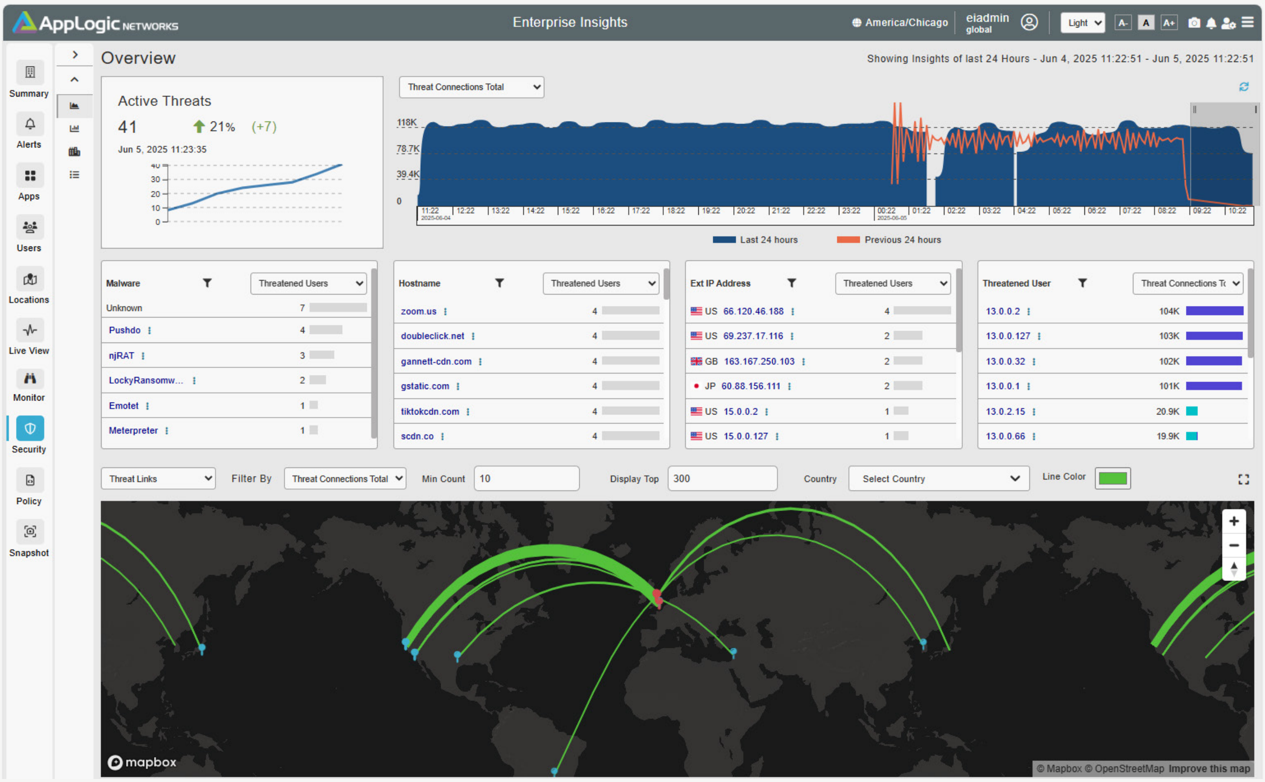
The information includes:

- Threat count
- Malware family
- Threat type
- Device category
- Country
- ISP
- Region
- City
- Confidence level
- Subscriber

The top threat data grid panel can be filtered by single or multiple locations by selecting a cluster on the map pane or by selecting various global filter options.

