Solve Challenging Cloud Use Cases with Gigamon

GigaVUE Cloud Suite Provides Visibility, Eases Migrations and Enhances Security with Superior ROI

Gigamon®

Overview

Organizations are migrating existing and new applications to hybrid clouds. They scale their cloud deployments with more servers and VMs, disperse and relocate compute nodes, leverage micro-segmentation and elasticity of containers, as well as routinely add and upgrade monitoring and security tools. While on-premises topologies benefit from network packet brokers (NPB), cloud infrastructure and tool vendors do not offer most of this functionality.

Administrators are forced to rely on built-in traffic mirroring services or elaborate tool-specific agents to acquire and send raw packets directly to their security and monitoring tools. The result is complex network designs, excessive bandwidth usage, tool contention for traffic access, overwhelmed tools that lose effectiveness, and needless scaling. IT is limited in their ability to analyze network traffic, customer experience, and application/flow information and have difficulties evaluating infrastructure and application health. Challenges faced include:

+ Obtaining packet and content visibility for East-West traffic, such as between VMs or VMs and containers; or from VMs and containers to platform as a service (PaaS), cloud-native services, and serverless computing
+ Safeguarding security of the apps and data
+ Offloading irrelevant traffic and costly pre-processing from security and monitoring tools, preventing needless scaling
+ Guaranteeing automation of raw packet acquisition via orchestration playbooks
+ Ensuring compliance with privacy regulations and sensitive data policies
+ Generating NetFlow and advanced metadata attributes with fidelity and without impacting network performance
+ Consolidating traffic and eliminating duplicated data flows to minimize processing and storage costs
+ Backhauling traffic when security and/or monitoring tools are on-premises or physical server-based

For IT, cloud, and security architects who face these challenges and must ensure an effective security and network posture in the hybrid cloud, the GigaVUE Cloud Suite™, part of the Gigamon Hawk Visibility and Analytics Fabric™ (VAF), is the solution. Gigamon provides an intelligent network traffic visibility platform that automatically acquires, optimizes and distributes selected traffic to various on-premises and cloud-based tools — increasing security, enabling operational efficiency, and giving the ability to scale across multiple zones and clouds. This enables enterprises to extend their security methods to infrastructure as a service (IaaS)

while assuring compliance and decreasing the time required to detect threats to mission-critical applications.

Companies no longer have to settle for less. Today, IT often implicitly assumes that the cloud may not be ready for mission-critical applications and runs those on-premises. They expensively backhaul all cloud traffic to on-premises tools. And they accept the incompleteness of NetFlow metrics and suffer from reduced network efficiency and traffic insights. Gigamon helps resolve many use cases involving visibility, security, and deployment — all with a cost-effective approach.

Comprehensive Visibility

VISUALIZE ALL CLOUD WORKLOAD TRAFFIC

To prevent blind spots and ensure proper security and performance, the tools responsible for these critical tasks must have access to all network packets and application data, including East-West, between individual VMs on monitored servers, and within container pods on worker nodes. Log data, such as from VPC Flow Logs, is insufficient for content inspection and unreliable as the source of truth because packet payloads are not included.

Obtaining packet-level details is critical, as malware hides in packets; logs do not convey much of what security tools require. Similarly, IaaS vendor offerings, including AWS CloudWatch and Azure Network Watcher, offer the ability to trigger packet capture on specific events, but this is primarily for troubleshooting and is reactive. Mirroring this traffic requires ultra-granularity involving internal and customer-facing applications and workloads in development, test, and production environments.

Granularity also has a temporal component. Although certain monitoring capabilities are provided by IaaS vendors, obtaining information at near real-time levels can be costly. Their approach tends to obtain data at intervals involving minutes, not seconds. One Gigamon customer said they were initially going to use a major cloud provider's information, which is available only at five-minute increments; while this is sufficient for most security and cloud teams, the customer wanted more granularity. Upon further analysis, sub-five-minute intervals were not adequate and would be prohibitively expensive.

