eBOOK

DataBee® BluVector® NDR

A Modern Approach to Network Detection and Response

databee.ai

DataBee® BLUVECTOR

Contents

03 **INTRODUCTION**
Overview of the evolving threat landscape and the need for modern NDR solutions.

03 **CHAPTER 1: MARKET CONTEXT — THE EVOLUTION OF NDR**
Historical perspective on malware detection and the emergence of Network Detection and Response.

04 **CHAPTER 2: THE CHALLENGES TODAY THAT ARE DRIVING THE NEED FOR NDR**
Key pain points in modern cybersecurity operations, including visibility gaps and alert fatigue.

05 **CHAPTER 3: HOW BLUVECTOR ADDRESSES THESE CHALLENGES**
BluVector's AI-powered detection, early prevention, and customizable engine.

06 **CHAPTER 4: CORE CAPABILITIES OF BLUVECTOR**
Deep dive into BluVector's capabilities, which extend beyond file analysis to encompass threat hunting, incident response, and encrypted traffic monitoring.

09 **CHAPTER 5: REAL-WORLD DEPLOYMENT — COMCAST USE CASE**
How Comcast uses BluVector across its infrastructure for advanced threat detection.

10 **CHAPTER 6: SPEED AND RESPONSIVENESS**
BluVector's rapid deployment, real-time alerting, and continuous learning.

11 **CHAPTER 7: INTEGRATION WITH DATABEE® — UNLOCKING THE POWER OF CONNECTED SECURITY DATA**
Strategic benefits of integrating BluVector with the DataBee security data fabric platform.

13 **TECHNICAL SUMMARY AT-A-GLANCE**
Tabular breakdown of BluVector's capabilities, integrations, and operational impact.

16 **CONCLUSION**
Final thoughts on BluVector as a strategic asset for modern security teams.

INTRODUCTION

In today's cybersecurity landscape, threats evolve faster than traditional defenses can adapt.

Signature-based detection methods, once the cornerstone of malware identification, now struggle to keep pace with zero-day exploits and AI-generated threats. Enter DataBee® BluVector®, a network detection and response (NDR) platform purpose-built to help meet the demands of modern security operations.

This ebook explores BluVector's origins, its unique capabilities, and how it empowers organizations to detect, analyze, and respond to threats with speed and precision.

Chapter 1:

Market Context — The Evolution of NDR

Fifteen years ago, malware detection was largely reliant on antivirus signatures and basic heuristics. But as nation-state actors and advanced persistent threats (APTs) began crafting malware that evaded these defenses, the need for a more intelligent, proactive solution became clear.

The NDR market emerged to fill this gap, offering visibility into network traffic and enabling threat detection beyond the endpoint. BluVector was born from this need—initially serving government clients—and has since evolved into a robust platform used by enterprises like Comcast, which deploys hundreds of BluVector sensors across its infrastructure.

Chapter 2:

The Challenges Today That are Driving the Need for NDR

As cyber threats grow more sophisticated, traditional security tools are struggling to keep up. Organizations face several persistent challenges that make threat detection and response slower, less accurate, and more resource-intensive.

1 Malware Creation Is Easier Than Ever

Modern malware is designed to exploit zero-day vulnerabilities, bypass signature-based detection, and evade traditional security controls. With the rise of AI-assisted malware development, attackers can rapidly generate new variants that slip past legacy defenses.

2 Fragmented Visibility Across the Network

Security teams often operate with blind spots in their network. Incomplete visibility makes it difficult to triage events, correlate alerts, and understand the full scope of an attack. Malware sandboxes, while useful, are limited by capacity and cannot detonate every suspicious file. Given the prevalence of new attacks that attempt to blend in with normal traffic, detailed accounting of traffic is critical to response efforts today.

3 Manual Analysis Slows Response Times

Security Operations Center (SOC) analysts are overwhelmed by alerts and forced to investigate threats using multiple siloed tools. This leads to analyst fatigue, slower response times, and missed opportunities to contain threats early.

