



Gigamon Growth Playbook for Sales and Marketing

See, Secure and Empower What Matters.

Welcome to the Gigamon Growth Playbook

This guide has been created as a tool to empower you to meet your revenue goals, but most importantly, this is a roadmap to align you with your prospective customer. To be successful in gaining trust, you will need to align your conversations with your prospect's unique needs and pain points. By first understanding their needs, you'll be able to use these various Use Cases to clearly align the value Gigamon will provide in a compelling way.

We have categorized the most common customer challenges into six "I want to" themes:

1. Optimize application and network performance
2. Improve on-premises security
3. Simplify and control access to network data
4. Improve security in public clouds
5. Enhance service provider infrastructure visibility
6. Maintain security during infrastructure transformation

These themes, and the subsequent Use Cases described in the Playbook, will help ensure a quick path to helping your customers and prospects understand the value of the Gigamon Visibility Platform. In addition to this playbook, you will find online content and assets that dive deeper into the buyer's journey.

Marketing will continue to develop supporting assets for these Use Cases throughout the year.

To get the most out of this guide:

- Keep it handy and treat it like a study guide.
 - Don't hesitate to make it your own by marking it up as you see fit.
- For Partners, check the Partner Portal or check with your Channel Account Manager for the latest updates on marketing programs and events, as well as new Use Cases and sales plays.
- Reach out to channel.marketing@gigamon.com with any questions or concerns.

Happy Selling!

Table of Contents

Welcome to the Gigamon Growth Playbook	2	Top Use Cases	25
Our Beliefs	5	Mapping Use Cases to Customer Need	26
Gigamon Messaging and Story	6	Mapping Use Cases to Role	27
Gigamon Visibility Platform	8	1. First Step to Visibility: Get Reliable Data Access for Tools	28
Product Portfolio	9	2. Visibility During Network Upgrades/Expanding Network Coverage	32
Ideal Customer Profile	10	3. Improve Threat Prevention Efficacy with Inline Bypass	35
Ideal Corporate Customer	11	4. Encrypted Traffic Management (TLS Decryption)	37
Top Gigamon Customers	11	5. Centralized NetFlow/IPFIX Generation	35
Ecosystem Partners	12	6. Extract Network Metadata to Optimize SIEMs	41
Ecosystem Partners: A Winning Combination	13	7. Leverage Application Intelligence to Optimize Tool Stack	43
Ecosystem Sales Cheat Sheet – Use Cases	14	8. Network Detection and Response– Gigamon Insight	46
Key Features	15	9. Visibility into Private Clouds (VMware ESX and NSX)	48
Go Further with Ecosystem Partners: Joint Marketing Tools	15	10. Visibility into Public Clouds (AWS and Azure)	52
Channel First	16	11. Visibility for NFV (OpenStack)	54
Sales Plays	21	12. Subscriber-Aware Visibility for Data, Voice and 5G Networks	56
Security	22	13. Lawful Intercept	58
Enterprise Network	23	14. Visibility into Remote Sites	60
Service Provider > Subscriber-Aware Visibility	24		

Table of Contents


Appendix	62
Visibility Platform Key Capabilities	63
Value Drivers	65
SecOps Value Drivers	67
NetOps Value Drivers	71
Service Provider Value Drivers	75

Our Beliefs

Five guiding principles that are the basis of everything we do.



We are focused as one force to support and assist our customers to achieve their unique journeys.




Employees First

Employees are a powerful asset. They are collectively valued, engaged and empowered for success.




Innovation

We combine the delivery of market-leading products with the nurturing of innovation in all we do.




Trust

We trust in our business, in each other, in our partners and in the collective team that represents Gigamon.



Collaboration

We believe communication and collaboration empower the success of our company, our partners and our customers.



Confidential and Proprietary. Not to be distributed without express written consent from Gigamon. © 2019 Gigamon. All rights reserved. 5

Gigamon Messaging and Story

See, Secure and Empower What Matters.

The Gigamon Visibility Platform

The Customer Challenge

IT truly needs our help. Their users want faster and faster access to an ever-growing variety and volume of data, while new threats are appearing at their gate each day. In fact, some are already hiding inside their environment, and the infrastructure itself is becoming more complex and evolving to include physical, virtual and cloud. With poor visibility into this hybrid infrastructure and an overworked staff, it's no wonder network operations teams (NetOps) are often highly resistant to any changes to their "but it ain't broke" network.

Yet security operations teams (SecOps) are constantly throwing new security tools into the mix, new XaaS environments are being deployed and users are still demanding faster performance and more applications. Wouldn't it be nice if there was a solution that not only provided clear visibility of the network but also allowed IT to accommodate change and upgrades to the infrastructure easily?

The Only Solution

The Gigamon Visibility Platform represents that "Essential Element" of modern infrastructure, delivering pervasive visibility into all the data in motion across the entire network – physical, virtual and cloud. It allows businesses, government agencies and service providers to see and secure everything in their increasingly complex networks.

Gigamon's unique approach to visibility is the foundation of all other benefits: network enhancements are easier and safer, security tools receive only the relevant traffic and can cover all surfaces of attack, tools gain an advantage with new intelligence about the traffic, and the NetOps and SecOps workload is dramatically reduced.

SEE

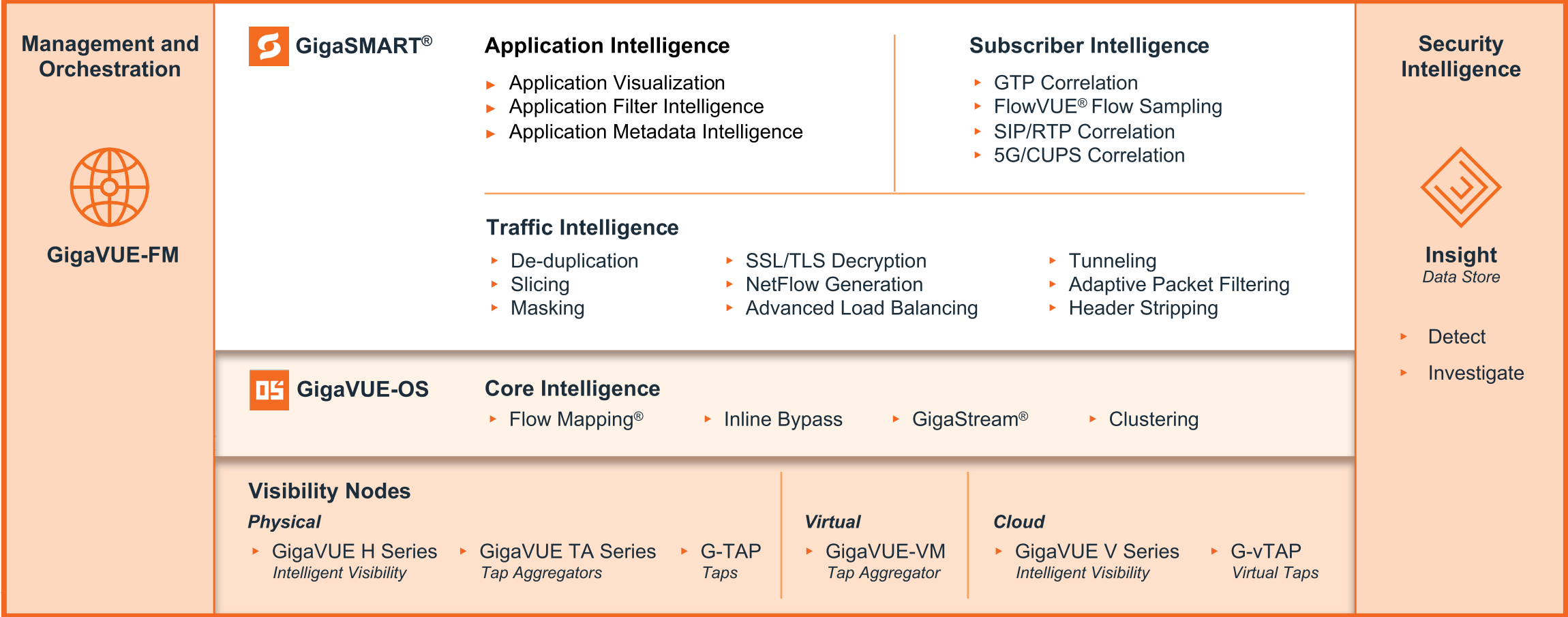
- > Pervasive visibility across physical, virtual and cloud infrastructure
- > Gain complete transparency into all data in motion
- > Remove the complexity from a complex network

SECURE

- > Reduce tool sprawl and cost by eliminating irrelevant and low-risk traffic
- > Secure all potential attack surfaces
- > Use network intelligence to hunt and respond to threats faster than ever

EMPOWER

- > Improve tool ecosystem effectiveness by bringing application-level awareness to each tool
- > Be ready for all future network upgrades and new tool additions
- > Dramatically reduce your team's workload through automation



Physical, Virtual and Cloud Infrastructure

Ideal Customer Profile

Ideal Corporate Customer

The ideal Gigamon customer is an enterprise or public sector entity with large, complex networks and a sufficient number of security and network monitoring tools in their infrastructure. Organizations that have diverse environments – physical, virtual and cloud – are also very good targets.

Target

- Enterprise environments (large companies with 1,000 or more employees)
- Public sector organizations (government, higher education, SLED)
- Primary roles:
 - SecOps Directors/Architects, CISOs
 - NetOps Directors/Architects
 - CloudOps Directors/Architects
 - Mobile Operators and Fixed-line Service/Content providers

Corporate Profile

Look for organizations that are:

- Looking to modernize their IT environment (for example, virtualization, cloud, internet of things, or IoT)
- Going through new data center build-outs or network upgrades
- Looking for visibility and access to all their data, including data in motion that traverses their network
- Struggling with a growing number of monitoring or security tools that are not keeping up with the speed or volume of data
- Looking to simplify their approach to accessing, controlling and securing data
- Struggling to gain visibility into their cloud environments, either for network monitoring or security purposes
- Concerned about their ability to growth operating budgets in line with the complexity of their environments

Top Gigamon Customers

Serving top companies across the globe, Gigamon acts as a catalyst for optimizing network performance and security tools – whether on-premises or in the cloud.



7 of the top ten
Global Banks



8 of the top ten
Healthcare Providers



10 of the top ten
U.S. Federal Agencies



8 of the top ten largest
Tech Companies



83 of the
Fortune 100



8 of the top ten
Mobile Phone
Network Operators

Ecosystem Partners: A Winning Combination

No one buys a Visibility Platform simply because they want to see network traffic. Customers buy because they need to manage and secure their networks and they want to deploy tools that enable them to do this in the most economical, efficient and effective way possible.

Our ecosystem of partners understands this. The chart below shows a selection of those who have joined our Technology Alliance Partners program to promote the value of a combined solution: best-in-class technology enhanced by the Gigamon Platform.

By optimizing the reach and efficiency of any tool design to analyze data flowing over the network (IP packet data or metadata extracted from that traffic), the Gigamon Platform allows customers to derive maximum value from investments made in our partners' security and performance technologies.



Ecosystem Sales Cheat Sheet – Use Cases

As you have learned, a wide variety of tools can benefit from the functionality Gigamon provides as part of our portfolio. To help you quickly understand how to position Gigamon with the network and security tools you encounter at prospects, we are providing the following two cheat sheets. The first refers to the Use Cases we covered earlier in this playbook – showing which Use Cases are applicable to the types of tools you are most likely to encounter.

Key Use Cases

	WAF	SIEM	ATP	DLP	DDoS	IPS	NGFW	NAC	NTA	NPM/APM	CEM
1. First Step to Visibility: Get Reliable Data Access for Tools	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2. Visibility During Network Upgrades/ Expanding Network Coverage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3. Improve Threat Prevention Efficacy with Inline Bypass	✓		✓		✓	✓	✓*				
4. Encrypted Traffic Management (TLS Decryption)	✓	✓	✓	✓	✓	✓	✓*	✓	✓	✓	
5. Centralized NetFlow/IPFIX Generation		✓							✓	✓	
6. Extract Network Metadata to Optimize SIEMs		✓							✓		
7. Leverage Application Intelligence to Optimize Tool Stack	✓	✓	✓	✓		✓			✓	✓	
8. Network Detection and Response									✓		
9. Visibility in Private Clouds (VMware ESX and NSX)	OOB	✓	✓	✓		OOB		OOB	✓	✓	OOB
10. Visibility in Public Clouds (AWS and Azure)	OOB	✓	✓	✓		OOB		OOB	✓	✓	OOB
11. Visibility for NFV (OpenStack)			✓							✓	✓
12. Subscriber-Aware Visibility for Data, Voice and 5G Networks			✓								✓
13. Lawful Intercept											✓
14. Visibility into Remote Sites	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

*When NGFW deployed as Layer-2 firewall/transparent mode

The second cheat sheet provides a quick reference to which major Gigamon features are particularly relevant for customers wanting to deploy each type of tool. If you run across a new tool, simply figure out which segment it fits into and you'll have a great guide on how deploying with Gigamon can enhance the effectiveness of that tool.

OOB = Out of Band

WAF = Web Application Firewall
SIEM = Security Information & Event Management
ATP = Advanced Threat Protection
DLP = Data Loss Prevention
DDoS = Distributed Denial of Service Attack Mitigation Tool
IPS = Intrusion Prevention System

NGFW = Next-Generation Firewall
NAC = Network Access Control
NTA = Network Traffic Analytics
NPM/APM = Network Performance Management/Application Performance Management
CEM = Customer Experience Manager (Usually SP)

Key Features

	WAF	SIEM	ATP	DLP	DDoS	IPS	NGFW	NAC	NTA	NPM/APM	CEM
Pervasive Visibility	P	P	P	P	P	P	P	P	P	P	P
Filtering	P	P	P	P	P	S			P	S	S
Gigastream Load Balancing	P	S	P	P	P	P	P	P	P	P	P
Traffic Aggregation	S	S	S	S	P	S	S	P	P	S	S
NetFlow Generation		P							P	S	S
Application Metadata Intelligence	S	P		S					P		
Asymmetric Routing Assistance	S		P		S	P	P	P			
Resilience & Control (Inline Bypass)	P		P		P	P	P	P			
SSL/TLS Decryption	P	P	P	P	P	P	P	P	P	S	
Header Stripping								S		P	P
Masking		P							P		
De-duplication	P	P	S	S					P	P	P
Subscriber-Aware Visibility										P	P
Cloud-Based Tools	S	P	OOB	P		OOB			P	P	P

OOB = Out of Band

WAF = Web Application Firewall
SIEM = Security Information & Event Management
ATP = Advanced Threat Protection
DLP = Data Loss Prevention
DDoS = Distributed Denial of Service Attack Mitigation Tool
IPS = Intrusion Prevention System

NGFW = Next-Generation Firewall
NAC = Network Access Control
NTA = Network Traffic Analytics
NPM/APM = Network Performance Management/Application Performance Management
CEM = Customer Experience Manager (Usually SP)

Go Further with Ecosystem Partners: Joint Marketing Tools

Find out more about a particular ecosystem partner or tool in the Gigamon Partner Portal. There you will find joint solution briefs, sales presentations, deployment guides and more. If you need one-on-one help, contact the Gigamon Alliances Team at ecopartners@gigamon.com.