THE GIGAMON CLOUD SOLUTION

GigaVUE Cloud Suite provides full visibility through virtual TAP functions for VMs (G-vTAP™ Module) and containers (G-vTAP Container) for acquiring traffic to/from each workload you wish to monitor; the former are instantiated on each monitored VM-resident workload; the latter are containerized and instantiated on each monitored worker node running on Docker with Kubernetes orchestration.

A key element of Cloud Suite is its packet brokering function (GigaVUE V Series), also instantiated within each virtual host environment — whether VM- or container-based. GigaVUE V Series offers a range of traffic processing capabilities for aggregating, replicating, optimizing, and distributing the acquired traffic to monitoring and security tools. Traffic can also be acquired using native built-in traffic mirroring services.

A large worldwide financial conglomerate used Cloud Suite to acquire and aggregate all East-West flows and forward to an enterprise event streaming services platform and then onward to various tools. They noted the need for unlimited visibility, otherwise admins would have more of a "black box," making troubleshooting difficult.

MULTI-CLOUD VENDOR DEPLOYMENTS

Surveys have routinely shown organizations prefer to use multiple public cloud vendors in addition to their on-premises or private cloud infrastructure. For example, Flexera revealed that over 90 percent of enterprises have a multi-cloud strategy and utilize an average of 2.6 public cloud vendors.[1] They take this approach to prevent vendor lock-in, ensure service redundancy, and take advantage of best-of-breed solutions.

One challenge is how to address multi-cloud deployments for complete oversight. IT has typically used the native tools as much as possible, but if they are, for example, in three clouds, they need to bounce from dashboard to dashboard to

conduct investigations. Such complexity is the enemy of security. This method doesn't scale, and organizations can miss breaches.

Gigamon GigaVUE-FM fabric manager is the overarching network packet broker management solution that works with various clouds simultaneously. Whether using a combination of multiple AWS VPCs, Azure VNets, or GCP VPCs, the FM console provides a unified dashboard from a central site with details of all acquired traffic. With Fabric Health Analytics, numerous health and other statistics can be obtained.

A Gigamon customer that provides loyalty and marketing services with over 20,000 employees has a hybrid deployment with on-premises, AWS, and Azure. The company used Cloud Suite to acquire, aggregate, and tunnel large volumes of traffic from public cloud workloads to a primary datacenter. This provided visibility for network and security tools that was previously unavailable. The outcome included reducing MTTR for identifying root causes from weeks to hours, eliminating a $350,000 packet capture device, and maintaining operations online to process credit card transactions.

ENSURE INTER-VPC/INTRACLOUD VISIBILITY

Large organizations can potentially establish thousands of virtual private clouds in AWS. In these scenarios, a network hub called transit gateways interconnects these VPCs and on-premises networks. This simplifies the network and puts an end to complex peering relationships. With transit gateways acting as a cloud router, each new connection is only made once. As the infrastructure expands globally, inter-region peering connects these gateways together. Benefits include simplified connectivity, superior visibility and control, improved security, and flexible multicasting. Users can even connect SD-WAN devices.

Yet these gateways are complex infrastructure elements that involve transit gateway maximum transmission units, routing tables, and route propagation aspects. Cloud Suite fully supports AWS transit gateways to ensure visibility across interconnected VPCs and on-premises tools.

One large North American enterprise that markets and distributes food, kitchen equipment, and other products to restaurants, healthcare, and educational institutions used more than 1,000 VPCs. They were concerned with the use of packet capture methods due to cost, complexity, and transit gateway support at scale. The business turned to Gigamon because our visibility platform works across VPCs where tools don't need to be in the same zone as the applications. Tools can even remain on-premises.

Cloud Suite can backhaul data to on-premises tools. And since pricing is based on volumes of traffic consumed rather than the number of VPCs, agents, visibility nodes, or centralized traffic management instances, it is highly cost-effective.

