BLUVECTOR®
A COMCAST COMPANY

BluVector visibility™

You can't protect what you can't see.

BluVector's NDR offering allows you to reduce false positives and alert fatigue, so your team can focus on real attacks.

Underspend. Overperform. Collect the right amount of data.

Some security teams choose to build their Zeek tools in-house. Many fail. Others find the development and maintenance cost prohibitively expensive. B2V bundles and packages it for you. We've tested and done the troubleshooting for you so you can deploy network visibility at scale.

SIEM/SOAR Integration

Our box plays nice with your system to provide the right info at the right time.

Better Visibility into East West traffic

Identity is the new perimeter. These days, attackers don't break in, they log in.

Visibility into encrypted traffic

Integration with break and inspect vendors and solutions, plus advanced capabilities that enable fingerprinting (with TLS handshake) for detailed insights

Identify threats in milliseconds

Get full visibility into all network event traffic in real-time. By analyzing all network data, presenting analysts with comprehensive network insight, and operating at line speed, B2V enables network defenders to react to threat actors at the delivery or pre-breach stage of the kill chain.

Broad MITRE ATT&CK® Coverage
Find threats and vulnerabilities faster. Detect at speed and scale.

Streamline threat investigations
Build queries and help speed up investigations with our unique analytic capabilities.

Detection at line speed & scale
Run Zeek and Suricata at line speed, up to 400 gbps in a single appliance and scalable to any network data rate.

Example: B2V Implementation and Performance Metrics at a Leading ISP Network

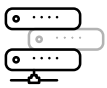
65+	315 Gbps	80 Gbps	~500M
Devices deployed	Max ingest rate	Capacity at VPN sites	Unique sessions per day

Get detailed visibility into attacks as they enter your network

Prevent your analysts from drowning in data. Conserve data center resources and give your people the ability to mitigate threats quickly and efficiently.

SOC Workload Reduction
Earlier alerts can stop threats from spreading and save time on clean-up.

Tuning Assistant
Reduce false positives and get maximum coverage with your signature set.



Free up Rack Space
Combine the full functionality of Zeek, Suricata, ClamAV, Yara, and Heuristic URL Interpreter (HURI) along with threat intel feeds in a single appliance.

Centralized Management
Gain a significant advantage over open-source Zeek with centralized configuration logging to easily manage your deployment.

Highly Configurable
Full visibility into rules and decision logic so you can fine tune existing rules and build / deploy new custom rules.

Frictionless upgrade to BluVector Advanced Threat Detection (ATD)

BluVector
4501 North Fairfax Drive, Arlington, VA 22203
www.bluvector.io

BLUVECTOR® A COMCAST COMPANY | COMCAST