Datasheet

Blue Hexagon for Network

Network Threat Protection Harnessing the Power of Deep Learning

Keeping Up with the Threat Tsunami

Here's the reality of the threat landscape today: More than 300,000 malware variants are produced each day. That's 231 new malware per minute, 4 every single second.[1]

When malicious, morphing malware is unleashed at that scale, traditional defenses are quickly overwhelmed. In fact, signature-based defenses cannot keep up with the speed and variants of new threats. Malware sandboxes have limitations with speed of analysis and file sizes, and are subject to evasion tactics.

A new approach to cybersecurity is needed to address the threat landscape of automated attacks:

- Threat detection must be at the speed malware is unleashed – in subseconds, not days, hours or minutes.
- Harnessing deep learning will deliver the speed and efficacy needed. Deep learning is the most advanced subfield of machine learning and AI, where artificial neural networks learn from large amounts of data. Neural networks trained with the massive threat data that exists today, can intelligently learn and make decisions on whether traffic is malicious.
- The best place to do this is closest to the source of attack – the network – to stop the threat as soon as possible and to prevent lateral movement deeper in the network.

Blue Hexagon's **Real-time Deep Learning** platform is proven in actual customer deployments to detect network threats at a *speed, efficacy,* and *coverage* that set a new standard for cyber defense.

Network Threat Protection Powered by Deep Learning

Blue Hexagon has built the industry's **FIRST** real-time deep learning platform for network threat protection. Built by a team with decades of machine learning and deep learning expertise, the Blue Hexagon proprietary neural network architecture is designed for speed and efficacy. Blue Hexagon detects known and unknown threats in **less than a second** at nearly **100% efficacy** and **10G wire speed** performance. The platform works out-of-the-box and requires no baselining. **Prevention** can be enabled via orchestrated enforcement to endpoints, firewalls and web proxies, to block malicious traffic at the network or application.

According to the Verizon Data Breach Report 2018, "in 87% of breaches, compromise occurs within 87 seconds". Only Blue Hexagon can address the speed of compromise – stopping the very first victim in the organization from being infected and preventing an attack from spreading. This can translate to tangible savings and efficiencies in the following – remediation costs, SOC analyst investigation efforts, data breach disclosure fines, infected machine clean-up operations.

Industry's First Real-time Deep Learning Platform

Detect threats in less than a second

Detect known and unknown threats, even zero days seen for the first time, in less than a second. Payloads and headers are inspected

Works out of the box on day one

Completely automated with pre-trained AI models, requires no baselining, and has no "learning delays"

Proven efficacy in real-world deployments

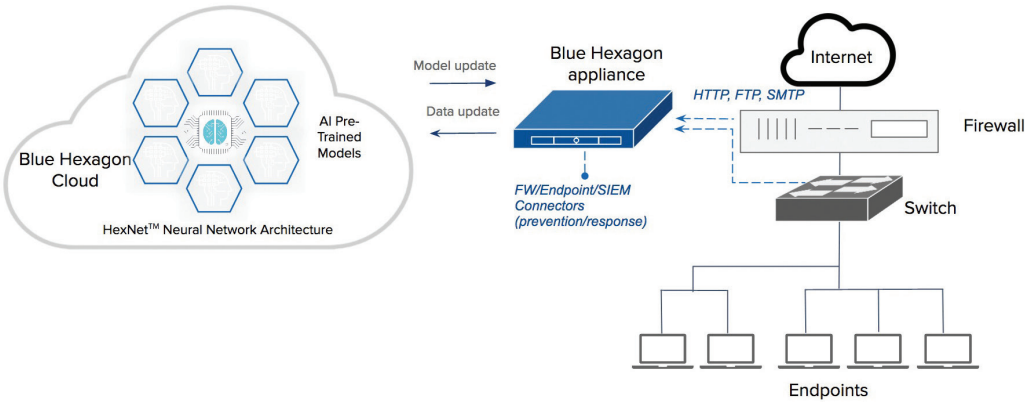
Unmatched detection rates and low false positives compared to sandbox and signature-based detection

