BLUVECTOR®

Next Generation Intrusion Detection

STAY **AHEAD** OF THE THREAT.

Defense against advanced cyber attacks for mid- to large organizations

BluVector's next generation Network Intrusion Detection System (NIDS), powered by patented machine learning and speculative execution technologies, enables organizations to minimize the risk of costly cyber incidents by accurately identifying advanced attacks designed to avoid anti-virus, mask malicious behaviors in sandbox detection and subvert traditional network defenses.

Additionally, BluVector's Intelligent Decision Support System delivers analysts the actionable insight and workflow automation needed to confirm and contain threats early in the kill chain.

With BluVector, organizations are protected against today's evasive and increasingly destructive threats, whether file-based or file-less; directed at an organization's headquarters or a remote office; and capable of evading even the most sophisticated sandbox or signature-based engine.

At the heart of BluVector are three components:

1. A patented, supervised machine learning engine (U.S. Patent 9,665,713), trained for 8 years by entities in intelligence, defense, and commercial sectors to accurately identify zero-day and polymorphic malware. With a Miercom lab certified detection rate of +99%, BluVector is recognized as amongst the most accurate in the market at detecting file-based malware threats.
2. A speculative execution engine that is the cybersecurity industry's first solution specifically designed to find fileless malware traversing the network, in real time.
3. Targeted Logger delivers context and visibility to threat security teams and their investigations by pre-correlating and highlighting log entries associated with events prioritized for analysis.

EARLY, ACCURATE DETECTION

Detection of advanced threats
Minimize risk of increasingly destructive cyber attacks by detecting threats early in the kill chain.

Low false positive/negative rates
Reduces operational cost associated with chasing "ghosts."

SMTP and HTTP support
Analyze both SMTP and HTTP on a single hardware appliance.

Moving defense
Utilizes self-evolving supervised machine learning algorithms to make each instance resistant to hacker evasion.

No rules tuning
Deployed in under 30 minutes and without rules or tuning.

Support for IPv4 and IPv6 environments
IPv6 compliance technology makes it possible for BluVector to support complex IoT environments.

INTELLIGENT DECISION SUPPORT

Probabilistic scoring
Derived from a series of formulas, hunt scores help prioritize analyst focus.

Targeted logging and search
Patented technology provides enriched and highlighted context around security event, enabling analysts to make decisions faster.

Hunt process automation
Increased analyst efficiency by up to 80% with incident investigation and confirmation with full automation.

TECHNICAL **ADVANTAGES**

Flexible Deployment

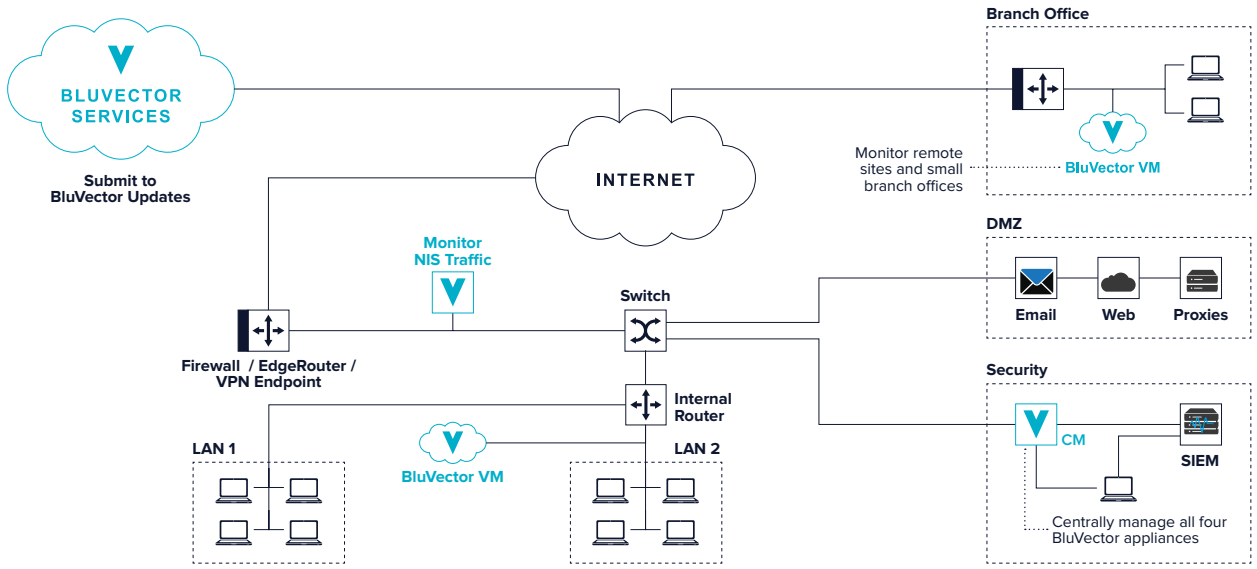
BluVector is available in a number of form factors and performance options. It is usually deployed via a network TAP or span behind traditional network security appliances such as next generation firewalls and web gateways. A rich connectors framework makes it possible for BluVector to receive and correlate data from a variety of threat intelligence sources, send events to SIEM solutions like Splunk and QRadar, or integrate with networking or Endpoint Detection and Response (EDR) solutions to enable blocking.

