Gigamon and vArmour Enable Application Relationship Management to Protect Cloud-Connected Enterprises

THE CHALLENGE

To effectively secure assets, InfoSec teams need to have complete visibility over their physical, virtual, and cloud environments. Considering the potential connectivity of any individual service – whether it is web services or fully outsourced application stacks – understanding application relationships is vital to effectively enable security in the modern enterprise.

THE SOLUTION

The vArmour partnership with Gigamon brings rich new telemetry and insights into the vArmour Relationship Graph, enriching the reach of application visibility and control of applications across the Enterprise.

JOINT SOLUTION BENEFITS

+ Centralized interface to visualize, configure, direct and control traffic from any network.
+ Contextualized visibility of an application across and within the connected enterprise.
+ Multi-level telemetry processing to build a holistic picture of application risk exposure and compliance scope.
+ Bi-directional information to gain context of the wider environment.
+ Metadata and application relationships to enable consistent policy enforcement.

Introduction

In order to understand and secure applications, particularly during cloud migrations, security teams must be able to visualize and control what is happening within their environments. They must also be able to understand how applications are behaving, otherwise teams cannot respond to attacks quickly and effectively due to a lack of visibility and context. For organizations implementing a Zero Trust security model, both operations and information security teams require consistent system and network visibility, and consistent enforcement of controls across both on-premises and cloud environments.

The Gigamon + vArmour Joint Solution

Deployed as a combined solution, vArmour and Gigamon enable both operations and information security teams to operate, detect and respond, and optimize their application environments for minimized risk. vArmour easily integrates with and leverages the Gigamon portfolio without requiring the deployment of any endpoint agents.

EASY ACCESS TO TRAFFIC FROM PHYSICAL NETWORKS

The Gigamon Deep Observability Pipeline for hybrid cloud enables traffic from across the network to be managed and delivered to tools efficiently and in the format they need.

With the Gigamon Deep Observability Pipeline and vArmour Application Controller working together, cloud operations and information security teams are able to visualize critical application relationships within any network, depicting communication and data behaviors. Providing an operational and security context, those teams are able to take action — modifying network policies or hardening specific systems from attack.

Moreover, by providing visibility into application dataflows — literally seeing the number of connections and data volumes passing between all services and systems within the application — teams can assess access, data processing, and storage requirements for both performance and security. Finally, having an application context overlaid on a network topology enables DevOps teams to proactively address performance or overhead bottlenecks.

KEY GIGAMON FEATURES THAT ENHANCE VARMOUR INCLUDE:

