JOINT SOLUTION BRIEF

Enhancing Impelix IMPACT with Flow Data

Integrated Solution

- Impelix IMPACT Platform is an integrated security, risk, and compliance management solution featuring unlimited data ingest
- Cubro TAPs and Packet Brokers process network packet data into flow metadata enriched with application Deep Packet Inspection
- NetFlow Optimizer compresses and further enriches the meta data for delivery to Impelix IMPACT

Solution Features

- Identify large amounts of data moved outbound to external sites or laterally within your network
- Enables identification of botnet command and control (C2) servers
- Flow data with user identity improves UEBA (User and Entity Behaviour Analytics)
- Fast identification of traffic and data movement anomalies in your network
- Assist with capacity planning and network segmentation
- Optimize cloud network traffic and storage costs

New Security Challenges - A New Approach

Strategies for protecting enterprise IT assets have changed dramatically in the last few years. Bring-your-own-device (BYOD), Work-from-Home (WFH), Internet of Things (IOT), along with increased use of Software-as-a-Service (SaaS) and multi-cloud computing, mean that the enterprise perimeter has disappeared. A new threat landscape has emerged, **Enterprises should simply assume that bad actors may already have access to their networks and data**.

To respond to this, a new approach to network security is also being developed: the Zero Trust Network Architecture. Some key principles of Zero Trust include:

- *Verification*
  - ○ Verify and authenticate on an ongoing basis
- *Give minimal access*
  - ○ Segment the network to create small zones of control
  - ○ Control access to applications, data, and resources
  - ○ Grant least privileged access based on need or role
- *Assume a breach and continually assess risk*
  - ○ Plan as if attackers are both inside and outside the network
  - ○ Forget the concept of a “trusted zone” (e.g., in the office)

A comprehensive understanding of cybersecurity and organizational risk has become a requirement for ongoing stability and success for every organization. Impelix IMPACT provides this cyber hygiene and risk information in a simple, automated dashboard.

Unlike legacy SIEM, SOAR, XDR, or GRC (Governance, Risk, Compliance) vendors, the Impelix IMPACT Platform provides a unified security, risk, and compliance management platform that includes automated incident investigation and response and real-time risk and compliance monitoring, by leveraging unlimited data ingestion at flat, predictable pricing.

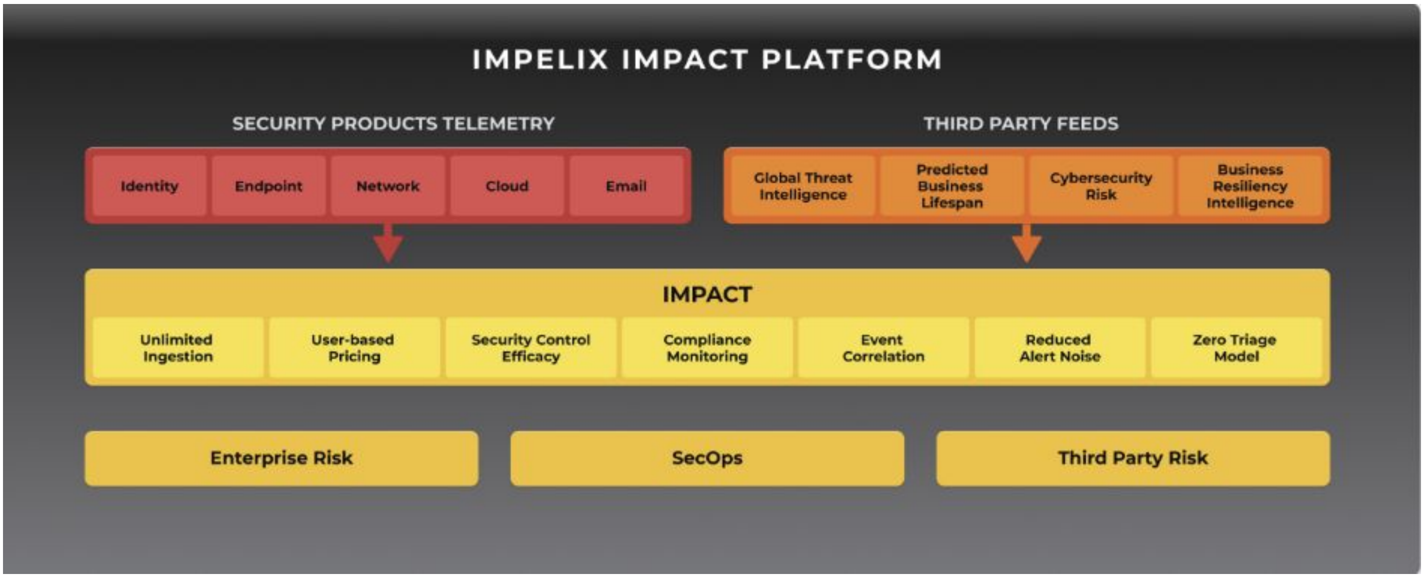
All of these aspects of the Impelix IMPACT platform can provide enhanced protection when combined with network flow data from Cubro Networks metadata generation platforms.