Figure 1

Security Overview Dashboard



Overview

Showing Insights of last 24 Hours - Jun 4, 2025 11:22:51 - Jun 5, 2025 11:22:51

Active Threats

41 21% (+7)

Jun 5, 2025 11:23:35

Threat Connections Total

Malware	Threatened Users
Unknown	7
Pushdo	4
njRAT	3
LockyRansomw...	2
Emotet	1
Meterpreter	1

Hostname	Threatened Users
zoom.us	4
doubleclick.net	4
gannett-cdn.com	4
gstatic.com	4
tiktokcdn.com	4
scdn.co	4

Ext IP Address	Threatened Users
US 66.120.46.188	4
US 69.237.17.116	2
GB 163.167.250.103	2
JP 60.88.156.111	2
US 15.0.0.2	1
US 15.0.0.127	1

Threatened User	Threat Connections To
13.0.0.2	104K
13.0.0.127	103K
13.0.0.32	102K
13.0.0.1	101K
13.0.2.15	20.9K
13.0.0.66	19.9K

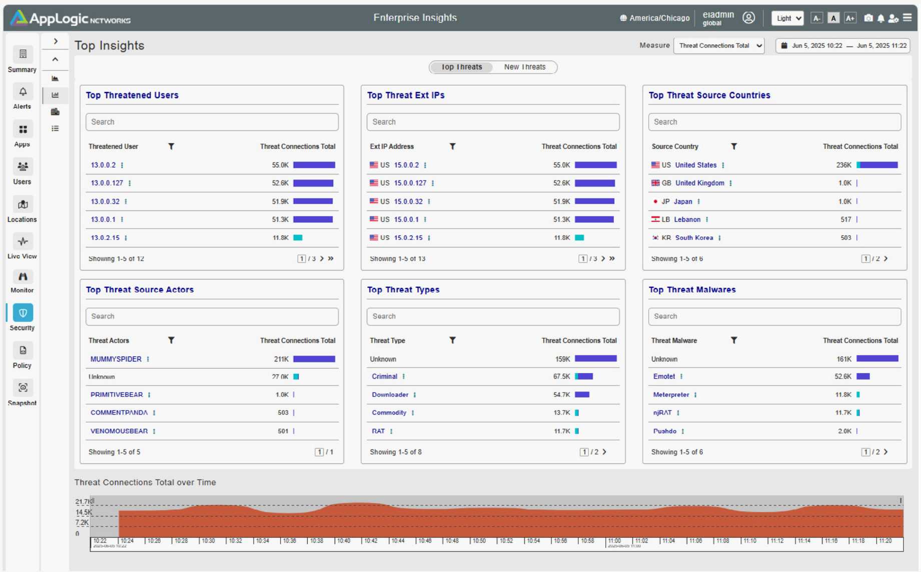
Threat Links Filter By: Threat Connections Total Min Count: 10 Display Top: 300 Country: Select Country Line Color: 🟩

Top Insights Dashboard

The security trends dashboard helps customers to visualize trends of different threat types over a selected time duration and analyze single or multiple threat types over different durations. The user can change network filter, global filters, and time filters, or select filtering capability by access technologies (slice, slice type, device connectivity, and access connectivity)

Figure 2

Security Top Insights Dashboard



Top Insights

Measure: Threat Connections Total | Jun 5, 2025 10:22 — Jun 5, 2025 11:22

Top Threatened Users

Threatened User	Threat Connections Total
13.0.0.2	55.0K
13.0.0.127	52.6K
13.0.0.32	51.9K
13.0.0.1	51.3K
13.0.2.15	11.8K

Showing 1-5 of 12 1 / 3

Top Threat Ext IPs

Ext IP Address	Threat Connections Total
US 15.0.0.2	55.0K
US 15.0.0.127	52.6K
US 15.0.0.32	51.9K
US 15.0.0.1	51.3K
US 15.0.2.15	11.8K

Showing 1-5 of 13 1 / 3

Top Threat Source Countries

Source Country	Threat Connections Total
US United States	236K
GB United Kingdom	1.0K
JP Japan	1.0K
LB Lebanon	517
KR South Korea	503