+ **Easy access to traffic from virtual networks? VMware/OpenStack/AWS/Azure**
  East-West data center traffic is growing increasingly fast. The Gigamon Deep Observability Pipeline is able to tap this traffic and incorporate it into the deep observability pipeline for delivery to the tools you are using on the physical network — ensuring all traffic can be monitored and analyzed together, avoiding blind spots, increasing the likelihood of spotting suspicious behavior, and removing the need to learn a new set of tooling for virtual environments.
+ **Accelerated Detection and Response**
  Visualization enables pinpoint detection of lateral movement, malware propagation, command and control (C2) communications, and/or suspicious shadow IT activity for a faster time to respond — either through attack forensics, or immediate isolation or containment of threats.
+ **Ease of Deployment and Easy Scalability**
  Provides coverage and scalability for even the most disparate networks, collecting environmental data and enforcing environmental policies without the use of agents.
+ **Filtering traffic to only send relevant traffic to tools**
  There's no point loading a tool with traffic. It will only drop after identifying it (such as database traffic going to a WAF). The Gigamon Deep Observability Pipeline can be configured to only send relevant traffic — or relevant sessions — to the connected tools.
+ **Load balancing to spread traffic across multiple devices**
  When traffic flows are larger than a single tool can cope with, the Gigamon Deep Observability Pipeline can be used to distribute the flows across multiple tools, while ensuring each session's packets are kept together and tool instances can be incrementally grown, as necessary, by adding new devices to those already connected.
+ **Aggregation to cover asymmetric routing and LAG**
  The Gigamon Deep Observability Pipeline can aggregate these together before sending them to the tool in order to minimize the number of ports that need to be used on the tool, but more importantly, most monitoring and security tools require all the packets in a session to be inspected by the same tool instance, otherwise incomplete sessions risk getting blocked or uninspected. The Gigamon Deep Observability Pipeline provides an intelligent and efficient way to ensure this happens in most architectures. By tagging the traffic, the Gigamon Deep Observability Pipeline ensures the source of traffic can be identified.
+ **Flow/metadata (NetFlow/IPFIX/CEF) generation to be consumed by tools**
  The Gigamon Deep Observability Pipeline can generate unsampled Layer 2 to 4 NetFlow/IPFIX metadata for any traffic flow. In addition to Layer 2 to 4 flow data, the Gigamon Deep Observability Pipeline can also generate extended metadata records for things like HTTP response codes and DNS queries, selectable from over 5,000 attributes across over 3,000 applications — this extended metadata can be used to provide very detailed contextual analysis when looking at network and security events.
+ **Resilience of solution (inline bypass and/or GRIP)**
  Deploy security devices inline and use the Gigamon Deep Observability Pipeline Inline Bypass functionality to provide physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure or malfunction. Or even selectively block traffic flows based on user configuration or automation from security applications.
+ **SSL decryption**
  The Gigamon Deep Observability Pipeline can be used to decrypt SSL encrypted traffic, including TLS 1.3, for inspection by security tools and any other devices connected out of band.

+ **Header stripping for effectiveness**
  If the connected tool doesn't want nor need to see specific protocol headers within the packet, the Gigamon Deep Observability Pipeline can remove them before sending the packet on to the tool for processing. This reduces load on the device since it doesn't need to parse over these protocols and increases its effectiveness if it doesn't recognize these protocols.

+ **Packet or Flow Slicing for efficiency**
  If the connected tool doesn't need to see the body information within the packet, the Gigamon Deep Observability Pipeline can remove it before sending the packet on to the tool for processing. This can be done on a packet-by-packet basis, or on a flow basis where the leading packets in a flow are forwarded intact and trailing packets are either sliced or dropped. This reduces load on the device and increases its efficiency without impacting its effectiveness.

+ **Masking for security/compliance**
  Certain industries and certain information have to be handled carefully (for example, credit card numbers in ecommerce or patient identification in healthcare records). The Gigamon Deep Observability Pipeline can be used to mask any sensitive data within packets before they are sent to other tools where they may be seen by operators or others.

  The combined Gigamon and vArmour approach effectively ensures compliance with regulatory or certification requirements through security monitoring and consistent access control of all 'in-scope' systems.

