RSA

Gigamon

Secure It: Best Practices for Securing, Analyzing, & Mitigating Threats to AWS Applications

Presented by Gigamon and RSA

Greg Mayfield
Sr. Director, Product Marketing

Mike Gallegos
Product Manager, RSA NetWitness Suite

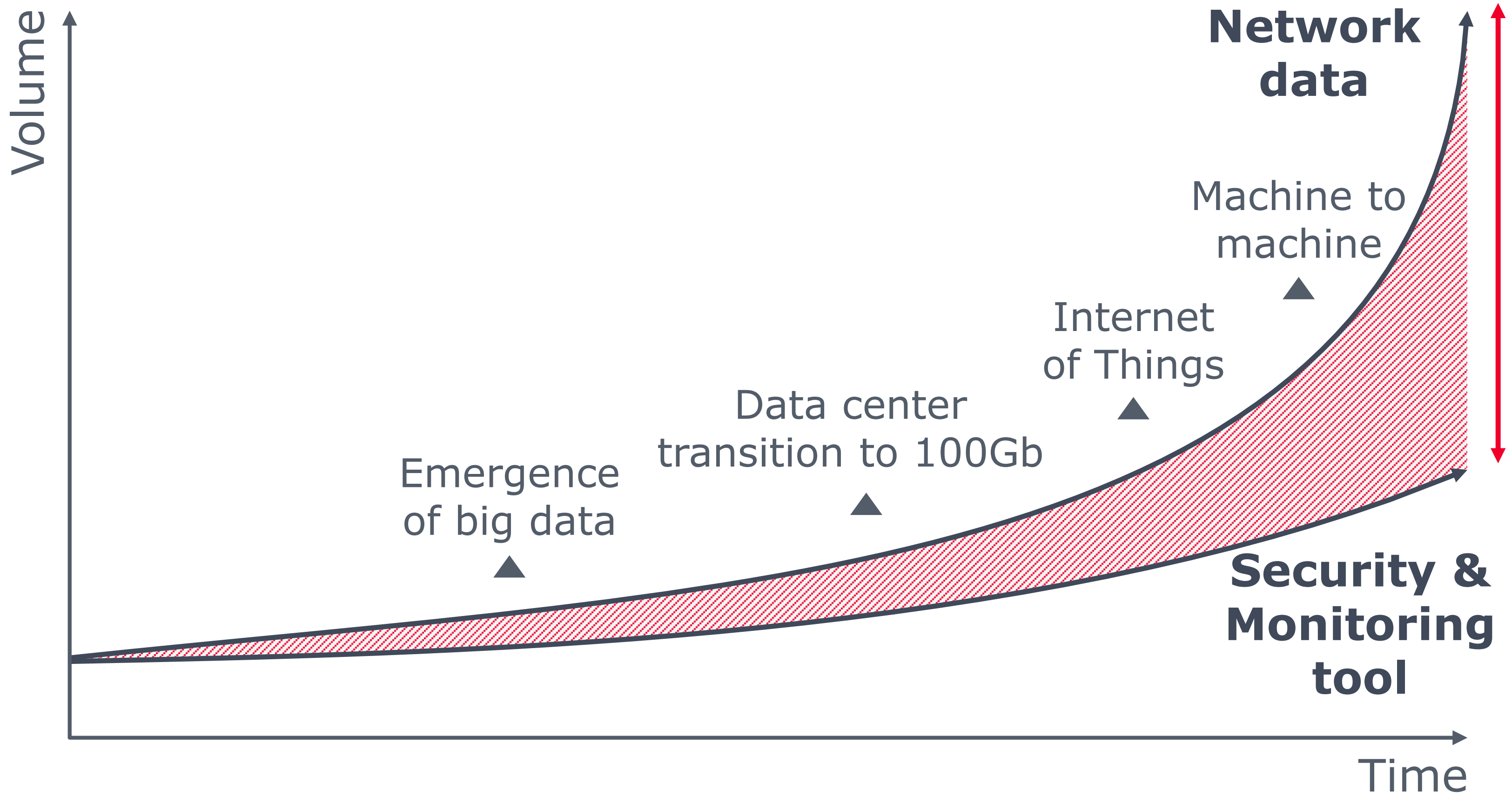
amazon web services | Partner Network

ADVANCED TECHNOLOGY PARTNER

AUTHORIZED PUBLIC SECTOR PARTNER

The Data-in-Motion Dilemma

Volume + Speed + Threats = Complexity + Risk + Cost



Tools do not scale as fast as data

- Slow time to detection and containment
- Unchanged security model
- Evolving traffic patterns
- Rising use of encryption

Visibility Is Essential

If you can’t see it, you can’t manage, secure or understand it.

75% of SecOps teams state that they need better network visibility or have very limited network visibility today.

Dan Conde, “Network Security Trends,” Enterprise Strategy Group (ESG), Research Insights Paper commissioned by Gigamon, Jan 2016. Retrieved from: https://www.gigamon.com/lp/esg-network-security-trends/index.html