GENERATION OF NETFLOW IN THE CLOUD

Obtaining flow or metadata in the public cloud is difficult at best, and the nature of the attributes

available is limited. Cloud infrastructure vendors only offer NetFlow (v5 and v9) and IPFIX (up to Layer 4 only). While this metadata generation is better than the flow logs users get from IaaS solutions, and customers can extract more data and have more visibility with their use, they are not sufficient to solve, quickly troubleshoot, and remediate application and network performance issues.

GigaVUE Cloud Suite provides complete, unsampled NetFlow data. It generates advanced metadata that covers Layers 3–7, yielding rich application and protocol attributes that third-party application performance monitoring (APM) and network performance monitoring and diagnostics (NPMD) tools, such as New Relic and Datadog, use to solve a myriad of problems. We have worked closely with these vendors to ensure straightforward interoperability. Customers routinely state that these tools from cloud infrastructure vendors are insufficient, especially for networking issues. They have found Cloud Suite overcomes this inadequacy.

A major North American organization providing workers' compensation services is moving fully to Azure and transitioning all resources and apps to that cloud. This will allow it to consolidate two security zones (one on-premises and one in the cloud) and eliminate an extra set of tools IT would otherwise need to manage. They use basic VAF features to acquire, aggregate, and send traffic to Snort/Bro. Our advanced NetFlow generation capability sends full unsampled flow data to an on-premises NetFlow collector where APM and NPMD tools are located; these will soon move to the cloud too.

In the process of migrating a critical customer-facing internet banking application to AWS, a large Latin American financial institution observed the application failed to work properly. End customers could not access it and IT could not locate the cause, impacting business operations. The bank used a network performance monitoring solution that quickly determined the problem and resolved the issue. It deployed Cloud Suite with traffic acquisition and optimized traffic processing, along with NetFlow generation, and sent the traffic and data to Viavi appliances hosted in the cloud for NPM.

Ensuring Security and Compliance

SECURING CONFIDENTIAL DATA TRANSMISSIONS

Confidentiality and compliance are crucial for a broad range of government and private organizations alike. Regulations in the financial, insurance, and healthcare industries require that sensitive data be protected. Penalties for non-compliance of such regulations can be severe, resulting in fines or even imprisonment. Masking payload content such as Social Security, bank account, or medical identifiers permanently obscures the data before sending it to security and monitoring tools and prevents them from being read by hackers. Regulatory and privacy compliance becomes easier because the sensitive data is never seen, processed, or stored by these tools.

The GigaSMART® Masking application supported on the GigaVUE Cloud Suite provides customizable data protection by overwriting specific packet fields with a set pattern, thereby safeguarding sensitive information during network analysis.

Other methods to protect data in motion include encrypting traffic in IPsec tunnels from the source via G-vTAP Modules and sending to a GigaVUE V Series virtual visibility node for data protection and integrity. For tools located outside the cloud, Gigamon works with AWS's Direct Connect and other cloud provider methods to support the backhauling of encrypted traffic.

ANOMALY DETECTION WITHOUT RAW TRAFFIC

CloudOps needs to identify and remediate advanced threats. Yet to do so requires more than basic network telemetry, but not full traffic for analytics based on packet data. Currently, IT does not generally consider network traffic to be useful for cloud-native workloads.

Legacy metadata is limited to NetFlow v5/v9/IPFIX with mostly Layer 2–4 attributes, which provides some details on "who and what" but is insufficient to understand the "how and why" applications of user behavior. There is a broad consensus among CloudOps that while basic metadata is nice to have, enriched application workload telemetry at Layers 5–7 is paramount for superior detection and compliance auditing.

Gigamon provides application-aware metadata with the GigaSMART Application Metadata Intelligence (AMI) application, which generates and potentially feeds thousands of attributes to SIEM and other security tools to find numerous security shortcomings. For more specific AMI use cases, please refer to the AMI Use Case document.