Showing 1-5 of 6 1 / 2

Top Threat Source Actors

Threat Actors	Threat Connections Total
MUMMYSPIDER	211K
Unknown	27.0K
PRIMITIVEBEAR	1.0K
COMMENTPANDA	503
VENOMOUSBEAR	501

Showing 1-5 of 5 1 / 1

Top Threat Types

Threat Type	Threat Connections Total
Unknown	159K
Criminal	67.5K
Downloader	54.7K
Commodity	13.7K
RAT	11.7K

Showing 1-5 of 8 1 / 2

Top Threat Malwares

Threat Malware	Threat Connections Total
Unknown	161K
Emotet	52.6K
Meterpreter	11.8K
njRAT	11.7K
Pushdo	2.0K

Showing 1-5 of 6 1 / 2

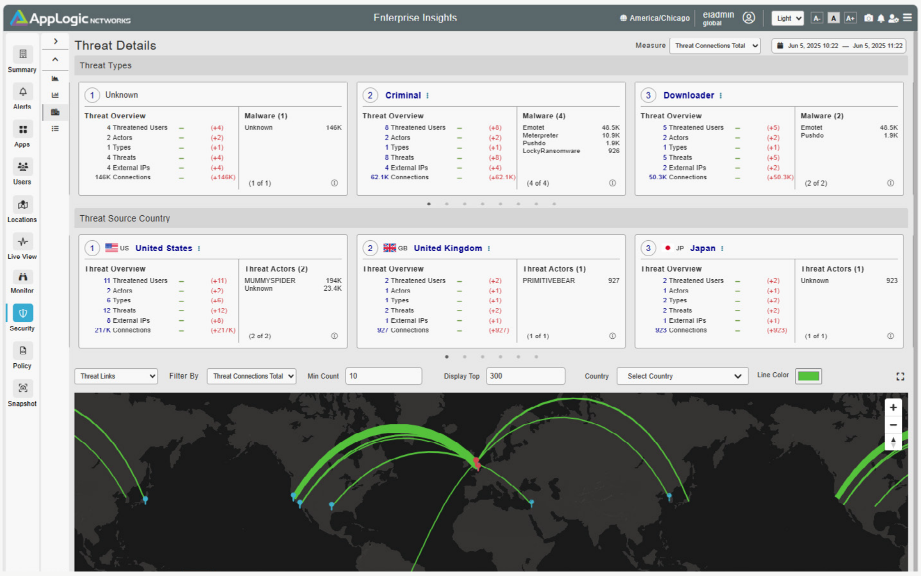
Threat Connections Total over Time

Threat Details Dashboard

The threats details dashboard provides detailed information on threats impacting individual users and trends over a selectable period.

Figure 3

Security Threat Details Dashboard



Threat Details

Measure: Threat Connections Total | Jun 5, 2025 10:22 — Jun 5, 2025 11:22

Threat Types

1 Unknown

Threat Overview			Malware (1)	
4 Threatened Users	–	(+4)	Unknown	146K
2 Actors	–	(+2)		
1 Types	–	(+1)		
4 Threats	–	(+4)		
4 External IPs	–	(+4)		
146K Connections	–	(+146K)	(1 of 1)	

2 Criminal

Threat Overview			Malware (4)	
8 Threatened Users	–	(+8)	Emotet	48.5K
2 Actors	–	(+2)	Meterpreter	10.9K
1 Types	–	(+1)	Pushdo	1.9K
8 Threats	–	(+8)	LockyRansomware	926
4 External IPs	–	(+4)		
62.1K Connections	–	(+62.1K)	(4 of 4)	

3 Downloader

Threat Overview			Malware (2)	
5 Threatened Users	–	(+5)	Emotet	48.5K
2 Actors	–	(+2)	Pushdo	1.9K
1 Types	–	(+1)		
5 Threats	–	(+5)		
2 External IPs	–	(+2)		
50.3K Connections	–	(+50.3K)	(2 of 2)	

