USE CASE BRIEF

AppLogic NETWORKS

Cyber Security

Identify and quantify threats to users and network infrastructure

KEY BENEFITS

- Detects infected devices and bad actors early to prevent widespread attacks
- Minimizes operational costs associated with the consequences of cyber attacks
- Provides detailed threat forensics and metadata for classification and deeper analysis
- Blocks infected traffic and applies rules on malicious activity
- Reduces risk of exposure and fines

EXECUTIVE SUMMARY

As cyber threats grow in scale and sophistication, Communications Service Providers (CSPs) face increasing pressure to protect their network and customers, ensure service integrity, and preserve brand trust. Traditional perimeter-based security models are no longer sufficient. The evolving threat landscape – from phishing schemes to malware campaigns – demands a deeper, more contextual understanding of attacks that often originate within the network.

Attackers exploit the anonymity of the Internet and the rapid data exchange facilitated by modern networks. While CSPs have visibility into broad network activity, they often lack granular insight into the “who, what, and where” of malicious traffic, such as which subscriber, device, or location is involved. This lack of context impairs their ability to respond effectively, especially to zero-day and advanced persistent threats that bypass traditional defenses.

Modern cyberattacks do not respect network boundaries. Internal devices can become launchpads for external attacks, and external actors can easily target vulnerable subscribers. In both cases, perimeter protection alone cannot detect or mitigate the full scope of the threat. What’s needed is enhanced visibility into subscriber behavior, geolocation of traffic sources, device profiles, and URL activity, enabling Telcos to shift from reactive to proactive defense.

To maintain a secure and resilient network, CSPs must embrace intelligent, network-native threat detection tools that operate beyond the edge, providing actionable insights across subscriber sessions and traffic flows. Only by combining perimeter defenses with deep, context-aware monitoring can Telcos effectively detect, isolate, and neutralize modern threats while ensuring customer trust and service continuity.

OPERATORS CYBERSECURITY CHALLENGES

Securing modern telecom networks, spanning millions of user devices, is a complex and evolving challenge. Public or private operators face increasing exposure to sophisticated cyber threats, especially as networks become more decentralized and user traffic surges.

Key challenges include:

- High-Value Targets: Public network operators are prime targets for attackers, as disruptions impact subscribers, critical business, and national 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 billions of IoT devices, many lacking basic security, operators 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.
- Unsecured WiFi Exposure: Offloading to public WiFi increases vulnerability, as unsecured networks expose user devices and data to elevated risk.

- **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.

Major Causes of Subscriber Infection

The most common approach for internet security at the subscriber level is through built-in features of major operating systems and/or client-based anti-malware software. Some of the major reasons why subscribers get infected with malicious software and are exposed to threat actors are described below:

- Platforms like iOS and Android are constantly evolving, and new vulnerabilities are discovered every day. New OS updates are constantly published. However, most users do not keep their security software, applications, and operating systems up to date.
- Most operators do not have any control over end-user devices, especially in a BYOD scenario.
- Downloading insecure applications from App stores is one of the major reasons.
- Most OS and client-based security solutions look for specific signatures to detect malware. A new generation of malware now operates in stealth mode and actively protects itself from detection and removal by client-based anti-malware software.
- On-the-go mobile subscribers usually make several network connections during the day, including hard handoffs to public WiFi hotspots. They interact with devices like USBs, laptops, or Bluetooth, or even become WiFi hotspots for other devices. They become highly vulnerable to “man-in-the-middle” attacks from other users or network devices in the operator’s network.
- The current generation of malware trends is more focused on DDoS attacks, making them a more serious problem for network operators and subscribers.
- In fixed home internet setups, children can inadvertently expose themselves and the home network, including family members, to online risks by accidentally downloading malware that could potentially threaten the family’s online activities and the operator.

APPLOGIC NETWORKS SOLUTION OVERVIEW

AppLogic Networks’ Security Solutions enable CSPs to manage and control the security of their network and protect their subscribers. It provides the additional threat detection and mitigation coverage that CSPs need beyond Firewalls to close security gaps. Our security solutions provide both detailed analytics and, for inline deployments, active threat mitigation. The following sections describe our cyber threat analytics and mitigation capabilities.