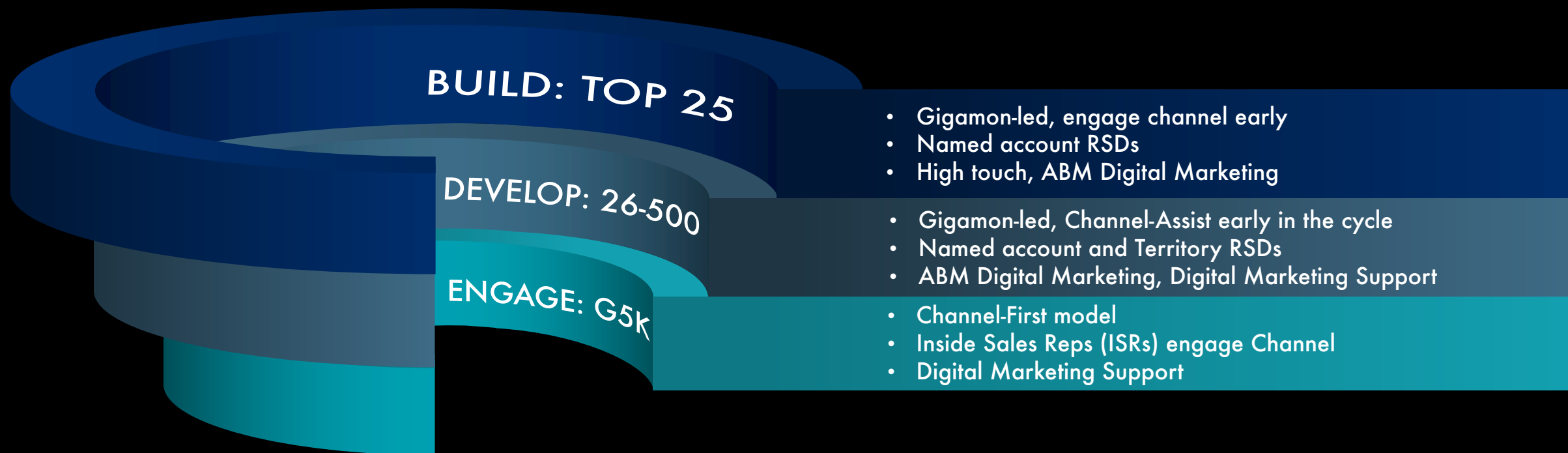
Channel First

A New GTM for a Channel First Transition

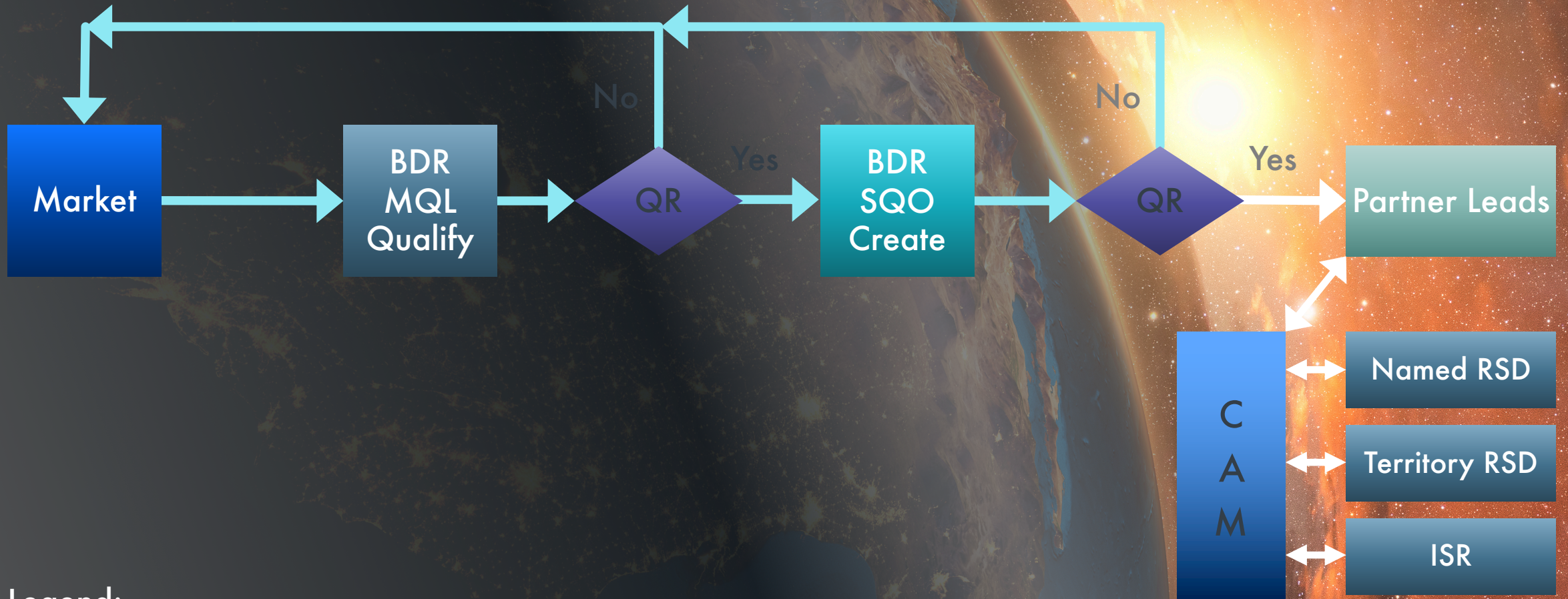


\$1.4B TAM

Go to Market Model



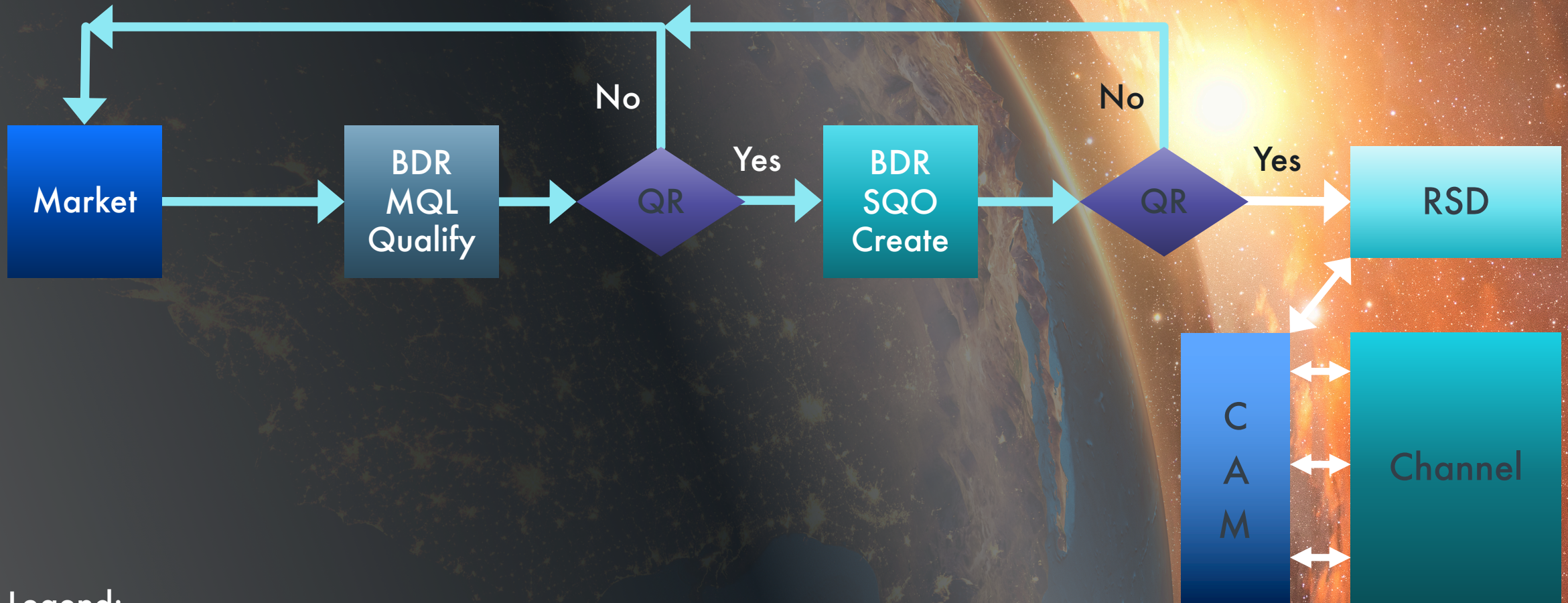
Gigamon Go-to-Market Model – Engage



Legend:

QR = Qualification Requirements
MQL = Marketing Qualification Lead
SQO = Sales Qualified Opportunity

Gigamon Go-to-Market Model – Build & Develop



Legend:

QR = Qualification Requirements
MQL = Marketing Qualification Lead
SQO = Sales Qualified Opportunity

Sales Plays

Sales Play: Security

Primary Target Prospect

- CISO
- Director SecOps
- Manager of SOC
- Security Infrastructure Architect

Value Drivers

- Minimize Complexity of a More Efficient Security Stack
- Improve Confidence in Your Overall Security Posture
- Reduce Risk Through Accelerated Threat Detection and Response

Top Differentiators

- One Complete Platform for Access to Data Anywhere
- Scale, Breadth and Depth of Traffic Intelligence
- High Quality and Reliability of Overall Solution
- Tangible and Prompt ROI
- Depth and Breadth of Integration with Leading Infrastructure and Tooling Vendors
- #1 Market Leader, Singular Focus of the Whole Company

Ecosystem and Third-Party Partner Tools Involved

- Intrusion Detection and Prevention (for example, Cisco, Trend Micro/ TippingPoint, McAfee)
- Next-Generation Firewall (for example, Palo Alto Networks, Check Point, Cisco)
- Network Forensics and Analytics (for example, RSA, Symantec/Blue Coat, NIKSUN)
- Web/Application Firewall (for example, Imperva, Fortinet, Forcepoint)
- Data Loss Prevention (for example, Symantec, Digital Guardian, Forcepoint)
- SIEM (for example, Splunk, LogRhythm, IBM QRadar)
- Network Traffic Analytics (for example, ExtraHop and Plixer)

Relevant Use Cases



Get Reliable
Data Access
for Tools



Visibility During
Network Upgrades/
Expanding Network
Coverage



Centralized
NetFlow/IPFIX
Generation



Leverage Application
Intelligence to
Optimize Tool Stack



Improve Threat
Prevention Efficacy
with Inline Bypass



Encrypted Traffic
Management
(TLS Decryption)



Extract Network
Metadata to
Optimize SIEMs



Visibility into
Public Clouds
(AWS and Azure)



Visibility into
Remote Sites



Visibility into Private
Clouds (VMware
ESX and NSX)



Network Detection
and Response

Sales Play: Enterprise Network

Primary Audience

- CIO
- Director of NetOps
- Network Architect

Value Drivers

- Maintain a Resilient and Flexible Network Infrastructure Ready to Absorb Change
- Access to and Control of Data for Improved Visibility Across Physical, Virtual and Cloud Infrastructure
- Reduce TCO of Monitoring During Network Traffic Growth and 40G/100G Network Upgrades

Top Differentiators

- One Complete Platform for Access to Data Anywhere
- Scale, Breadth and Depth of Traffic Intelligence
- High Quality and Reliability of Overall Solution
- Tangible and Prompt ROI
- Depth and Breadth of Integration with Leading Infrastructure and Tooling Vendors
- #1 Market Leader, Singular Focus of the Whole Company

Relevant Use Cases



Get Reliable
Data Access
for Tools



Visibility During
Network Upgrades/
Expanding Network
Coverage



Centralized
NetFlow/IPFIX
Generation



Improve Threat
Prevention Efficacy
with Inline Bypass



Encrypted Traffic
Management
(TLS Decryption)



Leverage Application
Intelligence to
Optimize Tool Stack



Visibility into
Public Clouds
(AWS and Azure)



Visibility into Private
Clouds (VMware
ESX and NSX)



Visibility into
Remote Sites

Sales Play:

Service Provider > Subscriber-Aware Visibility

Primary Target Prospect

- VP Infrastructure Architecture
- VP Service Assurance
- VP or Director of Network Operations
- VP of Product Management

Value Drivers

- Scale Infrastructure Analytics and Management to Support 5G Evolution
- Access to and Control of Data for Improved Visibility Everywhere
- Improve and Differentiate Through Subscriber Experience

Top Differentiators

- One Comprehensive Platform Accessing Communications Anywhere
- Scale, Breadth and Depth of Traffic Intelligence
- High Quality and Reliability of Overall Solution
- Strong and Rapid ROI of Subscriber-Aware Intelligence Solution
- #1 Leader in Visibility to Information-in-Motion Market; Singular Focus of the Company

Relevant Use Cases



Get Reliable
Data Access
for Tools



Visibility During
Network Upgrades/
Expanding Network
Coverage



Centralized
NetFlow/IPFIX
Generation



Leverage Application
Intelligence to
Optimize Tool Stack



Lawful
Intercept



Subscriber-Aware
Visibility for Data,
Voice and 5G
Networks



Visibility for NFV
(OpenStack)

Mapping Use Cases to Customer Need

Gigamon's 14 Key Use Cases address a wide range of customer needs. However, the breadth of capabilities that Gigamon provides can make it challenging to have a focused introductory discussion that leads to clear next steps. The most effective way to position Gigamon Use Cases to prospects is to identify specific customer needs and focus early conversations on the subset of Use Cases that can address those needs.

During initial discovery conversations, consider whether the customer wants to...

Optimize application and network performance	Improve on-premises security
Key Use Cases	Key Use Cases
First step to visibility: Get reliable data access for tools (1)	First step to visibility: Get reliable data access for tools (1)
Improve threat prevention efficacy with inline bypass (in addition to security, addresses app/net latency and avoids downtime) (3)	Improve threat prevention efficacy with inline bypass (3)
Encrypted traffic management (TLS decryption) (avoids performance degradation in addition to improving security visibility) (4)	Encrypted traffic management (TLS decryption) (4)
Centralized NetFlow/IPFIX generation (takes load off of switches in addition to improving security visibility) (5)	Centralized NetFlow/IPFIX generation (5)
Visibility into private clouds (VMware ESX and NSX) (9)	Visibility into private clouds (VMware ESX and NSX) (9)
Visibility into public clouds (AWS and Azure) (10)	Visibility for network functions virtualization (OpenStack) (11)
	Visibility into remote sites (14)
Simplify and control access to network data	Improve security in public clouds
Key Use Cases	Key Use Cases
First step to visibility: Get reliable data access for tools (1)	First step to visibility: Get reliable data access for tools (1)
Visibility during network upgrades/expanding network coverage (2)	Network detection and response (8)
Extract network metadata to optimize SIEMs (6)	Visibility into public clouds (AWS and Azure) (10)
Leverage application intelligence to optimize tool stack (7)	
Enhance service provider infrastructure visibility	Maintain security during infrastructure transformation
Key Use Cases	Key Use Cases
First step to visibility: Get reliable data access for tools (1)	First step to visibility: Get reliable data access for tools (1)
Visibility during network upgrades/expanding network coverage (2)	Visibility during network upgrades and coverage expansion (2)
Visibility for network functions virtualization (OpenStack) (11)	
Subscriber-aware visibility for data, voice and 5G networks (12)	
Lawful intercept (13)	

Mapping Use Cases to Role

In addition to aligning Use Cases with customer needs, it's also important to consider the role of the person you are speaking with and focus early conversations on the subset of Use Cases that are most likely to resonate with them. The table below includes all 14 Key Use Cases and maps them to the four types of buyers you are likely to encounter.

Up-to-date information about these Key Use Cases can always be found on [Gigamon.com](https://gigamon.com) Product and corporate marketing will create additional assets to support these Use Cases on an ongoing basis.

	Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
1. First Step to Visibility: Get Reliable Data Access for Tools	✓	✓	✓	✓
2. Visibility During Network Upgrades/Expanding Network Coverage	✓	✓	✓	
3. Improve Threat Prevention Efficacy with Inline Bypass	✓	✓		
4. Encrypted Traffic Management (TLS Decryption)	✓	✓		
5. Centralized NetFlow/IPFIX Generation	✓	✓	✓	
6. Extract Network Metadata to Optimize SIEMs		✓		
7. Leverage Application Intelligence to Optimize Tool Stack	✓	✓	✓	
8. Network Detection and Response		✓		
9. Visibility into Private Clouds (VMware ESX and NSX)	✓	✓		✓
10. Visibility into Public Clouds (AWS and Azure)	✓	✓		✓
11. Visibility for NFV (OpenStack)			✓	✓
12. Subscriber-Aware Visibility for Data, Voice and 5G Networks			✓	
13. Lawful Intercept			✓	
14. Visibility into Remote Sites	✓	✓		



Use Case: 1. First Step to Visibility: Get Reliable Data Access for Tools

Customer Pain:

Difficulty in getting reliable access to data for security analysis and application performance analysis. Pain is exacerbated by too much contention among various operational tools for network data due to SPAN limitations or departmental barriers.

Gigamon Solution:

- Physical or virtual taps
- Tap aggregators (GigaVUE® TA Series) or intelligent visibility nodes (H Series)
- GigaVUE-FM for management
- Key software capabilities: Flow Mapping®, Role-Based Access Control (RBAC)

Customer Pain	Gigamon Solution	Customer Benefits*
Organizational barriers make it difficult to access network data	Pervasive access with Visibility Platform and with Role-Based Access Control (RBAC)	<ul style="list-style-type: none">• Pervasive, nonintrusive access to network data anywhere in the infrastructure
Contention for SPAN ports delays critical projects	Pervasive and reliable data access with Visibility Platform	<ul style="list-style-type: none">• Pervasive, nonintrusive access to network data anywhere in the infrastructure• RBAC prevents unauthorized access
Poor reliability of SPAN data (especially during switch congestion) means loss of critical data	Tap recommended over SPAN	<ul style="list-style-type: none">• Ability to eliminate unreliability of SPAN ports• Tap once, distribute many times• Delivery to tools irrespective of network load
Limited access to environment: few ports available for analytic tools, many switches	Extract relevant data from anywhere in infrastructure using the Visibility Platform and deliver to analytic tools	<ul style="list-style-type: none">• Better utilization of limited analytic tool ports• Increased coverage by analytic tools• Increased ROI by sending only relevant traffic to analytic tools
Proof of concept (POC)/evaluation of multiple analytic tools happens serially	Feed live data to multiple analytic tools simultaneously	<ul style="list-style-type: none">• Accelerate time to evaluate multiple analytic tools• Evaluate tools with real-life data

*Results vary depending on the infrastructure and solution deployment.

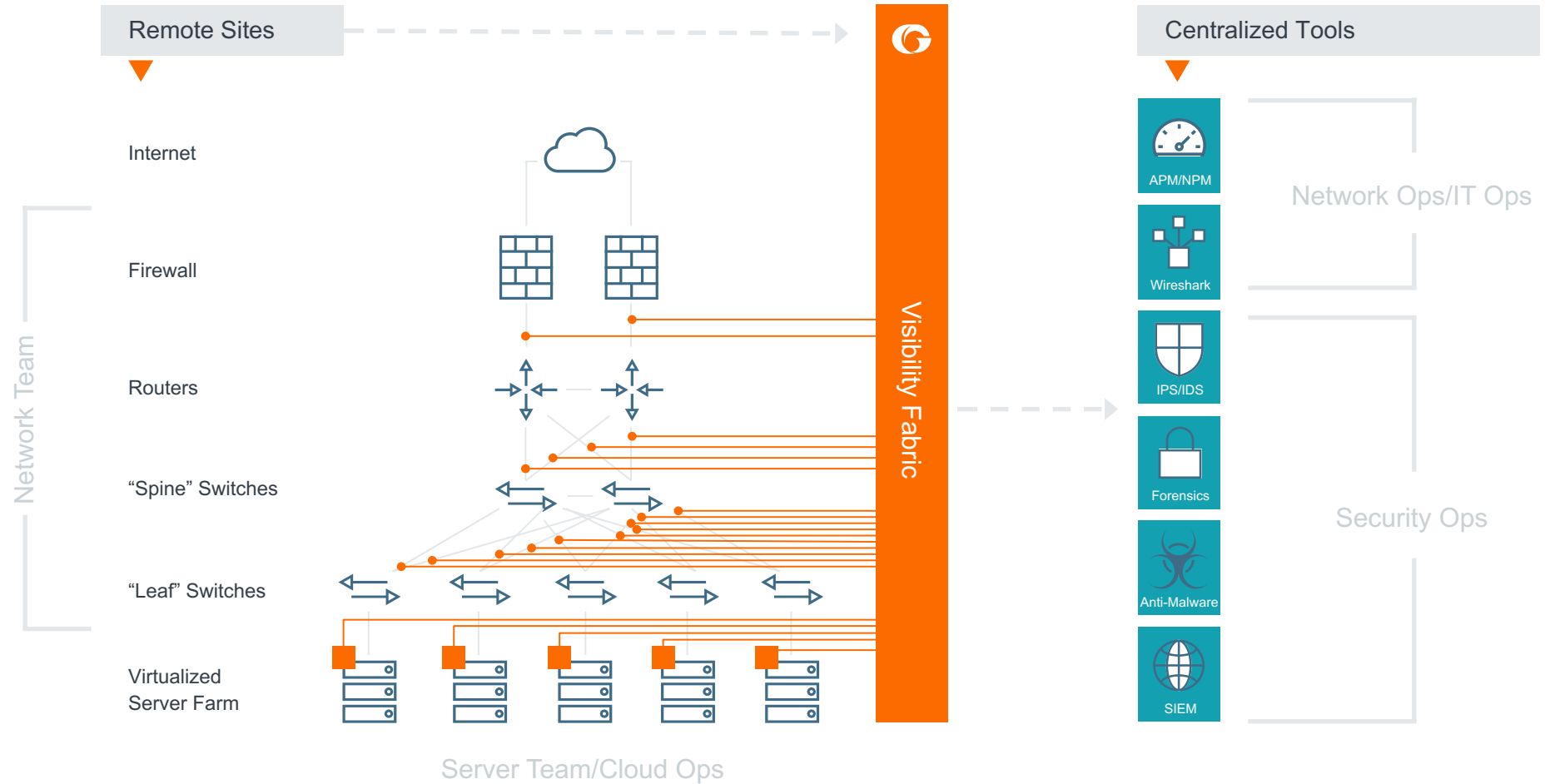
Ideal Ecosystem Partners: All

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓	✓	✓



Use Case:
1. First Step to Visibility: Get Reliable Data Access for Tools

Get quick and reliable access to network data for multiple teams with a common Visibility Platform



