AppLogic NETWORKS

Cyber Security

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.

AppLogic Networks' Cyber Security solutions enable CSPs to monitor malicious network traffic and activities in near real-time and, as a result, protect their network and subscribers from a wide range of threats. The solutions provide additional threat detection and mitigation coverage needed beyond Firewalls to close security gaps.

KEY CAPABILITIES

AppLogic Networks' Cyber Security solutions deliver powerful analytics and mitigation tools to address network threats.

FUNCTIONAL AREA	KEY CAPABILITIES
OVERALL	Highly efficient low-latency Deep Packet Inspection (DPI) that works with encrypted and non-encrypted traffic • Industry-leading traffic identification and analysis • Integrated with multiple use cases • 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	• Historical usage, measurements, and dimensions, including threat category, devices involved, and location • Multiple threat dashboards including: • Threat location map • Top Threats • Threat trends • Subscriber dashboard • Kafka data integration • Security data export
UNIQUE THREAT DETECTION	• Flow masquerading • DDoS attacks • Malware embedded in encrypted traffic • Address and Port scanning • Flow and SYN flooding
MALWARE CLASSIFICATION	Cyber-threat metadata: • Malware family • Malicious confidence • MITRE and Kill Chain • Target industries • Threat actors • Domain type • IP address type

THREAT METADATA	• Actor • Domain Type • IP Address Type • Kill Chain • Malicious Confidence • Malware • MITRE Attack • Status • Target • Threat Type • Vulnerability
THREAT TYPES	40+ threat types (Adware, Backdoor, Botnet, Click Fraud DDoS, Extortion, Key Logger, Malicious Script, Proxy Malware, etc.)

HOW CYBER SECURITY IS PACKAGED

For ANI customers, Cyber Threat Analysis (CTA) and Cyber Threat Management (CTM) are sold as two different use cases.

For App QoE customers, the two use cases (CTA and CTM) are sold as one, under the name Cyber Security.

REQUIRED SOLUTION COMPONENTS

- ActiveLogic
- Cyber Security Intelligence (CSI) database
- Geologic Database
- Insights Data Storage
- Deep Insights
- Maestro – for threat mitigation
- Maestro Security Engine – for threat mitigation

DEPLOYMENT

For Threat Analytics only, ActiveLogic can be deployed either inline or offline. For Threat Mitigation, ActiveLogic must be deployed inline.

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