Cyber Threat Analysis

Cyber Threat Analysis collects near-real-time information from the network, provides trending and analytics with crucial insights, and enables network operators and security specialists to choose the best approach to defining long-term strategies.

Using AppLogic Networks’ real-time data and analytics reporting interfaces, security teams can monitor and analyze malicious traffic and sources threatening network users and resources, such as botnet traffic, and active connections related to phishing scams and malware infections.

The solution is built on AppLogic Networks’ industry-leading application identification. It inspects all network traffic regardless of the network scale and augments it with a third-party database (CrowdStrike) for security-specific categorization of malicious traffic. Further enriched by the industry’s most trusted IP geolocation database, network operators 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, traffic identification, and analysis technology help track and analyze your network traffic. The analysis identifies abnormal or unidentifiable traffic patterns and matches these with the integrated, industry-leading CrowdStrike threat signature database to detect threats at 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

Malware Classification

Categorization and grouping provide visibility to the phases of an adversary attack's lifecycle (cyber kill chain, MiTRE ATTACK) and allow the response to be adapted accordingly.

Cyber Threat metadata available includes:

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

The location properties of each flow indicate the location (i.e., country, region, city, ISP, and latitude/longitude) of the remote hosts communicating with users (via GeoLogic Database). BGP ASN can be added if the customer optionally peers with BGP.

Cyber Threat Management

Cyber Threat Management protects subscribers from network threats and malicious traffic that can compromise equipment and data.

Cyber Threat Management is the answer to analyzing and solving security challenges in fixed, mobile, and satellite network operators' environments via AppLogic Networks' active network intelligence solution. It offers the capability to automatically act on identified threats and apply network policies in real time to protect the network and individual subscribers.

Cyber Security

Cyber Threat Management builds upon the Cyber Threat Analysis capabilities and adds the following:

- 'Filtering license' that enables rules to be created and applied to data traffic.
- Additional stats added to the dashboard indicate the number of threats subscribers were protected against (threats blocked) and actions applied.
- Address Scanning – Detects horizontal scanning activity aimed at enumerating live or vulnerable IP addresses within the network.
- Port Scanning – Identifies vertical reconnaissance attempts that probe a host for open or exploitable ports.
- Flow Flooding – Mitigates volumetric attacks that generate excessive connection attempts to saturate network devices or services.
- SYN Flooding – Protects against TCP-based denial-of-service attacks that exploit the handshake mechanism to deplete system resources.

By integrating behavioral threat detection directly into the data path, Network Operators can proactively secure their networks and maintain high-performance service delivery without overreliance on edge firewalls or external security appliances.

