COMCAST TECHNOLOGY SOLUTIONS

BLUVECTOR
A COMCAST COMPANY

BluVector™ Advanced Threat Detection (ATD)

Next-generation IDS, powered by AI

BluVector ATD is an advanced threat detection system that is transforming how security teams detect, triage, and respond to security events.

Trusted by the toughest

Deployed and actively in use across global government and commercial networks, BluVector is trusted to provide comprehensive threat coverage thanks to our people, our technology, and our commitment to our customers' success.

Loved by security operations

Committed to an open architecture, BluVector ATD is loved by security operations because it was built for analysts. Combining Zeek (formerly Bro) with Suricata, YARA rules, ClamAV, and HURI as well as BluVector's machine learning and fileless malware detection engine at speeds from 1G up to 20G in a single appliance or a 500MB VM, BluVector's modular design provides flexibility when needed.

Elevating Zeek

Many organizations rely on Zeek because it delivers detailed metadata about all network flows over a wide variety of protocols. BluVector ATD elevates Zeek by offering a variety of associated analytics that include automated correlation of Zeek threat metadata, automated correlation with Active Directory, configurable analyst workflows and threat scoring, and a built-in Zeek log search.

Innovation driven by real-world needs

As a machine learning innovator with more than a decade of experience applying AI to detect cyberthreats, BluVector ATD strengthens the cyber defenses for some of the world's most discerning customers. With multiple patents, BluVector continues to help customers leverage AI-based approaches to manage the volume, velocity, and polymorphic nature of today's and tomorrow's cybersecurity threats.

Customer benefits

Visibility and context
BluVector ATD offers the network visibility and context needed to successfully provide comprehensive threat coverage.

Detection with confidence
Better answers are good. More alerts are not. Providing quality threat indicators to help security analysts get answers is our passion.

Improved operational cost
BluVector ATD increases operational efficiency and reduces overhead by prioritizing actionable events with context.

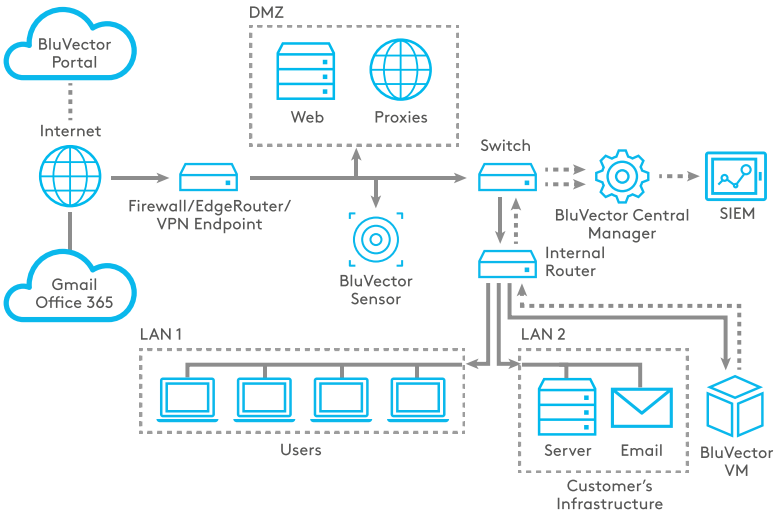
Complete coverage
Flexible deployment options and 100% network coverage meet the needs of any size enterprise.

Fully integrated
Organizations can operationalize the knowledge that BluVector ATD generates quickly — alone or with other pre-existing solutions through STIX/TAXII.

Scalable performance
BluVector appliances' modular design enables scale from remote offices to the data center core.

Complete detection coverage

Flexible deployment options and 100% network coverage meet the needs of any size enterprise. BluVector ATD can be deployed at the perimeter, at the data center, or behind the firewall to protect mission-critical assets.



Scalable performance

Designed to adapt to the customer's need, BluVector ATD is offered as both a VM, as well as 1U–2U hardware appliances.

Not a black box

Every security team has invested time, effort, and expense in tailoring their security stack to meet the needs of their business. With BluVector, security teams can continue to operate their custom Zeek/Bro scripts, YARA rules, or Suricata.

A better workflow

Successful security operations centers (SOCs) leverage technology that understands and improves the most crucial work. Driving that efficiency, BluVector ATD presents dataflow within the context of an event and the analyst's broader workflows to reinforce each time-saving feature. Events are correlated and scored so analysts can more efficiently understand where they should focus. Information including network metadata targeted around the event, Active Directory user information, results from an embedded sandbox, hex detail for fileless attacks, and the actual content payload are all easily accessible.

About BluVector

As a leader in advanced threat detection, BluVector is transforming how security teams detect, triage, and respond to security events. BluVector is empowering security teams to get answers about real threats, allowing businesses and governments to operate with confidence that data and systems are protected. To learn more, visit us at www.comcasttechnologysolutions.com/cybersecurity-suite/bluvector.

Technical features

Detection of advanced threats
The broad detection stack combines supervised machine learning, speculative code execution, Suricata, YARA, HURI, and ClamAV.

SMTP, HTTP, FTP, and SMB support
Analyze traffic across a range of protocols on a single hardware or virtual appliance.

Cloud email support
Support is provided for cloud email deployments of Office 365, Google, and similar IMAP-based services.

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

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

Targeted logging and search
Provide enriched and highlighted context around security events, enabling analysts to make decisions faster.

Hunt process automation
Help increase analyst efficiency with automated incident investigation and confirmation.

Highly extensible ecosystem
An OpenAPI makes it easy to integrate and orchestrate with existing security infrastructure.