Buy and run on Amazon EC2 awsmarketplace

Gigamon®

Visibility into Public Clouds

amazon web services | Partner Network

ADVANCED TECHNOLOGY PARTNER

AUTHORIZED PUBLIC SECTOR PARTNER

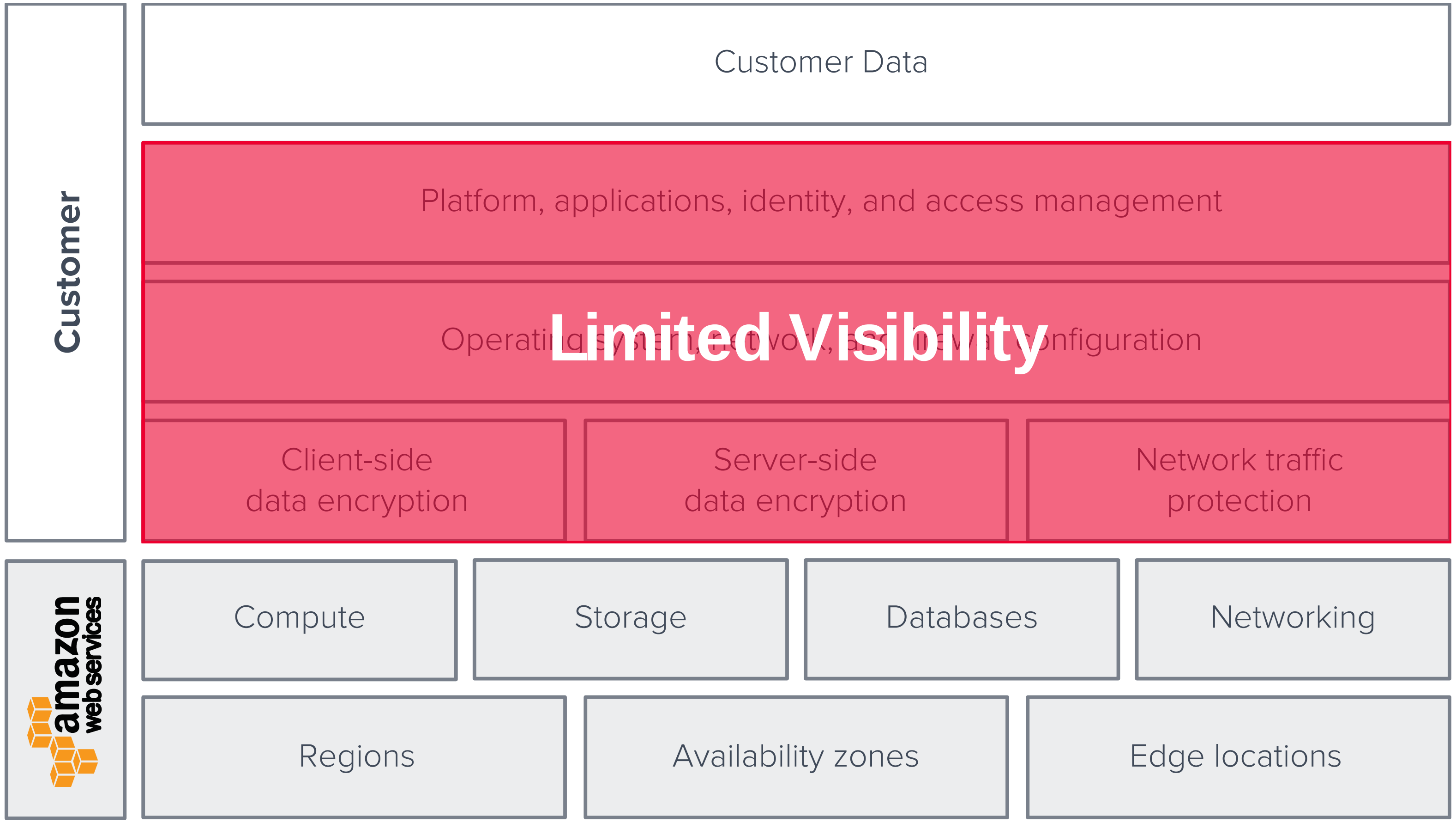
The industry’s first pervasive visibility platform for public, private and hybrid clouds

Gigamon Visibility Platform enables consistent and elastic visibility into data-in-motion across the entire enterprise

Available in Commercial and GovCloud

Public Cloud Deployment: Shared Responsibility

Need for Data-in-Motion Visibility



Customer

Customer Data

Platform, applications, identity, and access management

Operating system, network, and firewall configuration

Limited Visibility

Client-side data encryption

Server-side data encryption

Network traffic protection

amazon web services

Compute

Storage

Databases

Networking

Regions

Availability zones

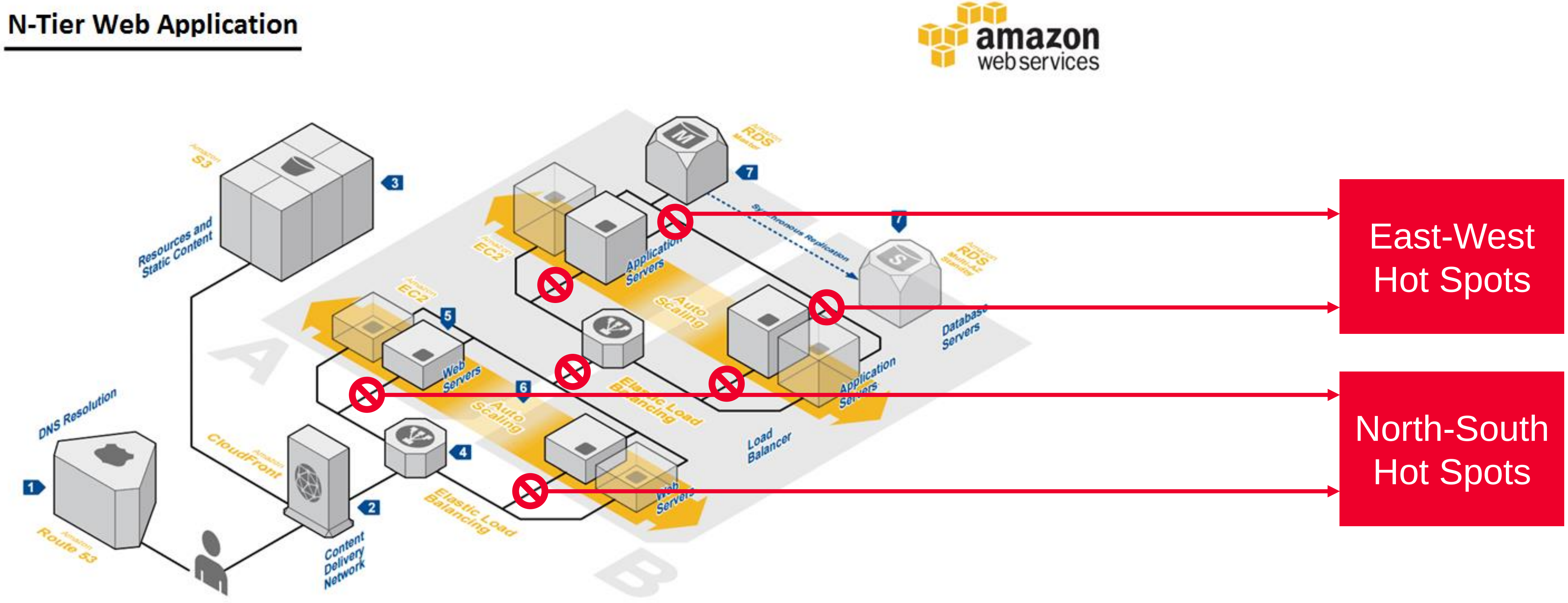
Edge locations

CloudOps
Analyze application hot spots,
Improve Customer Experience

SecOps
Content inspection (IDS, Forensics ..)