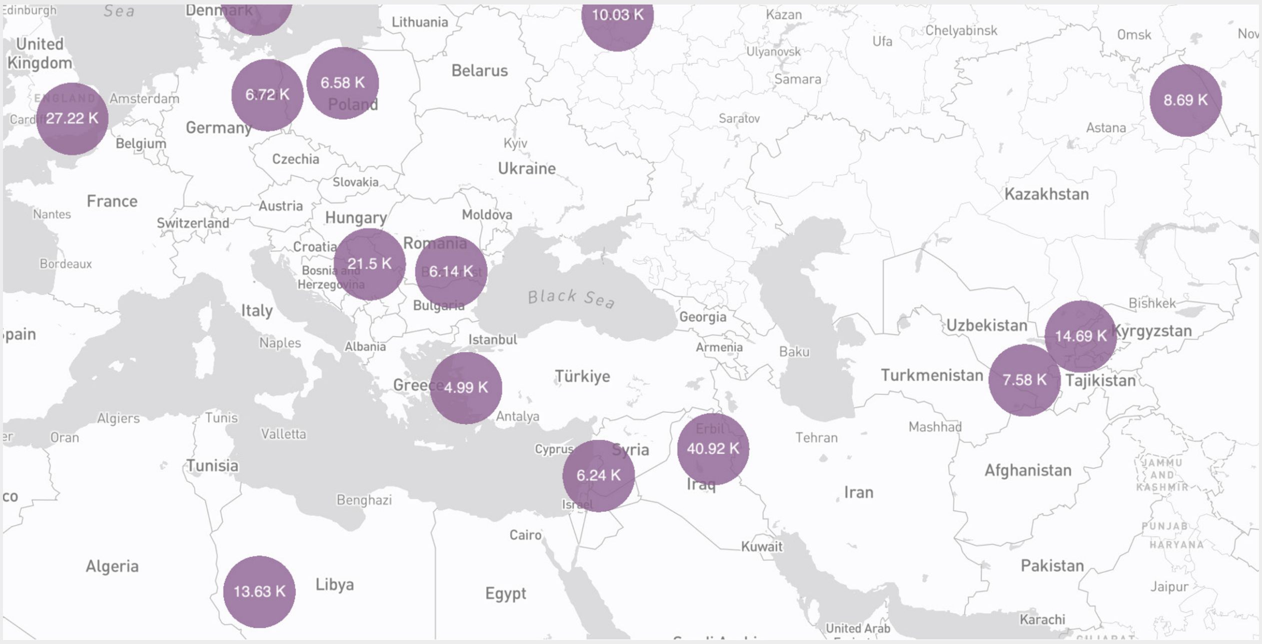
IP Geolocation and Cyber Security

A GeoLogic database is included with the Cyber Security Solutions and is updated and distributed through the Intelligence Feeds (iFeeds) product. 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.

Identifying the source of an attack with complete information on the country, region, ISP, ASN, longitude/latitude coordinates, etc, of the attacker(s) is often the decisive point in any major cybersecurity mitigation operation. With the help of IP geolocation technology, cybersecurity professionals like threat hunters and incident response specialists can objectively track and act on bad actors to prevent and stop the ongoing and future threats.

Figure 1

Distribution of cyber threats by attack origins, displayed geographically



Data Reporting and Visualization

Cyber Security and Cyber Threat stats are visualized from the rich data collected by ActiveLogic and stored within Insights Data Storage. Operators can see actions preceding the attacks, what happened in the network during the attack, where the attacks are coming from, and how policy changes were able to mitigate the impact of the attack traffic. They can then measure the impact of malicious traffic on QoE and detail which devices were involved or impacted by the attack. This intelligence is critical to detecting the correct mitigation strategy and selecting the most surgical policies.

In AppLogic Networks platforms, security related data is visualized or exported via the following interfaces and tools:

- **Purpose-Built Dashboards:** Ready-made dashboards that provide critical information for Cyber security teams. See the next section for details.
- **Custom Reports:** Depending on their requirements, CSPs can create their own custom reports or perform custom data analysis via AppLogic Networks' custom reporting capabilities or via third-party visualization and reporting tools. Insights Data Storage provides standards-based ODBC to access the underlying data stored. In this manner, AppLogic Networks provides ultimate flexibility in leveraging the value of the underlying data from the network.
- **LiveView real-time traffic monitoring:** Allows security and operations teams to deep-dive into individual subscriber activities and data connections in real-time. It 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.

SECURITY DASHBOARDS

AppLogic Networks' Security solutions includes purpose-built dashboards for network operations and security operations teams to monitor, track, and analyze security threats. This includes the following:

