JOINT SOLUTION BRIEF

End to End Prevention, Detection and Investigation for AWS

The Challenge

To secure your public cloud infrastructure network traffic must be inspected for known and unknown threats as it traverses the network and stored so that potential threats or known exploits that are discovered after the fact can be investigated and remediated.

Integrated Solution

FireEye Network Security applies state of the art, signatureless detection and protection against the most advanced threats, including zero-days. FireEye Network Forensics pairs the industry's fastest lossless network data capture and retrieval solution with centralized analysis and visualization. GigaVUE Cloud ensures you can use both to protect your public cloud infrastructure.

Joint Solution Benefits

- Pinpoint the data you need fast enough to make a difference
- Achieve continuous, lossless packet capture
- Detect threats others miss
- Respond to alerts that matter
- Mirror cloud network traffic to any tool that needs it

The combination of Network Security and Forensics products gives customers an incredibly powerful solution, providing end-to-end prevention, detection and investigation capabilities in a single platform. Network Security solutions inspect traffic and provides the alerting, Network Forensics products provide the data capture, investigation capabilities and even historical detection on previously captured traffic. The combination of these solutions ensure that organizations are safe from attacks as they happen, and as new attacks are discovered.

To protect networks, assets, data and users from known and unknown threats with confidence, organizations need a multi-vector defense. FireEye Network Security is a suite of products that provides advanced threat protection and investigative capabilities, wherever an organization's data resides – on-premise, in the datacenter, or even in the public cloud. Built on FireEye's proprietary detection engines and industry leading threat intelligence combined, advanced threat protection is delivered to the user regardless of form factor or location, giving organizations peace of mind regarding the security of their data.

When investigating alerts and incidents, analysts need to ensure they are looking all the data traversing the network. They need an investigation tool that provides rapid search capabilities, answering queries within minutes instead of days. FireEye Network Forensics provides a suite of tools that leverages extremely fast, loss-less packet capture in addition to an investigation console designed to get analysts the answers they need quickly. Used in conjunction with FireEye Network Security, organizations get to leverage FireEye's proprietary detection engines along with our industry-leading threat intelligence, all applied to any historical traffic.

To deploy both of these products in a public cloud infrastructure, both tools need to have access to copies of the network traffic and this is where the Gigamon platform excels. GigaVUE® Cloud is a cloud-native solution that acquires, optimizes and distributes selected traffic to security and monitoring tools. With the Gigamon solution, traffic can be fed to both FireEye Network Security and FireEye Network Forensics ensuring enterprises can extend their security posture to the public cloud and accelerate threat detection and investigation.

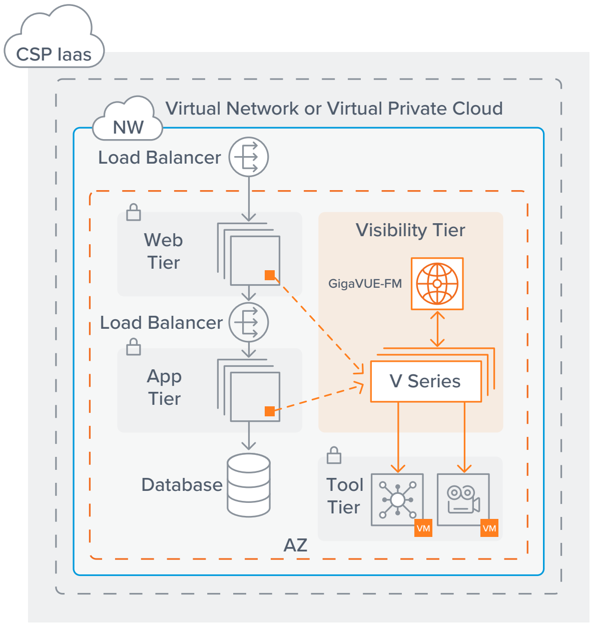

Figure 1: GIgaVUE Cloud uses AWS mirroring or a Gigamon agent to acquire and copy packet data to FireEye Network Security and Network Forensics.

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 8,200 customers across 103 countries, including more than 50 percent of the Forbes Global 2000.

About Gigamon

Gigamon delivers network visibility and analytics for digital applications and services across physical, virtual and cloud infrastructure enabling organizations to run fast, stay secure and innovate. Only Gigamon offers a full-stack solution with a common architecture across an organization's complex hybrid infrastructure to address performance and security needs. Since 2004, Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including over 80 percent of the Fortune 100 and the majority of the world's Top 10 banks, healthcare providers, technology companies, mobile operators and government agencies. Headquartered in Silicon Valley, Gigamon operates globally. For the full story on how Gigamon can help your organization, please visit www.gigamon.com.

For more information on Gigamon and FireEye solutions,
visit: www.gigamon.com and www.fireeye.com.

Gigamon®

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