Ideal Ecosystem Partners: All

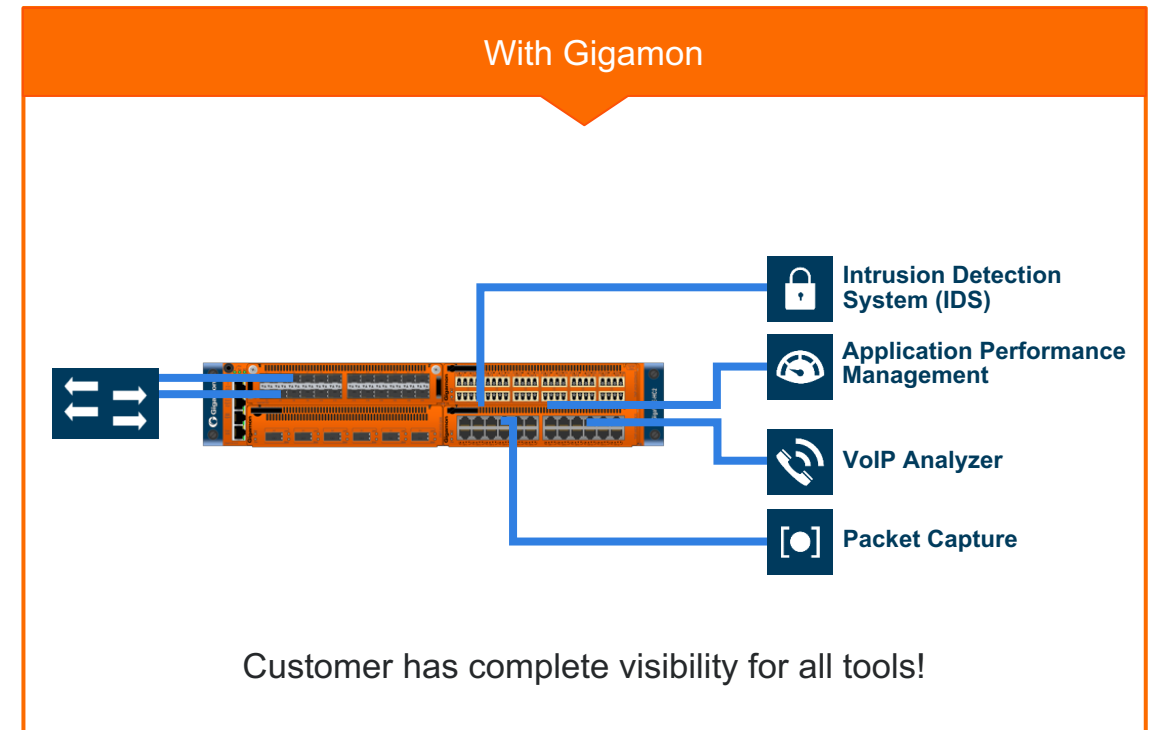
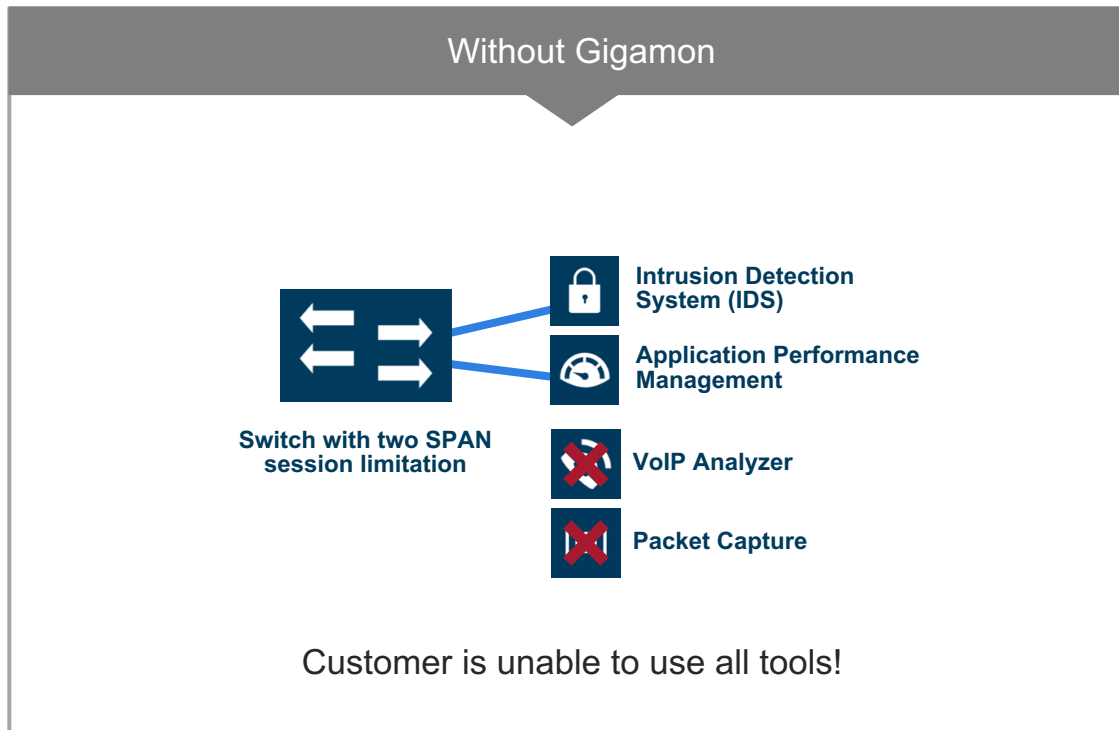


Use Case:

1. First Step to Visibility: Get Reliable Data Access for Tools

Eliminate SPAN Port Contention

Few SPAN ports, many operational and security tools



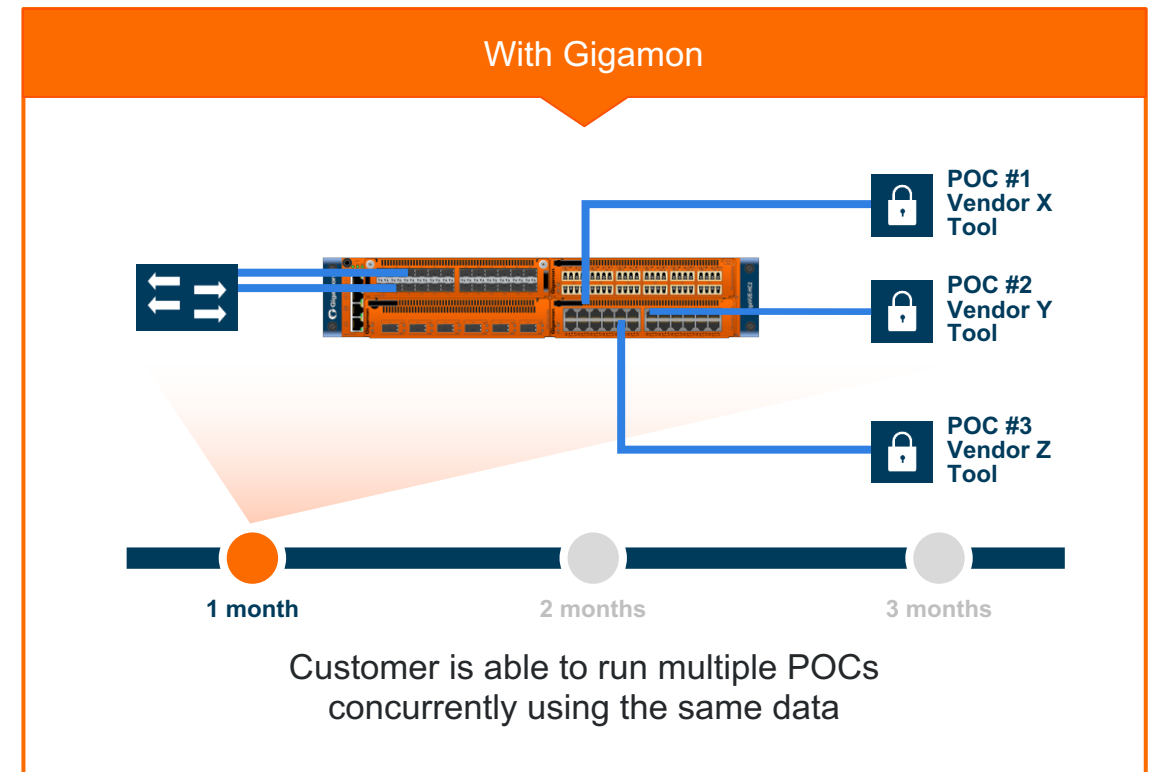
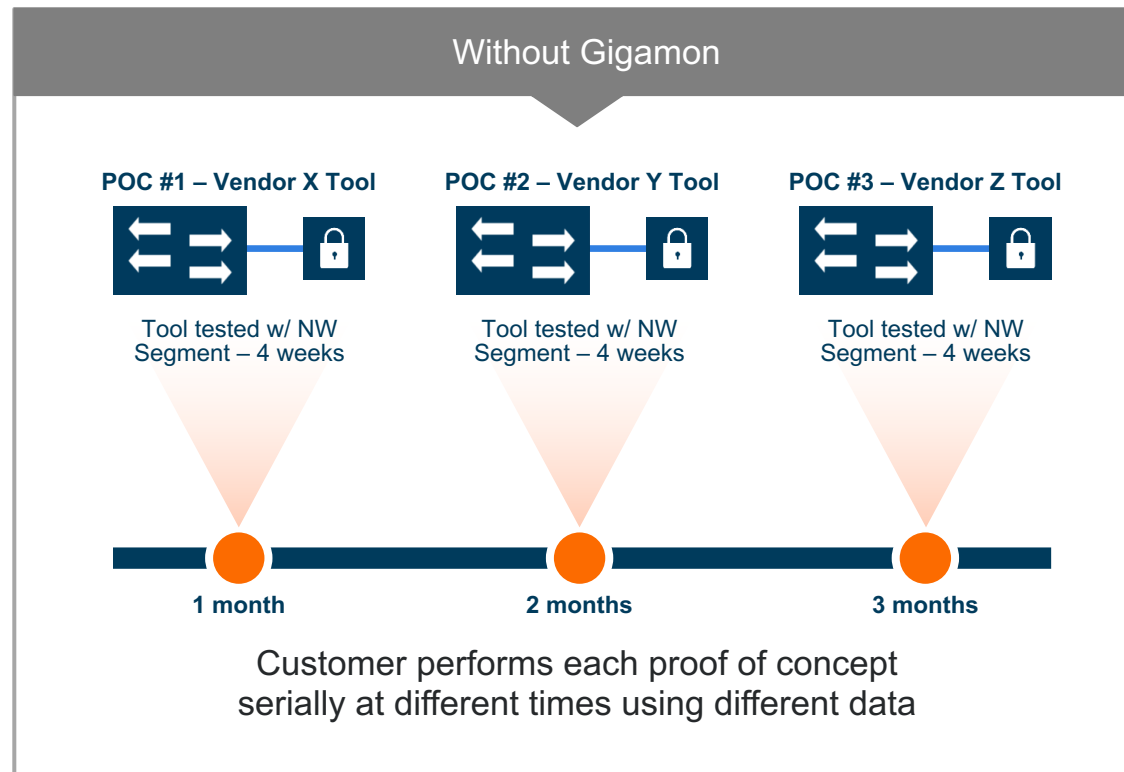
Ideal Ecosystem Partners: All



Use Case:
1. First Step to Visibility: Get Reliable Data Access for Tools

Run Multiple Proof of Concept in Parallel

Accelerate Certification of New Tools



Ideal Ecosystem Partners: All



Use Case: 2. Visibility During Network Upgrades/Expanding Network Coverage

Bring data to the tools versus bring tools to the data

Customer Pain:

- Security/operational tools do not operate at the same rate as the network; network upgrades force an unnecessary tool upgrade
- Security tools need more coverage: that is, pervasive visibility across infrastructure for best-in-class security infrastructure

Gigamon Solution:

- Physical or virtual taps
- Tap aggregators (GigaVUE® TA Series) or intelligent visibility nodes (H Series)
- GigaVUE-FM for management
- Key software capabilities: Flow Mapping®, Clustering, Fabric Maps, Role-Based Access Control (RBAC), GigaSMART® de-duplication

Customer Pain	Gigamon Solution	Customer Benefits*
Unnecessary security/monitoring tool upgrades due to network upgrade because network speeds and tool capacity do not match	<ul style="list-style-type: none">• Abstraction with the Visibility Platform. Select and deliver only traffic of interest; in other words, relevant traffic using Flow Mapping• Load balance traffic across tools with GigaStream®	<ul style="list-style-type: none">• Maintain existing tools even after a network upgrade• Load balance traffic across lower-capacity tools• Network can operate at a higher rate (such as 40G/100Gb), but by delivering only relevant traffic, tools can operate at a much lower rate
Security and operational tools need more coverage, but ad hoc deployment of tools is expensive and creates operational complexity	Visibility Platform: One complete platform for access to data anywhere (physical, virtual and cloud infrastructure)	<ul style="list-style-type: none">• Pervasive reach across physical, virtual and cloud to provide broader coverage and maximize tool utilization• Lower complexity: streamline new tool deployment• Greater agility: deploy new tools independently
Tool overload due to excessive traffic from network upgrade	GigaSMART intelligence (for example, de-duplication, slicing, App Filter Intelligence)	<ul style="list-style-type: none">• Increased ROI of tools by reducing traffic to just what is needed by tools
Organizational barriers make it difficult to access network data	Pervasive access with Visibility Platform and with Role-Based Access Control (RBAC)	<ul style="list-style-type: none">• Pervasive, nonintrusive access to network data across infrastructure• RBAC prevents unauthorized access

*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners: All

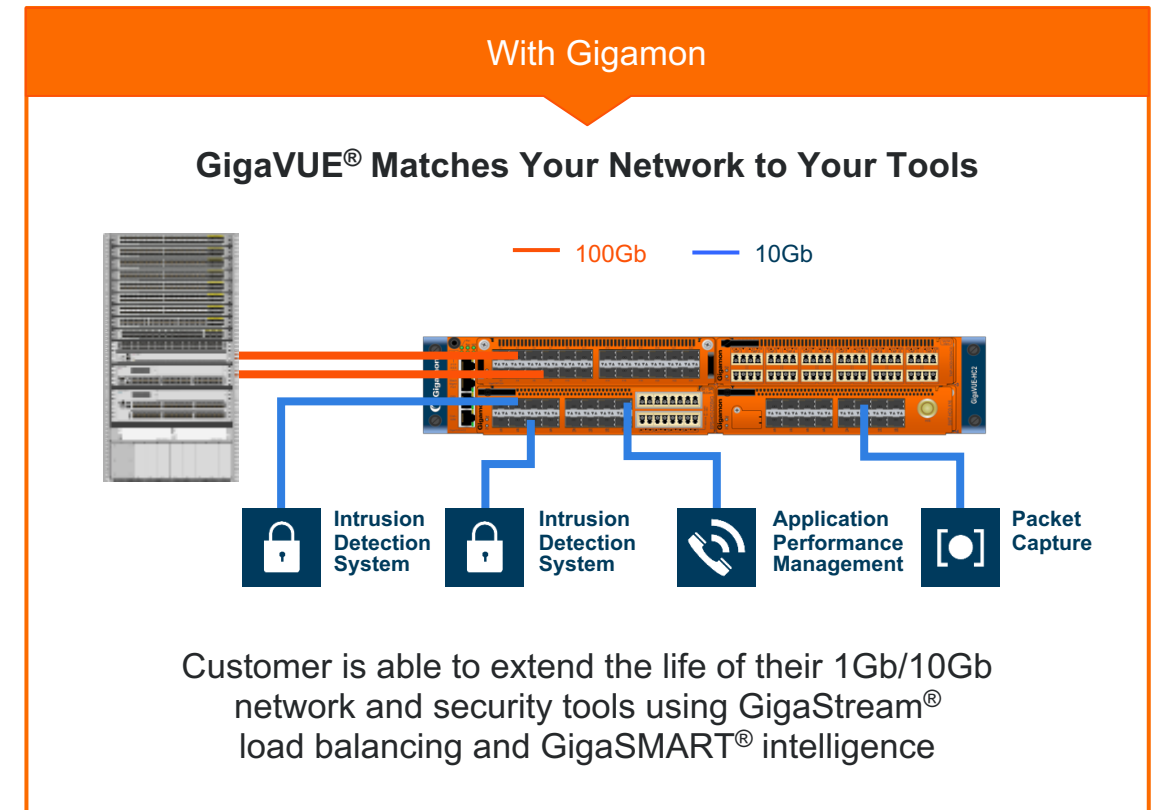
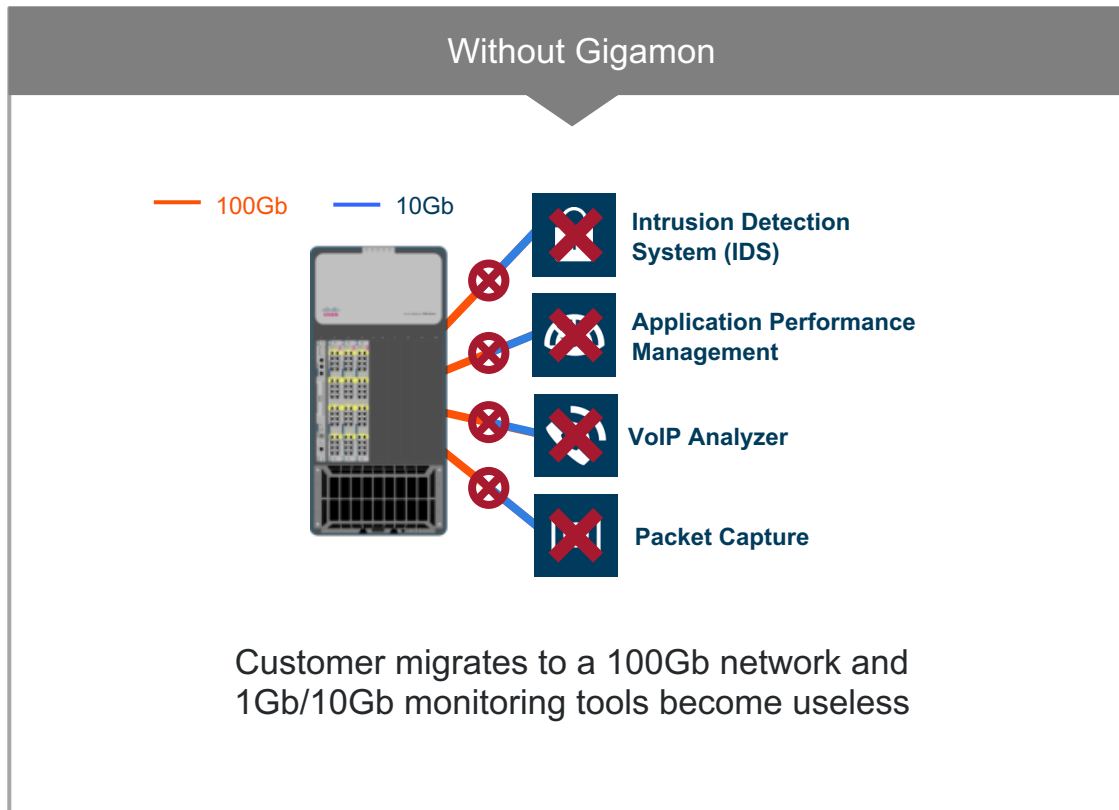
Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓	✓	