Security Overview Dashboard

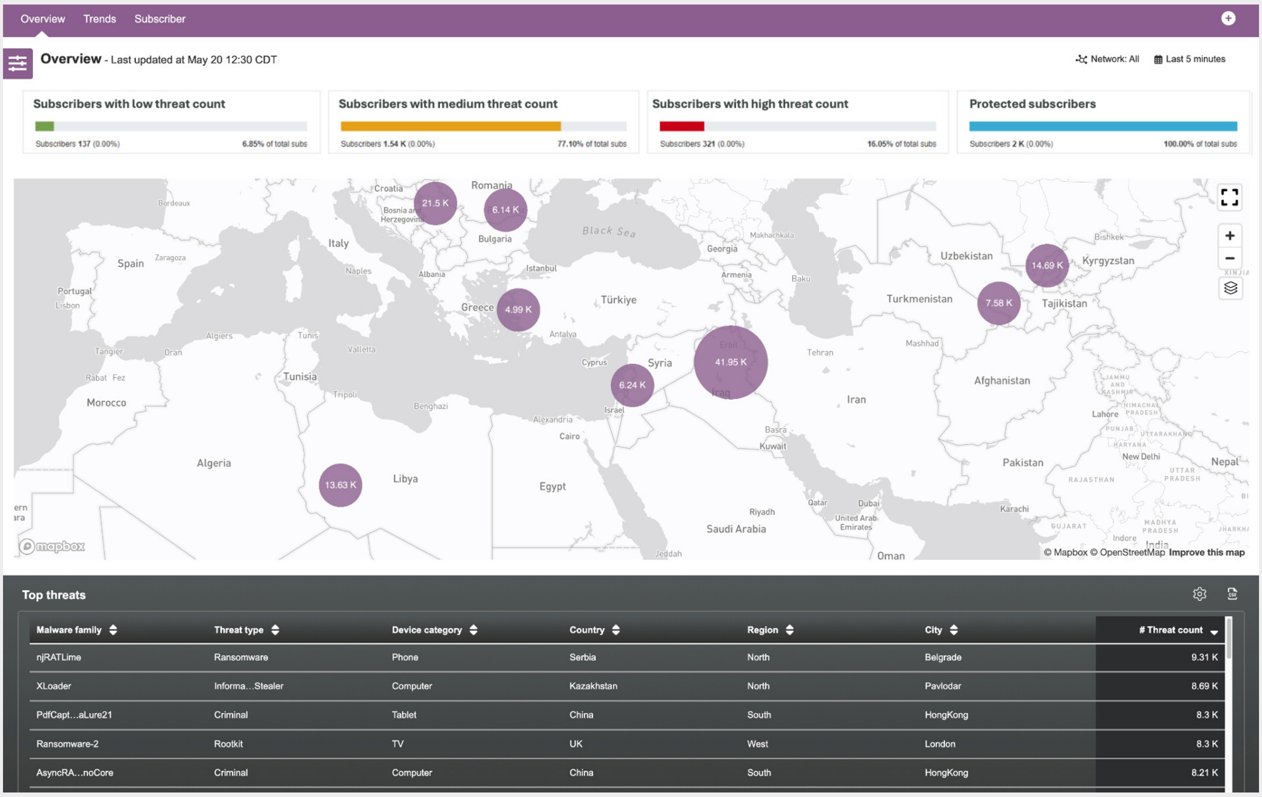
The overview panel presents statistics on detected low, medium, and high subscriber threats, protected subscribers, a threat location map, and a sortable table listing the threats.

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.

Cyber Security

Figure 2

Security Overview Dashboard



Overview - Last updated at May 20 12:30 CDT

Subscribers with low threat count	Subscribers with medium threat count	Subscribers with high threat count	Protected subscribers
Subscribers 137 (0.00%) 6.85% of total subs	Subscribers 1.54 K (0.00%) 77.10% of total subs	Subscribers 321 (0.00%) 16.05% of total subs	Subscribers 2 K (0.00%) 100.00% of total subs

Top threats

Malware family	Threat type	Device category	Country	Region	City	# Threat count
njRATLime	Ransomware	Phone	Serbia	North	Belgrade	9.31 K
XLoader	Informa…Stealer	Computer	Kazakhstan	North	Pavlodar	8.69 K
PdfCapt…aLure21	Criminal	Tablet	China	South	HongKong	8.3 K
Ransomware-2	Rootkit	TV	UK	West	London	8.3 K
AsyncRA…noCore	Criminal	Computer	China	South	HongKong	8.21 K

The top threats data grid panel displays information about the current threats on the network. By default it is it sorted by threat count. The user can click any column to sort the data, select additional information to display via the gear icon, or download a CSV file with the list of threats. The information enables operators to monitor malicious network traffic and activities in near real-time and, as a result, protect their subscribers from a range of prevailing network threats.