A leading Brazilian bank needed to monitor traffic in AWS for security purposes. After migrating most workloads there, IT noticed a new blind spot. No security events based on network traffic were being generated in the cloud, which raised the concern of attacks going undetected at a time when privacy laws (LGPD) with heavy fines are being enacted. It used Gigamon for traffic acquisition, data reduction via flow mapping, and de-duplication, combined with advanced metadata feeding cloud-based tools; the bank also leveraged ThreatINSIGHT, which provides threat detection and response capabilities.

CLOAK INTERNAL RESOURCE IDENTIFICATION

Servers use countless naming structures that need to be opaque to the external environment or to various tools; otherwise, malicious actors can obtain keen insights on where resources reside and how they are structured, even identifying potential applications and their known vulnerabilities; all of which can be used to improve the success of hacking attempts. Tools do not necessarily need to know the actual ID of the traffic source. If the tool is a SaaS-based solution with multi-tenancy, then IT would likely want to hide these details.

To hide details from the outside world and give IT an extra layer of security, Gigamon header transformation processed on the V Series visibility node can be used to perform many simple operations on network packets. Here, you can modify any monitoring session link's packet header — such as by changing the source and destination MAC or IP addresses, port numbers, or VLAN IDs — to ensure security and segregation of sensitive information. This technique also

prevents the information from being exposed to monitoring tools.

Gigamon also enables tunnel IDs to be modified to allow the same packet to be securely sent to one endpoint destination that has multiple tool instances, each with different functions; in this case, each instance is listening on different virtual interfaces for a specified tunnel ID.

Flexibility and Ease of Deployment

SEND TRAFFIC TO BOTH ON-PREMISES AND CLOUD-LOCATED TOOLS

Most organizations with cloud-based operations are utilizing a hybrid model with both on-premises datacenters and public clouds. Drivers behind this include limited cloud-enabled tools, security concerns with cloud storage, and the expense associated with high-throughput cloud processing.

IT needs the ability to flexibly choose which tools and locations to use and select which traffic is seen by which tools. They want to reuse existing on-premises tools, as many cloud-based versions (particularly APM and NPMD) are not available, are not robust, or duplicate expenditures. To simplify operations, IT does not want separate tools for on-premises and cloud; visibility across environments is needed, preferably using the same toolset.

Gigamon provides common workload visibility in any location with virtual TAPs. For workload acquisition, users can flexibly choose between native traffic mirroring services, although relatively expensive, for more simplified operations or Gigamon G-vTAP Modules with added security and traffic filtering based on VM and port. Once the various sources are aggregated and optimized on GigaVUE V Series, the replicated traffic can be directed using flow mapping rules to cloud-based tools or backhauled to on-premises located tools. Gigamon reduces expensive backhauling data charges via various GigaSMART applications: De-duplication, Slicing, Adaptive Packet Filtering, and Application Filtering Intelligence.

Monitoring tools, regardless of their deployment, cannot always distinguish the traffic coming from multiple VPCs with the same subnet range. One way to overcome this is to use custom flow logs; for AWS, these provide subnet ID, VPC ID, and so on to distinguish VPC traffic. Gigamon takes this a step further; our header transforms enabled on GigaVUE V Series can simplify traffic distribution and indirectly improve security. CloudOps can add VLAN ID, VLAN priority, and DSCP bits to the header for distinguishing the traffic coming from multiple VPCs with the same subnet range. This helps ensure that traffic does not get transmitted to the wrong tools.

SUPPORT ANY CLOUD MIGRATION STRATEGY

Many organizations are in the process of decommissioning datacenters and taking a cloud-first approach. There are several strategies for transitioning to cloud, including rehost, refactor, or rebuild (aka replatform), and infrastructure elements need to support all methods. Surveys have revealed that the majority of organizations go with rehosting (aka lift and shift), which is the least expensive (at least initially) and quickest way to migrate, with no bifurcation of the code base needed

Fewer operations choose to refactor, and an even smaller percentage undergo a "born in the cloud" migration, with a rebuild involving cloud-native architectures. The method used can vary by the vertical market involved; for instance, manufacturing and healthcare primarily choose rehosting, whereas finance and education tend to use refactoring. Nevertheless, in most cases they tend to take their time.

