



KEY BENEFITS

- Increased security threat detection coverage and elimination
- Reduced risk of exposure and fines by identifying and eliminating additional threats embedded in network traffic
- Eliminate threats before they reach sensitive information by identifying these earlier in encrypted network traffic
- Detailed threat forensics and metadata for classification and deeper analysis

Enterprises are (and have always been) targets of choice for cyber criminals and they will continue to be for a long time. 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.

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

ENTERPRISE NETWORK SECURITY

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.

AppLogic Networks industry-leading deep packet inspection and traffic identification and analysis technology scrutinize your network traffic to identify abnormal 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).

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

- Flow masquerading
- DDoS attacks
- Malware embedded in encrypted traffic
- Address and Port scanning
- Flow and SYN flooding

The AppLogic Networks ContentLogic Cyber Threat Intelligence (CTI) Database provides a continuously updated stream of high-confidence Indicators of Compromise (IoC), sourced from 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.

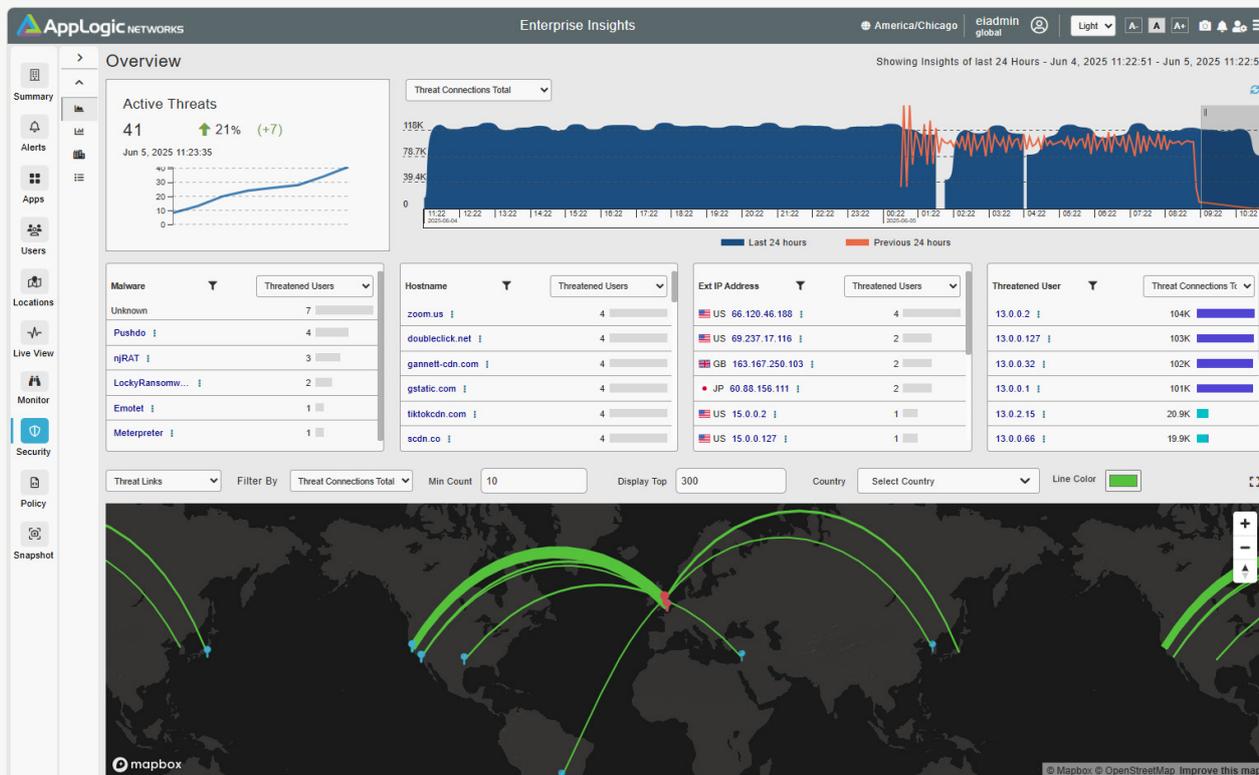
When integrated with AppLogic technology, this feed enables:

- **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.

Enterprise Network Security also provides detailed forensic metadata to help enterprises report and track malicious threats. All of this information on threats and the forensic data are stored in our Insights Data Storage and surfaced in rich dashboards with Enterprise Insights.

Figure 1

Enterprise Security Insights Overview Dashboard



CONCLUSION

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.

KEY CAPABILITIES

FUNCTIONAL AREA	KEY CAPABILITIES
OVERALL	<ul style="list-style-type: none"> • Highly efficient low-latency Deep Packet Inspection (DPI) that works with encrypted and non-encrypted traffic • Industry-leading traffic identification and analysis • Integrated industry-best • Real-time flow matching across multiple Indicator of Compromise (IoC) parameters: URL, hostname, TCP/UDP port, protocol type, subnet • Real-time threat activity monitoring and analysis • Asymmetric threat detection • LiveView real-time traffic monitoring
ANALYTICS & VISUALIZATION	<ul style="list-style-type: none"> • Historical usage, measurements, and dimensions, including threat category, devices involved, and location • Multiple threat dashboards including: <ul style="list-style-type: none"> • Threat location map • Top Threats • Threat trends • User dashboard • Kafka data integration • Security data export
UNIQUE THREAT DETECTION	<ul style="list-style-type: none"> • Flow masquerading • DDoS attacks • Malware embedded in encrypted traffic • Address and Port scanning • Flow and SYN flooding
MALWARE CLASSIFICATION	<p>Cyber-threat metadata:</p> <ul style="list-style-type: none"> • Malware family • Malicious confidence • MITRE and Kill Chain • Target industries • Threat actors • Domain type • IP address type
THREAT METADATA	<ul style="list-style-type: none"> • Actor • Domain Type • IP Address Type • Kill Chain • Malicious Confidence • Malware • MITRE Attack • Status • Target • Threat Type • Vulnerability
THREAT TYPES	<ul style="list-style-type: none"> • 40+ threat types (Adware, Backdoor, Botnet, Click Fraud DDoS, Extortion, Key Logger, Malicious Script, Proxy Malware, etc.)

DEPLOYMENT WITH SIE

AppLogic Networks' Enterprise packages are deployed using AppLogic Networks Simplified Installation Engine (SIE) on customer provided commercially available servers from Dell Technologies™. SIE is a state-of-the-art deployment and management tool that is simple, intuitive, and incredibly efficient. It is a one-click install, fully automated system that allows for installation, configuration, and auto testing. It is based on pre-packaged solutions that include the optimal configuration of AppLogic Networks products for a given set of use cases and features. SIE allows customer to deploy with flexibility, utilizing fully customizable Dell portfolio parts, accessories, and refitting possibilities.

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.