Threat Source Country

1 US United States

Threat Overview			Threat Actors (2)	
11 Threatened Users	–	(+11)	MUMMYSPIDER	194K
2 Actors	–	(+2)	Unknown	23.4K
6 Types	–	(+6)		
12 Threats	–	(+12)		
8 External IPs	–	(+8)		
217K Connections	–	(+217K)	(2 of 2)	

2 GB United Kingdom

Threat Overview			Threat Actors (1)	
2 Threatened Users	–	(+2)	PRIMITIVEBEAR	927
1 Actors	–	(+1)		
1 Types	–	(+1)		
2 Threats	–	(+2)		
1 External IPs	–	(+1)		
927 Connections	–	(+927)	(1 of 1)	

3 JP Japan

Threat Overview			Threat Actors (1)	
2 Threatened Users	–	(+2)	Unknown	923
1 Actors	–	(+1)		
2 Types	–	(+2)		
2 Threats	–	(+2)		
1 External IPs	–	(+1)		
923 Connections	–	(+923)	(1 of 1)	

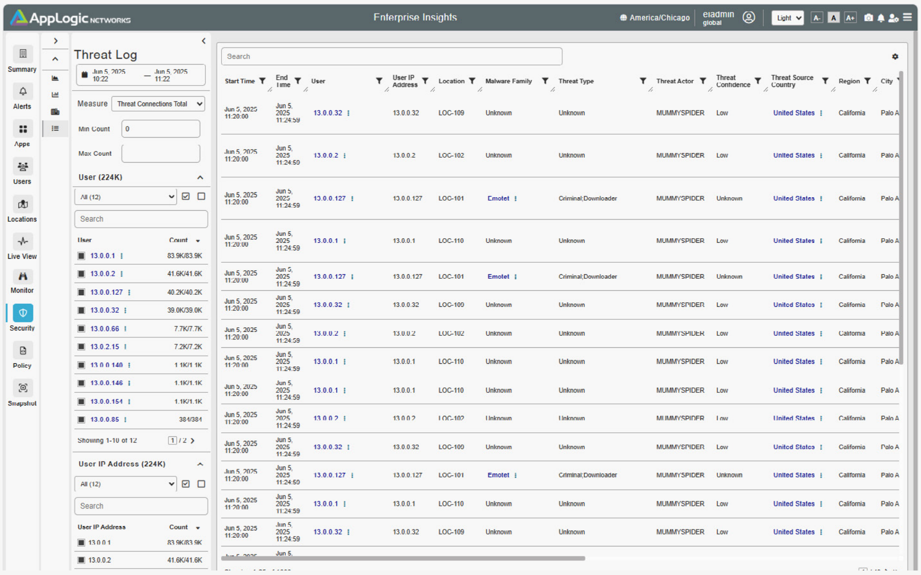
Threat Links | Filter By: Threat Connections Total | Min Count: 10 | Display Top: 300 | Country: Select Country | Line Color: 🟩

Threat Log Dashboard

The threats log dashboard shows log information on all threats detected and provides the ability to filter and search the logs.

Figure 4

Security Threat Log Dashboard



Threat Log

Jun 5, 2025 10:22 — Jun 5, 2025 11:22

Measure: Threat Connections Total

Min Count: 0

Max Count:

User (224K)

All (12) ☑ □

Search

User	Count
13.0.0.1	83.9K/83.9K
13.0.0.2	41.6K/41.6K
13.0.0.127	40.2K/40.2K
13.0.0.32	39.0K/39.0K
13.0.0.66	7.7K/7.7K
13.0.2.15	7.2K/7.2K
13.0.0.140	1.1K/1.1K
13.0.0.146	1.1K/1.1K
13.0.0.154	1.1K/1.1K
13.0.0.85	384/384

Showing 1-10 of 12 1 / 2

User IP Address (224K)