Extensible Detection Architecture

Multiple threat detection engines run in parallel, ensuring that even the most sophisticated of attacks can be identified. For more advanced users, on-board Docker containers assure that custom analytics can be introduced in minutes, and added to the BluVector threat detection ecosystem.

High Performance and Scalability

Built to support speed and performance requirements of Defense, Intelligence, and the Fortune 10 commercial sector, BluVector's line rate analysis for a wide variety of office sizes.



DEFINING NEXT GENERATION NIDS

Threat Category	NIDS	BluVector
C2 Detection	✓	✓
Fileless Malware – Known threat	✓	✓
File-Based Malware – Known threat	✓	✓
Fileless Malware – Unknown threat	✗	✓
File-Based Malware – Unknown threat	✗	✓
Spearphishing	✗	✓
Credential & Password Compromise	✓	✓
Insider Threats	✓	✓
XSS, SQL Injections	✓	✓
Brute Force Scanning	✓	✓

BUSINESS **BENEFITS**

Minimizes Risk of Destructive Cyber Incident

BluVector is a highly effective network intrusion detection system that helps organizations protect themselves from increasingly impactful cyber breaches by helping security teams find, confirm, and contain attacks at the point of delivery, early in the kill chain.

Focuses Security Team on Alerts That Matter

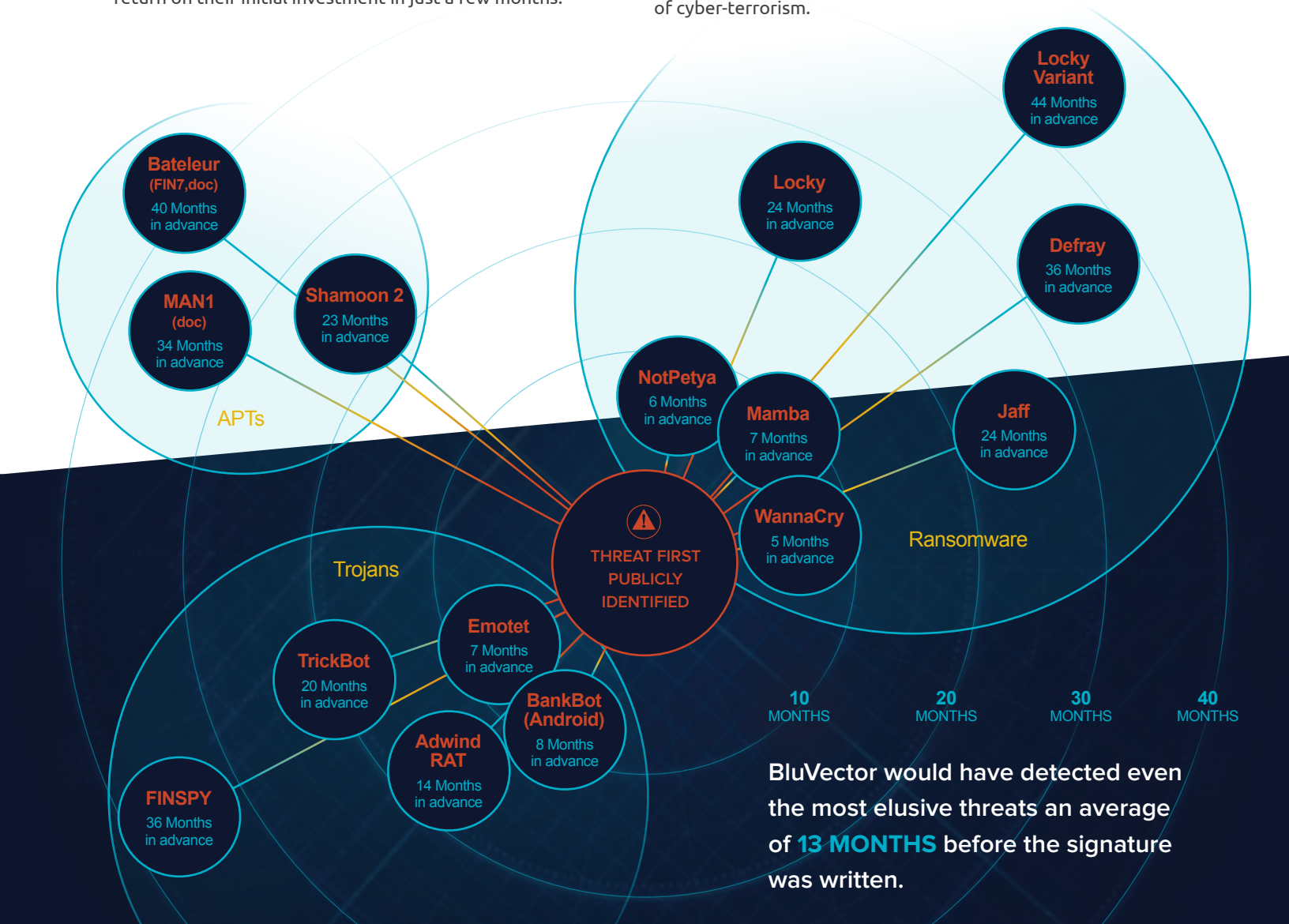
BluVector's Intelligent Decision Support System delivers actionable insights to analysts. BluVector customers report an 80% decrease in the time it takes to find and contain security incidents, which results in a return on their initial investment in just a few months.

