Solution Brief

FlowIntelligence™ Cyber Security XDR

Identify threats to your information systems environment and see how the intruders operate from the moment they breach the preventive controls to the instance where they attempt to steal your organization's intellectual property and bring them to a complete stop!

Its only a matter of time before it happens …

A user inadvertently accesses a malicious website or clicks on a link in an email and malware bypasses the firewall, intrusion preventative system and anti-virus software. As a result, neither of these solutions have recognized the threat to the organizations' information systems. 18 Minutes - The time in which the malware coordinates with command and control, performs reconnaissance, begins lateral movement, takes over a target and the compromise has occurred. The timebomb is ticking and then boom: In that time your organization's data or intellectual property is being stolen, 10's or 100's of millions of credit card records are pilfered, banking accounts are exposed, patient data or a patient's life is put at risk, or even more sinister is shutting down critical services such as power, water or gas. These are facts and they already happened.

We can look at the news everyday and see a new threat. We know why it occurs, *five percent* - the total number of alerts that an analyst can process at any given time. With thousands, millions or more of alerts during a 24 hour period, this creates significant risk to an organization. This is compounded by gaps in visibility of threats, data silos, the number of disparate security technologies and simply put, information overload!

Now the analyst has a capability that truly provides visibility across the entire enterprise and allows them to detect, analyze and mitigate the full spectrum of sophisticated cyber threats. This is accomplished with advanced detection technology, analytics and response automation that leverages threat fusion, behavioral analysis, machine learning-data science and threat intelligence to uncover known or previously unknown attacks. FlowIntelligence™ Cyber Security XDR ensures analyst can identify and mitigate incidents in real-time which makes it easier to stop an breach before it can impact business operations.

So how do we get left of boom?

XDR - Extended Detect and Respond

FlowIntelligence Cyber Security is the Extended Detect and Respond solution that enables any organization to definitively and rapidly detect, identify and mitigate cyber threats or attacks that have bypass the border preventative technologies and attempts to take control of endpoints in the enterprise. The combination of distributed, machine learning-enabled sensing technology for network analysis, scalable machine learning-enabled analytics coupled the integration of the organization's EDR data, leveraging behavioral analysis, data science and threat intelligence which provides the most complete threat picture for any organization. It exposes scale, scope and phase of the attack where it can deliver deeper insight to the analyst. It enables the analyst to make intelligent decisions on the mitigation strategy and implement them through an automated response process utilizing visual workflows.

FlowIntelligence Cyber Security XDR:

- Monitor, Analyze and Identify threats or attacks in North-South network flows at speeds to 100Gbps
- Monitor, Analyze and Identify threats or attacks in East-West network flows or attacks in virtual workloads at 10Gbps across multiple hypervisors
- Deliver distributed analytics and unparalleled threat observability and visibility with the analytics fabric
- Incorporate the organization's EDR data for complete situational awareness
- Identify new, complex, targeted or unknown threats with real-time machine learning and data science through tensor decomposition to aid the analyst in stopping attacks
- Empower analysts with ability to understand the scale, scope and phase of an attack. Reduce the response time by 87% and increase the SOC team effectiveness by 30x.
- Realize immediate ROI

Capabilities and Benefits

A comprehensive, scalable solution for your enterprise. FlowIntelligence Cyber Security XDR is the only scalable solution that extracts and analyzes North-South, East-West network traffic. It combines endpoint telemetry data in the analysis to refine the threat picture utilizing MITRE ATT&CK®.

Advanced threat and business context. The analytics fabric identifies malicious threats across multiple data sets and correlates the data to alerts, logs, and events found in network flows and endpoints. The incorporation of threat intelligence dynamically drives prioritization of the analysis process and defines the mitigation strategies for business assets based on the MITRE ATT&CK model.

Automated behavior analytics. Identify application and user behaviors with the XDR solution. Analyst leverage machine learning to assess and mitigate threats from internal and external actors. Go beyond traditional analysis and decompose network flows with Tensor to extract the needle from the haystack thereby enriching the analysis process with refined data to highlight the key attack behaviors. This dramatically accelerates the speed-to-detection and speed-to-mitigation process.

Hunt, Find and Investigate. FlowIntelligence Cyber Security XDR provides advanced, feature rich analytics that enables the analyst to create custom, unique queries across multiple data indexes and couple those with visualizations to drive the hunt, find and investigate process. It enables analyst to identify the network attack or data exfiltration during the period of the threat. Specifically, the analyst is empowered with data to connect unique incidents that may have occurred over a long period of time and expose the magnitude of the threat.

Slow or stop threat actors with deception. Implement autonomous deception to slow or stop internal or external threat actors utilizing machine learning. Create bread crumbs, lures and baits that target threat actors, drive them to deception system and direct them away from the real corporate assets.

Automation, Orchestration and Response. Reduce the response time through security automation and orchestrate the delivery of mitigation processes through a visual workflow engine. Increase the collaboration between DevOps and SecOps teams for a more secure IT operating environment.

Scalable, flexible architecture. FlowIntelligence Cyber Security XDR can be deployed in the cloud, on-premise or virtually. The solution scales to your organization's environment, grows with you and addresses your unique requirements as well as priorities. This makes the solution a good fit for SMB's, Enterprise and customers with a global presence.

Unified security operations. FlowIntelligence Cyber Security XDR unifies the analysis and operationalizes the situational awareness for the organization with network and endpoint telemetry providing advanced cyber intelligence for organization's operational needs.

About Bivio Networks

Bivio Networks is dedicated to providing leading-edge networking products that enable enterprise, government agencies and service providers to operate, control, monitor and secure critical cloud and network infrastructure. A leader in cloud, cyber intelligence, cyber security and network control solutions, Bivio products are deployed in a wide range of environments by a global customer base including enterprises, leading government agencies, and service providers. Bivio is privately held and is headquartered in the San Francisco Bay Area.

Bivio Networks, Inc.

4457 Willow Road, Suite 240

Pleasanton, CA 94588

Tel: +1 925 924 8600