Gigamon is agnostic when it comes to which method should be chosen and supports all three. Multiple methods of traffic acquisition are available for flexible, simplified deployments for applications moved to the cloud: lightweight agents automatically instantiated and configured on any workload VM; embedded code in workload golden images; or cloud-native traffic mirroring (with or without an external network load balancer). With rebuilds, going cloud-native often means containerized apps.

Gigamon provides a container-based virtual TAP for acquisition where Kubernetes is used in conjunction with Flannel network overlays or Calico interfaces, which are extremely useful for the ephemeral nature of containers. The visibility nodes and GigaVUE-FM can be deployed in support of any or all such cloud migrations.

MULTIPLE TOOL SUPPORT

Many organizations use a plethora of tools for both monitoring and security. Yet a considerable number of APM/NPMD solutions are not available on the various marketplaces. While most leading third-party security tools are available in the cloud, existing IaaS-provided security solutions are extremely limited and are not necessarily best of breed. Vendors primarily offer identity and access management (IAM), security groups, logs, and web application firewalls (WAF). However, these each have restrictions:

+ IAM: Once an attacker has successfully hacked credentials, they won't need to undertake noticeable activity that gets alerted. The time to detection can be weeks or months
+ Security groups: Despite allowing access to only necessary ports, security group configurations have no application context. Malware or data exfiltration can happen on those ports at Layer 7
+ Logs: These only convey metrics about conversations and application access; no packets are included. When silent attacks operate within limits of threshold violations, logs are of no help
+ WAF: Cloud-native WAFs have very limited functionality compared to industry leading WAFs and generally only provide out-of-the-box protection from the OWASP (Open Web Application Security Project) top ten attacks

Gigamon has validated its VAF with an extensive number of monitoring and security vendors for deployment in the cloud. Partners include NPMD (e.g., SevOne, Riverbed Networks), SIEM (e.g., Splunk, QRadar), AI-enhanced application performance monitoring (e.g., Dynatrace), endpoint security (e.g., Tanium, Fortinet), network detection and response (NDR) (ExtraHop), sandboxing (e.g., FireEye), and others. Refer to our Technology Partner site for a complete list — and don't forget integration and deployment with the Gigamon ThreatINSIGHT NDR.

Unlike existing traffic mirroring services, Gigamon can replicate and send each traffic source to an unlimited number of tools.

A large North American banking conglomerate deployed multiple tools in both public cloud and on-premises. Cloud-based tools included SIEM, enterprise firewall, policy management control, automation, protocol analysis, and NDR. On-premises tools involved DNS, directory services, and email. The customer turned to GigaVUE Cloud

Suite, recognizing the platform's ability to support multiple tools regardless of location. The ability to replicate and send the same packets to multiple selected tools, rather than using the native traffic mirroring methods, was a major deciding factor.

AUTOMATED SCALABILITY

It has been stated that cloud is not about building software — it's about operating it at scale. Infinite scalability is at the heart of public cloud's value, but it must be viable. With potentially tens of thousands of workloads, the constant addition of new or deletion of existing VMs, and workload movement within and across VPCs, automation is paramount. On top of this, dozens of tools and associated flow mappings must be managed in real time.

GigaVUE-FM seamlessly interoperates with automation and orchestration management suites from AWS CloudWatch, Azure Network Watcher, third-party vendors including Terraform, and open-source solutions such as Ansible to handle any size workload deployment. Virtual TAPs and visibility nodes are automatically instantiated, configured, and monitored.