Integrates with existing security solutions

Orchestrate prevention to existing security products – endpoints, firewalls and network proxies

[1] *AV-Test GmbH - "How AI Can Help Stop Cyberattacks", Wall Street Journal*

Real-time Deep Learning for Network Threat Protection



The Blue Hexagon deep learning platform consists of the Blue Hexagon Cloud and on-premises Appliances. The Blue Hexagon Cloud is where the proprietary HexNet™ architecture of deep learning models are optimized and trained. These models are then delivered locally on Blue Hexagon Appliances that can be in physical or virtual form factors. The appliances are installed at the ingress of the network in network tap mode to inspect the complete network traffic flow; payloads and headers are inspected. Installation takes minutes and threat detection works out of the box immediately without requiring any baselining. Prevention can be enabled on endpoints, firewalls or web proxies.

Features:

Architecture Optimized for Efficacy - The HexNet™ architecture has been designed to detect threats in less than a second. The proprietary architecture of neural networks works seamlessly to deliver threat verdicts.

AI-Curated Threat Data for Training - The same deep learning techniques used by Blue Hexagon for threat detection are also applied to the massive amount of threat data that is used for training.

Real-time Deep Learning Inspection for Payload and Headers - Inspection of the complete network flows delivers higher efficacy and perspective on mal-intent. Deep learning inspection is performed payloads and network headers (including C2 communications and URLs) in less than a second.

- Protocols: HTTP, FTP, SMTP, DNS
- Cross-platform threat detection: Windows, Linux, Mac, BSD, Android
- Detection of malware in various file types: EXE, PDF, MS Office, DLL, Adobe Flash, Java Script, VBS
- Detection of malicious documents with exploit-based scripts: VBA, VB Script, encoded VB Script
- Detection of threats in archive files: ZIP, 7z, RAR and SFX

Real-time Classification - Every threat detected is automatically classified by the HexNet™ neural networks in real-time. Threat family information and indicators of compromise are provided for deeper analysis by security teams.

Dashboard and Kill Chain Visualizer - Security teams receive access to a dashboard in the cloud with threat details, including complete kill chain visibility into infected systems and hosts such as communication between systems/hosts, and external communications to malicious domains.

Global Threat Cloud - Blue Hexagon incorporates deep learning to classify threats from various intelligence sources. This data is shared with all customers to deliver predictive intelligence into the types of attacks that are targeting specific industries.

Automated and Orchestrated Prevention - Enterprises can orchestrate prevention to endpoints, firewalls and network proxies. Syslog integration into SIEMs is also supported.

Blue Hexagon Labs - Every customer deployment benefits from the elite deep learning and cybersecurity experts within Blue Hexagon. The team provides analysis of industry and company specific attacks to customers.

Hardware Specifications:

Specifications	Performance	Size	Interface
Blue Hexagon 10G Appliance	10G	1 RU	2x10 GB SFP+ (fiber) 2x1 GB RJ45
Blue Hexagon 1G Appliance	1G	1 RU	4x1 GB
Blue Hexagon VM Appliance	1G	Requires 16 cores, 32 GB RAM running VMWare ESXi 6.5 or later	

Blue Hexagon is a deep learning innovator focused on protecting organizations from cyberthreats. The company's real-time deep learning platform is proven to detect known and unknown network threats with speed, efficacy, and coverage that set a new standard for cyber defense. Blue Hexagon is headquartered in Sunnyvale, CA, and backed by Benchmark and Altimeter Capital. For more information, visit www.bluehexagon.ai or follow @bluehexagonai.

Headquarters
298 S. Sunnyvale Avenue, Suite 205
Sunnyvale, CA 94086
www.bluehexagon.ai
inquiries@bluehexagon.ai

BLUEHEXAGON