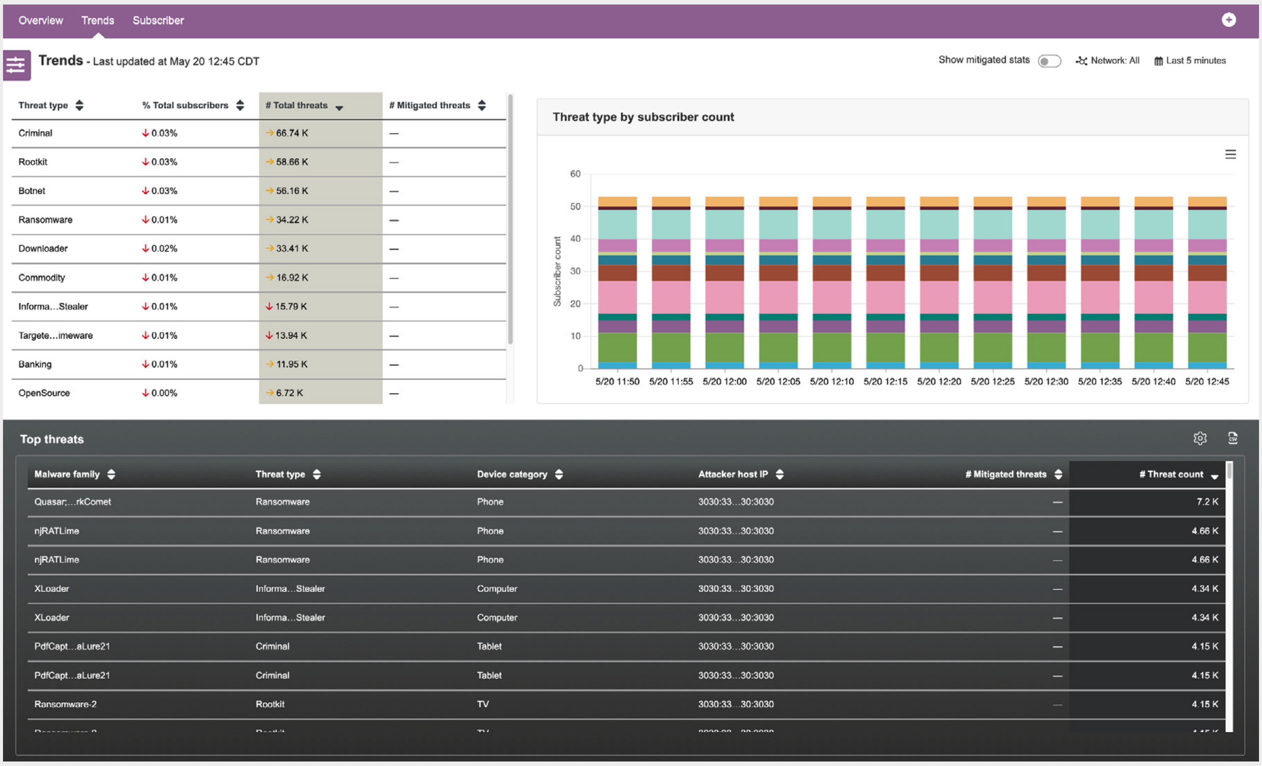
Trends Dashboard

This dashboard helps customers 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)

Cyber Security

Figure 3

Trends Dashboard



Trends - Last updated at May 20 12:45 CDT

Threat type	% Total subscribers	# Total threats	# Mitigated threats
Criminal	↓ 0.03%	→ 66.74 K	—
Rootkit	↓ 0.03%	→ 58.66 K	—
Botnet	↓ 0.03%	→ 56.16 K	—
Ransomware	↓ 0.01%	→ 34.22 K	—
Downloader	↓ 0.02%	→ 33.41 K	—
Commodity	↓ 0.01%	→ 16.92 K	—
Informa…Stealer	↓ 0.01%	↓ 15.79 K	—
Targete…imeware	↓ 0.01%	↓ 13.94 K	—
Banking	↓ 0.01%	→ 11.95 K	—
OpenSource	↓ 0.00%	→ 6.72 K	—