As new workloads come online or relocate, GigaVUE-FM communicates via APIs to ensure comprehensive visibility in these dynamic environments. GigaVUE-FM works with these suites to automatically identify new and relocated workloads, instantiate and scale visibility nodes, and configure new traffic policies as needed. GigaVUE-FM provides a single-pane-of-glass network packet broker orchestration and management solution with visualization across any hybrid network.

A worldwide provider of multiplayer entertainment gaming platforms leveraged GigaVUE Cloud Suite to automatically manage the visibility of over 25,000 workload instances. Without automation, this would have been an impossible task with an error-prone and prohibitively expensive manual process.

Cost Effectiveness

SIMPLIFIED TRAFFIC ACQUISITION – PREVENT AGENT SPRAWL

Organizations often use numerous cloud-based tools. Between security, network monitoring and application performance solutions, it is not uncommon to have a dozen tools. For each of these to acquire traffic, the tools often install an agent on every workload. Such an approach adds a great deal of complexity and needless additional bandwidth usage. Automating the instantiation process of numerous instances on each VM is challenging.

When new VMs emerge, keeping them updated is a further difficulty. As the packets are sent from every workload to the various tools, CPU processing spikes as well. With just a few tools involved, their collective processing power can be excessive. Typically, agents each consume 2 to 5 percent of CPU cycles, and this adds up fast. If the instances involved have limited speeds and memory, a few agents alone can easily max out available CPU power, and more virtual NIC bandwidth will be required for each VM to send a copy to each tool.

With Gigamon, only one agent (G-vTAP) acting as the virtual TAP is needed, which can copy, apply basic filtering, and forward workload traffic to a visibility node. This single agent can displace all other tool-based agents and typically uses under 5 percent of the server compute cycles. As traffic is sent from the agent to the virtual visibility node (GigaVUE V Series) aggregation point, processed and forwarded to the tools as specified, the number of data connections and total network traffic flow decreases dramatically. Cloud architects look to collocate tools together. The Gigamon virtual TAP is capable of filtering traffic based on VM/port and allowed/denied IP addresses to further prevent superfluous flows.

HIGH-CAPACITY PROCESSING FOR DEMANDING WORKLOADS

Cloud network traffic levels can be extremely high for certain applications and large content-processing organizations. While fully virtualized cloud infrastructures lack dedicated, purpose-built hardware, they make up for it through automated and clustered servers with high VM or container density. Further, these environments offer advanced processing methods such as the Data Plane Development Kit (DPDK), which consists of libraries to accelerate packet processing workloads running on a wide variety of CPU architectures. Some packet-processing functions have been benchmarked up to hundreds of millions of frames per second, using 64-byte packets with a PCIe NIC.

A very large aeronautical engineering and manufacturing firm required the ability to support 10Gbps links carrying the AWS VPC traffic to and from the corporate internet and an internet gateway. It also needed to process 18Gpbs of traffic through the V Series function. Leveraging DPDK and the second-generation GigaVUE Cloud Suite, the company was able to handle these loads and obviate the need for multiple high capacity cores that would have been cost prohibitive. It also used increased filtering and traffic reduction capabilities available in this version. The Cloud Series components (V Series, vTAPs, and GigaVUE-FM) were automatically scaled as throughput demands dictated.

SUPPORT NATIVE TRAFFIC MIRRORING SERVICE AT SCALE

AWS VPC Traffic Mirroring provides the ability to dynamically copy and filter traffic from the elastic network interfaces of EC2 instances. These mirrored packets are then streamed using VXLAN-encapsulated tunnels to the GigaVUE V Series virtualized visibility nodes. VPC traffic mirroring provides the benefits previously mentioned as well as enhancing security via packet capture at the elastic network interface, which cannot be tampered with or disabled.

The issue arises when cloud processing charges are added in. The mirroring service has a limit of 10 to 100 sources per target, depending on instance type, and can become prohibitively expensive as compute instances mount with workload levels. GigaVUE Cloud Suite supports external network load balancers on AWS to provide essentially an unlimited number of VPC traffic sources that can target our V Series function; the algorithm used to

balance traffic is based on volume, not target count, to further minimize visibility node processing. The V Series function automatically scales with volume to improve efficiency and further minimize CPU demands.