All (12) ☑ □

Search

User IP Address	Count
13.0.0.1	83.9K/83.9K
13.0.0.2	41.6K/41.6K

Search

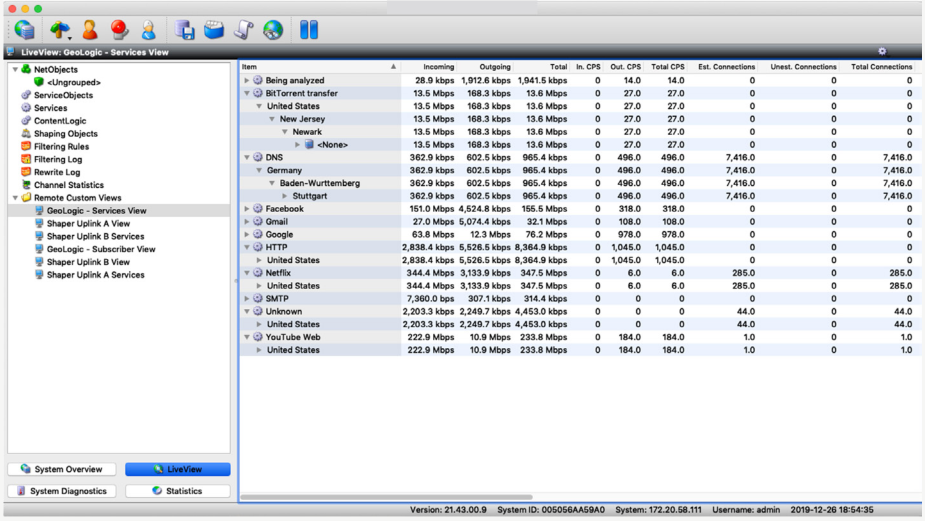
Start Time	End Time	User	User IP Address	Location	Malware Family	Threat Type	Threat Actor	Threat Confidence	Threat Source Country	Region	City
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.32	13.0.0.32	LOC-109	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:50	13.0.0.2	13.0.0.2	LOC-102	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.127	13.0.0.127	LOC-101	Emotet	Criminal;Downloader	MUMMYSPIDER	Unknown	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.1	13.0.0.1	LOC-110	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.127	13.0.0.127	LOC-101	Emotet	Criminal;Downloader	MUMMYSPIDER	Unknown	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.32	13.0.0.32	LOC-109	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.2	13.0.0.2	LOC-102	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.1	13.0.0.1	LOC-110	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.1	13.0.0.1	LOC-110	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.2	13.0.0.2	LOC-102	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.32	13.0.0.32	LOC-109	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:50	13.0.0.127	13.0.0.127	LOC-101	Emotet	Criminal;Downloader	MUMMYSPIDER	Unknown	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.1	13.0.0.1	LOC-110	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A
Jun 5, 2025 11:20:00	Jun 5, 2025 11:24:59	13.0.0.32	13.0.0.32	LOC-109	Unknown	Unknown	MUMMYSPIDER	Low	United States	California	Palo A

LiveView

LiveView helps identify and scrutinize the flows that the network and subscriber protection policies detect as malicious. It delivers real-time information about the network, locations, nodes, and even individual subscribers, making it an enormously powerful tool for diagnostics and troubleshooting. It helps the operations team isolate problems before handing it over to the 2nd line security operations teams for a deeper dive. Various custom views can be created to view active threats and affected subscribers.

