BLUVECTOR

SOLUTION BRIEF

BluVector protects critical networks and delivers visibility with AI-powered Network Detection and Response (NDR). Developed for and deployed at government agencies and enterprise networks, BluVector helps cybersecurity teams centrally manage the detection of and rapid response of ransomware and zero-day exploits.

Comprehensive network visibility

BluVector helps your security operations see and understand the activities happening on your network. Security teams can use the visibility insights and metadata to monitor, detect, investigate and respond to threats. Organizations can meet NDR and IDS requirements set in standards and regulations with BluVector.

Early threat detection and prevention

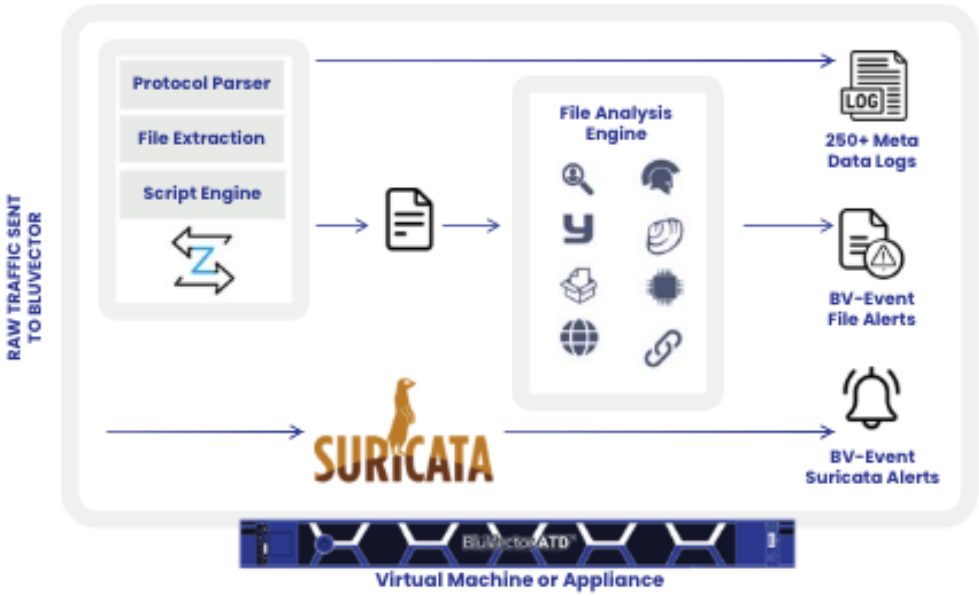
Detect zero-day attacks first and improve your detection and response metrics with BluVector. Immediately stop threats that keep targeting your organization. Fight new and polymorphic attacks with defense-in-depth that uses machine learning (ML) and multiple file analysis tools.

Contextualized threat hunting

When BluVector finds a threat, we give the details that matter so you can contain and eradicate it. BluVector shows you what happened on your network, the Sandbox testing results, and content payload analysis of the suspicious files.

Adaptable for your environment

BluVector meets the needs of your unique threat landscape. Bring your custom YARA and Suricata rules and Zeek scripts and use findings local to your network to re-train Hector, BluVector's ML engine, to detect specific threat groups or malware families. This enables increased accuracy and supports air gapped or highly sensitive environments.

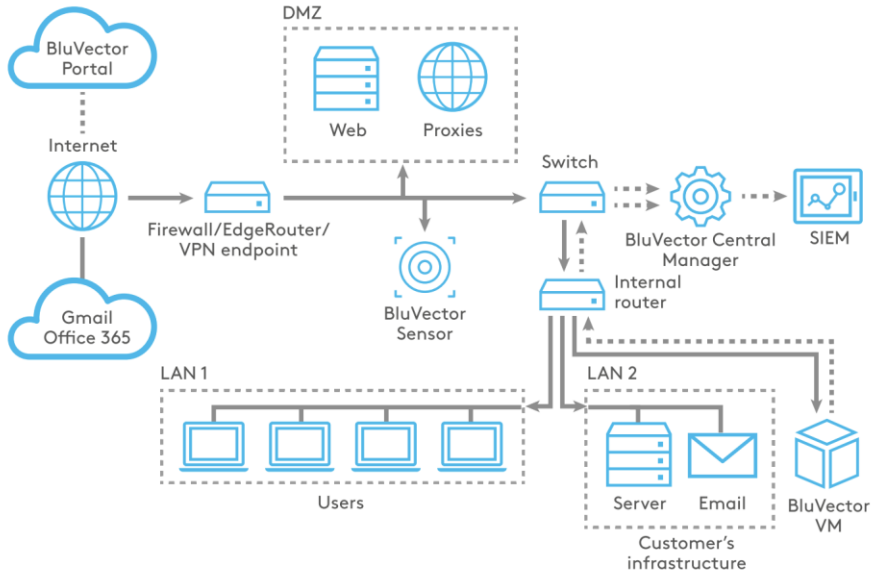


Technical BluVector Features

BROAD DETECTIONS Detect stealthy attacks and threats using a multi-layered approach that includes Suricata, YARA, HURI, and ClamAV and combines it with BluVector's proprietary supervised ML engine for anomaly and signature-based detection.	**TRAFFIC ANALYSIS** Analyze traffic across popular application and network protocols such as SMTP, HTTP, FTP, SMB and IPv4 and IPv6 for malware detection.	**FILE ANALYSIS** Analyze 40+ filetypes with ML to quickly detect unknown threats and protect against zero-day attacks. BluVector supports executables like .exe and .dmg, Microsoft Office filetypes, scripts and more.
MODULAR & FAST Designed to scale for remote offices to the data center core, BluVector appliances can support the ML detection engine at speeds from 5G, 10G, and 25G in a single appliance or in a 500MB VM.	**OPERATIONALIZE ZEEK** Correlate Zeek threat metadata with additional analytics to make the insights more actionable. Security teams can use the built-in Zeek log search directly in BluVector and configure analyst workflows and threat scoring.	**FLEXIBLE DEPLOYMENT** Deploy at the perimeter, at the data center, or behind the firewall to protect mission-critical assets. BluVector appliances are available in multiple speeds and BluVector Virtual Sensors are available for hybrid and private cloud infrastructure.

EXTENSIBLE ECOSYSTEM

Integrate and orchestrate with existing security infrastructure with an OpenAPI. BluVector logs and telemetry can be operationalized to respond in downstream tools like SIEMs and DataBee or with other pre-existing solutions through STIX/TAXII.



Get started with BluVector

BluVector is a multi-patented, industry recognized NDR solution that can fit in any sized environment. Visit us at **https://www.databee.ai** to help you transform how your security team can use network visibility for detection, triaging, and responding to security events.

DataBee A COMCAST COMPANY | BLUVECTOR