Top threats

Malware family	Threat type	Device category	Attacker host IP	# Mitigated threats	# Threat count
Quasar;…rkComet	Ransomware	Phone	3030:33…30:3030	—	7.2 K
njRATLime	Ransomware	Phone	3030:33…30:3030	—	4.66 K
njRATLime	Ransomware	Phone	3030:33…30:3030	—	4.66 K
XLoader	Informa…Stealer	Computer	3030:33…30:3030	—	4.34 K
XLoader	Informa…Stealer	Computer	3030:33…30:3030	—	4.34 K
PdfCapt…aLure21	Criminal	Tablet	3030:33…30:3030	—	4.15 K
PdfCapt…aLure21	Criminal	Tablet	3030:33…30:3030	—	4.15 K
Ransomware-2	Rootkit	TV	3030:33…30:3030	—	4.15 K

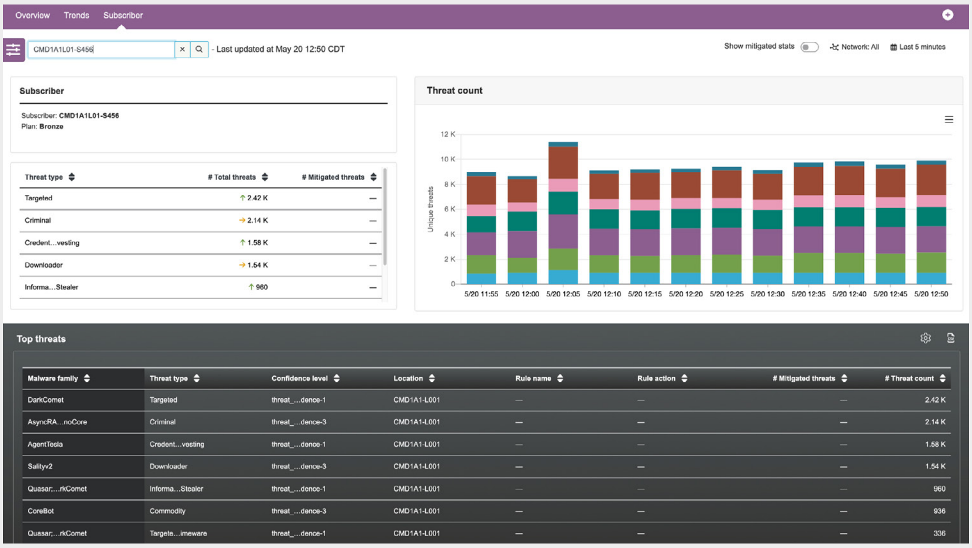
For inline deployments that include Cyber Threat Management capabilities, a supplementary field provides users with information on the number of mitigated threats. The dashboard shows the overall established inbound, outbound, and total number of connections.

Subscriber Dashboard

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

Figure 4

Subscriber Dashboard



CMD1A1L01-S456 - Last updated at May 20 12:50 CDT

Subscriber

Subscriber: **CMD1A1L01-S456**
Plan: **Bronze**

Threat type	# Total threats	# Mitigated threats
Targeted	↑ 2.42 K	—
Criminal	→ 2.14 K	—
Credent…vesting	↑ 1.58 K	—
Downloader	→ 1.54 K	—
Informa…Stealer	↑ 960	—

Top threats

Malware family	Threat type	Confidence level	Location	Rule name	Rule action	# Mitigated threats	# Threat count
DarkComet	Targeted	threat_…dence-1	CMD1A1-L001	—	—	—	2.42 K
AsyncRA…noCore	Criminal	threat_…dence-3	CMD1A1-L001	—	—	—	2.14 K
AgentTesla	Credent…vesting	threat_…dence-1	CMD1A1-L001	—	—	—	1.58 K
Salityv2	Downloader	threat_…dence-3	CMD1A1-L001	—	—	—	1.54 K
Quasar;…rkComet	Informa…Stealer	threat_…dence-1	CMD1A1-L001	—	—	—	960
CoreBot	Commodity	threat_…dence-3	CMD1A1-L001	—	—	—	936
Quasar;…rkComet	Targete…imeware	threat_…dence-1	CMD1A1-L001	—	—	—	336