Figure 5

Service view by location through LiveView Tool



LiveView: GeoLogic - Services View

- NetObjects
  - <Ungrouped>
- ServiceObjects
- Services
- ContentLogic
- Shaping Objects
- Filtering Rules
- Filtering Log
- Rewrite Log
- Channel Statistics
- Remote Custom Views
  - GeoLogic - Services View
  - Shaper Uplink A View
  - Shaper Uplink B Services
  - GeoLogic - Subscriber View
  - Shaper Uplink B View
  - Shaper Uplink A Services

Item	Incoming	Outgoing	Total	In. CPS	Out. CPS	Total CPS	Est. Connections	Unest. Connections	Total Connections
Being analyzed	28.9 kbps	1,912.6 kbps	1,941.5 kbps	0	14.0	14.0	0	0	0
BitTorrent transfer	13.5 Mbps	168.3 kbps	13.6 Mbps	0	27.0	27.0	0	0	0
United States	13.5 Mbps	168.3 kbps	13.6 Mbps	0	27.0	27.0	0	0	0
New Jersey	13.5 Mbps	168.3 kbps	13.6 Mbps	0	27.0	27.0	0	0	0
Newark	13.5 Mbps	168.3 kbps	13.6 Mbps	0	27.0	27.0	0	0	0
<None>	13.5 Mbps	168.3 kbps	13.6 Mbps	0	27.0	27.0	0	0	0
DNS	362.9 kbps	602.5 kbps	965.4 kbps	0	496.0	496.0	7,416.0	0	7,416.0
Germany	362.9 kbps	602.5 kbps	965.4 kbps	0	496.0	496.0	7,416.0	0	7,416.0
Baden-Wurttemberg	362.9 kbps	602.5 kbps	965.4 kbps	0	496.0	496.0	7,416.0	0	7,416.0
Stuttgart	362.9 kbps	602.5 kbps	965.4 kbps	0	496.0	496.0	7,416.0	0	7,416.0
Facebook	151.0 Mbps	4,524.8 kbps	155.5 Mbps	0	318.0	318.0	0	0	0
Gmail	27.0 Mbps	5,074.4 kbps	32.1 Mbps	0	108.0	108.0	0	0	0
Google	63.8 Mbps	12.3 Mbps	76.2 Mbps	0	978.0	978.0	0	0	0
HTTP	2,838.4 kbps	5,526.5 kbps	8,364.9 kbps	0	1,045.0	1,045.0	0	0	0
United States	2,838.4 kbps	5,526.5 kbps	8,364.9 kbps	0	1,045.0	1,045.0	0	0	0
Netflix	344.4 Mbps	3,133.9 kbps	347.5 Mbps	0	6.0	6.0	285.0	0	285.0
United States	344.4 Mbps	3,133.9 kbps	347.5 Mbps	0	6.0	6.0	285.0	0	285.0
SMTP	7,360.0 bps	307.1 kbps	314.4 kbps	0	0	0	0	0	0
Unknown	2,203.3 kbps	2,249.7 kbps	4,453.0 kbps	0	0	0	44.0	0	44.0
United States	2,203.3 kbps	2,249.7 kbps	4,453.0 kbps	0	0	0	44.0	0	44.0
YouTube Web	222.9 Mbps	10.9 Mbps	233.8 Mbps	0	184.0	184.0	1.0	0	1.0
United States	222.9 Mbps	10.9 Mbps	233.8 Mbps	0	184.0	184.0	1.0	0	1.0

Version: 21.43.00.9 System ID: 005056AA59A0 System: 172.20.58.111 Username: admin 2019-12-26 18:54:35

Enterprise Network Security

Data Export Options

Enterprises can use the Enterprise Network Security data to:

- Creating custom reports, specific to internal requirements, using the BI tool of their choice
- Merge AppLogic Networks data with existing data pools from other sources and correlate between network-centric KPIs with other business and operational KPIs

Flow-based metrics from the dataplane (AL) and Insights dataset from the IDS database can be exported through multiple real-time industry-standard interfaces. AppLogic Networks offers this data with detailed patterns of usage behavior of individual subscribers and a lot more that can be enriched with other contexts like service, application, location, device, etc. AppLogic Networks can export traffic and score datasets that provide the data for many use cases and use case-specific datasets.