Lift-and-Shift
Preserve Tool ROI, Hybrid Cloud

Visibility ‘Hot Spots’ in a Sample Web Application



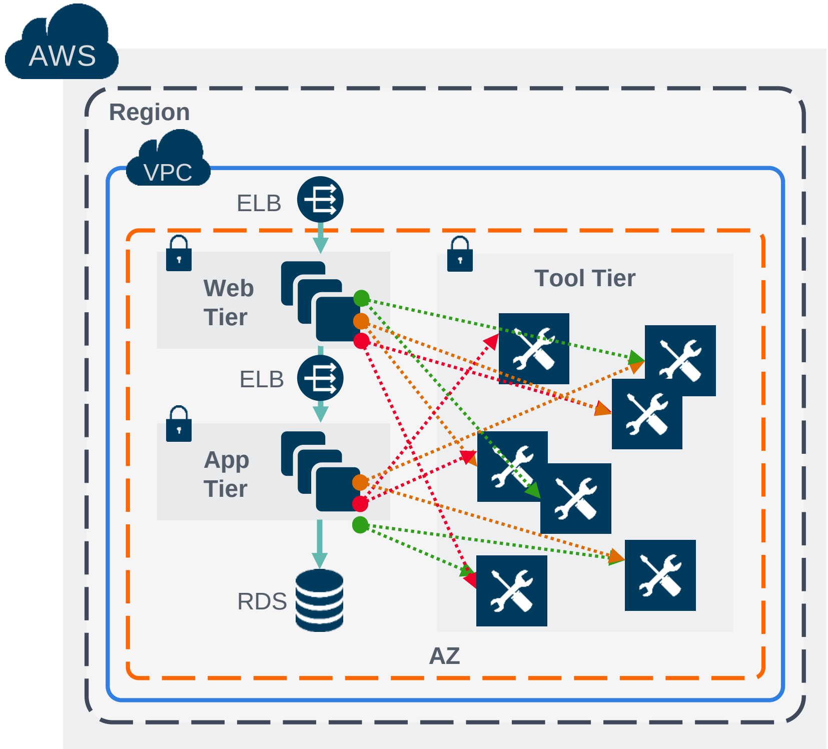
East-West Hot Spots

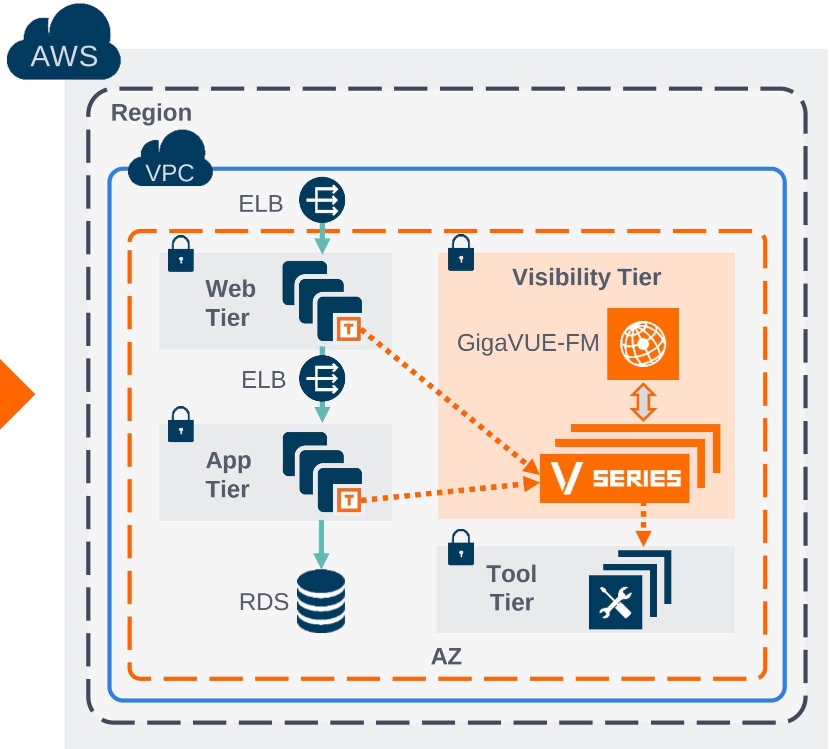
North-South Hot Spots

“I want to move applications to the public cloud but I am worried I will not have adequate visibility”

“My organization is running multiple, independently-managed VPCs in the public cloud and I spend more time and money deploying security tools for each VPC”

Public Cloud Visibility Challenges and Gigamon Solution



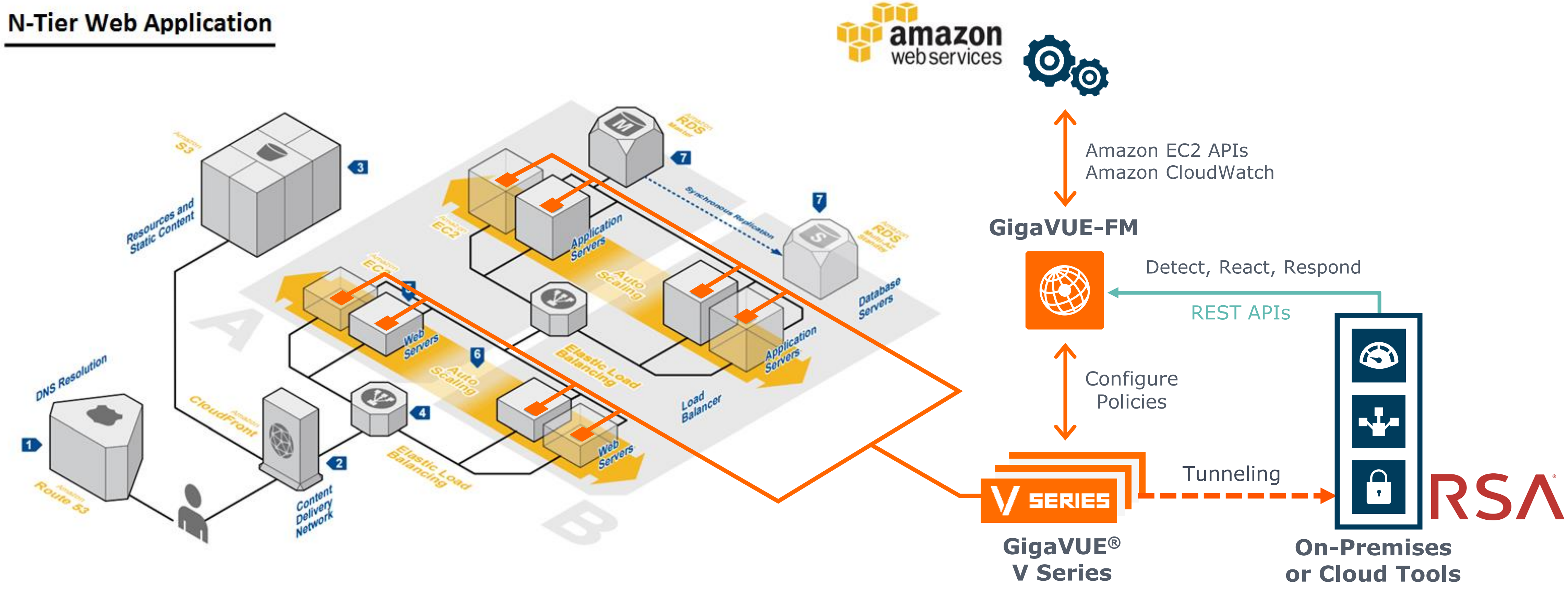


- ✗ Discreet vendor monitoring agents per instance
- ✗ Impacts workload and VPC performance
- ✗ Increases complexity and cost
- ✗ Static visibility with heavy disruption