Use Case: 2. Visibility During Network Upgrades/Expanding Network Coverage

Change Media and Speed

10Gb, 40Gb or 100Gb Traffic to 1/10Gb Tools

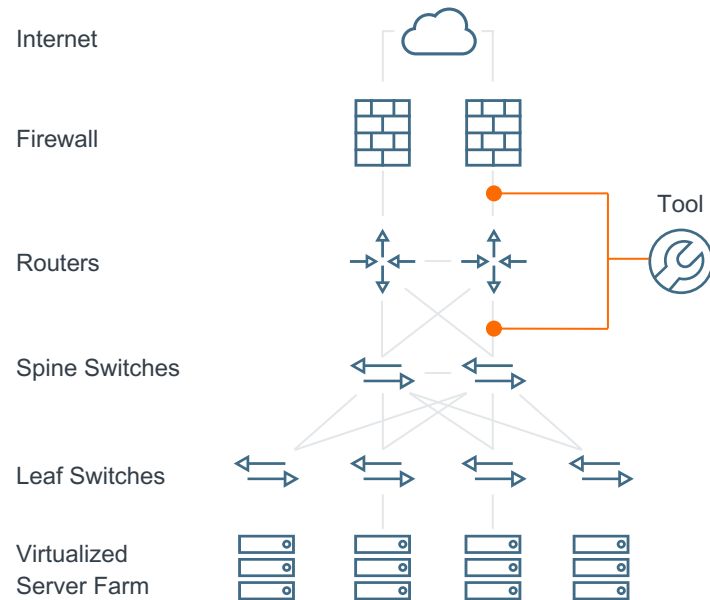


Ideal Ecosystem Partners: All



Use Case: 2. Visibility During Network Upgrades/Expanding Network Coverage

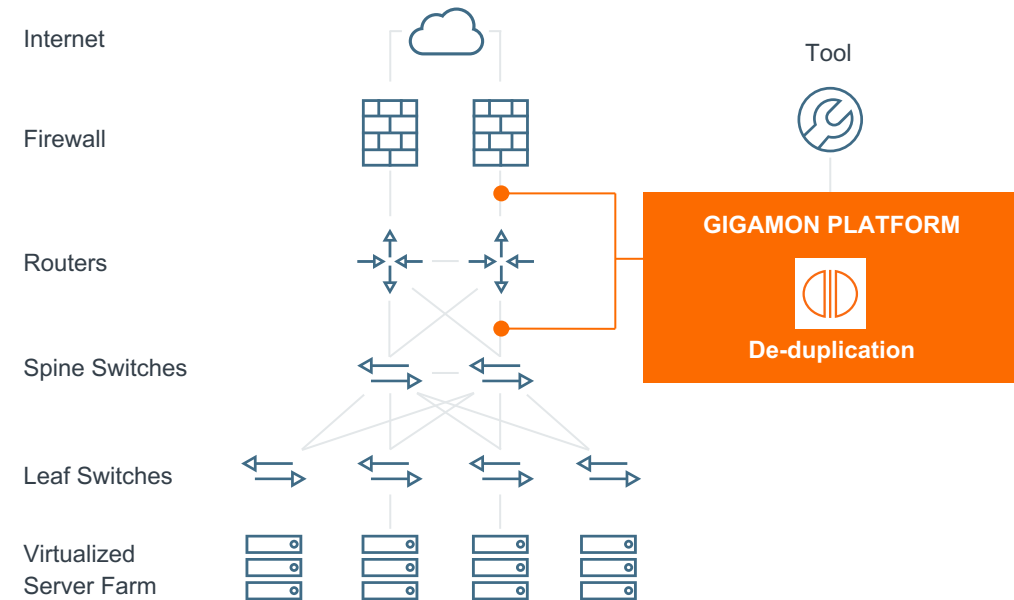
Benefit of De-duplication



Without Gigamon

- Same network packet is monitored at different tap points / SPAN points in infrastructure > multiple copies of same packet sent to tool
- Inaccurate performance measurements due to duplicates
- Tool overload due to additional processing incurred
- For packet recorders/forensics tools: Reduction in retention period because of storing duplicate packets

Ideal Ecosystem Partners: All



With Gigamon

- Gigamon Platform de-duplicates multiple copies of the same network packet to send a single copy of the packet to the tool
- Increase ROI: Typical benefit of 2x to 3x savings in tools
- Lower overhead on tools: offload processing overhead of duplicate detection from tools
- Higher tool performance, higher retention period for packet recorders/forensics tools
- Selectable fields to determine duplicates/control detection interval



Use Case: 3. Improve Threat Prevention Efficacy with Inline Bypass

Customer Pain:

- For NetOps: Inline threat prevention tools process all traffic, affecting network performance and application latency. Tool failure causes network failure.
- For SecOps: Difficulty with inline tool upgrades, traffic inspection and inline placement.)

Gigamon Solution:

- GigaVUE-HC1/HC2/HC3 with inline bypass module
- GigaVUE-FM for orchestration and management
- Key software capabilities: Inline Bypass, GigaStream®

Customer Pain	Gigamon Solution	Customer Benefits*
For network ops team:		
All inline tools process all traffic, thereby affecting network performance and application latencies	<ul style="list-style-type: none">• Select and deliver only traffic that needs to be processed by each inline tool• Share traffic load across multiple tools	<ul style="list-style-type: none">• Maximize tool efficacy• Reduce impact to network and application performance
Failure of a single inline security tool causes network failure	<ul style="list-style-type: none">• Bypass unhealthy tools• Integrated physical bypass protection• Resilient inline architecture	<ul style="list-style-type: none">• Maximize availability and resiliency of network
For security ops team:		
Difficulty in upgrading inline tools due to coordination between network and security teams	Add, remove, and upgrade tools seamlessly without coordinating maintenance windows	<ul style="list-style-type: none">• Reduce security effort for security team• Reduce time of exposure from weeks to hours/minutes when critical vulnerabilities need to be fixed
Need to inspect traffic with a variety of security tools	Integrate inline, out-of-band, flow-based tools and metadata	<ul style="list-style-type: none">• Achieve pervasive security via Security Delivery Platform
Not all security tools can or should be placed inline continuously	Dynamically move a security tool from monitor mode to inline mode and back	<ul style="list-style-type: none">• Programmatically take action to block malicious flows• Validate new software on prevention tool before moving inline• Minimize impact to network flows until anomaly is detected

*Results vary depending on the infrastructure and solution deployment.

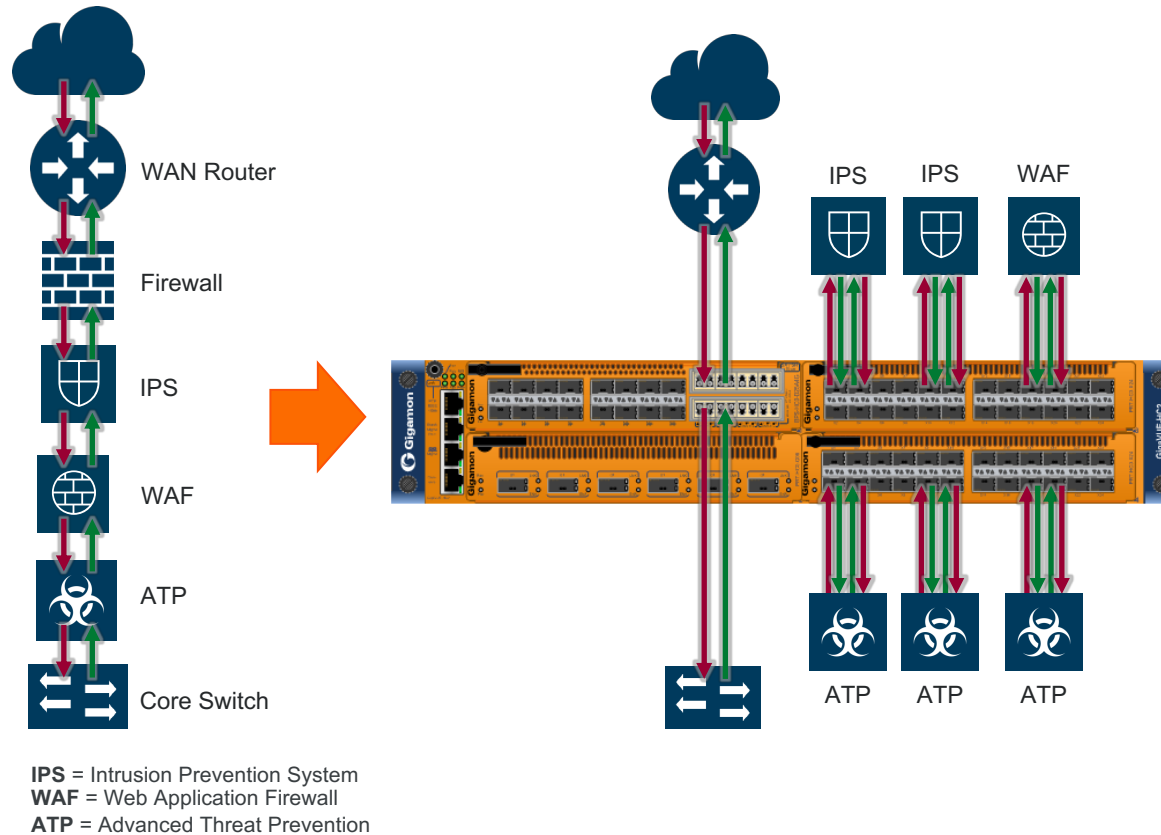
Ideal Ecosystem Partners:



Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓		



Use Case: 3. Improve Threat Prevention Efficacy with Inline Bypass



Maximize availability & resiliency (for network teams)

- Maximize tool efficacy
- Increase scale of security monitoring
- Bypass protection with advanced health checks to maximize availability

Maximize operational agility (for security teams)

- Add, remove, upgrade tools seamlessly: reduce risk and security effort
- Migrate tools from detection to prevention modes (and vice versa)
- Integrate inline, out-of-band, flow-based tools and metadata to a common platform

Ideal Ecosystem Partners:





Use Case: 4. Encrypted Traffic Management (TLS Decryption)

Customer Pain:

- Lack of visibility and control of growing TLS traffic causes blind spots
- Inability to inspect malware using TLS for Command and Control communications
- Performance degradation with TLS decryption in existing tools

Gigamon Solution:

- GigaVUE® HC1/HC2/HC3 appliance
- GigaSMART® module with TLS decryption
- GigaVUE-FM for orchestration and management

Customer Pain	Gigamon Solution	Customer Benefits*
Lack of visibility and control of growing TLS/SSL traffic entering/leaving enterprise causes blind spots	Automatic visibility into TLS/SSL traffic regardless of port or application	<ul style="list-style-type: none">• Complete, automatic visibility into TLS/SSL traffic regardless of port or application that is entering/ leaving the enterprise
Inability to inspect malware using TLS tunnels for Command and Control (C2) communication	Decrypt egress traffic exiting an enterprise to detect C2 activity	<ul style="list-style-type: none">• Expose hidden threats, malware, and data exfiltration attempts to accelerate incident detection and response
Existing tools suffer up to 80% performance degradation when TLS decryption is enabled	Centralized, high-performance TLS decryption that enhances existing security tools	<ul style="list-style-type: none">• High-performance, scalable and flexible deployment options that enhance existing security tools without hindering performance or throughput
Ensuring data privacy and policy compliance within encrypted networks	Selective decryption policies based on URL categorization, domain names and more	<ul style="list-style-type: none">• Bypass known, good traffic while decrypting suspicious or unknown traffic• Compliance with existing rules and regulations, inside and outside the enterprise
Cost and latency hit by decrypting network traffic on each tool	Decrypt once, inspect many times	<ul style="list-style-type: none">• Lower cost, lower application latency and reduced admin overhead by centralizing the decryption function

*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners:



IMPERVA



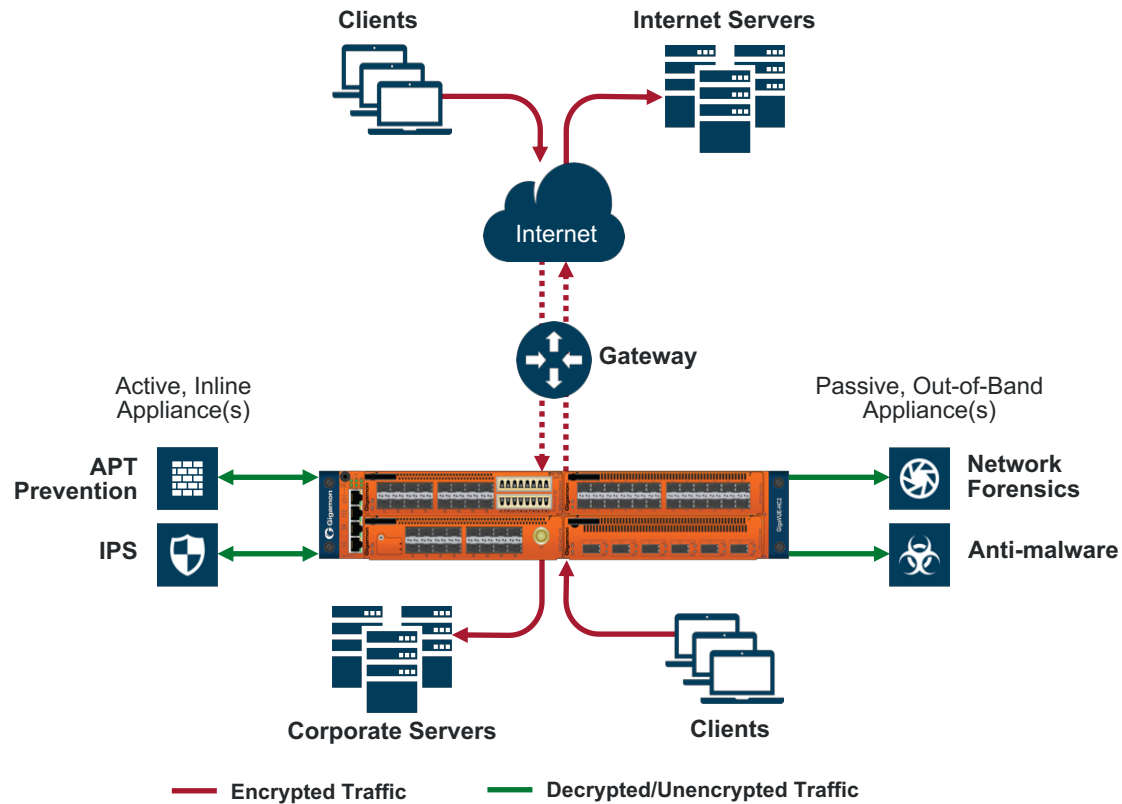
RSA

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓		



Use Case: 4. Encrypted Traffic Management (TLS Decryption)

Key Capabilities



Automatic SSL/TLS detection
on any port or application:
inbound and outbound



Scalable interface support
(1Gb to 100Gb)



Decrypt once,
feed many tools



Strong crypto support:
PFS, DHE, Elliptic Curve ciphers



Certificate validation and
revocation lists: strengthens
organizations' security posture



Strong privacy compliance:
categorize URL before decryption

Ideal Ecosystem Partners:



IMPERVA



RSA



Use Case: 5. Centralized NetFlow/IPFIX Generation

Customer Pain:

NetFlow (IPFIX) generated by network switches provides limited visibility that, in turn, degrades security and negatively impacts traffic flow performance.

Gigamon Solution:

- GigaVUE® HC1/HC2/HC3 appliance
- GigaSMART® module with IPFIX/NetFlow decryption
- GigaVUE-FM for orchestration and management

Customer Pain	Gigamon Solution	Customer Benefits*
Lack of ubiquitous flow record generation capabilities across infrastructure	Centralized, high-fidelity, unsampled NetFlow record generation	<ul style="list-style-type: none">• Security tools have complete view of network, versus isolated network segment traffic
High impact on network switches generating NetFlow flow records	High throughput, out-of-band NetFlow generation on Visibility Platform	<ul style="list-style-type: none">• No performance impact on production switches
Switches generate sampled NetFlow that are inadequate for security	Unsampled 1:1 NetFlow generation	<ul style="list-style-type: none">• Complete and precise picture of network activity for security analysis without loss of fidelity
Different IPFIX formats across different switch manufacturers create management complexity	Generate and export flow records in all standard formats (NetFlow v5, NetFlow v9, IPFIX and Common Event Format, or CEF)	<ul style="list-style-type: none">• Compatibility with legacy and next-generation IPFIX/ NetFlow collectors• Consistent flow record format across entire network
Lack of flexibility in picking target networks/ applications for NetFlow Generation	Combine Flow Mapping® with NetFlow generation for high-fidelity output	<ul style="list-style-type: none">• Combine Flow Mapping with NetFlow generation for high-fidelity output
Troubleshooting and incident analysis requires both flow record and packet analysis	Common platform for both deep packet analysis and flow record analysis	<ul style="list-style-type: none">• Integrated monitoring strategy that combines both packet and flow record analysis• Up to 99% traffic reduction using NetFlow analysis
Vanilla NetFlow records do not contain metadata beyond basic flow info	Optional enhanced metadata added to flow records	<ul style="list-style-type: none">• Advanced insight with enhanced application metadata