4 Exploitation Of Existing Tools and Credentials

Attackers frequently exploit legitimate tools and encrypted channels to move laterally within networks, often bypassing endpoint defenses or perimeter-based systems like firewalls. NDR provides critical visibility into these otherwise hidden behaviors by continuously monitoring network traffic for anomalies and patterns that indicate compromise both as the threats enter and as they move laterally within the network. It acts as a source of truth that cannot easily be tampered with, since all malicious activity—no matter how subtle—must generate network signals at some point. NDR complements endpoint and identity-focused defenses by detecting threats that originate in unmanaged devices, compromised credentials, or third-party systems that lack agent coverage.

Chapter 3:

How BluVector Addresses These Challenges

BluVector was purpose-built to tackle these modern security challenges head-on, offering a unified, intelligent approach to network detection and response.

1 AI-Powered Detection

BluVector uses machine learning and AI to detect threats that evade traditional methods. Its proprietary engine, Hector, analyzes files in milliseconds, enabling real-time detection of zero-day malware and evasive threats. AI/ML file-based analysis supplements signature updates, allowing detection of the previously unseen threat without compromising detections of known threats.

2 Early Threat Detection and Prevention

BluVector goes beyond signatures and heuristics to identify threats before they execute. It can even operate in air-gapped environments, making it ideal for sensitive sectors like government and finance.

3 Unified Visibility and Deep Analysis

By integrating tools like Zeek and Suricata, BluVector provides deep network visibility—not just IPs and ports, but full context including domains, DNS queries, and API calls. This enables:

- Retrospective analysis
- Campaign tracking
- Threat hunting across the entire network
- Network segmentation policy monitoring

4 Flexible, Customizable Detection Engine

BluVector supports bring-your-own rulesets, including:

- JA4 modules and signatures
- Suricata signatures
- YARA/YARA-X rules
- Zeek scripts

Its in-situ retraining capability allows organizations to locally retrain the ML engine using their own benign and malicious files—without sending data to the vendor, or to the cloud. This ensures:

- Reduced false positives
- Improved detection accuracy
- Better control over detection logic

SOLUTION

Chapter 4:

Core Capabilities of BluVector

BluVector delivers a powerful and multifaceted approach to network detection and response, combining advanced machine learning, deep file inspection, and full-spectrum traffic visibility. Its capabilities extend beyond file analysis to encompass threat hunting, incident response, and encrypted traffic monitoring—making it a cornerstone of modern cybersecurity operations.

Advanced Threat Detection

BluVector's strength lies in its ability to detect zero-day threats and novel malware—files that evade signature-based detection and lack known indicators of compromise (IOCs).

The platform scans all network traffic and files using a combination of:

- Custom supervised machine learning models
- Signature and heuristic analysis
- Intel indicator hunting
- Deep file inspection tools
- Suspicious network behavior signatures

This multi-layered approach helps ensure that even the most sophisticated threats are flagged before they reach users. BluVector also includes traditional intrusion detection system (IDS) capabilities, powered by open-source and commercial rule sets, to detect known threats and support zone-based monitoring.

Machine Learning Engine: Hector

At the heart of BluVector is Hector, its proprietary machine learning engine.

Hector analyzes over 40 unique file types, including:

- PDFs
- Office documents
- Executables
- Android/iOS apps
- Scripts (JavaScript, VBScript)
- Image files

Each file type is processed by a dedicated classifier tailored to its structure and behavior. Hector operates with remarkable speed—under 40 milliseconds per file—making it faster than traditional sandboxing solutions and ideal for real-time detection.

Deep File Analysis and IOC Extraction

BluVector doesn't just scan files—it dissects them. Using tools like Extractor, it opens multi-level archives and pulls out embedded objects. It also identifies IOCs buried within files, such as malicious URLs in PDFs, before users interact with them, presenting these findings with its IOC Hunter tool.

This granular visibility enables:

- Retrospective threat hunting
- Campaign tracking
- SOC workflow optimization

These capabilities are further enhanced by Pinpoint, which allows threat hunters to group, sort, and filter metadata about files, threats, and network delivery mechanisms.

Network Traffic Visibility and Beacon Detection

BluVector provides full traffic summarization and detailed protocol decoding, giving analysts deep insight into network flows.