- ✓ Consistent way to access network traffic
- ✓ Distribute traffic to multiple tools
- ✓ Customize traffic to specific tools
- ✓ Elastic Visibility as workloads scale-out

Gigamon Visibility Platform for AWS

Sample Web Application: AWS Reference Architecture



N-Tier Web Application

Amazon EC2 APIs
Amazon CloudWatch

GigaVUE-FM

Detect, React, Respond

REST APIs

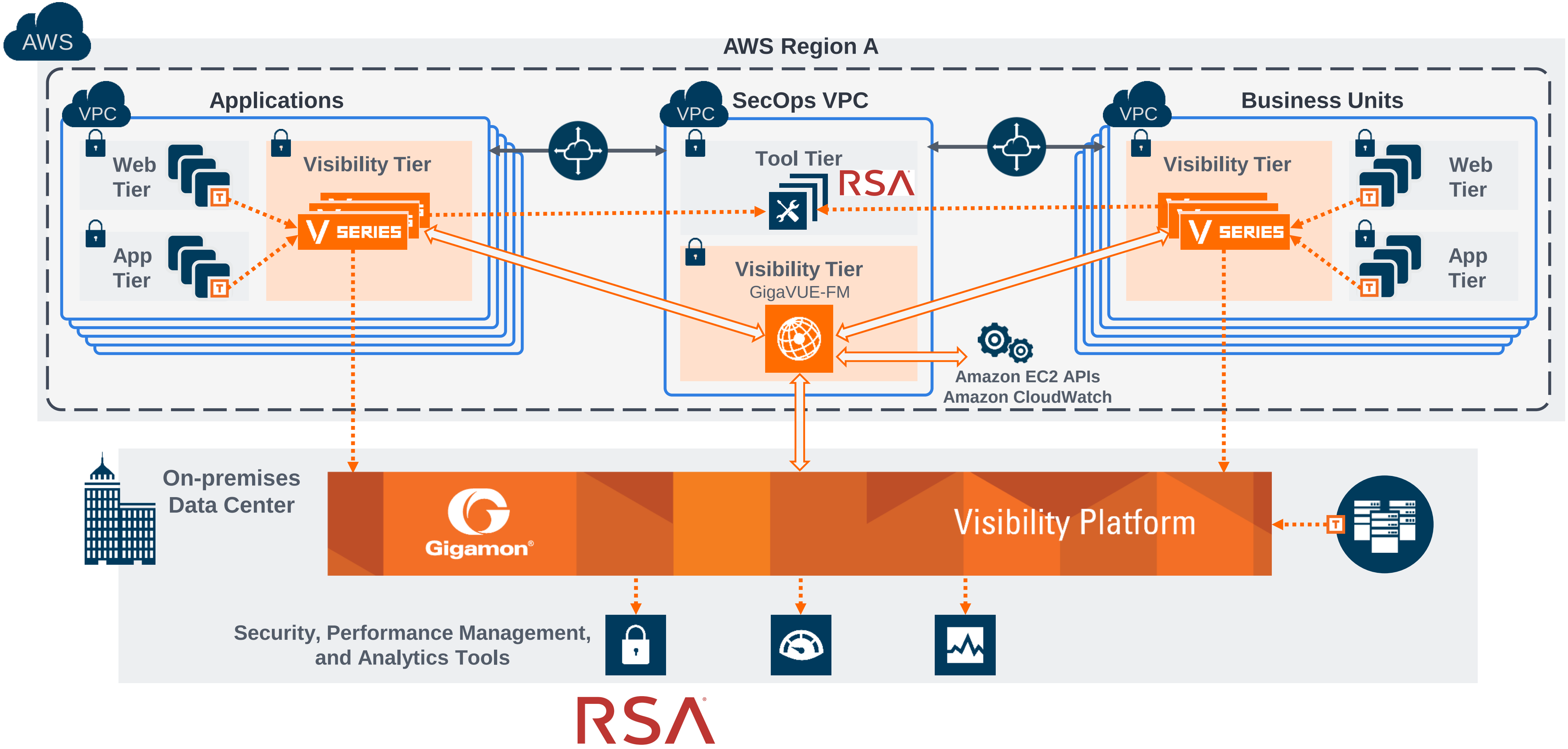
Configure
Policies

Tunneling

GigaVUE®
V Series

On-Premises
or Cloud Tools

Centralized Visibility and Security



Summary: Key Capabilities

- Patented Flow Mapping® to customize and distribute traffic of interest
- GigaVUE-FM: Intuitive drag-and-drop user interface for rapid turn-up