*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners:



plixer



splunk>

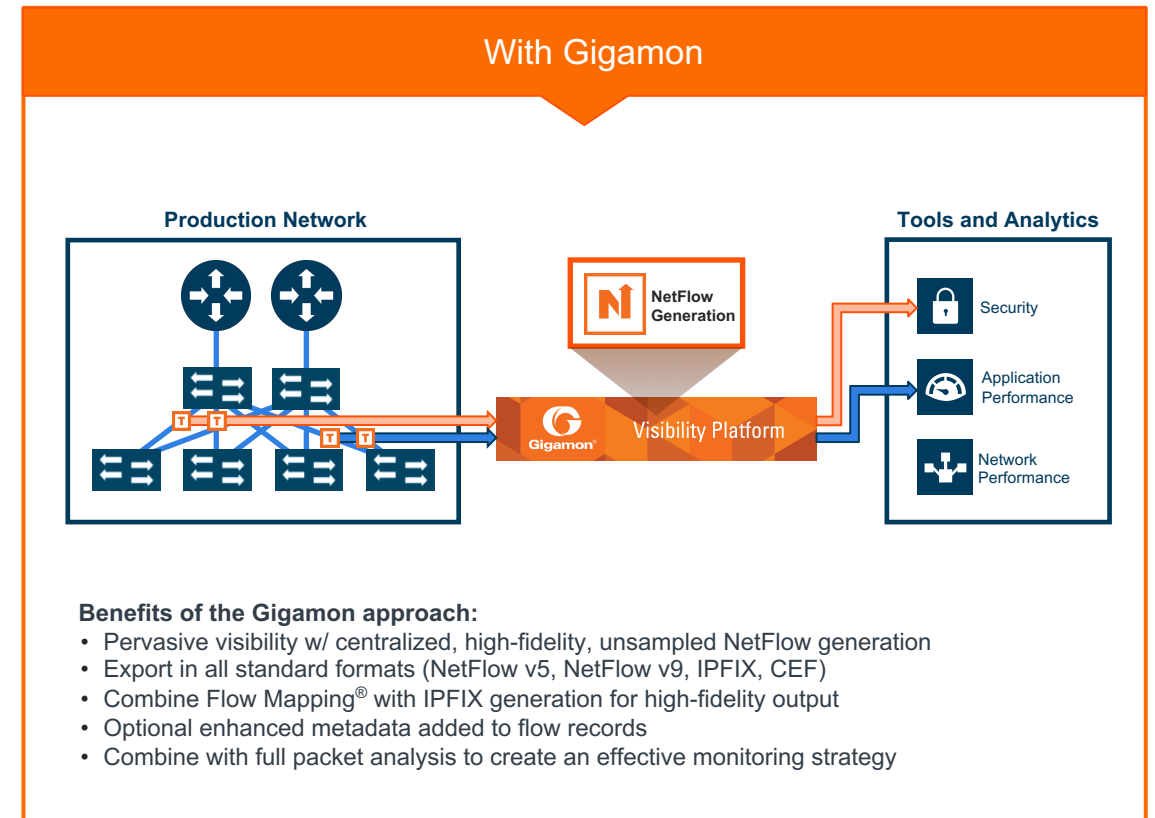
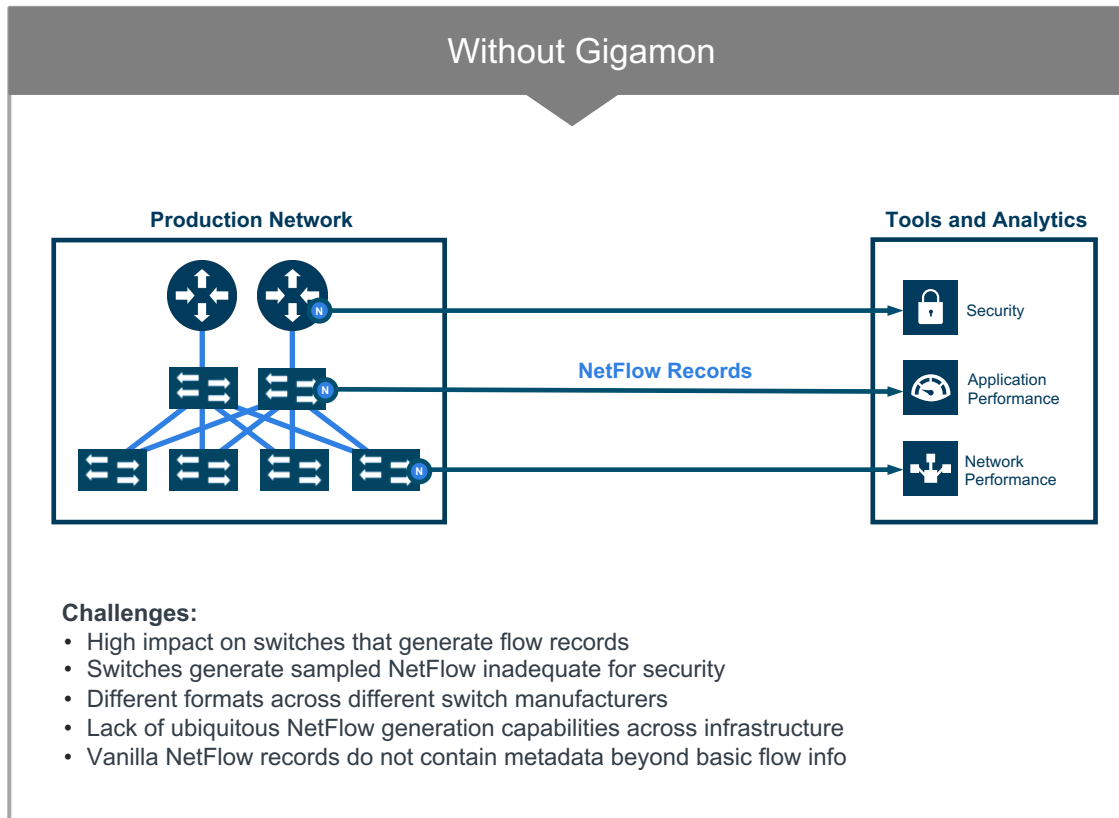


Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓	✓	



Use Case: 5. Centralized NetFlow/IPFIX Generation

The Power of the Platform: NetFlow/IPFIX Generation



Ideal Ecosystem Partners:



plixer



splunk





Use Case: 6. Extract Network Metadata to Optimize SIEMs

Customer Pain:

- Log data is not reliable for SecOps as the source is not controlled by SecOps
- Network traffic is too voluminous and cannot be fed directly to SIEMs
- High cost of SIEM
- Limited SOC resources overwhelmed with false positives

Gigamon Solution:

- GigaVUE® HC1/HC2/HC3 appliances
- GigaSMART® application metadata intelligence
- GigaVUE-FM for orchestration and management

Customer Pain	Gigamon Solution	Customer Benefits*
Device logs are not reliable for SecOps as the source is not controlled by SecOps. Device logs do not provide a complete picture of actual network behavior.	<ul style="list-style-type: none">• Extract application metadata from network traffic and feed to SIEMs• Over 5000+ metadata elements generated corresponding to 3000+ detected applications• Export metadata in multiple formats (CEF, IPFIX with extensions)• Apps for third-party platforms (Splunk, IBM QRadar) that leverage the app metadata	<ul style="list-style-type: none">• Extract important application and transaction metadata using network traffic as the source of truth (for example, DNS, TLS, HTTP)• Reduced load on SIEMs and other analytic tools by precisely defining only the relevant fields necessary for a customer's use case• Reduced load on source (such as an app server) that was generating the log data
Network traffic is too voluminous for early detection of attacker activity, especially when critical business apps need to be protected	Use application metadata extracted from network traffic for first-order analysis	<ul style="list-style-type: none">• Reduce the quantity of data ingested by several orders of magnitude, complement with full packet visibility for more detailed analysis• Faster time to root cause isolation
High cost of SIEM	Metadata reduces quantity of data ingested by several orders of magnitude	<ul style="list-style-type: none">• Reduced indexing costs on SIEM
Limited SOC resources overwhelmed with false positives	Gigamon Insight™ provides cloud network detection and response service based on network metadata	<ul style="list-style-type: none">• Cut through the noise and enjoy high-confidence threat detection, investigation and response capabilities on a common platform with Gigamon Insight• Low maintenance: Gigamon Insight is delivered as a SaaS

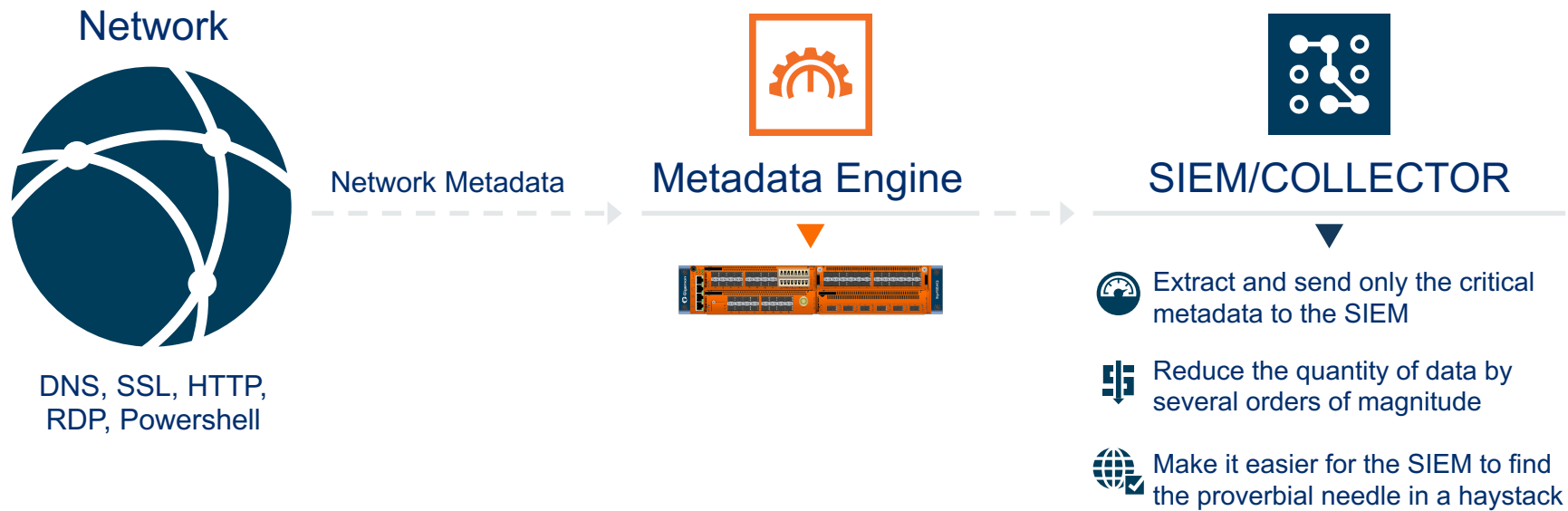
*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners:    

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
	✓		



Use Case:
6. Extract Network Metadata to Optimize SIEMs



Ideal Ecosystem Partners: splunk> IBM #LogRhythm MICRO FOCUS



Use Case: 7. Leverage Application Intelligence to Optimize Tool Stack

Customer Pain:

- Limited visibility to applications running in a network
- Low-risk, high-volume traffic hogging limited tool capacity
- Reduced detection performance/increased risk due to limited scope of coverage

Gigamon Solution:

- GigaVUE® HC1/HC2/HC3 appliances
- GigaSMART® application filter intelligence and application monitoring
- GigaVUE-FM for orchestration and management

Customer Pain	Gigamon Solution	Customer Benefits*
For security ops team:		
Low-risk, high-volume traffic (for example, social media streams) hogs limited capacity of security tools, leading to unnecessary overprovisioning of tools	Application Filter Intelligence: <ul style="list-style-type: none"> • Take include/exclude filter actions to identify relevant applications to deliver to tools • Bulk actions based on app categories (for example, all SCADA traffic, social networks, P2P) 	<ul style="list-style-type: none"> • Filter out high-volume, low-risk traffic • Filter in high-risk, application-specific traffic
Attackers bypass defenses with port spoofing, forcing security admins to inspect all data	Identify applications and network protocols independent of encapsulation, port number or encryption	<ul style="list-style-type: none"> • Ability to do targeted inspection of network protocols and apps of interest
Reduced detection performance/increased risk due to limited scope of coverage	Distribute apps of interest to the right tool at the right time from anywhere in the infrastructure	<ul style="list-style-type: none"> • Distribute tool investment across a larger attack surface by focusing on high-risk/business-critical apps
Custom applications developed in an enterprise are difficult to isolate	Custom regular expression-based application session filtering extracts the entire application session of interest and nothing more	Quickly isolate the custom application of interest for performance analysis, security analysis or root cause identification

*Results vary depending on the infrastructure and solution deployment.

Solutions continued on next page

Ideal Ecosystem Partners:



Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓	✓	



Use Case: 7. Leverage Application Intelligence to Optimize Tool Stack

Customer Pain:

- Limited visibility to applications running in a network
- Low-risk, high-volume traffic hogging limited tool capacity
- Reduced detection performance/increased risk due to limited scope of coverage

Gigamon Solution:

- GigaVUE® HC1/HC2/HC3 appliances
- GigaSMART® application filter intelligence and application monitoring
- GigaVUE-FM for orchestration and management

Customer Pain	Gigamon Solution	Customer Benefits*
For network ops team:		
<ul style="list-style-type: none">• Limited visibility of apps in a network for performance, troubleshooting and shadow IT awareness• Lack of operational context/tool overprovisioning due to processing of irrelevant application data	<ul style="list-style-type: none">• Application Monitoring extends visibility to Layer 7 applications• Identify over 3200 apps• Application Filter Intelligence lets actions be taken to filter applications of interest to the tools team	<ul style="list-style-type: none">• Improve tool performance, detection efficacy
Custom applications developed in an enterprise are difficult to isolate	Custom regular expression-based application session filtering extracts the entire application session of interest and nothing more	Quickly isolate the custom application of interest for performance analysis, security analysis or root cause identification

*Results vary depending on the infrastructure and solution deployment.

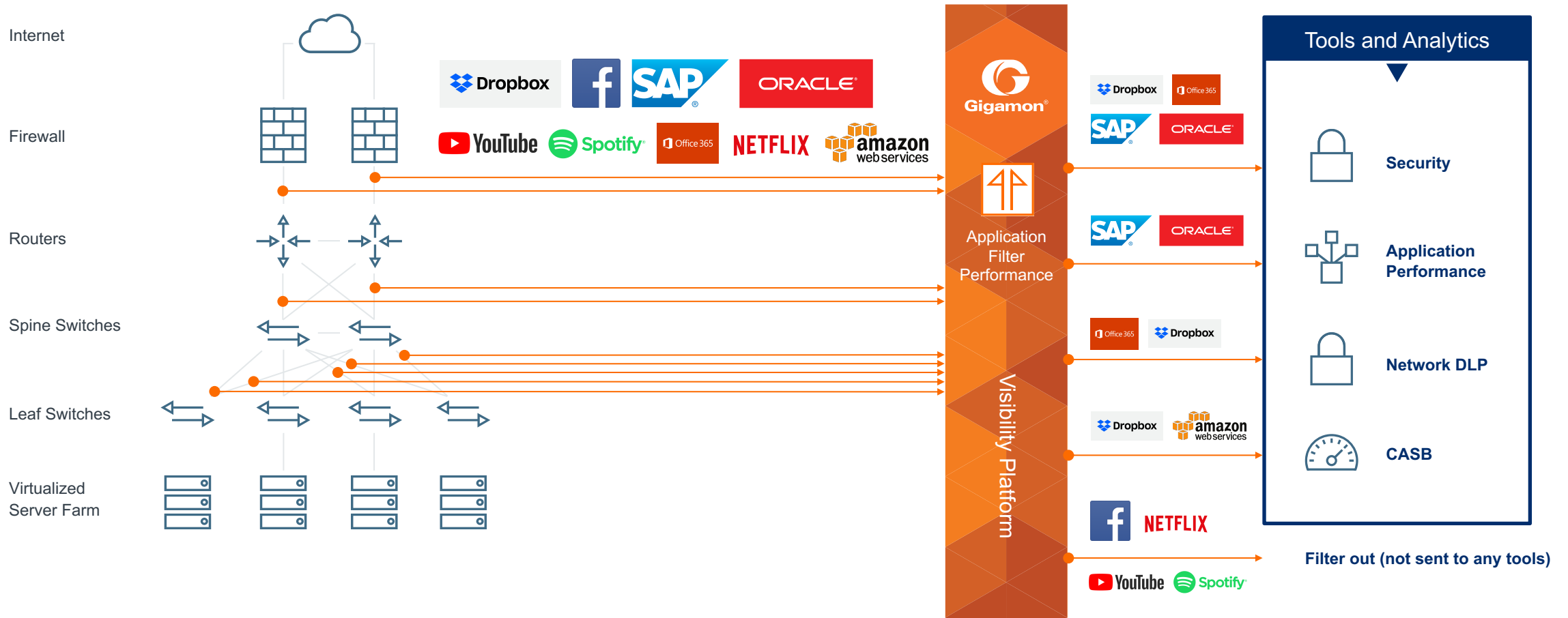
Ideal Ecosystem Partners:



Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓	✓	



Use Case: 7. Leverage Application Intelligence to Optimize Tool Stack



Ideal Ecosystem Partners: endace VIAT LiveAction FireEye



Use Case: 8. Network Detection and Response– Gigamon Insight

Customer Pain:

- Cannot see device, file, identity and other network activity
- Cannot detect/investigate incidents quickly enough due to excessive alert fatigue, false positives/negatives
- Cannot respond due to lack of quick access to the necessary data

Gigamon Solution:

- Gigamon Insight™

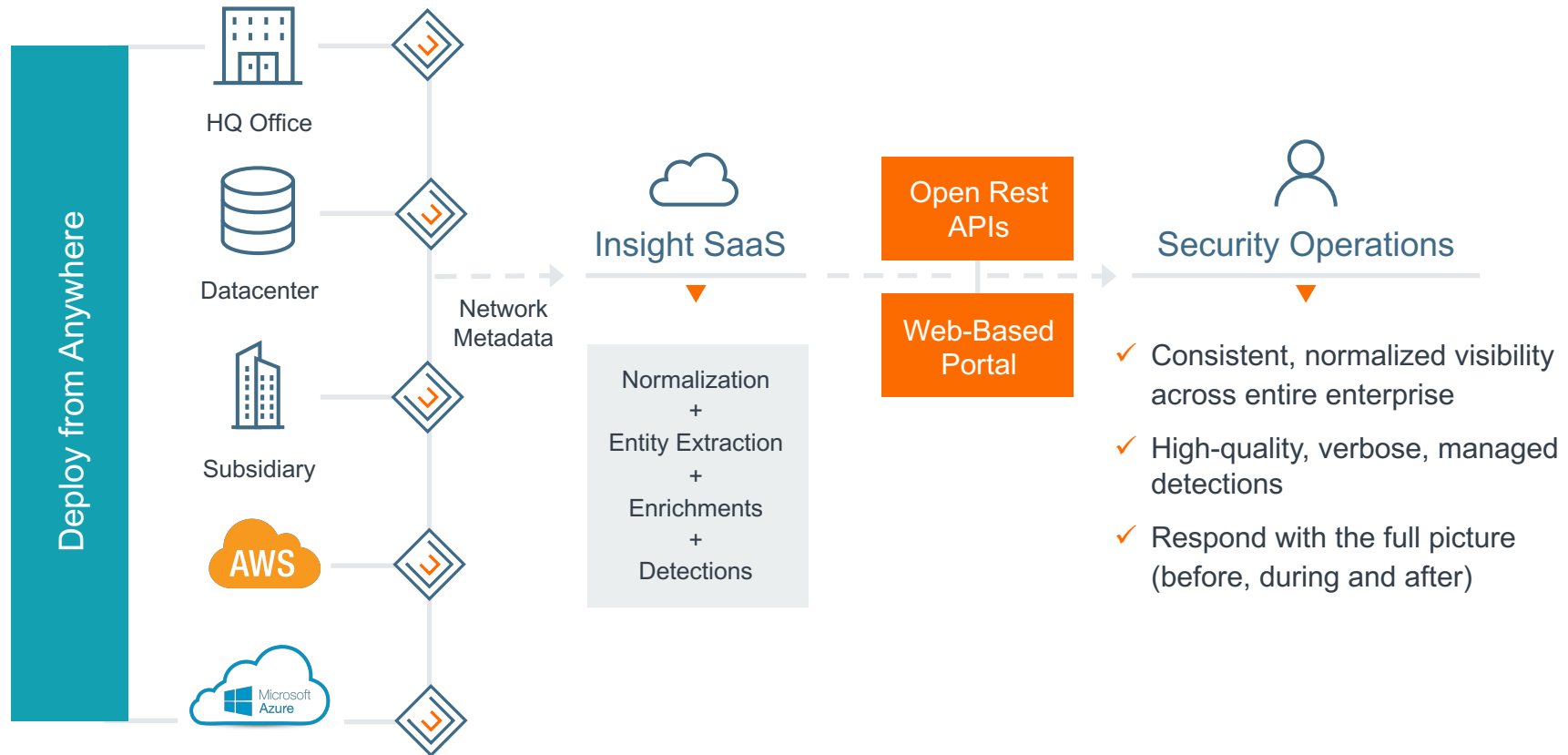
Customer Pain	Gigamon Solution	Customer Benefits*
Cannot See: Lack of necessary visibility – broad situational awareness of device, file, identity and other network activity	<ul style="list-style-type: none">• Insight platform, a cloud-based network detection and response (NDR) solution• SaaS solution that extracts and stores metadata from network traffic and offers applications that use this data to detect and investigate threats	<ul style="list-style-type: none">• SaaS delivery model accelerates time to value and friction with IT teams during deployment• Cut through the noise and enjoy high-confidence threat detection, investigation and response capabilities
Cannot Detect: Too much noise results in alert fatigue, low confidence in detections (false positives) and missed security events (false negatives). Difficult to demonstrate compliance. Consequence: High Mean Time to Detection (MTTD)	<ul style="list-style-type: none">• “Detect” app along with the elastic scale of a SaaS offering frees Incident Response (IR) teams from building the infrastructure and focuses their time instead on identifying the highest-priority threats/ incidents that require action	<ul style="list-style-type: none">• Do more with real-time access to current and historical network metadata for superior threat detection, investigation, response and hunting• Perform complete investigations, in real time, without switching between multiple applications
Cannot Respond: Lack quick access to the necessary data to make confident, actionable response decisions Consequence: High Mean Time to Response (MTTR)	<ul style="list-style-type: none">• “Investigate” app offers entity graphs, a rich query language and real-time access to data to empower fast analysis• Next step guidance helps accelerate intelligence response• Backed by a world-class Applied Threat Research team	<ul style="list-style-type: none">• Cloud solution designed and maintained by responders, for responders, for usability and performance.• Fast access to data helps optimize the efficiency of IR teams

*Results vary depending on the infrastructure and solution deployment.

