Solution Brief

Extending Human Capacity

AI Driven Cyber Defense by BlueVoyant

The only end-to-end, inside-out threat detection and remediation solution built with AI at its core.

Artificial intelligence (AI) is changing the way businesses operate, but the same can be said of threat actors. While businesses incorporate AI in their products or implement AI-based tools to facilitate workflow, threat actors can also make use of certain AI tools to increase the scope and volume of their attacks.

Between deepfake impersonations, optimizing malware code, AI-supported credential stuffing, and automated website cloning, the threat of AI-supported cyberattacks is clear.

The types of attacks organizations face largely remain the same, but the volume of those attacks can increase exponentially when aided by AI programs – which means an even greater burden on security teams

AI isn't new – BlueVoyant has been leveraging AI and machine learning (ML) to augment its products and facilitate scalability since the company was founded.

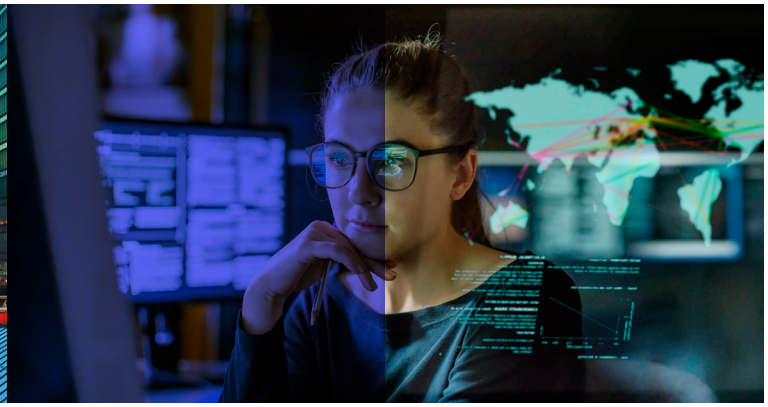
Our expert cyber threat analysts pool their knowledge of threat actor behavior and tendencies to create the building blocks of our AI and ML-enhanced harvesting systems. As the algorithms are constantly being trained and updated with new threat activity data, the platform iterates and improves on itself on a rolling basis.

While the threat of attackers using AI to greatly magnify the scale of their attacks looms large, BlueVoyant remains one step ahead of them with cutting-edge algorithms that scan an unrivaled collection of sources to deliver the most accurate threat data on the market – and peace of mind to security teams that are stretched thin.

Key Differentiators

- Continuous monitoring of and real-time validated alerts for exposed corporate data leveraging our cutting-edge AI and ML-driven algorithms.
- Unlimited rapid phishing takedowns leveraging exclusive partnerships with domain registrars, social media platforms, and hundreds of app stores.
- AI and ML continuously improve data ingestion, threat detection, and eliminate false positives to cut down on alert-related noise.
- Unmatched external threat data sources including proprietary global DNS datasets, invite-only IM channels that we access using AI programs, real-time breach data, and exclusive cybercrime forums.
- AI and ML footprinting using corporate firmographics and seeds for analytics, including Natural Language Processing (NLP), image recognition, Convolutional Neural Network (CNN), and more to score internet infrastructures belonging to an entity.

BlueVoyant



Features

External Threat Protection

Data leakage detection and identification of phishing websites (including malicious look-alikes), rogue or malicious apps, and social media impersonation attempts targeting the business using AI and ML to aggregate and validate threat data.

Entity Identification

AI-driven algorithms identify corporate credentials being shared or for sale, corporate executives being targeted, images and videos containing sensitive corporate data, and more.

Cyber Threat Takedowns

Real-time detection and takedowns of threats to the client's customers and employees emanating beyond the perimeter, including automated takedowns for web-based threats.

AI-Powered Analytics

Ensemble of algorithms "score" Internet infrastructure as belonging to an entity using NLP, CNN, image recognition and more to deliver key insights and reduce false positives.

Advanced Image Recognition

Proprietary AI image recognition engine examines tens of thousands of sites regularly for phishing and look-alike websites.

SOC Rules Engine

Pluggable expert system that triages events/alerts to prioritize and tune vendor generated false positives, correlating related events into a single alert to provide analysts with the full picture.

Ready to get started?
Schedule a demo.