AppLogic Networks offers the following data export options:

- Flow records export via Kafka or CSV (directly from dataplane ACTIVELOGIC)
- ODBC access to security data tables in the Insights Database System
- Insights stats data export from IDS via Kafka (processed data from IDS)

CONCLUSION

While firewalls, end-point security, and other tools are very good and essential pieces of an enterprise's security portfolio, these are not enough to provide complete protection from modern cyber-threats. Every organization needs additional network-oriented security tools to complement their security portfolio, fill security gaps, and provide additional protection for network-based threats.

Enterprise Network Security provides the extra level of security coverage enterprise's require and allows organizations to fill their remaining security gaps, all leading to reduced risk of attack and exposure. The unique, best-in-class traffic identification and analysis that can even see inside encrypted traffic, combined with the CrowdStrike threat database, detailed forensics, and easy to use dashboards, makes Enterprise Network Security an essential part of an organization's security strategy.

Enterprise Network Security is an integrated part of AppLogic Networks Enterprise Solution portfolio which also includes Network Observability and Network Optimization solutions to help organizations analyze, optimize, and security their enterprise networks to increase the network Quality of Experience (QoE) and lower their network costs.

ABOUT APPLOGIC NETWORKS

AppLogic Networks' cloud-based App QoE portfolio helps customers deliver high quality, optimized experiences to consumers and enterprises. Customers use our solutions to analyze, optimize, and monetize application experiences using contextual machine learning-based insights and real-time actions. Market-leading classification of more than 95% of traffic across mobile and fixed networks by user, application, device, and location creates uniquely rich, real-time data that significantly enhances interactions between users and applications and drives revenues. For more information visit **https://www.applogicnetworks**.com or follow AppLogic Networks on X **@AppLogic Networks**.

USA
5800 Granite Parkway
Suite 170
Plano, TX 75024
USA

EUROPE
Neptunigatan 1
211 20, Malmö
Skåne
Sweden
T. +46 340.48 38 00

CANADA
410 Albert Street,
Suite 201, Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
Arliga Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333

Copyright ©2025 AppLogic Networks Corporation. All rights reserved. Any unauthorized reproduction prohibited. All other trademarks are the property of their respective owners.

This documentation, including all documentation incorporated by reference herein such as documentation provided or made available on the AppLogic Networks website, are provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by AppLogic Networks Corporation and its affiliated companies ("AppLogic Networks"), and AppLogic Networks assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect AppLogic Networks proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of AppLogic Networks technology in generalized terms. AppLogic Networks reserves the right to periodically change information that is contained in this documentation; however, AppLogic Networks makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

ABOUT APPLOGIC NETWORKS

AppLogic Networks' cloud-based App QoE portfolio helps customers deliver high quality, optimized experiences to consumers and enterprises. Customers use our solutions to analyze, optimize, and monetize application experiences using contextual machine learning-based insights and real-time actions. Market-leading classification of more than 95% of traffic across mobile and fixed networks by user, application, device, and location creates uniquely rich, real-time data that significantly enhances interactions between users and applications and drives revenues. For more information visit **https://www.applogicnetworks**.com or follow AppLogic Networks on X **@AppLogic Networks**.

AppLogic NETWORKS

USA
5800 Granite Parkway
Suite 170
Plano, TX 75024
USA

EUROPE
Neptunigatan 1
211 20, Malmö
Skåne
Sweden
T. +46 340.48 38 00

CANADA
410 Albert Street,
Suite 201, Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
Arliga Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333

Copyright ©2025 AppLogic Networks Corporation. All rights reserved. Any unauthorized reproduction prohibited. All other trademarks are the property of their respective owners.

This documentation, including all documentation incorporated by reference herein such as documentation provided or made available on the AppLogic Networks website, are provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by AppLogic Networks Corporation and its affiliated companies ("AppLogic Networks"), and AppLogic Networks assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect AppLogic Networks proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of AppLogic Networks technology in generalized terms. AppLogic Networks reserves the right to periodically change information that is contained in this documentation; however, AppLogic Networks makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.