BLUVECTOR

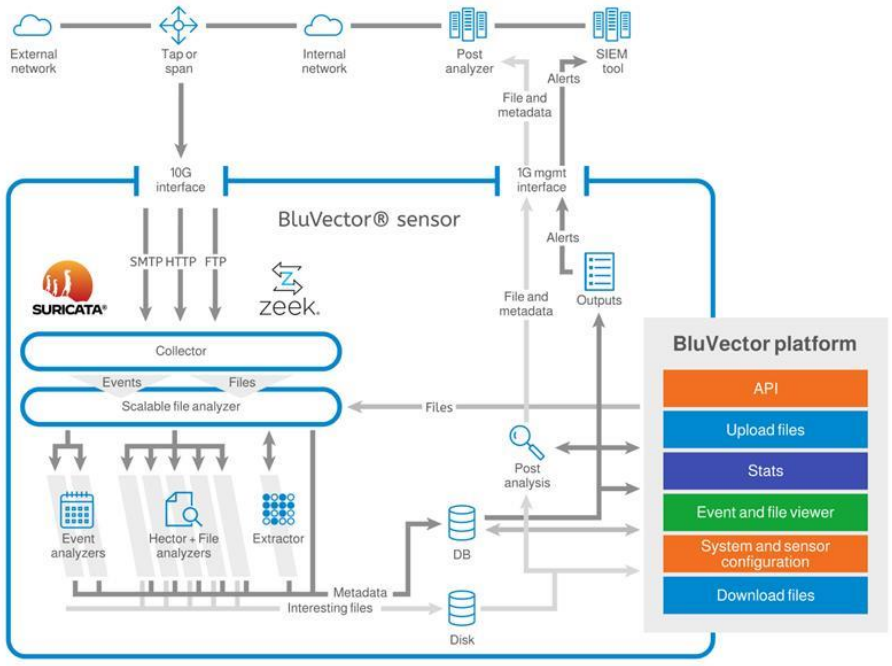
PRODUCT BRIEF

BluVector® protects critical networks and delivers visibility with AI-powered Network Detection and Response (NDR).

How BluVector Works

BluVector helps cybersecurity teams centrally manage the detection of and rapid response to ransomware and zero-day exploits.

Security and network operations teams can deploy at the perimeter, at the data center, or behind the firewall where live network traffic and files are sent to BluVector for threat detection and analysis.



The multi-layered detection stack and Hector, BluVector's supervised machine learning (ML) detection engine, detect zero-day malware before your other tools. The ML engine and classifiers can be refined on specific threat groups and samples to enable increased detection accuracy. Sensitive and air gapped environments can keep findings strictly internal, without sending it back to BluVector.

When BluVector detects a threat, your analysts have actionable file and network traffic telemetry and details about the malware payload. This enables greater downstream tool efficacy and can help improve incident response workflows.

AT A GLANCE

Challenges

- Network blind spots and no usable network telemetry
- Bad actors are using automation, AI, and zero-day malware
- Highly sensitive networks need an air gapped NDR solution

Benefits

- Comprehensive network visibility
- Early threat detection and prevention
- Contextualized threat hunting
- Adaptable for your environment

Key capabilities

- Machine learning malware detection and support for Zeek with built-in search
- Anomaly and signature-based detections that run Suricata, YARA, HURI and ClamAV
- Supports SMTP, HTTP, FTP, SMB and IPv4 and IPv6 protocols
- Analysis for 40+ different filetypes
- Speed availability of 5G, 10G, and 25G or 500 MB on a virtual machine
- Integrate with existing security stack including DataBee®

DataBee A COMCAST COMPANY | BLUVECTOR