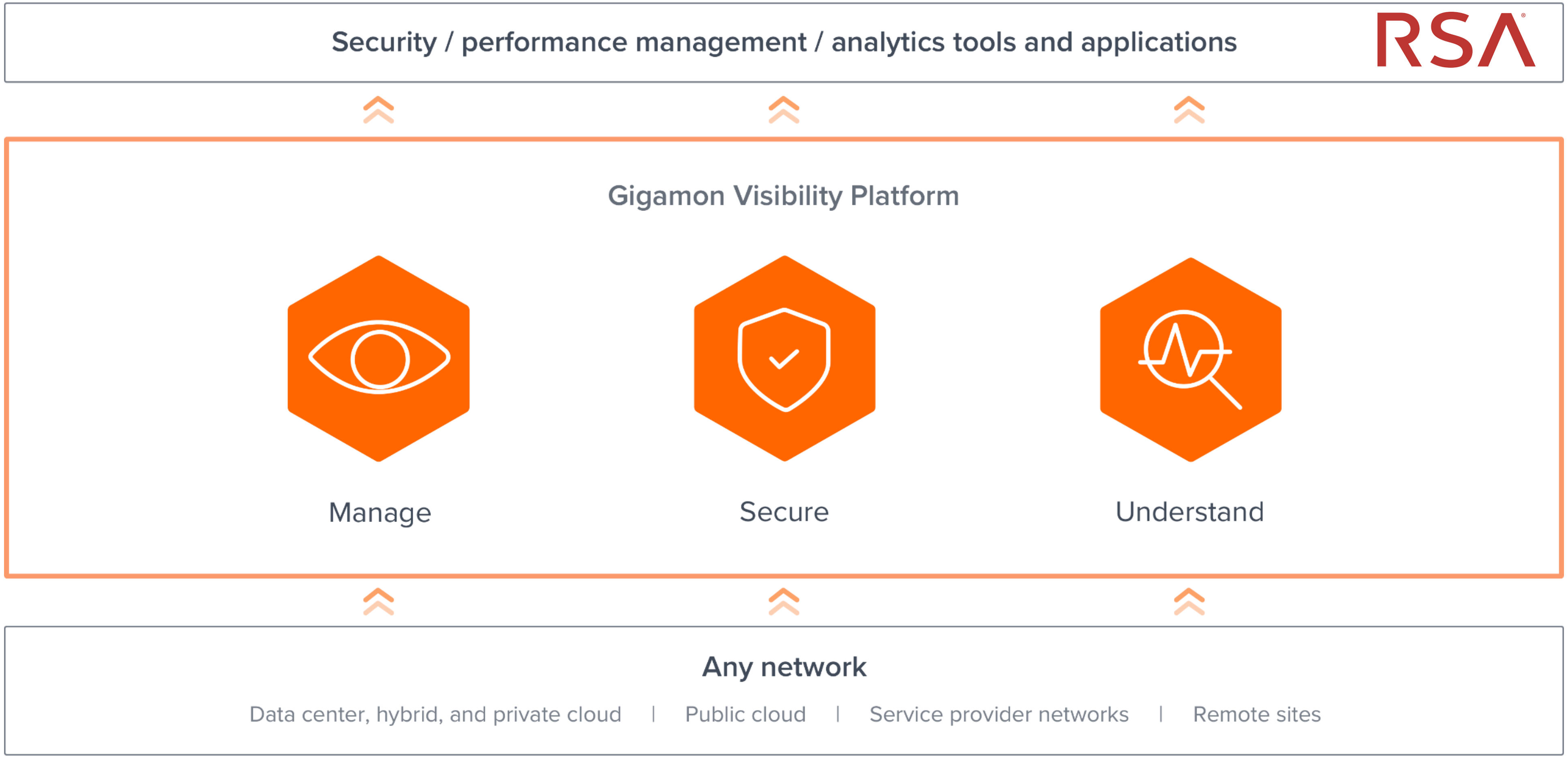
- Automatic target selection: Elastic and automated visibility for new EC2 instances
- Open REST APIs for Automation/Orchestration incl. integration with Amazon EC2 API, Amazon CloudWatch

- Patented GigaSMART® traffic intelligence: Slicing, Masking, Sampling
- Optimize Tool performance, reduce network backhaul

- Flexible deployment models: Tools anywhere
- Agnostic platform: Benefits any tool any where that needs network traffic for analysis

Gigamon Visibility Platform

See more. Secure more.



Security / performance management / analytics tools and applications

RSA

Gigamon Visibility Platform

Manage

Secure

Understand

Any network

Data center, hybrid, and private cloud | Public cloud | Service provider networks | Remote sites