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
	✓		



Use Case:
8. Network Detection and Response— Gigamon Insight





Use Case: 9. Visibility into Private Clouds (VMware ESX and NSX)



Customer Pain:

Organizations lack adequate visibility into private clouds and struggle to detect lateral threat propagation

Gigamon Solution:

- GigaVUE-VM for virtual visibility
- GigaVUE-FM for orchestration
- GigaVUE® H Series with GigaSMART® header stripping and IPFIX generation

Customer Pain	Gigamon Solution	Customer Benefits*
Blind spots for east-west traffic make it difficult to detect lateral threat propagation	Access, select, filter and distribute virtual traffic to be inspected by centralized out-of-band security tools	<ul style="list-style-type: none"> • Remove east-west blind spots in a software-defined data center • Increase ROI from tool investments with a common tool stack for physical and virtual infrastructure • Early identification of threats in the kill chain
Continuous visibility during VM migration (vMotion)	Integration with vCenter to detect vMotion events and auto-migrate visibility policies	<ul style="list-style-type: none"> • Continuous visibility and security during VM migration without any human intervention
Visibility and security gap when applications scale out (new VMs spun up)	API integration with VMware NSX: automatically associate visibility policies to new spun-up VMs, allowing for continuous visibility	<ul style="list-style-type: none"> • Automated visibility and security as applications scale out • VMware NSX-certified (network and security partner)
Micro-segmentation forces tool replication and inefficient resource utilization	Aggregate traffic from different microsegments. Deliver traffic corresponding to specific tenants.	<ul style="list-style-type: none"> • Reduce tool sprawl: Gain tenant-level visibility across multiple tenants with common tooling infrastructure.
Security tools unable to process new SDN-overlay transport (VXLAN)	De-capsulate VXLAN traffic (remove headers)	<ul style="list-style-type: none"> • Preserve ROI of existing tools that do not support SDN overlays • Gain tenant-level visibility by filtering specific VXLAN IDs
Lack of flow summaries (NetFlow/IPFIX data) as customers migrate to Cisco ACI architectures	Centralize NetFlow/IPFIX and metadata generation	<ul style="list-style-type: none"> • High-fidelity NetFlow/IPFIX and metadata generation for physical and virtual traffic

*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners:    All out-of-band tools

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓		✓

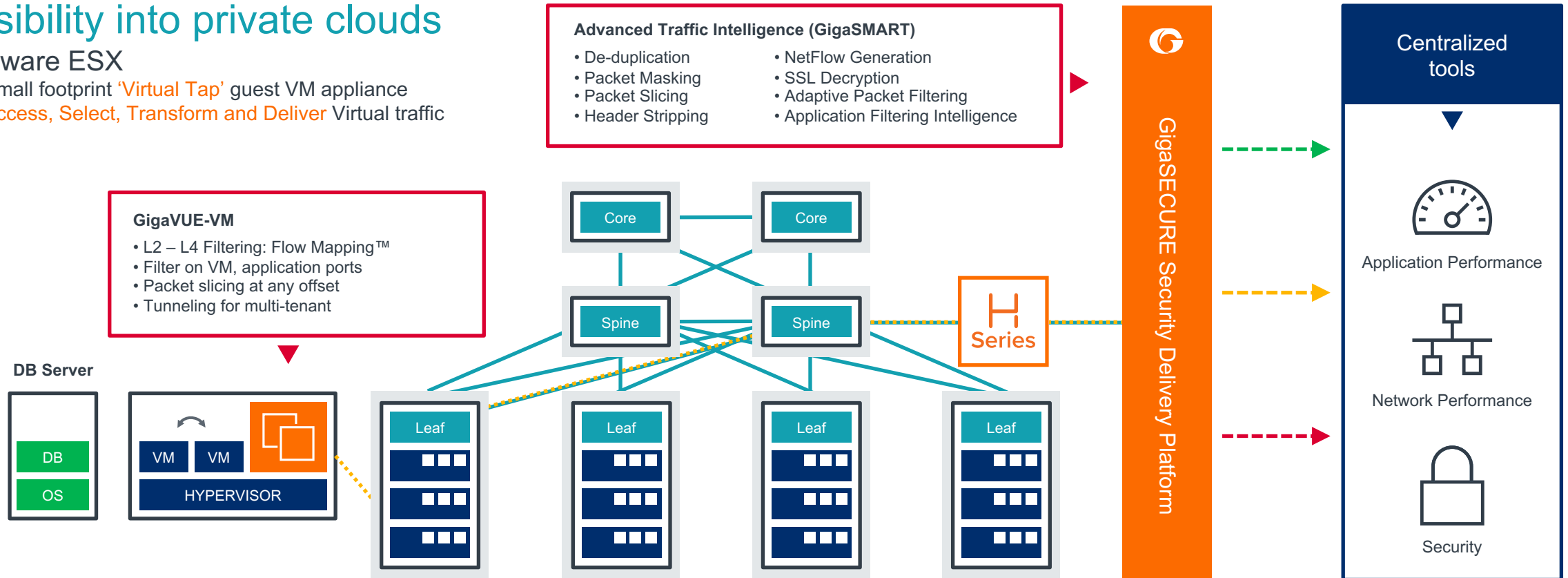


Use Case:
9. Visibility into Private Clouds (VMware ESX and NSX)

Visibility into private clouds

VMware ESX

- Small footprint 'Virtual Tap' guest VM appliance
- Access, Select, Transform and Deliver Virtual traffic



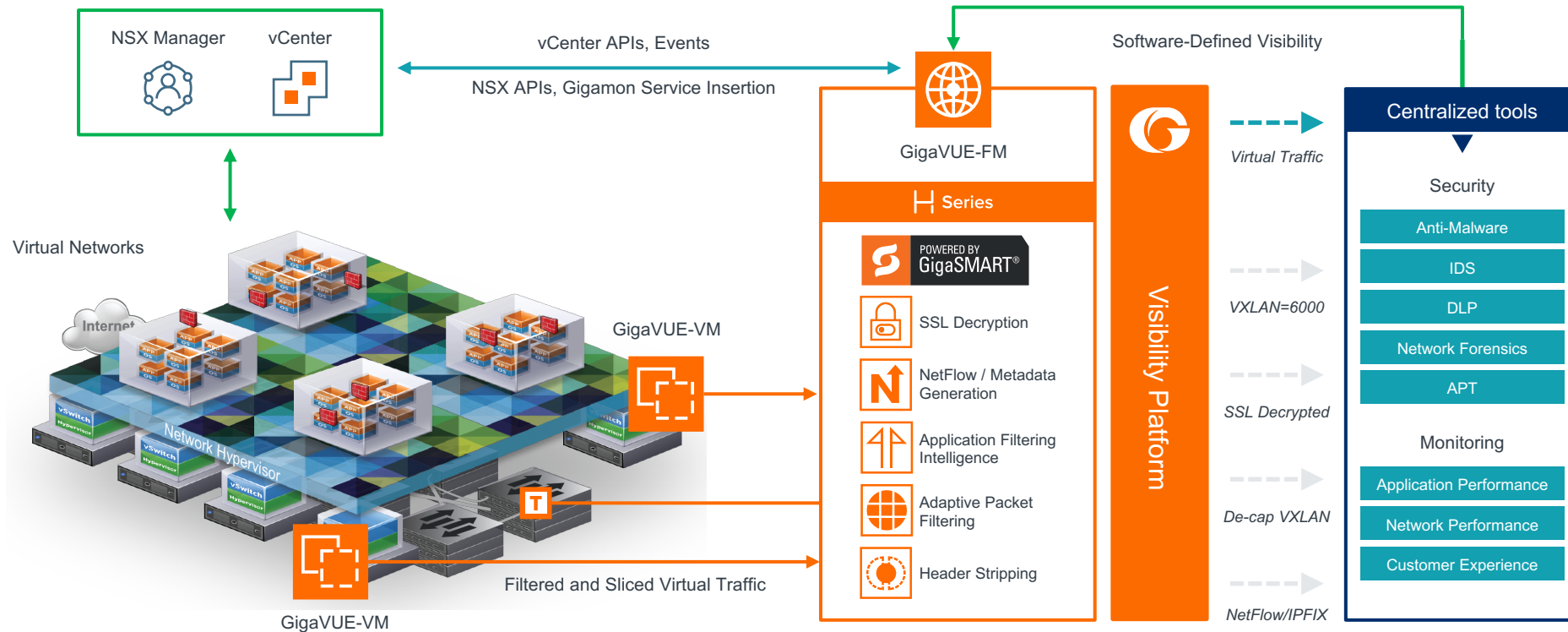
Ideal Ecosystem Partners: vmware cisco RSA All out-of-band tools



Use Case:
9. Visibility into Private Clouds (VMware ESX and NSX)

Visibility into private clouds

VMware NSX: Software-Defined Data Center/Monitoring for Tenant Visibility



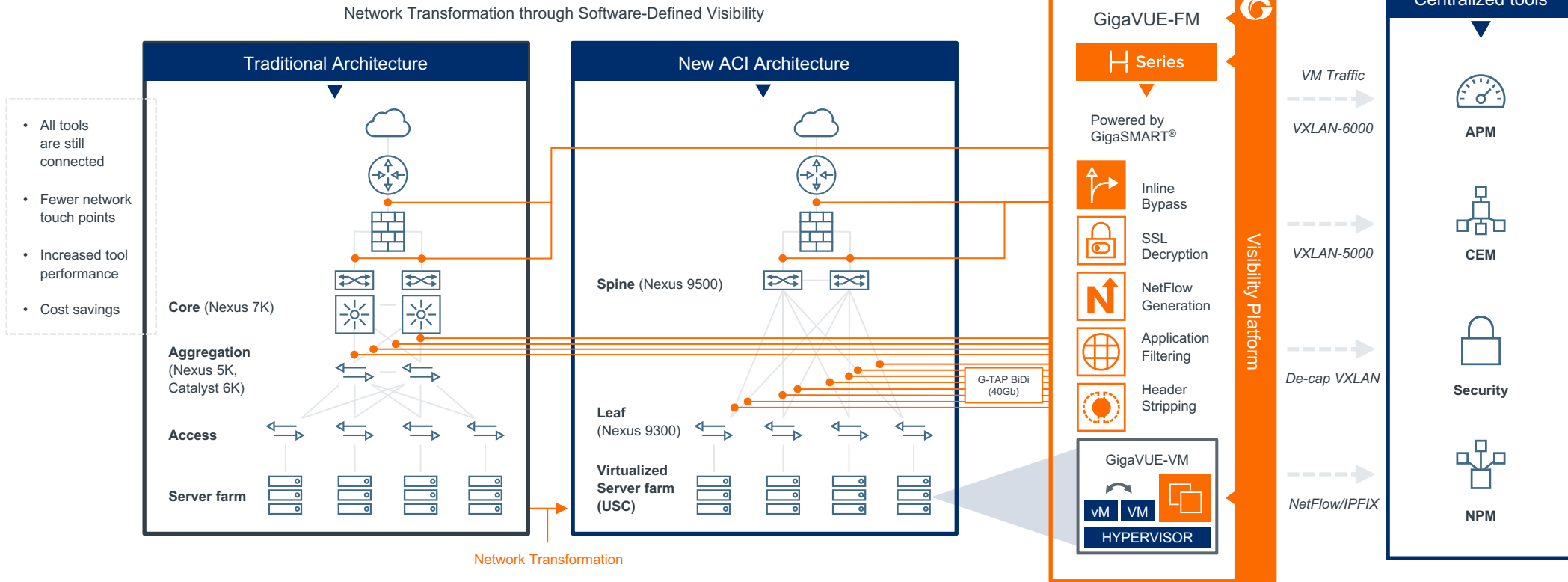
Ideal Ecosystem Partners: All out-of-band tools



Use Case: 9. Visibility into Private Clouds (VMware ESX and NSX)

Visibility into private clouds

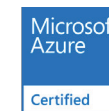
Cisco ACI: Tool centralization with Gigamon Visibility Platform



Ideal Ecosystem Partners: All out-of-band tools



Use Case: 10. Visibility into Public Clouds (AWS and Azure)



Customer Pain:

The use of public cloud infrastructure creates operational complexities for security and cloud admins and limits visibility into application workloads/infrastructure running in the public cloud. Identity and access controls alone do not suffice; network security controls in the cloud are required to ensure the right security posture.

Gigamon Solution:

- GigaVUE® V Series for AWS, Azure
- Gigamon Insight™ with Detect and Investigate apps

Customer Pain	Gigamon Solution	Customer Benefits*
Deploy a well-defined cloud security architecture: ensure that the public cloud is being used securely across the entire enterprise without purely relying on identity and access management controls	<ul style="list-style-type: none">• GigaVUE V Series for AWS and Azure: provides visibility into data in motion between application workloads	<ul style="list-style-type: none">• Complete visibility across public cloud, private cloud and on-prem infrastructure• Deploy more applications in the public cloud while meeting the needs of compliance and security
Security operations need to monitor activity across multiple virtual private clouds (VPCs)	<ul style="list-style-type: none">• Centralized visibility into all enterprise VPCs	<ul style="list-style-type: none">• See More, Secure More: Mitigate risk, ensure compliance. Improve scale, effectiveness, performance of security tools.
Multiple analytic tools need data. Per-tool agents in workloads impact compute/ VPC performance, add cost and complexity.	<ul style="list-style-type: none">• Eliminate per-tool agents• One consistent method to access and optimize traffic before delivering to tools	<ul style="list-style-type: none">• See What Matters: Deep, elastic visibility. One consistent way to deliver network data to multiple tools.
Difficult-to-understand choke points between application components without full network visibility	<ul style="list-style-type: none">• Gain full transparency into data exchanged between application components	<ul style="list-style-type: none">• Understand More: Identify vulnerable blind spots and choke points between workloads
Infrastructure components split between on- premises and cloud, creating operational complexity	<ul style="list-style-type: none">• Flexible deployment models: all-in-cloud, hybrid, multi-VPC, multi-region	<ul style="list-style-type: none">• Enables organizations to pace their cloud adoption• Flexible deployment models maximize choice
Detect and respond to security or network anomalies, detect lateral movement of threats and data exfiltration attempts	<ul style="list-style-type: none">• Gigamon Insight: SaaS-based network detection and response; deliver traffic from GigaVUE V Series to Gigamon Insight	<ul style="list-style-type: none">• Cloud-native detection and response offered as a SaaS service

*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners:

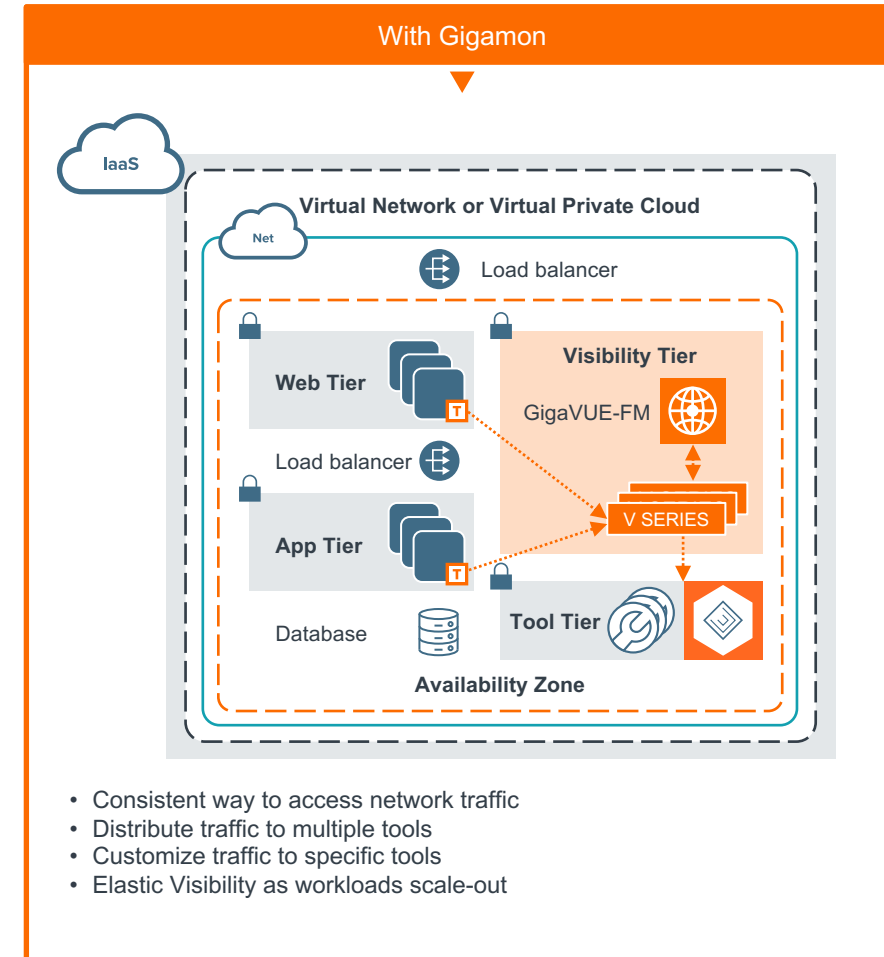
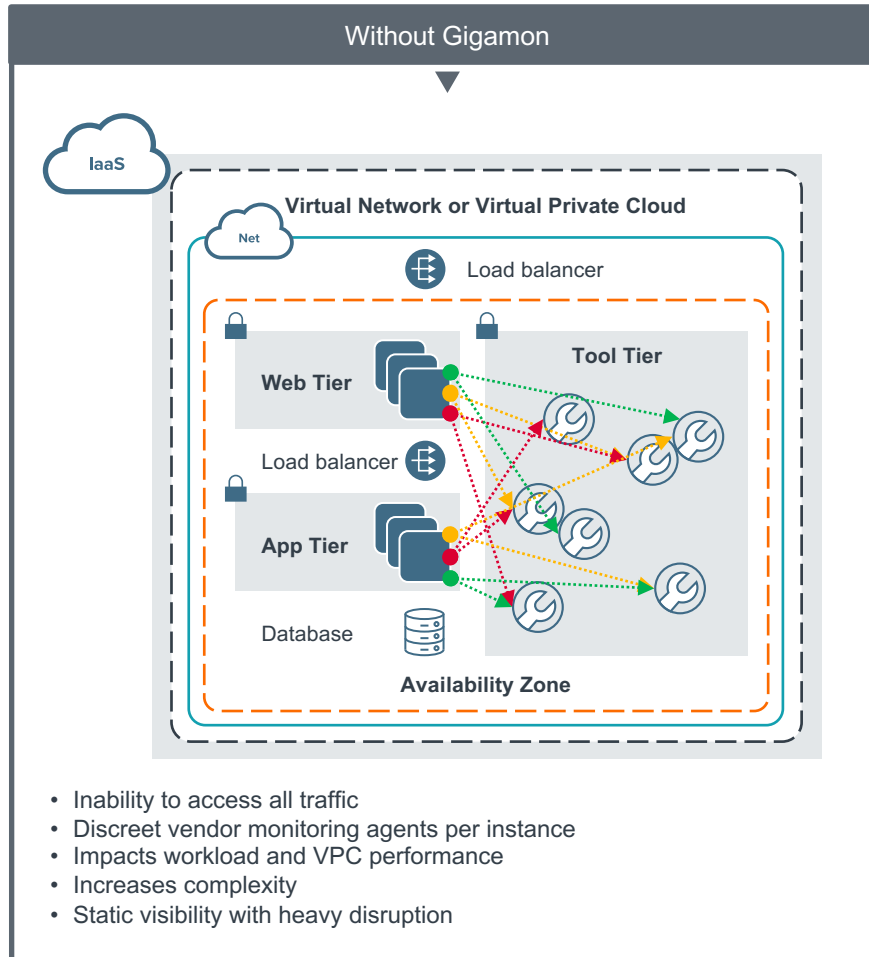


Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓		✓





Use Case: 10. Visibility into Public Clouds (AWS and Azure)



Ideal Ecosystem Partners:





Use Case: 11. Visibility for NFV (OpenStack)

Customer Pain:

- Control and user data separation (CUPS) and 5G evolution demand new virtualized infrastructure.
- East-west traffic between virtual network functions (VNFs) need to be efficiently obtained in a disaggregated virtualized infrastructure.
- Commodity solutions send more traffic to tools, overwhelming tools and adding complexity and cost.

