DataBee® COMCAST TECHNOLOGY SOLUTIONS | BLUVECTOR®

Solution Brief

IT, IoT & OT convergence with DataBee® and BluVector™

The Purdue Enterprise Reference Architecture (PERA), also known as the Purdue Model for Industrial Control Systems (ICS), has provided guidance for IT and Internet of Things (IoT) and operational technology (OT) systems segmentation and separation to help organizations reduce the risk of cyberattacks and operational disruptions. However, this separation has led to the proliferation of an additional and parallel stack of security tools, each with its own data silo. Furthermore, the larger and more complex the organization, the more likely it is to have a separate cybersecurity team for IT and OT.

This architecture provides significant challenges for organizations attempting to assess compliance or conduct forensic analyses holistically across the organization. For example, a well-designed OT network will aggressively filter ingress and egress traffic from the environment, making it more difficult to access the valuable log data contained within. This can create blind spots when attempting to reconcile a full timeline of events as the visibility and insights stop at the IT or IoT/OT environment's border. Ultimately, this can result in significant challenges in protecting the organization due to the sensitive nature of OT networks and the safety risks associated with a breach or malicious actor gaining access to the environment.

Introducing DataBee and BluVector for IT and IoT/OT convergence

When your critical network infrastructure requires critical — and real-time — actionable insights, fusing IT and IoT/OT devices and network data together can give you visibility to protect what matters.

Together, DataBee® and BluVector™ from Comcast Technology Solutions deliver connected insights about your IT and IoT/OT infrastructure and network that is woven with additional security and non-traditional data feeds and business context. Now, with a security data fabric platform rich with network visibility and context, your team can answer questions, including:

- What are the network interactions between IoT/OT devices accessing or transiting IT infrastructure?
- How are end users interacting with devices or applications between IT and IoT/OT networks/devices?
- Are there network activities from users that suggest insider threat behaviors?
- How are our IoT/OT configurations meeting compliance and controls standards such as NIST 800-53 or NIST 800-171?
- Are there obsolete or vulnerable protocols visible on the network (e.g., telnet, ftp, old TLS versions)?

The power of a security data fabric for IT and IoT/OT convergence

DataBee and BluVector leverage patent-pending entity resolution technology to identify and merge every instance of an entity such as a user or device across the enterprise environment, so you know who is accessing what and when, whether that is on the IT or IoT/OT side.

BluVector sensors provide visibility into monitored segments with 1) detailed traffic logs including protocol decode, 2) security scanning for malicious content in packets, and 3) identification of malware in files. BluVector can be configured to collect all observed traffic, picking up traffic from IT, IoT, and OT devices.

DataBee has direct integration to consume the BluVector raw traffic data and detection events, transforming and normalizing to the Open Cybersecurity Schema Framework (OCSF) format and ready for long-term storage in the same data lake as your existing enterprise data. In addition to the typical enterprise data sources, DataBee supports ingest or IoT/OT management tools into the same data fabric.

With DataBee and BluVector, you can:

Adhere to PERA requirements with more holistic visibility.

- DataBee features flexible connector options for IT data, allowing easy ingestion and onboarding of IoT and OT data sources.
- As security and network data streams and processes through DataBee, data is normalized, and entities are resolved to the same data lake as IT data.
- BluVector can be deployed as a hardware or virtual sensor solution to accommodate a range of environments and network throughput rates.
- BluVector passively listens to a tap/span of available traffic; this can be single links or aggregated collections of data feeds. For high-bandwidth links, traffic can be load-balanced across multiple BluVector sensors.

Receive actionable insights for secure access and safe operations.

- DataBee automatically correlates user and entity details and enables analysts to search over network traffic.
- DataBee can analyze large datasets like BluVector detections to surface security events for IoT/OT devices that may be missed by current enterprise tools.

Improve analysis for monitoring and detection.

- DataBee provides prebuilt business intelligence (BI) dashboards for Tableau and Power BI to highlight controlled and uncontrolled inventory.
- BluVector provides network flow logs with Zeek that can directly import into DataBee, which can improve detection capabilities, enable better incident response, and optimize network performance.
- BluVector provides a central management platform for easy configuration and detection capabilities in sync.

Find out more

Ready to see how an enterprise-ready security, risk, and compliance data fabric can help you better understand your IT and IoT/OT environment? Request a custom DataBee demo | comca.st/databee

DataBee Safe Harbor Statement

This datasheet is intended to identify only our planned product offerings, enhancements, changes, and/or modifications. It is intended for illustrative purposes only and should not be relied upon in making purchasing decisions. Comcast makes no warranties, whether express, implied, or statutory, regarding or relating to the accuracy of this datasheet, including, but not limited to any warranty that the products or services will meet certain requirements. The development, release, and timing of any product offerings, enhancements, changes, and/or modifications shall be at the sole discretion of Comcast. This datasheet shall be deemed the proprietary and confidential information of Comcast and may not be copied, distributed, or published, in whole or in part, for any purpose.

DataBee COMCAST TECHNOLOGY SOLUTIONS | BLUVECTOR