RSA®

EMPOWER ANY ANALYST TO IDENTIFY, UNDERSTAND, AND MITIGATE ADVANCED THREATS

NetWitness Suite for AWS

Mike Gallegos
Product Manager, RSA NetWitness Suite

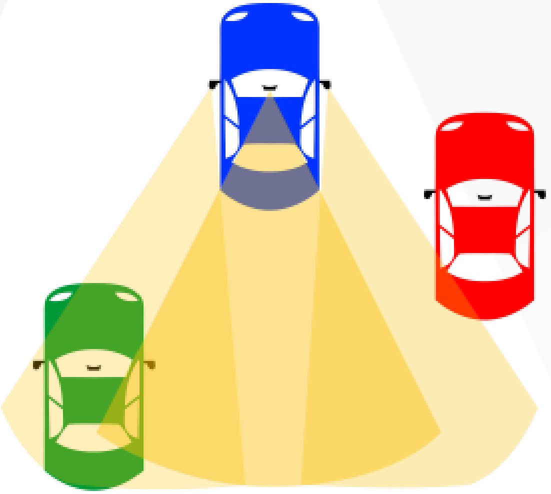
WHY ARE ATTACKERS SUCCESSFUL

People

Process

Lack of prioritization
Response plan is disjointed

Technology

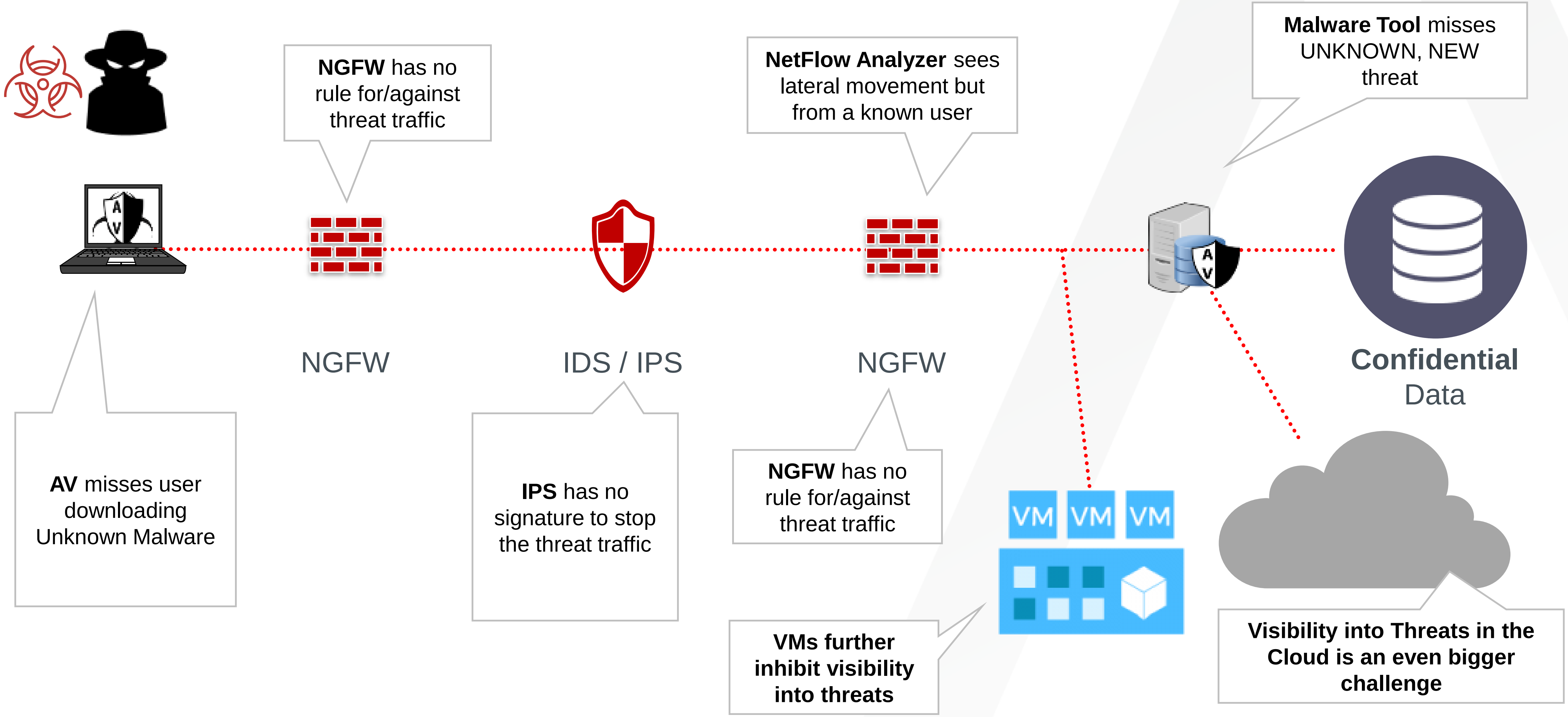


Blind spots
Disparate security tools

Orgs Cannot Connect the Dots in Cloud

TODAY'S SECURITY ISN'T WORKING

Cloud, virtualization create blind spots



NGFW has no rule for/against threat traffic

NetFlow Analyzer sees lateral movement but from a known user

Malware Tool misses UNKNOWN, NEW threat

AV misses user downloading Unknown Malware

IPS has no signature to stop the threat traffic

NGFW has no rule for/against threat traffic

VMs further inhibit visibility into threats

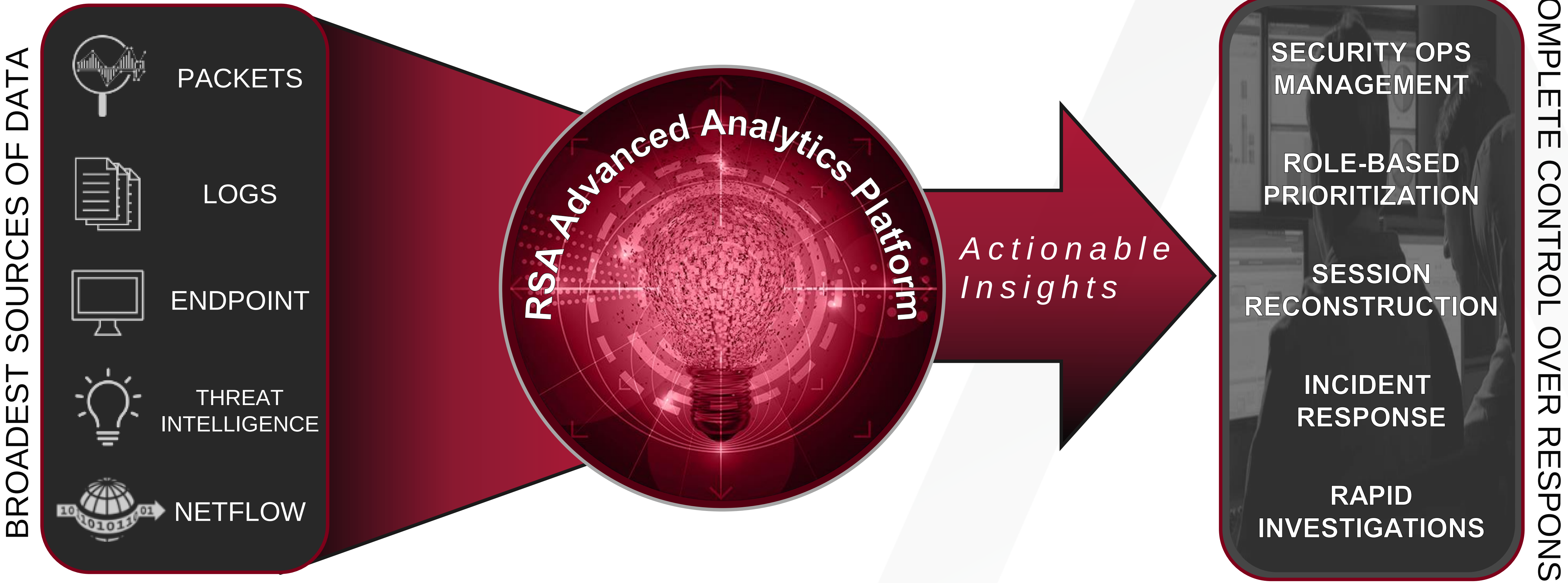
Visibility into Threats in the Cloud is an even bigger challenge

Cloud IT spending will be 46% of total expenditures on enterprise IT infrastructure by 2019*