Gigamon Solution:

- V Series for OpenStack
- GigaVUE-FM for management and orchestration

Customer Pain	Gigamon Solution	Customer Benefits*
Blind spots for east-west traffic between virtual network functions (VNFs)	<ul style="list-style-type: none">• iTraffic acquisition options using a choice of methods: VNF monitoring, tap as a service (TaaS), open virtual switch (OVS)-based mirroring or third-party tunnels to handle different deployment scenarios• Pre-filtering minimizes traffic backhauled from VNF• GigaVUE® V Series further aggregates, optimizes and distributes traffic to tools	<ul style="list-style-type: none">• Access, select, filter and distribute virtual traffic to be analyzed by centralized tool rail• Eliminates need for per-tool agents• Future-proof solution to handle different deployment scenarios including DPDK, SRIOV and more
Excessive traffic sent to tools overwhelms tool capacity, adding complexity and cost	<ul style="list-style-type: none">• Elastic-scale V Series that aggregates and applies multiple service functions (for example, Flow Mapping®, slicing, masking, NetFlow, sampling, overlapping map rules)• Service chaining of multiple functions in V Series	<ul style="list-style-type: none">• Send just the right traffic to the right tool
No traffic visibility for a tenant owner in an OpenStack-powered cloud	<ul style="list-style-type: none">• Lightweight G-vTAP module accesses traffic in a tenant's VM: to be inspected and distributed to centralized out-of-band security tools	<ul style="list-style-type: none">• Provides tenant owner the necessary controls to get visibility for east-west traffic, without needing NFVi (NFV infrastructure) owner's permissions• Centralized visibility for a multi-tenant deployment
Control and user data separation (CUPS) and 5G evolution demand new virtualized infrastructure	<ul style="list-style-type: none">• Single visibility solution including management across diverse environments (physical, virtual, cloud)	<ul style="list-style-type: none">• Lower cost of ownership; lower OpEx

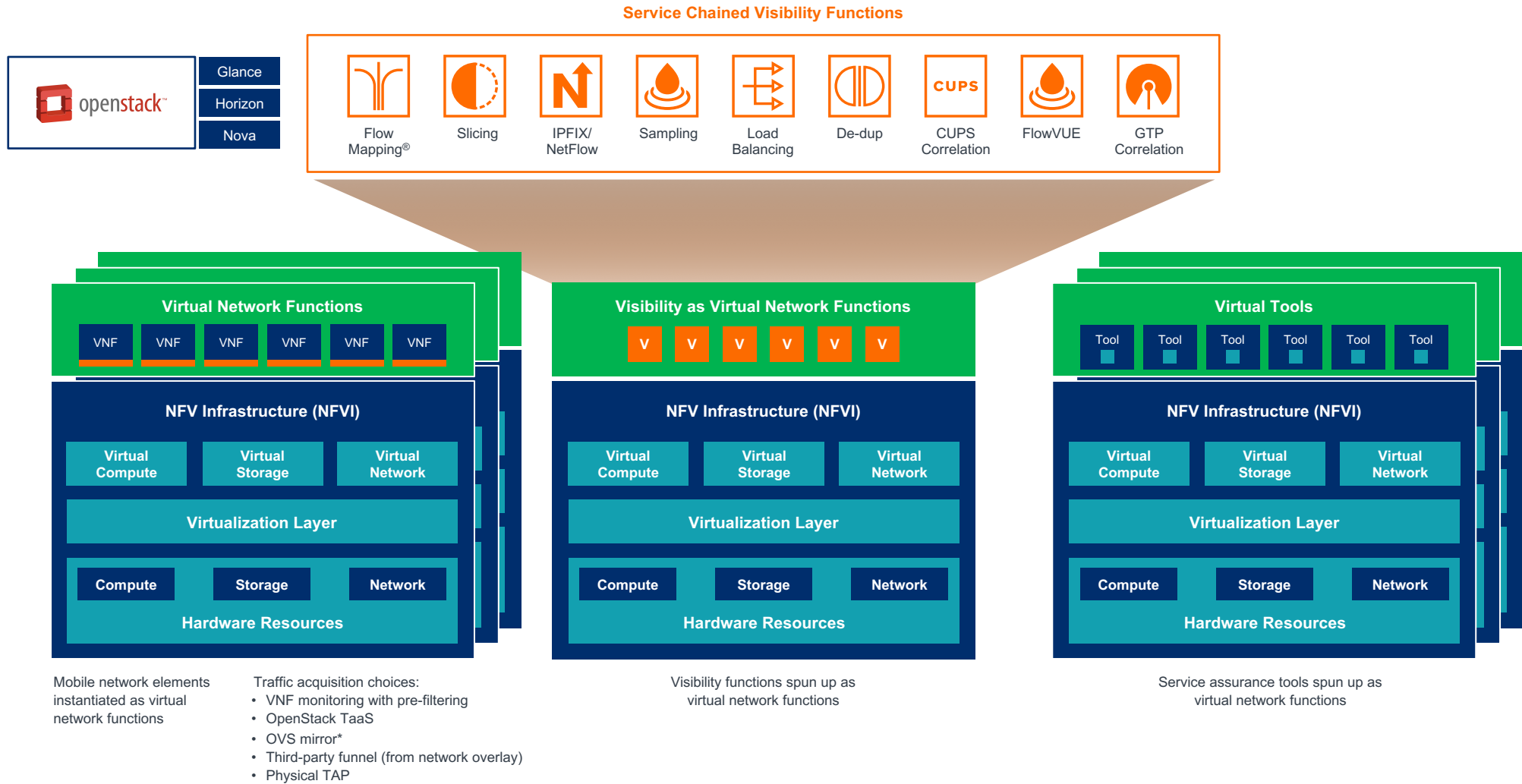
*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners: **VIAXI**

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
		✓	✓



Use Case:
11. Visibility for NFV (OpenStack)



Ideal Ecosystem Partners:

*Check for availability



Use Case: 12. Subscriber-Aware Visibility for Data, Voice and 5G Networks

Customer Pain:

Mobile service providers have too much traffic to analyze and too little budget to spend on tools. Impending transition to 5G is exacerbating this issue.

Gigamon Solution:

- GigaVUE® HC3 and GigaVUE-TA Series appliances
- GigaSMART® with GTP Correlation, SIP/RTP Correlation and FlowVUE® software
- GigaVUE V Series for virtual coverage
- Flow Mapping® with clustering
- GigaVUE-FM for orchestration and management

Customer Pain	Gigamon Solution	Customer Benefits*
<ul style="list-style-type: none"> • Traffic volume is overwhelming analytic probe capacity, with 5G dramatically exacerbating the issue • Analytic probes failing to keep up with growth in traffic/focused on low-value (irrelevant) network traffic • Excessive spend on current tooling 	<ul style="list-style-type: none"> • Correlation: Use GTP Correlation, SIP/RTP Correlation to offload expensive correlation tasks from tools • FlowVUE traffic scaling: Scale the traffic to fit tool capacity 	<p>See More. Secure More.</p> <ul style="list-style-type: none"> • Pervasive visibility across enterprise • Rapidly detect anomalous activity at remote sites • Maximize reach of security tools
Control and user data separation (CUPS) demanding new virtualized infrastructure	Single visibility solution including management across diverse environments (physical, virtual, cloud)	Lower cost of ownership; lower OpEx
Require solutions that maximize Average Profitability Per User (APPU)	FlowVUE scaling and whitelisting shifts monitoring resources to focus on high-value traffic	Reduce subscriber cost, increase subscriber profitability by recognizing that not all subscribers and not all data on the network are created equal
Lack of business and operational efficiencies: Multiple business units unable to share the same network traffic and subscriber data	<ul style="list-style-type: none"> • Common subscriber-aware visibility platform that supports multiple operational tools • Tool-agnostic platform with open integration capabilities with existing tools (for example, Tek, NetScout, BSS/OSS) 	<p>Gain an operational advantage by gaining:</p> <ul style="list-style-type: none"> • Deep insight into subscriber patterns to maximize customer experience • Reduce support costs

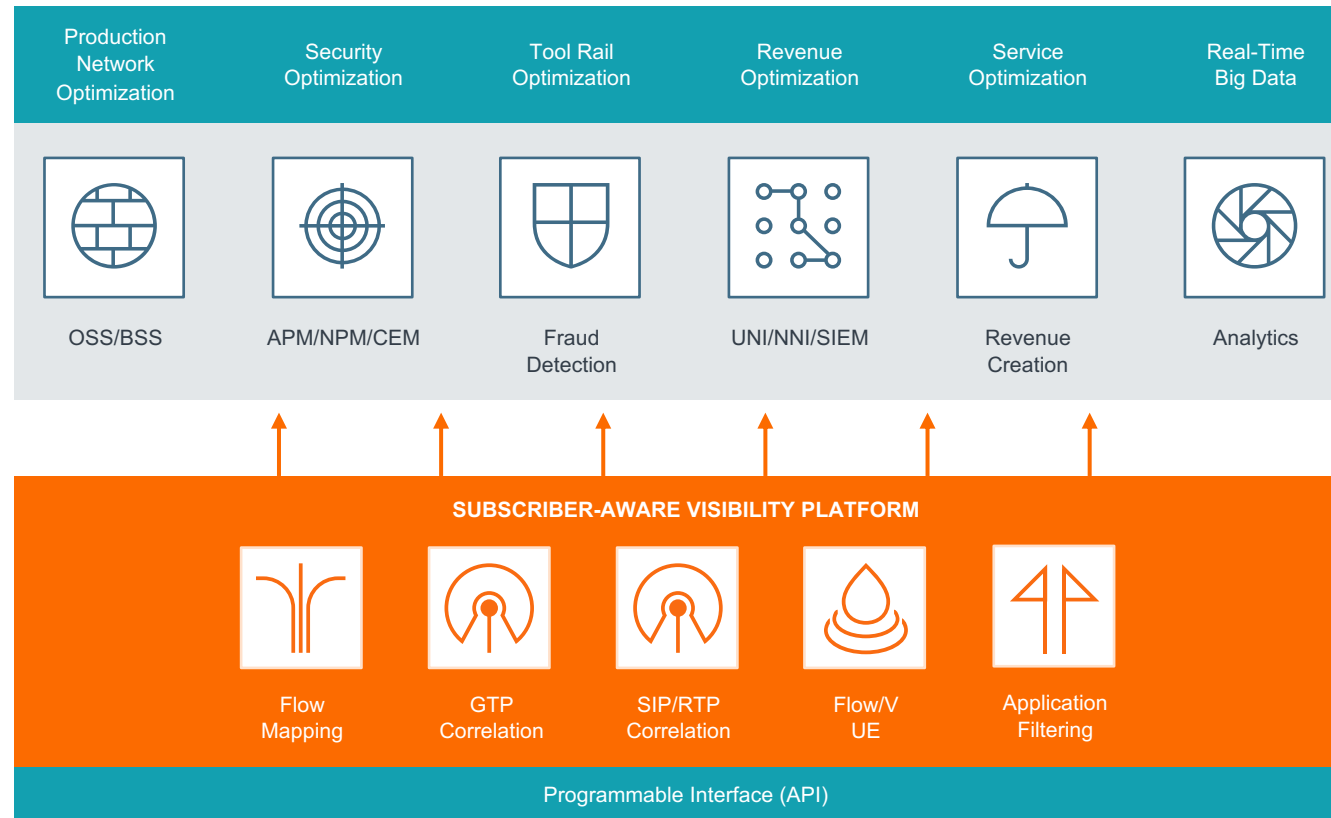
*Results vary depending on the infrastructure and solution deployment.

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
		✓	



Use Case:
12. Subscriber-Aware Visibility for Data, Voice and 5G Networks

Key Components





Use Case: 13. Lawful Intercept

Customer Pain:

Trying to identify a network threat is akin to finding a needle in a haystack. It's a difficult task that requires gaining access to all traffic while also ensuring compliance with the letter of the law to avoid collection of the wrong information.

Gigamon Solution:

- GigaVUE-HC3 with GigaVUE-TA Series
- GigaVUE-FM for orchestration and management
- Software: Flow Mapping®, Clustering, Fabric Maps

Customer Pain	Gigamon Solution	Customer Benefits*
Issues gaining access to traffic	Pervasive visibility to all traffic across the network	<ul style="list-style-type: none">• Tap traffic without interference to operation of existing network• Solve SPAN or Mirror Port contention issue
Finding the needle in a haystack	Finding the correct traffic faster speeds up warrant execution	<ul style="list-style-type: none">• Reduced amount of traffic to search through• Continue to capture LI traffic as target moves
Staying within the law	Select packet header, payload body or both – or trigger on specific fields of information to record	<ul style="list-style-type: none">• Comply with the letter of the law• Reduce fines from collecting the wrong information
Avoiding manual data collection	Resident Lawful Intercept (LI) capability prevents the need to ship staff and equipment	<ul style="list-style-type: none">• Substantially cut costs of complying with the letter of local laws for LI• Collect information on demand and as needed

*Results vary depending on the infrastructure and solution deployment.

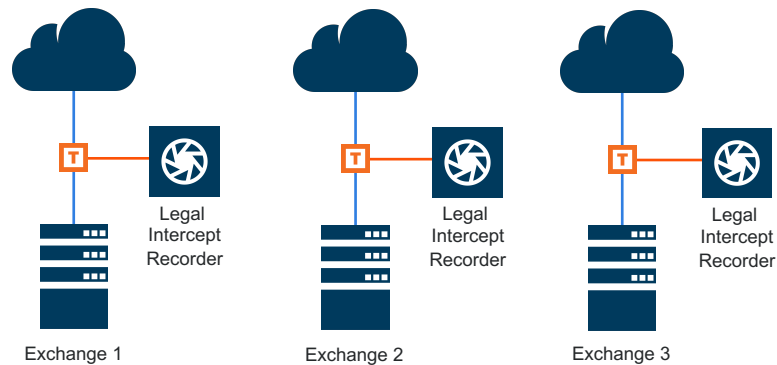
Ideal Ecosystem Partners: 

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
		✓	



Use Case: 13. Lawful Intercept

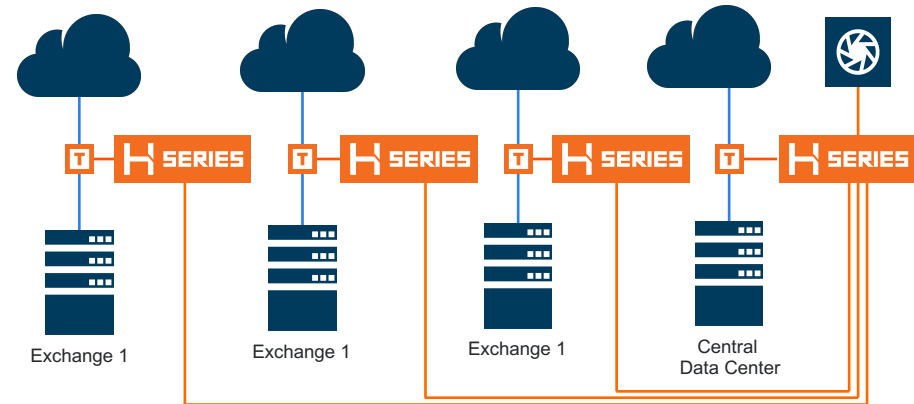
Without Gigamon



Challenges:

- Expensive, ad hoc approach
- Deploy equipment and staff as needed to each exchange/CO
- Requires staff and equipment to be immediately ready to deploy in order to satisfy the legal dates/terms on the government warrant

With Gigamon



Benefits of the Gigamon approach:

- Higher ROI: GigaVUE® nodes at each exchange tunnel traffic to a centralized Legal Intercept Recorder
- Flow Mapping® policies select only traffic that needs interception
- Ability to filter application flows to narrow traffic of interest

Ideal Ecosystem Partners:  endace



Use Case: 14. Visibility into Remote Sites

Customer Pain:

For multiple reasons, remote sites are tough to secure. They often lack sufficient security and operations personnel and budgets rarely allow replication of tools to remote sites.