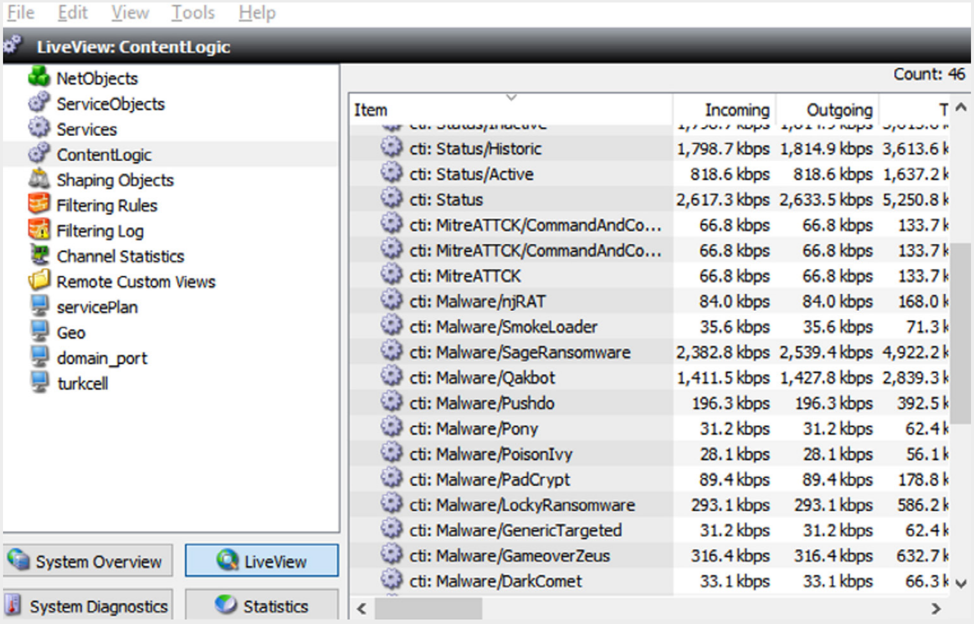
Cyber Security

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

LiveView Tool



Count: 46

Item	Incoming	Outgoing	T
cti: Status/Inactive	[illegible]	[illegible]	[illegible]
cti: Status/Historic	1,798.7 kbps	1,814.9 kbps	3,613.6 k
cti: Status/Active	818.6 kbps	818.6 kbps	1,637.2 k
cti: Status	2,617.3 kbps	2,633.5 kbps	5,250.8 k
cti: MitreATTCK/CommandAndCo…	66.8 kbps	66.8 kbps	133.7 k
cti: MitreATTCK/CommandAndCo…	66.8 kbps	66.8 kbps	133.7 k
cti: MitreATTCK	66.8 kbps	66.8 kbps	133.7 k
cti: Malware/njRAT	84.0 kbps	84.0 kbps	168.0 k
cti: Malware/SmokeLoader	35.6 kbps	35.6 kbps	71.3 k
cti: Malware/SageRansomware	2,382.8 kbps	2,539.4 kbps	4,922.2 k
cti: Malware/Qakbot	1,411.5 kbps	1,427.8 kbps	2,839.3 k
cti: Malware/Pushdo	196.3 kbps	196.3 kbps	392.5 k
cti: Malware/Pony	31.2 kbps	31.2 kbps	62.4 k
cti: Malware/PoisonIvy	28.1 kbps	28.1 kbps	56.1 k
cti: Malware/PadCrypt	89.4 kbps	89.4 kbps	178.8 k
cti: Malware/LockyRansomware	293.1 kbps	293.1 kbps	586.2 k
cti: Malware/GenericTargeted	31.2 kbps	31.2 kbps	62.4 k
cti: Malware/GameoverZeus	316.4 kbps	316.4 kbps	632.7 k
cti: Malware/DarkComet	33.1 kbps	33.1 kbps	66.3 k

Data Export Options

Operators worldwide regularly leverage big data analytics for their security events, log management, and analytics, which helps them on the operational and strategic fronts, and this practice is only accelerating. Big data activities provide security managers with better threat information on their networks. These operators use data export for many reasons to big data systems:

- 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
- Experiment with data visualizations (e.g., MicroStrategy reports)

Flow-based metrics from the dataplane (AL) and Insights dataset from the IDS database can be exported to operators' big data systems 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 ANI use cases and use case-specific datasets.