Overview of Impelix IMPACT

The Impelix IMPACT platform is a turnkey SaaS platform that enables teams to understand their security posture and implement a continuous improvement program using real-time data on cyber readiness and risk, compliance readiness, and tool, staff, and resource efficacy (including ROI, operational efficiency, and third-party risk).

While the security team tracks the current threat landscape and responds to ongoing breach attempts, the risk team can continually monitor compliance status and deliver incremental, continuous improvements to the security posture of the organization.

Traditional SIEMs require security analysts to do a lot of the heavy lifting. Associating internal events to external threats, building parsers to ingest data and normalize objects for corroboration, and investigating and remediating breaches, are manual tasks that require time and skill, both in high demand. The Impelix IMPACT platforms provides a way to automate these processes and simplify the efforts of enterprise staff.



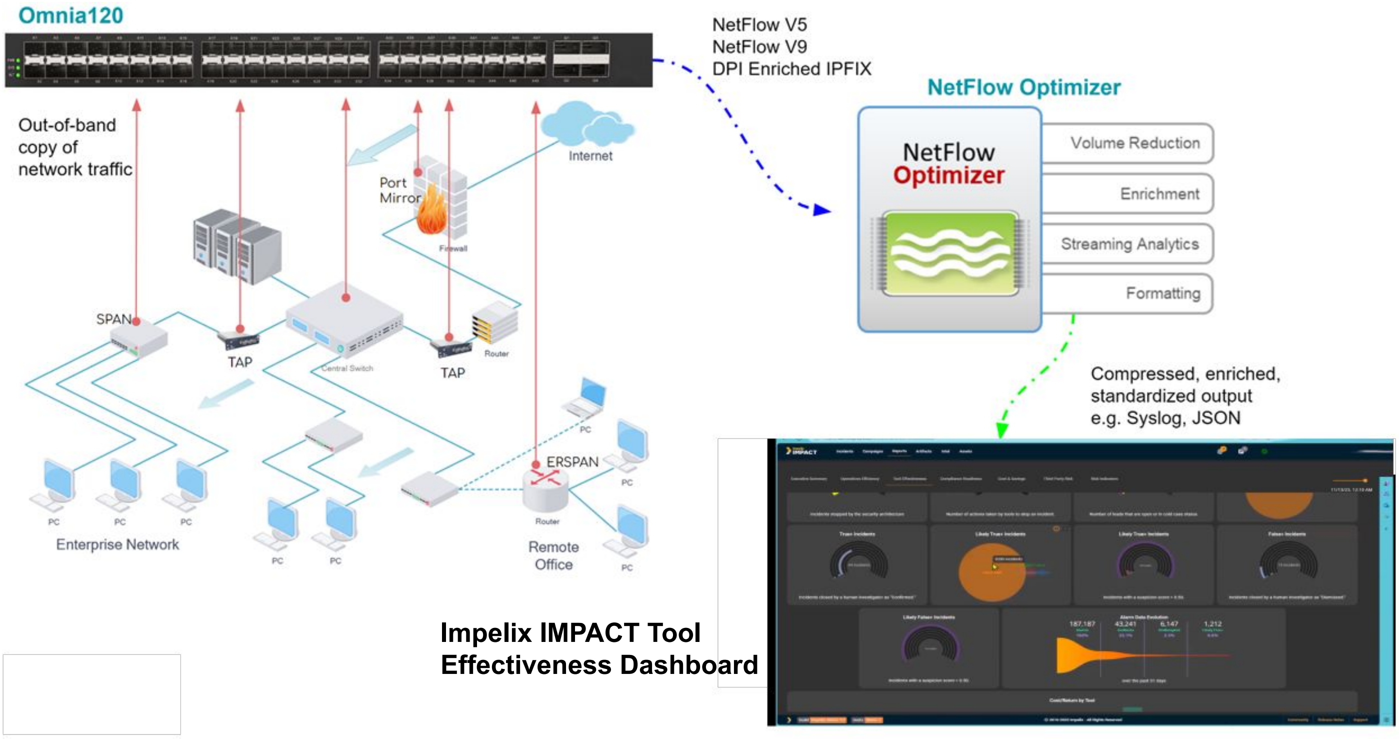
To understand the complex relationships between thousands of entities across the LAN, WAN, datacenter and cloud, organizations need not only all of their security data, but also all of the non-security logs for the critical telemetry data they provide. This combination of data sources is critical for understanding the complex relationships between assets and the blast radius of an attack as it spreads across the enterprise.