Features include:

- Federated traffic log search across distributed environments
- Targeted logging that automatically surfaces relevant traffic flows
- Monitoring of encrypted and unencrypted traffic

Its Intel Framework supports the detection of all types of traffic to suspicious destinations on the Internet. Its custom Beacon Detection analytic identifies anomalous traffic patterns consistent with interactive command-and-control (C2) beaconing activity, even in encrypted sessions.

In-Situ Retraining for Custom Environments

BluVector's supervised machine learning models can be retrained locally using customer-specific data. This process, called in-situ retraining, enables organizations to:

- Reduce false positives
- Improve detection accuracy
- Tailor classifiers to their unique threat landscape

Importantly, no data leaves the customer's environment, addressing privacy concerns and ensuring compliance with internal policies.

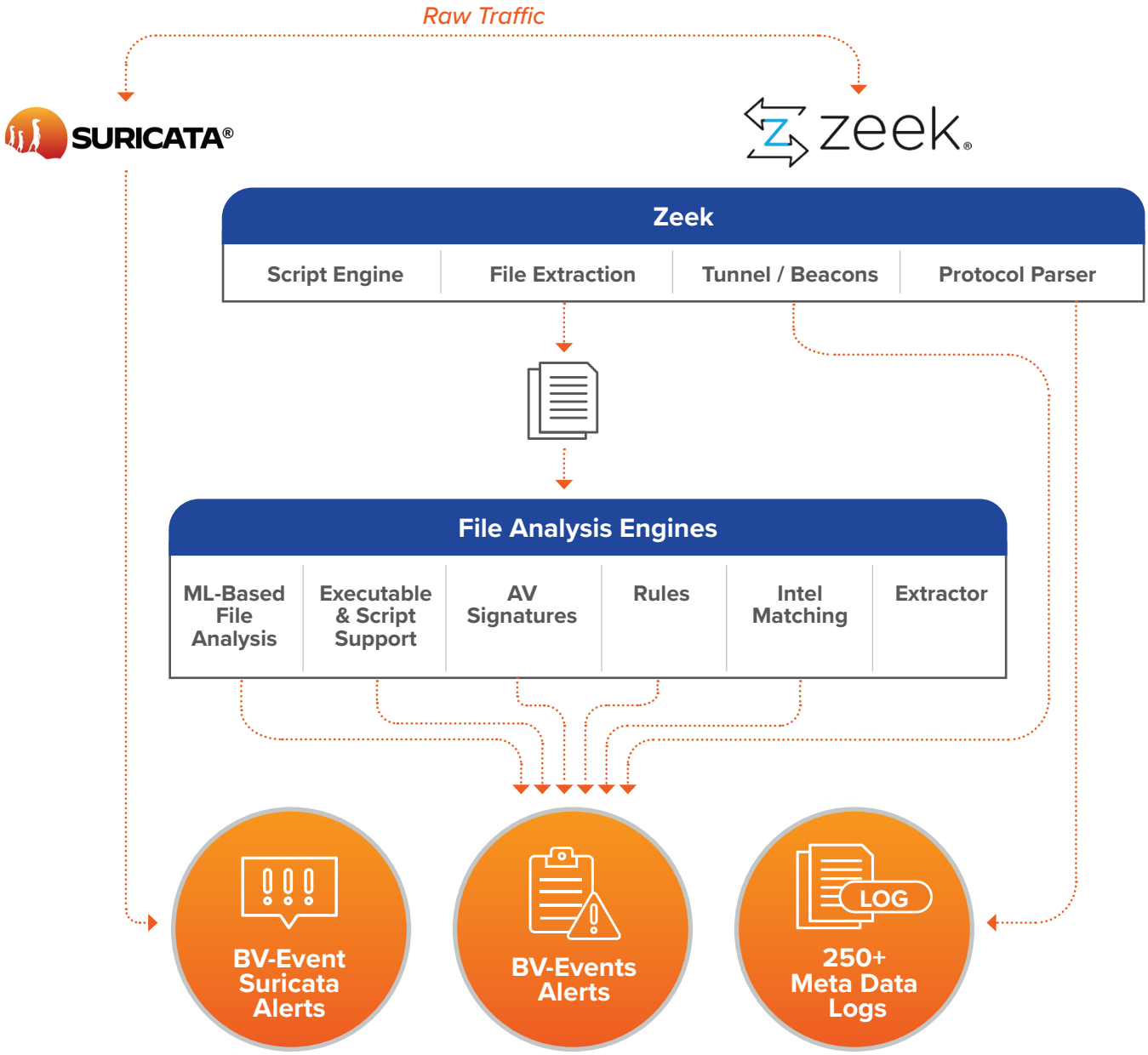
Integrated Incident Response Workflows

BluVector integrates seamlessly with existing incident response (IR) workflows. Its IR tools bring event data and associated files directly into the analyst's workflow, enabling:

- Rapid triage and investigation
- Context-rich alerts
- Streamlined response actions

This integration ensures that detections are not only accurate but also actionable within the broader security operations ecosystem. Related events can be aggregated into specialized views called Threat Vectors enabling analysts to automatically triage and prioritize investigations.

BluVector Functional Architecture



BluVector ATD™

Virtual Machine or Appliance 1Gbps to 25Gbps

databee.ai

Chapter 5:

Real-World Deployment — Comcast's Use Case

BluVector was founded in 2012, originally a spinout of aerospace, defense and security company Northrup Grumman. In 2019, Comcast was looking for an NDR solution and was so impressed with BluVector, that it bought the company. Since then, Comcast Cybersecurity has deployed over 200 BluVector appliances across its vast network and continues to work collaboratively with the DataBee BluVector team on new enhancements and capabilities that make BluVector a very desirable solution, especially for large enterprises and government agencies.

Comcast's adoption of BluVector illustrates its scalability and effectiveness. The company uses BluVector for:

- Network threat detection
- Advanced malware analysis
- Detailed network visibility via integrated tools like Zeek

BluVector replaced legacy threat detection systems and now serves as a source of truth for network activity, helping Comcast isolate traffic, enforce segmentation, and respond to incidents with confidence.

> "DataBee BluVector is a powerhouse, working behind the scenes at Comcast to provide advanced threat detection, including the ability to detect and contain AI-based malware and zero-day threats as early as possible."
>
> **Noopur Davis,** *Executive Vice President, Chief Information Security and Product Privacy Officer,* Comcast Corporation and Comcast Cable

Chapter 6:

Speed and Responsiveness

BluVector is designed for immediate impact. Upon deployment, it begins detecting threats using pre-trained classifiers. Its machine learning engine outpaces traditional methods, enabling real-time alerts and integrations with security orchestration, automation and response (SOAR) platforms.

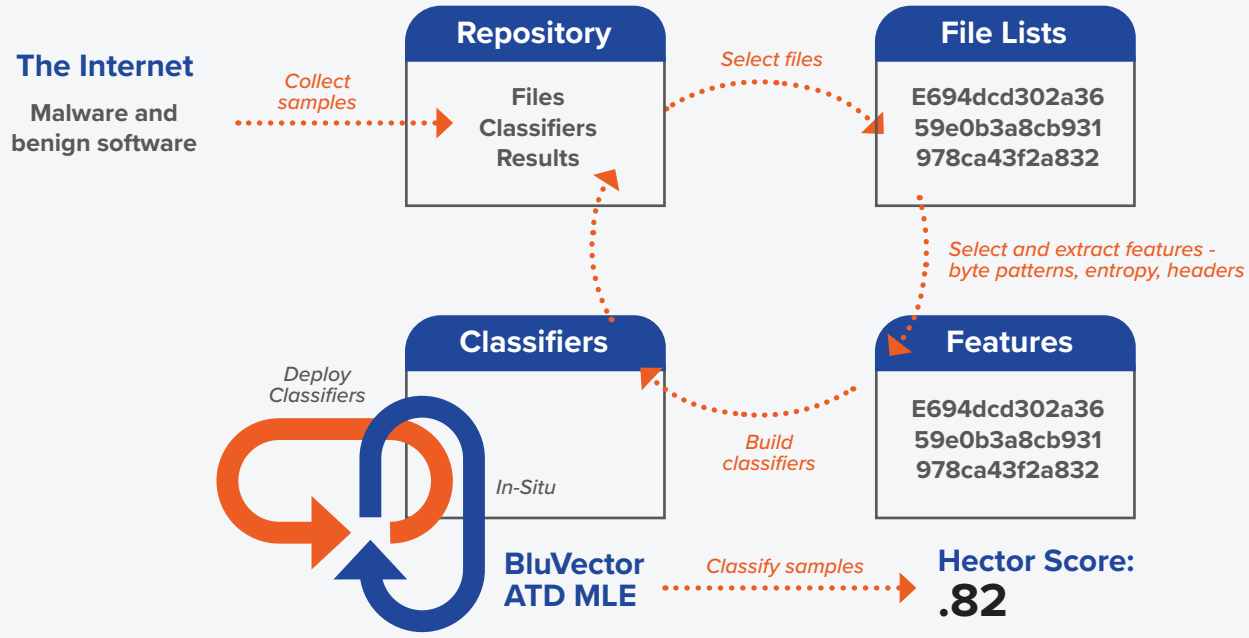
Over time, the system becomes even more effective as it learns from:

- False positives
- Customer-provided benign and malicious files
- Operator-driven rules and feedback

This continuous improvement helps BluVector remain aligned with the evolving threat landscape.

HOW IT WORKS

Ready Out of the Box – Gets Better Over Time



Chapter 7:

Integration with DataBee – Unlocking the Power of Connected Security Data

In today's complex security environments, data fragmentation is one of the biggest barriers to effective threat detection and response. Security teams often struggle to correlate telemetry across disparate tools, leading to blind spots, delayed investigations, and missed threats. The integration of BluVector with the DataBee security data fabric platform addresses this challenge head-on, transforming raw network telemetry into actionable intelligence.

A Unified Security Data Fabric

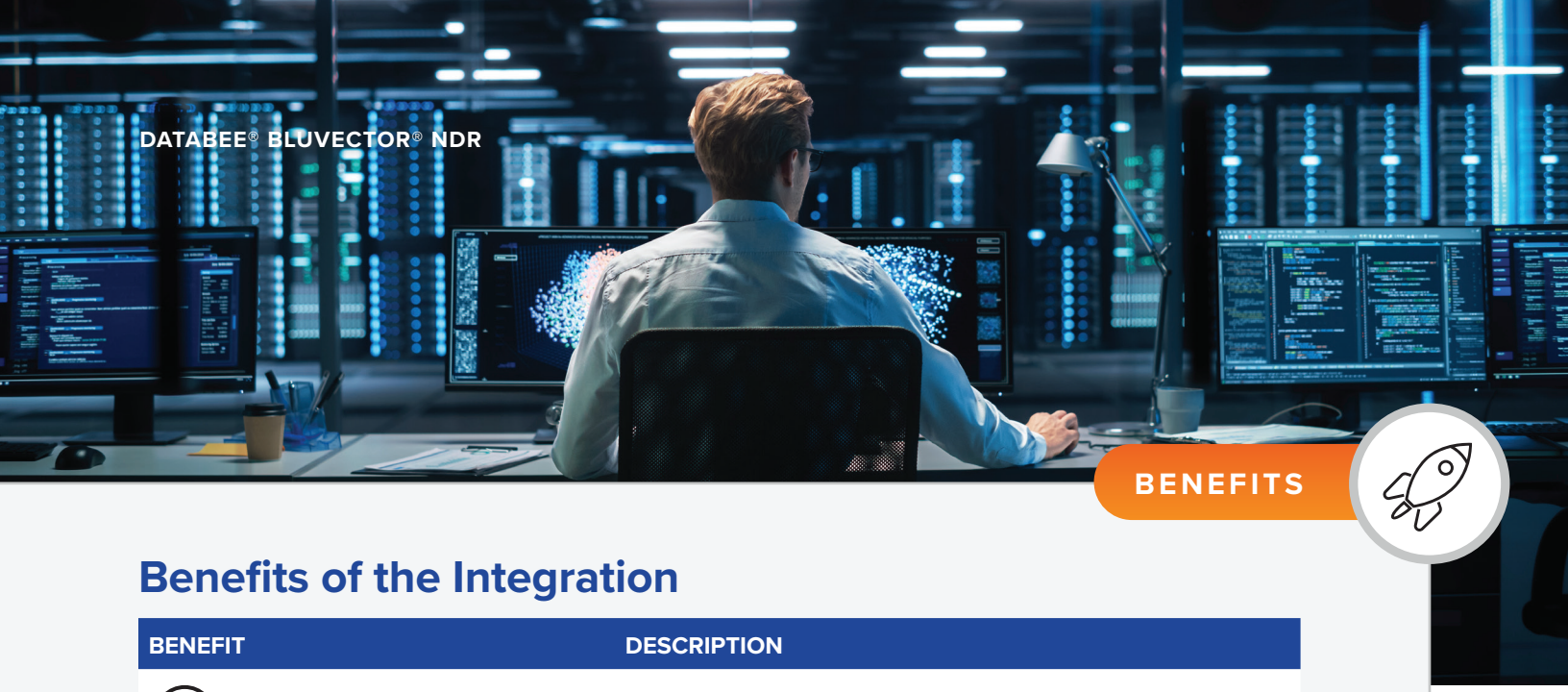
DataBee is designed to unify and operationalize security, risk, and compliance data across the enterprise. By integrating BluVector's high-fidelity network telemetry into DataBee's fabric, organizations gain a centralized, enriched view of their threat landscape. This enables:

- Real-time threat correlation across network, endpoint, and identity data
- Streamlined compliance reporting with enriched context from BluVector detections
- Accelerated incident response through automated workflows and enriched alerts

Operationalizing BluVector Telemetry

BluVector generates rich metadata from network traffic, including file analysis results, protocol behaviors, and threat scores. When ingested into DataBee, this telemetry becomes part of a broader evidence-centric data layer that supports:

- Threat hunting across historical and real-time data
- Campaign tracking with full visibility into attacker behaviors
- SOC optimization through reduced alert fatigue and improved triage accuracy



BENEFITS

Benefits of the Integration

BENEFIT	DESCRIPTION
Enhanced Visibility	Combines BluVector's deep network insights with DataBee's cross-domain data fabric
Rapid Response Times	Enables automated enrichment and correlation for rapid triage and containment
Enhanced Accuracy	Helps reduce false positives by contextualizing alerts with broader enterprise data
Scalable Intelligence	Supports large-scale environments with distributed sensors and centralized analytics
Compliance Readiness	Facilitates audit trails and reporting with enriched, structured threat data

Built for Enterprise and Government

This integration is especially valuable for large enterprises and federal agencies that require:

- Air-gapped deployment options
- Customizable detection logic
- Privacy-preserving data workflows

BluVector's ability to operate independently while feeding into DataBee's centralized intelligence layer ensures both operational flexibility and strategic alignment with enterprise security goals.

BluVector Technical Summary At-a-Glance

Extensible Ecosystem

CAPABILITY	DESCRIPTION	INTEGRATION METHODS	OPERATIONAL IMPACT
Open API	Enables integration and orchestration with existing security infrastructure	Restful API	Facilitates automation, data exchange, and workflow customization
Log & Telemetry Sharing	Exports BluVector-generated data for external use and response	Syslog, JSON, Kafka, STIX/TAXII, Edge Writer	Enhances visibility and enables threat response in downstream platforms
SIEM Integration	Supports ingestion into SIEM platforms for centralized monitoring	Syslog, API, Kafka	Enables correlation, alerting, and incident response workflows
DataBee Compatibility	Operationalizes telemetry within DataBee's data fabric	Native support or via API	Supports advanced analytics, compliance, and data enrichment
STIX/TAXII Support	Facilitates standardized threat intelligence sharing	STIX 2.1 over TAXII 2.0	Promotes interoperability with threat intel platforms and automated response systems
Custom Tool Integration	Allows connection with proprietary or legacy security tools	API, STIX/TAXII, custom connectors	Adapts BluVector to unique enterprise environments and workflows

Broad Detections

CAPABILITY	DESCRIPTION	INTEGRATION METHODS	OPERATIONAL IMPACT
Multi-layered Detection	Detects stealthy threats using layered technologies	Suricata, YARA/YARA-X, HURI, ClamAV, ML engine	Boosts detection accuracy to help reduce false positives
Anomaly & Signature-Based	Combines behavioral and signature-based techniques	Supervised machine learning + rule engines	Identifies known and unknown threats effectively

BluVector Technical Summary At-a-Glance (cont.)

