Joint Solution Brief

Securing the Hybrid Enterprise

The Challenge

Perimeter-focused security architectures and controls have failed. Despite increasing investments in security, a new model is needed. The ever-growing use of virtualized infrastructure and the increase in targeted attacks mean enterprises need help detecting and responding to threats before they do damage to the business.

Integrated Solution

RSA NetWitness Suite is a network security monitoring and investigation platform that combines logs, network packets, NetFlow, and end-point visibility to detect, investigate, and take targeted action against even the most advanced of attacks. Gigamon's GigaSECURE® Security Delivery Platform provides complete access to the virtual traffic data RSA NetWitness Suite needs.

Joint Solution Benefits

- Detect APTs through lateral movement within East-West traffic even when it doesn't touch the physical network
- Full visibility of physical, virtual and public cloud traffic managed by a single console and correlated within one security tool
- Fully integrated with VMware vCenter, OpenStack/KVM and Amazon Web Services to extend visibility policies across the enterprise
- Automated migration of VM-level monitoring policies for continuous visibility during lateral VM migration
- Advanced filtering of any traffic using Adaptive Session Filtering
- Monitor and analyze unsampled NetFlow data generated by the GigaSECURE platform

Introduction

Despite increasing investments in security, breaches are still occurring at an alarming rate. Whether the result of cyber criminals sending phishing or malware attacks through company emails, nation states targeting organization's IP, or insiders misusing sensitive data, depending on preventing perimeter breaches has become ineffective. Successful attacks bypass each layer of prevention using valid user credentials, trusted access paths, or by exploiting unknown or unpatched vulnerabilities, thus going unnoticed by preventive controls.

In addition, with the introduction of network virtualization, enterprise IT organizations are facing a new challenge of securing IT infrastructure across both physical and virtual networks as well as those they choose to run in the public cloud. Just monitoring physical connections leaves you blind to a large and vital part of your infrastructure; using virtualized security tools within your datacenter often means the physical and virtual traffic cannot be correlated for analysis. A new approach is needed.

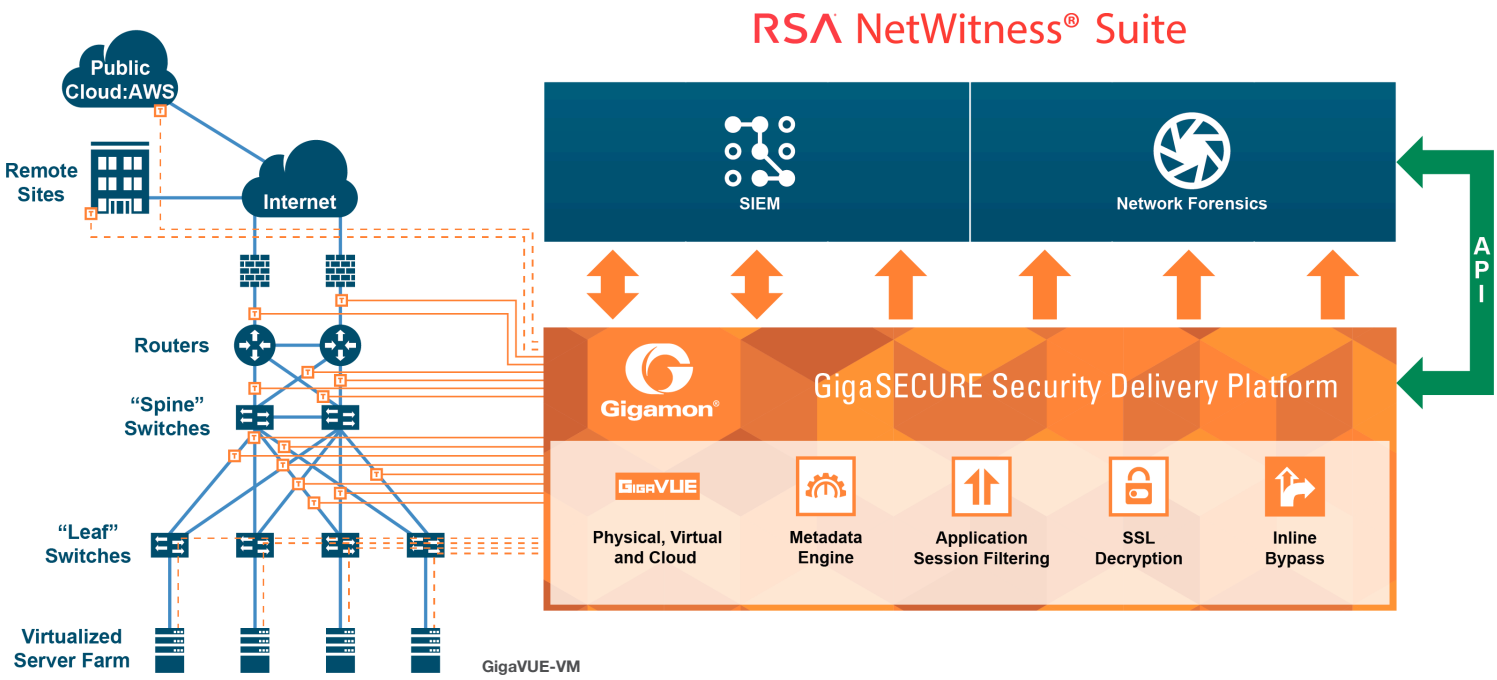
The Gigamon and RSA Joint Solution

Together RSA NetWitness Suite and the GigaSECURE Security Delivery Platform provide pervasive and intelligent visibility into the physical and virtual networks for OpenStack, VMware, including NSX, powered private clouds plus Amazon Web Services public clouds.

RSA NetWitness Suite provides a monitoring and investigation platform to detect advanced threats, while focusing on the most important incidents so security teams can rapidly investigate. It provides real-time collecting, filtering, enrichment and analysis of network packets, NetFlow, endpoint and log data via a highly configurable infrastructure.

Ensuring that RSA NetWitness Suite has access to the right virtual traffic and network metadata from all across the network is where GigaSECURE platform comes in. The platform consists of distributed physical (GigaVUE H Series platforms) and virtual (GigaVUE-VM) nodes that provide an advanced level of filtering intelligence, managed as a single fabric. At its heart is Gigamon's patented Flow Mapping® technology that identifies and directs incoming traffic to single or multiple tools based on user-defined rules.

The GigaVUE-VM solution delivers the same traffic identification, selection and direction capabilities as exists on Gigamon's physical nodes. This enables RSA NetWitness to establish visibility to virtual network traffic within the hypervisor/VPC or across multiple hypervisors/VPCs. The GigaSECURE platform is able to detect workloads moving hosts and automatically maintain continuous visibility.



This combination is an ideal solution for organizations interested in enabling their IT organization to investigate what was targeted, how the exploit occurred, how the attacker moved laterally and the magnitude of the attack – across physical and virtual infrastructures.

Learn More

For more information on the RSA and Gigamon solution, contact:

RSA
www.rsa.com

Gigamon®
www.gigamon.com

3171-03 11/16

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