The Impelix IMPACT predictable user-based pricing model with unlimited ingestion means that the included application flow metadata provided by the Cubro Network Visibility infrastructure is now extremely cost-effective. Adding network flow data to the telemetry feeds already ingested by IMPACT provides the ability to identify important threats that other security tools might often miss: Data exfiltration and intellectual property theft, the establishment of command and control networks for Distributed Denial of Service attacks, as well as baseline users and entity behaviour analytics.

Adding flow analytics to Impelix IMPACT is straightforward. Cubro network TAPs passively copy network traffic that is fed to Cubro Omnia-line of Packet Brokers. The traffic is analyzed in the Omnia platform with Cubro's advanced Deep Packet Inspection engine indicating which specific application are being used on the network.

The Omnia Packet Broker generates industry standard IPFIX metadata - enriched with application data from the Deep Packet Inspection. Before sending to the Impelix IMPACT platform, the IPFIX metadata is sent to Netflow Optimization software, where the metadata is further enriched with end-user names an other network information such as geo-location or domain names.

Although Impelix IMPACT supports unlimited ingestion with user-based pricing, network meta-data must be transported, and is often stored for historical requirements. The Netflow optimizer compresses the IPFIX data with at least a 10:1 ratio, and delivers the results to Impelix IMPACT via JSON or SYSLOG, typical of usual SIEM telemetry.



Impelix IMPACT Tool Effectiveness Dashboard

Some enterprises might be tempted to use existing routers as SPAN ports to capture network flow data. Many of these devices are also capable of generating Netflow metadata. However, these tasks are the lowest priority for these devices, and simply stop functioning when the infrastructure gets busy. For example, during a security breach! Just when you need the data most, it is not available. This is why it doesn't make sense to base the foundation of security tools on this best effort collection approach.

Let Cubro and Impelix show you how your enterprise can move past the limits, noise, cost, and complexity of legacy SIEMs. We helps organizations stay ahead of the ever-changing regulatory landscape, proactively identify and mitigate risks, and ensure compliance with industry standards.

Cubro Network Visibility
EMEA USA APAC
support@cubro.com