Product Brief
Visibility Platform for Microsoft Azure

Introduction
As enterprises move to the public cloud to take advantage of scale, elasticity, and availability, cloud architects and enterprise decision makers need to recognize the security expectations on the enterprise. Specifically, infrastructure-as-a-service (IaaS) cloud providers operate under a “shared responsibility” model – the cloud provider is responsible for security of the cloud, i.e. of the cloud infrastructure whereas the IaaS customer is responsible for security in the cloud, i.e. of the data and applications.

Based on the shared responsibility model, security of the data and applications, along with organizational/regulatory compliance, rests on IT/cloud and security architects, who must ensure that applications and workloads are being deployed securely by everyone within the organization. Enterprises who migrate to the cloud typically rely on techniques like workload security, perimeter security, prevention-only solutions, and reliance on identity and access management to mitigate security risks. Today’s threat landscape means that prevention only security techniques are insufficient; they need to be complemented with additional detection and response techniques to detect early signs of security anomalies and deviations from expected behavior. For this to happen, organizations need to have accurate visibility into virtual machine network traffic to implement a multi-tiered security model. Without such visibility, the move of mission-critical applications to the cloud would be stunted.

Key Considerations for IT/Cloud and Security Architects
IT/Cloud and security architects responsible for charting a cloud strategy for their enterprise must address the following questions before they can successfully deploy mission-critical applications in a IaaS public cloud such as Microsoft Azure:

• As part of the shared responsibility model, how do we assure that Azure is being used securely by everyone in our enterprise?
• How do we run more mission-critical apps on Azure while meeting the needs for applying compliance and security controls?
• If zero-day security vulnerabilities are exploited in software that is yet to be patched, what backstops do we have to detect them?
• How do we detect and respond to security or network anomalies while deploying applications on Azure?
• How do we extend our enterprise security posture to workloads running in Azure?
• What methods do we have to detect deviations from organization’s cloud usage policy in real-time?

Failure to comprehensively address these considerations prevents or slows down the migration of mission-critical applications to the cloud, and leaves an organization vulnerable to potential security breaches, with severe consequences to reputation and brand. Thus, a well-defined cloud security architecture that accelerates application migration to the cloud is essential.

The Solution
The Gigamon Visibility Platform for Microsoft Azure is a cloud-native network traffic visibility solution that enables enterprises to extend their security posture to Azure, assuring compliance and accelerating the time to detect threats to mission-critical applications. With this solution, organizations can:

- **Reduce risk** by leveraging a common Visibility Platform across their entire IT environment
- **Ensure SLAs** due to tight integration with Azure APIs and Azure Monitor to automatically detect changes in Azure virtual networks (VNets)
- **Increase ROI** by reusing existing network security tools in hybrid cloud deployments
- **Lower costs** by leveraging traffic intelligence to deliver just the right traffic to the right tools

The solution consists of three key components:
- Traffic acquisition using G-vTAP agents
- Traffic aggregation, intelligence and distribution using GigaVUE® V Series
- Orchestration and management using GigaVUE-FM

For traffic acquisition, the solution leverages G-vTAP agents, which are deployed on each virtual machine (VM) and mirror traffic to be sent to the GigaVUE V Series. These lightweight agents minimize the impact of agent overload as only one agent needs to be deployed per VM. Application downtime is also reduced as there is no need to redesign applications when adding new tools that require visibility to network traffic, as agents scale out along with the applications.

Traffic aggregation, intelligence and distribution occurs within the GigaVUE V Series visibility nodes that sit within the visibility tier (see Figure). These visibility nodes aggregate, select, optimize and distribute traffic to tools located anywhere in the IT environment, be it in Azure, a different public cloud or on-premises. Using patented Automatic Target Selection, traffic of interest can be automatically extracted anywhere in the
infrastructure without the need to explicitly specify target VMs. Flow Mapping® policies allow for the selection of Layer 2 through Layer 4 traffic of interest. Example policies that could be set up using Flow Mapping, include selection of IPv4 and IPv6 traffic, TCP/UDP ports, protocols and more. Advanced policies, including overlapping rules and nested conditions can be created to distribute this traffic to different tools that may require different subsets of traffic. This traffic can be further optimized by applying GigaSMART® intelligence to slice, sample, and mask packets to reduce tool overload. The GigaVUE V Series enables elastic scale with the ability to automatically scale based on load and without a performance penalty.

Centralized orchestration and management of the entire Visibility Platform is done by GigaVUE-FM. Tight integration with Azure APIs enables GigaVUE-FM to detect VM changes in the Azure virtual network (VNet), and automatically adjust the visibility tier. GigaVUE-FM publishes open REST APIs, which can be used to integrate with third-party systems, with tools to dynamically adjust traffic received or to orchestrate new traffic policies. A drag-and-drop intuitive user interface on GigaVUE-FM enables operators to autodiscover and visualize end-to-end topology of the visibility tier and VMs and VNets.

**Conclusion**

Whether already in Azure or considering a future migration to Azure, the Gigamon Visibility Platform provides intelligent network traffic visibility for mission critical workloads. Enterprises can obtain complete network traffic visibility into virtual machines, an essential requirement for building multi-tiered security stacks. The platform integrates with Azure APIs and deploys a visibility tier in all virtual networks (VNets) that collects aggregated traffic and applies advanced intelligence prior to sending selected traffic to security tools. With this platform, organizations can obtain consistent visibility into their infrastructure across both Azure and their on-premises environment and extend their security posture to Azure.

To learn more visit [www.gigamon.com/azure](http://www.gigamon.com/azure).