A major North American retailer deployed several security tools and needed comprehensive visibility with the ability to separately send full packet flows to each appliance — automatically. They used AWS traffic mirroring to successfully obtain full insight into all workloads of interest. They could not, however, simultaneously direct VPC Traffic Mirroring-oriented traffic to multiple tools.

To solve the problem, the company turned to our GigaVUE Cloud Suite for AWS. All VPC Traffic Mirroring sources were properly aggregated by the V Series nodes, under the auspices of GigaVUE-FM, and traffic was properly forwarded to all the security tools. With Cloud Suite's deep integration into the AWS management suite, the customer leveraged their existing knowledge for a fast, efficient, automated deployment.

IMPROVED TOOL CAPACITY

As more tools of all types are deployed for security and monitoring and traffic levels continue to rise, they can face overwhelming processing demands. With business models typically involving volume-based pricing, having to manage all content from all workloads can be cost prohibitive with excessive scaling demands. To make matters worse, obtaining all VM visibility can lead to duplicated packets, potentially exceeding 40 percent of all traffic. Not all content is equal, either, and some payload data and flows can be ignored.

To improve tool effectiveness and accuracy while reducing traffic processing levels, scaling demands and cost, Gigamon provides a multitude of ways to offload the burden from tools. GigaSMART Packet De-duplication eliminates redundant packets. Packet Slicing enables IT to select and remove payload content starting from specified offsets within certain packets. Adaptive Packet Filtering (APF) provides basic app-level detection that identifies and filters any content in headers or payloads by searching for string patterns at specified offsets; APF even finds headers within complex encapsulation protocols, including GRE, IP-in-IP (IPv4 and IPv6), MPLS, and VXLAN. Header stripping can remove overhead for protocols such as GRE, MPLS, and VXLAN, as tools do not need this information. Application Filtering Intelligence (AFI), previously mentioned, provides the granular filtering, visualization, and selective traffic forwarding to the proper tools based on detection of applications. Read the AFI Use Case brief for more insights.

Conclusion

The holistic multi-cloud GigaVUE Cloud Suite resides completely in the cloud, overcoming VM and container visibility challenges and their ramifications for organizations making this transition. Cloud Suite is certified and available on the AWS and Azure Marketplaces, with full interoperability with their own and third-party orchestration management suites.

Our “Any Cloud” solution can be applied to other IaaS environments, including Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), and IBM Cloud. Cloud Suite provides a range of GigaSMART features that function exactly the same as on our physical GigaVUE HC Series hardware platforms, including AFI and AMI.

Key benefits include:

+ Improved tool capacity: Virtual security and monitoring tools are offloaded from burdensome tasks to improve effectiveness, reduce scaling needs, and minimize costs
+ Fully automated infrastructure: Automatically identify new and relocated workloads, instantiate and scale visibility nodes, and configure new traffic policies as needed
+ Application awareness: Automatically identify thousands of apps in real time, filter based on these, and selectively forward as appropriate with advanced metadata for contextual insights
+ Single-pane-of-glass: Provides centralized orchestration and management with a single-pane-of-glass visualization across any hybrid or multiple public cloud environment
+ Choice of traffic acquisition: Flexibly choose between cloud provider solution for more simplified operations or G-vTAPs with added security and filtering
+ Increased security: Visibility into East-West flows for both virtual machine and container-based apps enables identification and blocking of laterally spreading malware

References

1. Flexera 2021 State of the Cloud Report. Flexera, 2021. https://info.flexera.com/CM-REPORT-State-of-the-Cloud.

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate.

Gigamon has been awarded over 75 technology patents and enjoys industryleading customer satisfaction with more than 3,000 organizations, including 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally.

For the full story on how Gigamon can help you, please visit www.gigamon.com.

Gigamon®

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

01.22_02