AppLogic Networks offers the following ANI-based data export options:

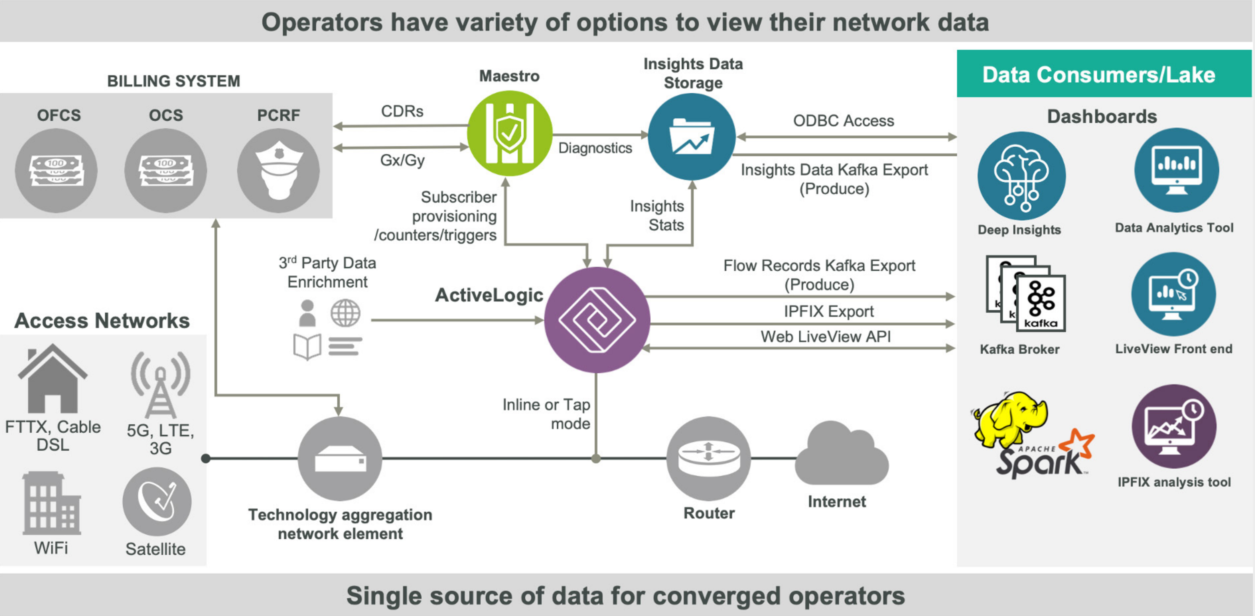
1. Flow records export via Kafka or CSV (directly from dataplane ACTIVELOGIC)
2. ODBC access to Insights Vertica DB (access to traffic/score and use case-specific schema/tables)
3. Insights stats data export from IDS via Kafka (processed data from IDS)

The diagram on the following page shows the system architecture and export options.

Cyber Security

Figure 6

System architecture and export options



CONCLUSION

While firewalls are an essential component of a CSP's security architecture, firewalls are not sufficient to protect your customers and your network from modern cyber-threats. Every CSP needs additional security tools to fill security gaps and provide the protection your customers expect.

AppLogic Networks' Security solutions provide the extra level of threat protection needed to plug security gaps, reducing your risk of attack and legal exposure. Best-in-class traffic identification and analysis (that can even monitor encrypted traffic), combined with the CrowdStrike threat database, detailed forensics, and easy to use dashboards, makes AppLogic Networks' Security solutions an essential part of every CSP's security strategy. AppLogic Networks' Security solutions are an integrated part of AppLogic Networks' Telco portfolio which includes Network Analytics, Optimization, and Monetization capabilities.

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.applogic**networks.com.

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

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.