*IDC

RSA NETWITNESS® SUITE

Connecting The Dots for Threat Detection and Response…



BROADEST SOURCES OF DATA

PACKETS

LOGS

ENDPOINT

THREAT INTELLIGENCE

NETFLOW

RSA Advanced Analytics Platform

Actionable Insights

SECURITY OPS MANAGEMENT

ROLE-BASED PRIORITIZATION

SESSION RECONSTRUCTION

INCIDENT RESPONSE

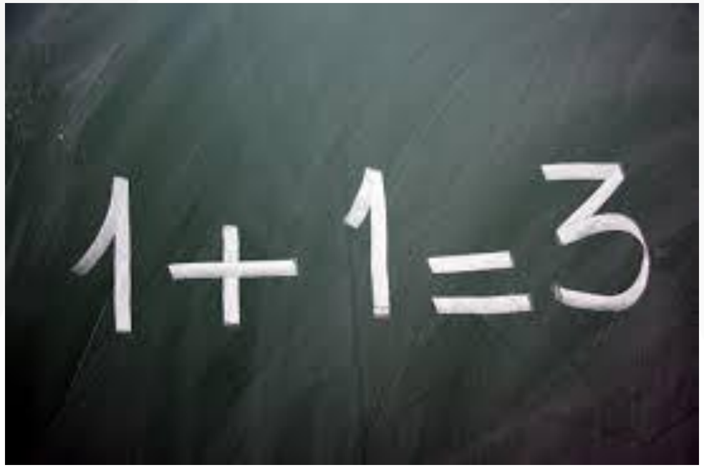
RAPID INVESTIGATIONS

COMPLETE CONTROL OVER RESPONSE

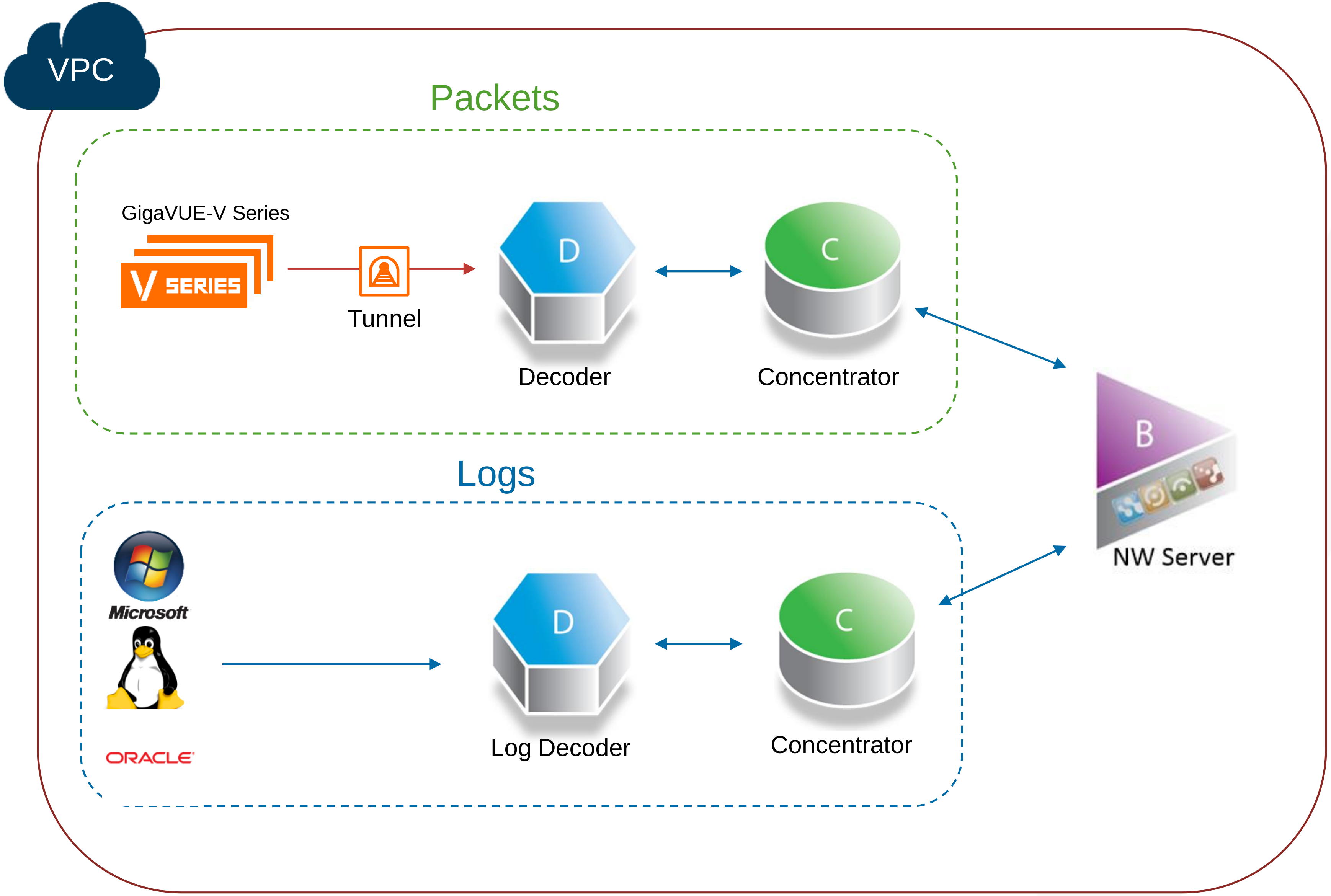
*RESPOND IN **MINUTES**…NOT **MONTHS***

WHY CUSTOMERS CHOOSE RSA & GIGAMON FOR MONITORING IN AWS

- Enables VISIBILITY across physical, virtual and cloud architectures
- Solution scales from 1-100Gbps
- Gigamon provides:
  - Single source filtering
  - Selective capture of network traffic for analysis and storage
  - Visibility into private (virtual) and public (AWS) clouds
- RSA NetWitness Suite:
  - Combines network visibility with log and endpoint visibility
  - Provides unmatched visibility, forensics and threat detection



NETWITNESS SOLUTION – FULL STACK



Packet Decoder (Visibility)

- The packet data is collected using a host called Decoder. The Decoder captures, parses, and reconstructs all network traffic from Layers 2 – 7.

Log Decoder (Visibility)

- Collects log events from hundreds of devices and event sources.

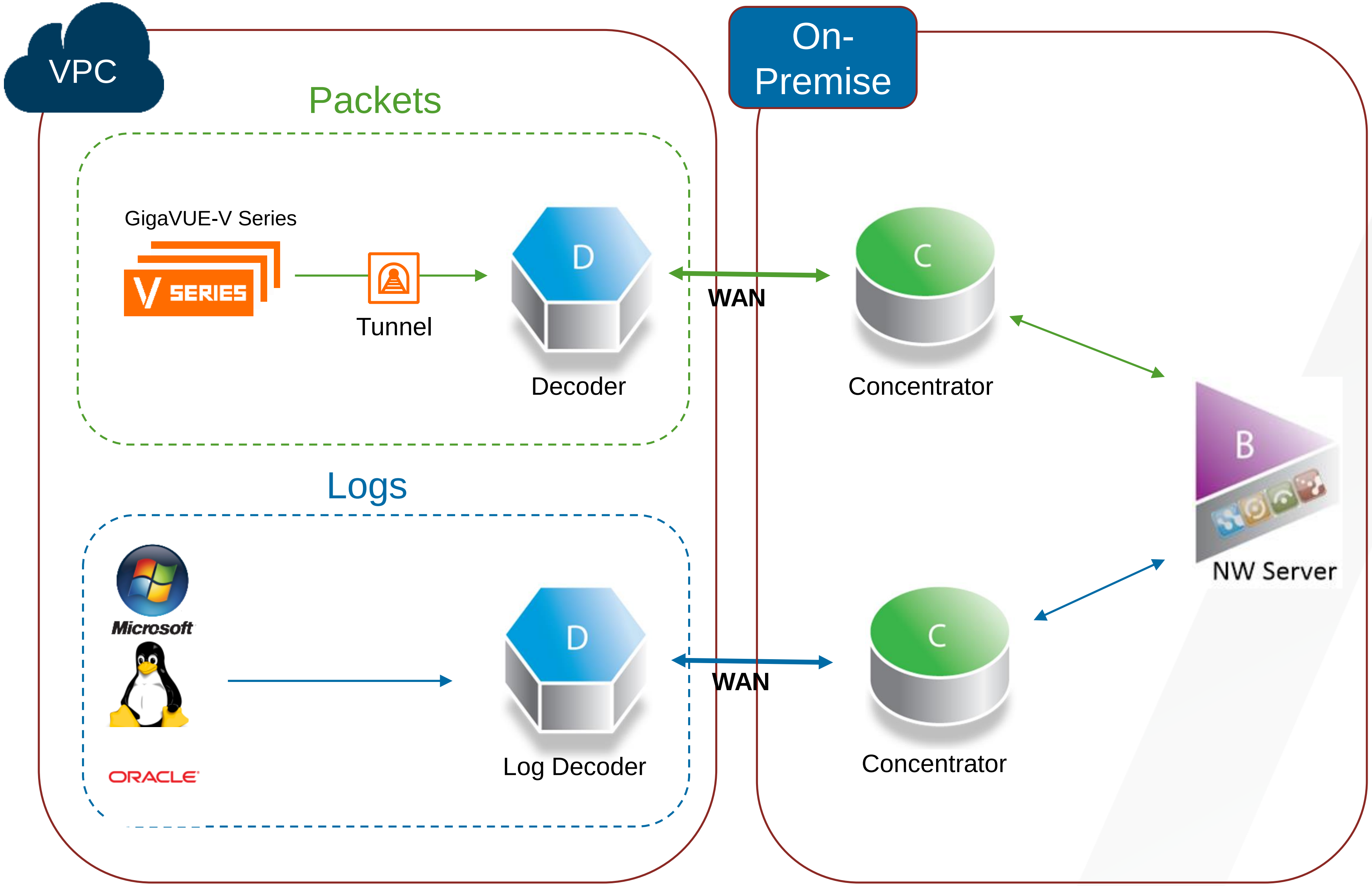
Concentrator (Analysis)