Traffic Analysis

CAPABILITY	DESCRIPTION	INTEGRATION METHODS	OPERATIONAL IMPACT
Protocol Inspection	Analyzes traffic across common application and network protocols	IPv4/6, ICMP, TCP, UDP with detail for many apps (SMTP, HTTP, FTP, SMB, etc.)	Enables deep packet inspection for malware and threat detection
Malware Detection	Identifies malicious activity within network traffic	Protocol-aware analysis	Enhances visibility into lateral movement and data exfiltration

File Analysis

CAPABILITY	DESCRIPTION	INTEGRATION METHODS	OPERATIONAL IMPACT
ML-Based File Scanning	Uses machine learning to detect unknown threats in files	40+ filetypes including .exe, .dmg, Office docs	Detects zero-day threats and evasive malware
Executable & Script Support	Supports analysis of binaries and scripts	Executables, scripts, documents	Broadens threat coverage across user and system-generated files
AV Signatures	Traditional antivirus signatures	Automatically syncs to received ClamAV signatures	Allows for common detections, relevant for devices without EDR
Rules	Open, flexible framework for adding community or private rules	Yara or Yara-x rules	Allows users to add customer detections
Intel Matching	Search for intel IOCs within the file	Connect to your intel provider	Find IOCs in a delivered file before execution
Extractor	Extract objects from archives for analysis	Most archive types with password cracking	Find threats hidden in archives

BluVector Technical Summary At-a-Glance (cont.)

Modular & Fast

CAPABILITY	DESCRIPTION	INTEGRATION METHODS	OPERATIONAL IMPACT
Scalable Architecture	Supports deployment from edge to core	5G, 10G, 25G appliances; 500MB VM	Adapts to enterprise size and performance needs
High-Speed ML Engine	Maintains detection performance at high throughput	Hardware and virtual options	Ensures consistent threat detection across environments

Operationalize Zeek

CAPABILITY	DESCRIPTION	INTEGRATION METHODS	OPERATIONAL IMPACT
Zeek Metadata Correlation	Enhances Zeek logs with BluVector analytics	Built-in Zeek log search and pivot/sort feature with Pinpoint for event metadata	Makes threat insights more actionable for analysts
Workflow Configuration	Enables custom analyst workflows	UI-based configuration	Streamlines investigation and response processes

Flexible Deployment

CAPABILITY	DESCRIPTION	INTEGRATION METHODS	OPERATIONAL IMPACT
Versatile Placement	Deployable across various network zones	Perimeter, data center, behind firewall	Protects critical assets across hybrid environments
Virtual Sensor Support	Supports cloud and hybrid infrastructure	Private cloud, hybrid cloud	Extends threat detection to modern infrastructure

Form Factors

CAPABILITY	DESCRIPTION
Appliance Models	4 available models: 1Gbps, 5Gbps, 10Gbps, and 25Gbps

DataBee BluVector is more than an NDR platform—**it's a strategic asset** for organizations seeking to stay ahead of cyber threats. With its powerful machine learning engine, deep file analysis, and customizable training capabilities, BluVector delivers the speed, accuracy, and adaptability that modern security teams demand.

Whether you're a government agency, financial institution, or enterprise, BluVector offers the visibility and intelligence needed to protect your network—today and tomorrow.

databee.ai

CONTACT US

Learn more by watching the BluVector demo video or contact us for a personalized product demo.

For more technical information on BluVector, documentation is available **here.**

About DataBee®, A Comcast Company

DataBee®, a Comcast company, offers the DataBee security, risk and compliance data fabric platform, and DataBee BluVector®, an on-premises network detection and response (NDR) platform, to some of the world's large enterprises and federal agencies. We help our customers work smarter with an evidence-centric approach to security that prepares them for what's next. Developed and proven at scale, DataBee delivers connected security and compliance data and insights that can work for everyone in an organization. Built to protect critical government and enterprise networks, DataBee BluVector delivers AI-powered NDR for visibility across network, devices, users, files, and data to discover and hunt skilled and motivated threats.