Delivers Immediate ROI

With an implementation time of under 30 minutes, customers can expect to be fully operational on day one.

Protects Against Catastrophic Cyber Attack

One of the first security solutions on the market to receive the U.S. Department of Homeland Security's Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act Designation, so customers who deploy BluVector are able to benefit from liability protection against catastrophic acts of cyber-terrorism.



BluVector would have detected even the most elusive threats an average of **13 MONTHS** before the signature was written.

TECHNICAL **SPECIFICATIONS**

Specification	Virtual Machine / ESXi	Hardware Appliance
Performance	Up to 500 Mbps	Up to 1Gb or 10Gb
Network Monitoring Ports*	1	**1Gb BluVector** (4) SFP ports for 10/100/1000 BASE-T **10Gb BluVector** (2) SFP+ ports 10G BASE-SR/SW 850nm (2) SFP+ ports 10G BASE-SR/SW 850nm (LC Multimode)
Networking Management Ports	1	(1) 10/100/1000 BASE-T Port
Network Port Mode of Operation	vNIC (Management port) Passthru (monitoring port)	N/A
Form Factor	Virtual Appliance	2U Rack Mount/19-inch rack mountable
Hypervisor Support	VMWare ESXi 6.0, 6.5	N/A

**Pass-through mode for netmap-optimized drivers. 500Mbps not guaranteed if vNIC does not support netmap-optimized drivers.*

BLUVECTOR®

STAY AHEAD OF THE THREAT.

BluVector has reinvented network intrusion detection with machine learning so that it can finally deliver on its promise. Stop waiting for breaches to happen, stay ahead of the advanced threats with BluVector.

www.bluvector.io | 571.565.2100