- The Concentrator indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while also facilitating reporting and alerting.

NetWitness Server (Action)

- Hosts Reporting, Investigation, Administration, Respond and other aspects of the user interface.

NETWITNESS SOLUTION – HYBRID



Packet Decoder (Visibility)

- The packet data is collected using a host called Decoder. The Decoder captures, parses, and reconstructs all network traffic from Layers 2 – 7.

Log Decoder (Visibility)

- Collects log events from hundreds of devices and event sources.

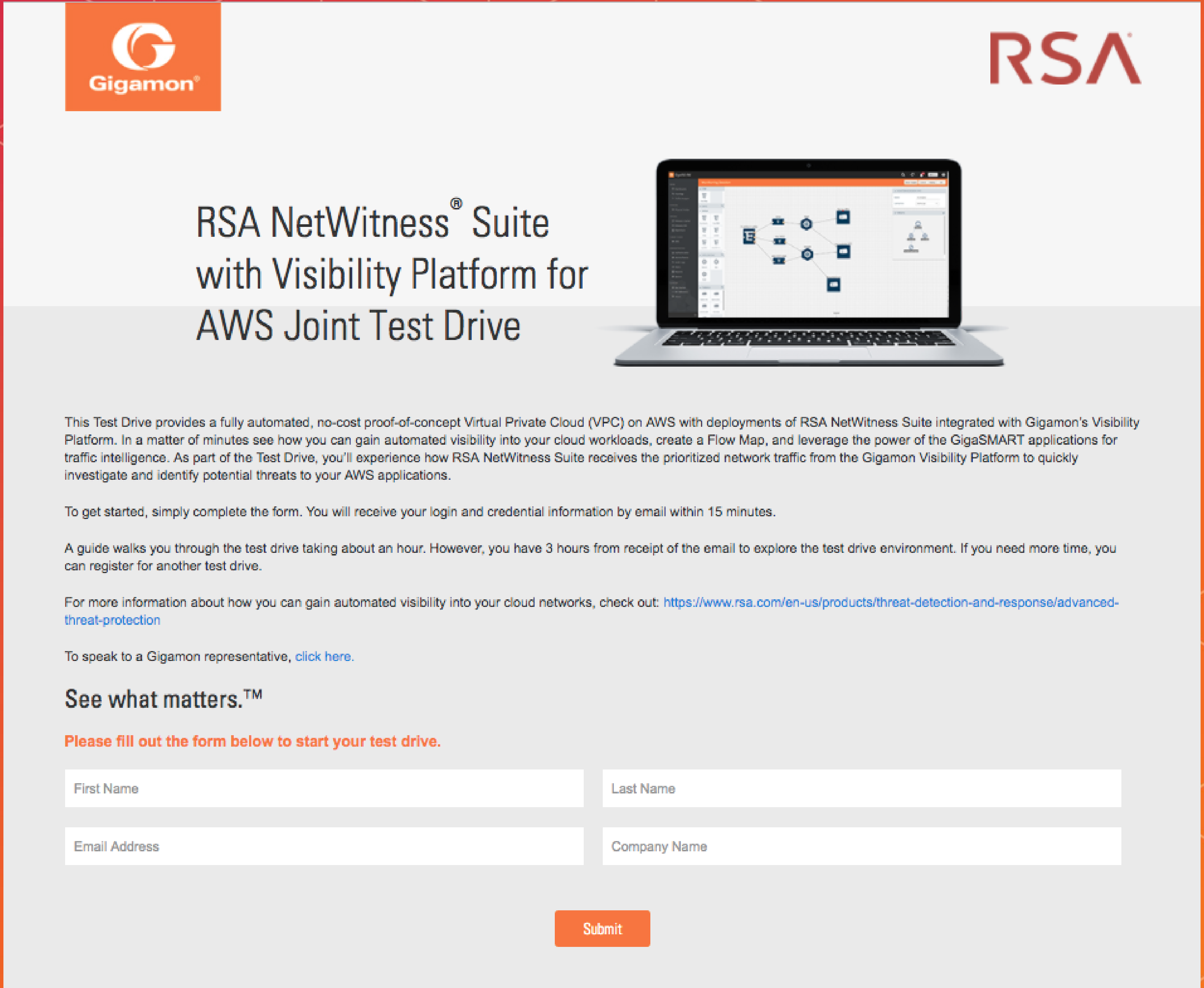
Concentrator (Analysis)

- The Concentrator indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while also facilitating reporting and alerting.

NetWitness Server (Action)

- Hosts Reporting, Investigation, Administration, Respond and other aspects of the user interface.

Demo Video



RSA NetWitness® Suite with Visibility Platform for AWS Joint Test Drive

This Test Drive provides a fully automated, no-cost proof-of-concept Virtual Private Cloud (VPC) on AWS with deployments of RSA NetWitness Suite integrated with Gigamon's Visibility Platform. In a matter of minutes see how you can gain automated visibility into your cloud workloads, create a Flow Map, and leverage the power of the GigaSMART applications for traffic intelligence. As part of the Test Drive, you'll experience how RSA NetWitness Suite receives the prioritized network traffic from the Gigamon Visibility Platform to quickly investigate and identify potential threats to your AWS applications.

To get started, simply complete the form. You will receive your login and credential information by email within 15 minutes.

A guide walks you through the test drive taking about an hour. However, you have 3 hours from receipt of the email to explore the test drive environment. If you need more time, you can register for another test drive.

For more information about how you can gain automated visibility into your cloud networks, check out: https://www.rsa.com/en-us/products/threat-detection-and-response/advanced-threat-protection

To speak to a Gigamon representative, click here.

See what matters.™

Please fill out the form below to start your test drive.

First Name	Last Name
Email Address	Company Name

Submit

https://www.gigamon.com/aws-rsa