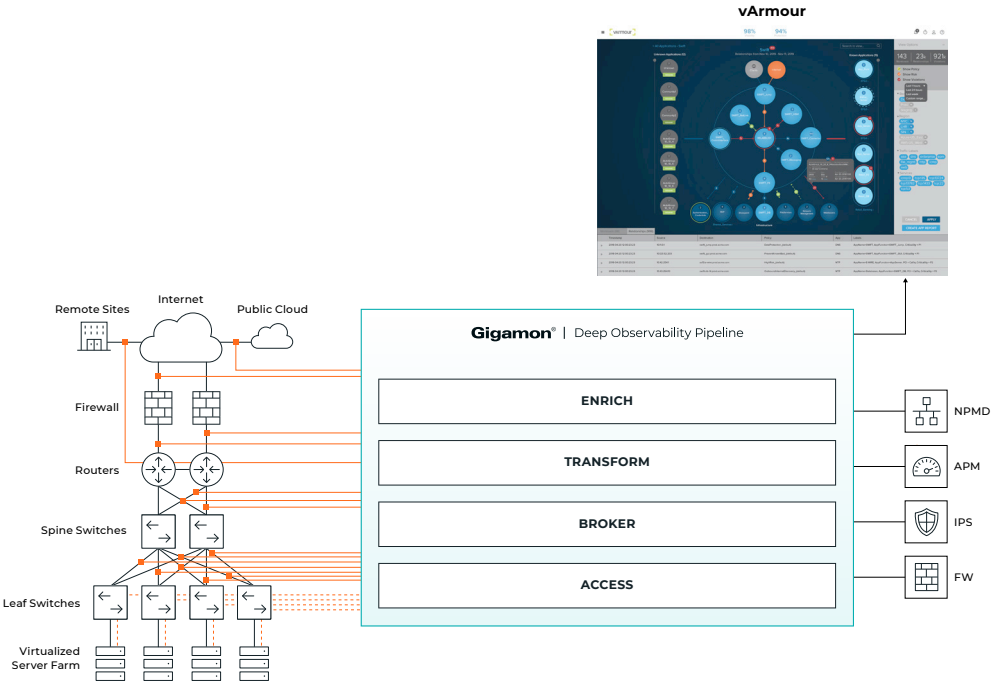
+ **Adhere to regulatory standards**
  Provides the means to map application and network scope for regulated or certified operating environments. Secondarily, this visibility enables the definition and enforcement of access control, security and performance monitoring, and endpoint security controls within a cloud connected network. It also allows compliance with privacy laws by selective policies to not decrypt certain flows or to mask out specific data.

+ **De-duplication**
  Pervasive visibility means that you will be tapping or copying traffic from multiple points in the network, which, in turn, means you are very likely to see the same packet more than once. To avoid the unnecessary overhead on your tool backhaul feeds and on your tools' processing the same network packets more than once, the Gigamon Deep Observability Pipeline has a highly effective de-duplication engine to remove these duplicates before they consume resources.

+ **Flow sampling**
  The Gigamon Deep Observability Pipeline, with its FlowVUE™ feature, can forward a user-defined sample (percentage, forward-list) of flows to the tool, which provides a reduction in total traffic load whilst maintaining visibility across the extent of traffic.

+ **Application-aware visibility**
  With Application Filtering Intelligence, the Gigamon Deep Observability Pipeline can identify and filter traffic based on application, for over 3,000 unique applications, which enables intelligent prioritization of applications for tool processing.

  - Application-aware visibility across the estate provides clear visibility into application relationships and network behavior between connected environments, without the use of agents and across multiple cloud environments.
  - Application Intelligence: Provides both the ability to track application traffic, flag shadow IT activities and rogue apps on the network, and to re-route application traffic through appropriate security channels and tools. Enables both operations and information security to secure applications without compromising the user experience.
  - Application discovery with telemetry: Provides multi-level telemetry using Application Controller — building a holistic picture of application connectivity, server/workload configurations, and communication patterns within non-Gigamon monitored environments.
  - The Gigamon Deep Observability Pipeline and vArmour Application Controller enables contextualization of critical applications to enable a Zero Trust security model. Provided with that context, security and/or network operations team response times can be reduced — fine tuning notifications based on relevant application indicators — whether for security or performance. With this combined solution, enabling consistent delivery of clear, concise, and accurate application allows for rapid detection of potential cyberattacks.



+ **Subscriber-aware visibility**
  The Gigamon Deep Observability Pipeline also offers 5G correlation, GTP correlation, SIP and RTP correlation capabilities that enable intelligent prioritization of subscriber or user traffic for tool processing. 5G and GTP correlation is mainly for mobile service provider customers, but SIP and RTP correlation was developed for a broad range of enterprise and service provider customers.

About vArmour

vArmour is the leading provider of application relationship management. Enterprises around the world rely on vArmour to control operational risk, increase application resiliency and secure hybrid clouds — all while leveraging the technology they already own without adding costly new agents or infrastructure. Based in Los Altos, California, the company was founded in 2011 and is backed by top investors including Highland Capital Partners, AllegisCyber, Redline Capital, Citi Ventures, and Telstra.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

For more information on Gigamon and vArmour solutions visit: gigamon.com and varmour.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com