Gigamon Solution:

- GigaVUE-HC1 for remote sites with GigaVUE® HC2/HC3 in data center
- GigaSMART® traffic intelligence: De-duplication, slicing, NetFlow/IPFIX
- GigaVUE-FM for orchestration and management

Customer Pain	Gigamon Solution	Customer Benefits*
Insufficient visibility into remote sites: • Remote offices • Critical infrastructure	Complete visibility into remote sites using an enterprise-wide Visibility Platform	See More. Secure More. • Pervasive visibility across enterprise • Rapidly detect anomalous activity at remote sites • Maximize reach of security tools
Proliferation of tools at remote sites increases complexity and cost	Visibility Platform approach: Extract data in motion remotely, analyze data centrally	More for Less. • Increased ROI by leveraging existing tools to analyze data in motion from remote sites
Low-bandwidth links to remote sites makes traffic visibility a challenge	GigaSMART Traffic Intelligence (for example, de-duplication, slicing, NetFlow, metadata) to reduce traffic backhauled	More for Less. • Increased ROI by sending only traffic of interest from remote sites to centralized monitoring and security tools
Limited number of operations engineers at remote sites	Full-service compact node GigaVUE-HC1. Part of our enterprise-wide Visibility Platform. Delivers flow records, metadata and traffic visibility.	Reduce Security and Operational Effort. • Shorten time to deploy security and other operational tools
Inline and out-of-band security tools at remote sites hard to maintain	Flexibility to deploy/maintain tools either inline or out of band	Add/remove/upgrade tools without impacting network availability

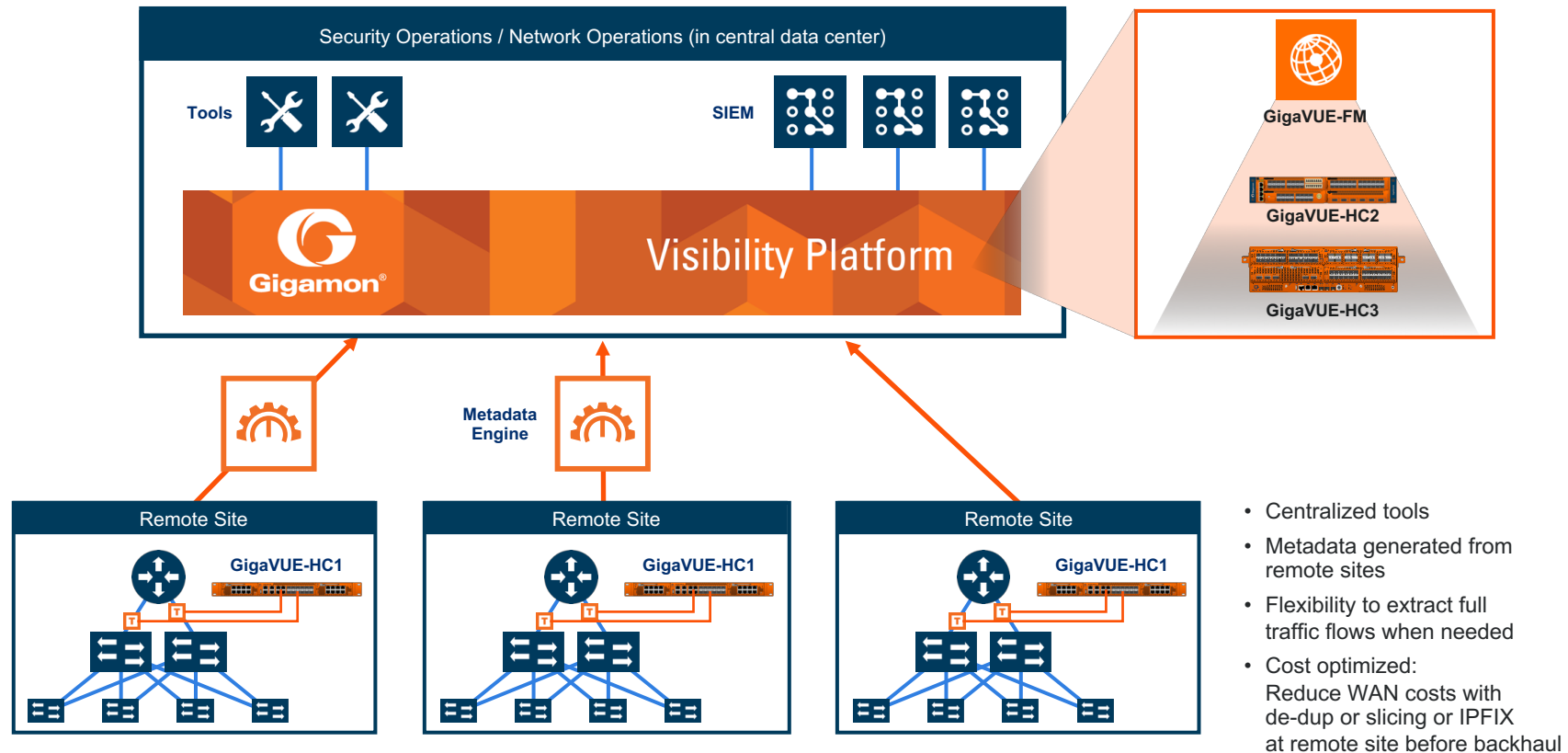
*Results vary depending on the infrastructure and solution deployment.

Ideal Ecosystem Partners: All

Ent NetOps	Ent SecOps	SP NetOps	Cloud Ops
✓	✓		



Use Case: 14. Visibility into Remote Sites



Ideal Ecosystem Partners: All

Visibility Platform Key Capabilities

Pervasive Visibility	The fundamental benefit of the Gigamon Visibility Platform. This innovative platform enables organizations to manage, secure and understand all of the data in motion traversing their networks – whether in physical or virtual environments; or in private, hybrid or public clouds.
Flow Mapping	Flow Mapping® is a foundational technology that takes traffic from a physical/virtual network tap or a SPAN/mirror port and sends it through a set of user-defined policies (rules) to select the traffic to be sent to tools. Typical policies are based on Layer 2–4 attributes, encapsulation headers such as VXLAN, VNTag, GTP, MPLS and more. The policies ensure that only the right data is sent to the right tool/set of tools at the right time.
Application Filter Intelligence	There is no point loading a tool with traffic that it will only drop after identifying it or that it will have no use for. Application Filter Intelligence detects and classifies over 3000 business and network applications/protocols and allows you to automatically filter them in or out before forwarding to tools. Custom applications can also be detected and filtered.
GigaStream® Load Balancing	When traffic flows are larger than a single tool can manage, the Visibility Platform can be used to split the flow across multiple security tools, while ensuring that sessions are kept together and the number of security tools can incrementally grow by adding new devices to those already connected. This is a GigaSMART feature.
Traffic Aggregation	Where links have low traffic volumes, the Visibility Platform can aggregate these links together before sending them to the security tool to minimize the number of ports that need to be used. By tagging the traffic, the Visibility Platform ensures that the source of traffic can be identified. This is a GigaSMART feature.
NetFlow Generation	Gigamon devices can generate unsampled NetFlow/IPFIX metadata for any traffic flow. Gigamon also generates extended metadata records for things like HTTP response codes and DNS queries – this extended metadata can be used to provide far more detailed contextual analysis when looking at network and security events. This is a key GigaSMART feature.
Application Metadata Intelligence	Utilizing Application Intelligence, this feature allows users to select applications they are interested in and have the Visibility Platform generate specific metadata from just that traffic. This enables users to have relevant context around business applications to quickly identify suspicious activity and remediate issues.
Asymmetric Routing Assistance	Most security devices require all the packets in a session to be inspected by the same device, as incomplete sessions risk being blocked. The Gigamon Visibility Platform provides an intelligent and efficient way to ensure that this happens in most architectures.
Inline Bypass	Deploy security devices inline and use the Gigamon Inline Bypass functionality to provide physical bypass traffic protection in the event of power loss, and logical bypass traffic protection in the event of an inline tool failure. This is a key GigaSMART feature providing additional network resilience and control.
SSL/TLS Decryption	On average, over 50 percent of enterprise network traffic is encrypted with SSL/ TLS, increasing the risk of hidden malware that evades detection. The Gigamon Visibility Platform provides scalable SSL/ TLS decryption to support and feed inline and out-of-band deployments with both active (such as NGFW, IPS) and passive (such as DLP, forensics, anti-malware) security tools. This is a key GigaSMART feature.
Header Stripping	If the connected tool doesn't need to see the body information within the packet, the Visibility Platform can remove it before sending the packet header to the tool for processing. This reduces load on the device and increases its efficiency. This is a key GigaSMART feature.
Masking	Certain industries must handle select information very carefully in support of compliance mandates (for example, credit card numbers in ecommerce or patient identification in healthcare records). The Visibility Platform can selectively mask any sensitive data within packets before they are sent to other tools where they may be seen by operators or administrators. This is a GigaSMART feature.

Visibility Platform Key Capabilities (continued)

De-duplication	Pervasive visibility means that you will be tapping or copying traffic from multiple points in the network, which, in turn, means you may well see the same packet more than once. To avoid unnecessary overhead on your tools of processing packets more than once, the Visibility Platform has a highly effective de-duplication engine to remove these duplicates before they consume network and system resources. This is a key GigaSMART feature.
Packet Slicing	This GigaSMART feature reduces the packet size of traffic sent to security tools. As a result, the security tools process fewer bits while maintaining the vital, relevant portions of each packet analyzed.
Subscriber-Aware Visibility	The GigaSMART Flow Mapping®, GTP Correlation, FlowVUE™ and Application Session Filtering (ASF) capabilities enable intelligent prioritization of subscriber traffic for tool processing. These capabilities are purpose-built for service provider customers.

Value Drivers

What Are Value Drivers?

- These are the things that the prospect is likely proactively looking for or needing
- These are generally revenue, cost or risk related
- The top-of-mind customer topics that exist even if Gigamon doesn't
- They could cause a buyer to re-allocate discretionary funds
- They support a value-based sales track (mutually exclusive, collectively exhaustive)

We explain these drivers in the following structure:

1. The **before scenario**, and the **negative consequences** of it
2. The **after scenario**, and the **positive business outcomes** from it
3. The **required capabilities**, and the **metrics** to prove success

What Are Differentiators?

- They can influence technical buyers' decision criteria through required capabilities.
- Each differentiator contains a **description, customer value, defensibility** and **trap-setting**.
- There are three types:
 - **Unique** – Not available from any other vendor. Leading products or services that only Gigamon can provide
 - **Comparative** – Superior attributes when compared to other companies, often feature- or service-based
 - **Holistic** – Attributes of Gigamon that would make a customer feel good about doing business with us

We explain the differentiators using:

1. The differentiator itself (such as One Complete Platform for Access to Data Anywhere)
2. Its value to the customer (in revenue, cost, and risk)
3. Its defensibility, similar to proof points, our customer's point of view
4. Trap-setting questions; the topics you'll want to bring up to drive prospects to the differentiator

SecOps Value Drivers

Our Customers' Value Drivers

- **Minimize complexity of a more efficient security stack:** Identify, enhance and deliver the most relevant traffic to capacity-limited security tools
- **Improve confidence in your overall security posture:** Rapidly deploy and update security technologies with minimal disruptions
- **Reduce risk through accelerated threat detection and response:** Leverage pervasive network visibility to accelerate detection and incident response

Defensible Differentiators

- One complete platform for access to data anywhere
- Scale, breadth and depth of traffic intelligence
- High quality and reliability of overall solution
- Tangible and prompt ROI
- Depth and breadth of integration with leading infrastructure and tooling
- Vendors #1 market leader, singular focus of the whole company

SecOps Value Driver: Minimize Complexity for a More Efficient Security Stack

(Director of SecOps/Manager of SOC /Security Infrastructure Architect/CISO)

Before	<ul style="list-style-type: none"> Limited visibility and lack of control across diverse environments (physical, virtual, cloud) Network impact concerns obstruct new security deployment or expansion plans Deployment and operational compromises limit tool value and overall security effectiveness Lack of intelligent network traffic control impedes performance of security and mission-critical applications SSL and other security challenges frustrate cloud migration and SaaS adoption efforts
Negative Consequences	<ul style="list-style-type: none"> Increased risk of breach; damaged reputation and lost customers Lack of visibility into increasing amounts of encrypted traffic Lack of collaboration and increased contention between networking and security Slower detection and response to active threats due to limited current and historical visibility Employee burn-out and churn; loss of expertise and continuity in security monitoring
After	<ul style="list-style-type: none"> Fast, consistent, pervasive visibility across physical, virtual and cloud environments Optimized security solutions receive appropriate network traffic, pre-filtered, decrypted and on time Security tools receive data at a consumable rate while preserving overall network performance Reduce departmental friction and increase alignment between network and security teams Able to adapt to infrastructure changes rapidly due to integrated security platform approach

Positive Business Outcomes	<ul style="list-style-type: none"> Reduced risk of breach; protecting reputation, revenue and both investor and customer trust Meet internal and industry compliance requirements; pass security audits from stakeholders Improved utilization of resources and security tools; reduced cost of security tools Reduce pressure and demands on security teams; attract and retain higher-skilled talent Quickly and easily adopt new security and business solutions delivering fast time-to-value
Required Capabilities	<ul style="list-style-type: none"> Common platform to deliver traffic, metadata and flow records to SIEMs and network security tools Visibility across diverse enterprise environments (physical, virtual, cloud) Modular and scalable with common architecture to feed inline and out-of-band tools Integrated bypass capability to bypass security tool overload and failures and prevent network disruption Security tool agnostic traffic intelligence delivers relevant data to the right tools
Metrics	<ul style="list-style-type: none"> Time to rollout new security initiatives; rate of completion of proactive security projects Percentage of assets and network segments under surveillance Security tool utilization rate and latency Planned and unplanned downtime Expenditure on security tools; cost of entire security stack Time to detection and resolution by security tools Reducing rate of false positive detection Threat detection rate within encrypted traffic

SecOps Value Driver: Improve Confidence in Your Overall Security Posture

(Director of SecOps; Manager of SOC; Security Infrastructure Architect; CISO)

Before	<ul style="list-style-type: none"> Irrelevant data overloads security tools and requires upgrades or unnecessarily large clusters Protection gaps during infrequent and time-consuming security tool deployments and upgrades Compliance requirements (MIFID, GDPR, HIPAA) are increasingly hard to meet Challenges/concerns migrating security tools from out-of-band to inline deployments Budget pressure to ensure ROI of all investments
Negative Consequences	<ul style="list-style-type: none"> Increased risk of breach; damaged reputation and lost customers Extended security gaps and system vulnerabilities wait response on rare maintenance windows Extensive resources needed for new security deployments, maintenance, updates and upgrades Overspending on security tools to support an increasingly busy and diverse network environment Inefficient use of security tools creates security gaps and unnecessary expenditure
After	<ul style="list-style-type: none"> Security tools are optimized for maximum throughput without impacting network performance Smooth updates, upgrades or other maintenance without security gaps or downtime Reduce time to PoC, deploy, reconfigure, update and upgrade security tools Significantly improved scaling of new and existing security solutions, stop tool sprawl and contain costs Improved compliance with regulatory requirements through pervasive network traffic visibility

Positive Business Outcomes	<ul style="list-style-type: none"> Reduced risk of breach; protecting reputation, revenue and both investor and customer trust Quickly and more easily adopt new security and business solutions delivering fast time-to-value Meet internal and industry compliance requirements and pass security audits from stakeholders Improved utilization of resources and security tools; reduced cost of security tooling Increased productivity and innovation; security enables technology adoption
Required Capabilities	<ul style="list-style-type: none"> Common platform to deliver traffic, metadata and flow records to SIEMs and network security tools Packet transformation capabilities (e.g., data masking for compliance, decryption for visibility) Programmable interface to enable automated incident response and rules Ability to deploy the same appliance inline and/or out-of-band Advanced traffic selection controls and load balancing to minimize security tool overload
Metrics	<ul style="list-style-type: none"> Time to rollout new security initiatives; rate of completion of proactive security projects Percentage of assets and network segments under surveillance Security tool utilization rate and latency Planned and unplanned downtime Expenditure on security tools; cost of entire security stack Time to detection and resolution by security tools Rate of false positive detection (lower = better) Threat detection rate within encrypted traffic Headcount in security operations to incident resolution Time to plan and execute security upgrades (e.g., during software upgrade)

SecOps Value Driver: Reduce Risk Through Accelerated Threat Detection and Response

(Director of SecOps; Manager of SOC; Incident Responders; CISO)

Before	<ul style="list-style-type: none"> Minimal, inconsistent or unreliable network active-threat detection capability Detection and investigation tools are inconsistent, making detection and response more complicated Low confidence in detections (false positives), and missed security events (false negatives) Maxing out SIEM for data collection, correlation and query capabilities, despite visibility limitations Development and maintenance of in-house custom tools to fill some of the network detection and response gaps
Negative Consequences	<ul style="list-style-type: none"> Increased risk due to high mean-time-to-response (MTTR) and high mean-time-to-detection (MTTD) Strained response teams as siloed information can take hours or days to effectively triage alerts Lack of quick access to relevant data reduces visibility, detection and response capabilities Wasted effort and actions based on partial information Limited response capabilities from lack of actionable data
After	<ul style="list-style-type: none"> Broad, unified visibility for threat detection and response across diverse environments Fewer false positives, and ability to quickly investigate and validate alerts Fast access to extensive current and historical metadata to support a confident, actionable response Powerful usability from a tool built by responders, for responders Able to continually enhance the security posture with efficient threat hunting to identify gaps

Positive Business Outcomes	<ul style="list-style-type: none"> Decrease risk due to reduced MTTD and MTTR Reduce analyst fatigue with a more efficient detection, investigation, and response solution Responsive threat hunting helps in the discovery of the most advanced threats Lower costs and greater team effectiveness by reducing in-house tool dependencies More effective security teams, greater retention of skilled security personnel
Required Capabilities	<ul style="list-style-type: none"> Real-time collection and historical retention of device, file, entity and other network activity data Full support for modern networks of physical, virtual and cloud infrastructure for complete visibility Fast access, measured in seconds, to a complete unified network activity data repository Scalability as a cloud platform and through Gigamon Security Delivery Platform support Extensible with APIs to support third-party applications that leverage the metadata repository Full NDR solution designed and maintained by experienced responders
Metrics	<ul style="list-style-type: none"> Reduction in false positive rates Reduction in time dismissing false positives MTTD MTTR Average dwell time over a fixed period

NetOps Value Drivers

Our Customers' Value Drivers

- **Maintain a resilient and flexible network infrastructure ready to absorb change:**
Improve the agility of the network infrastructure to address evolving business requirements
- **Access to and control of data for improved visibility across physical, virtual and cloud infrastructure:** Manage, monitor and control network traffic across diverse environments
- **Reduce TCO of monitoring during network traffic growth and 40G/100G network upgrades:**
Break the cycle of making high-cost monitoring investments as network speeds increase

Defensible Differentiators

- One complete platform for access to data anywhere
- Scale, breadth and depth of traffic intelligence
- High quality and reliability of overall solution
- Tangible and prompt ROI
- Depth and breadth of integration with leading infrastructure and tooling vendors
- #1 Market leader, singular focus of the whole company

NetOps Value Driver: Maintain a Resilient and Flexible Network Infrastructure Ready to Absorb Change

Before	<ul style="list-style-type: none"> • Network upgrades result in high-cost management and security tool investments • Challenging to simultaneously achieve high network availability, performance and security protection • Slow to rollout new or upgrade existing security prevention solutions • Security tool upgrades to inline protection demand lengthy and business-impacting maintenance windows • Adoption of cloud strategies impacting management and security operations
Negative Consequences	<ul style="list-style-type: none"> • Network upgrades delayed due to high total cost of execution that in turn impacts business performance • IT organization perceived as holding back the business • Increased demands on NetOps and SecOps resources to undertake maintenance activities off-hours • Potential for a lack of collaboration and/or increased contention between networking and security teams • Increased risk of breach; damaged reputation and lost customers
After	<ul style="list-style-type: none"> • Network and IT infrastructure remaining in lock-step with business demands and growth • Ability to scale management and prevention tools in line with the network infrastructure • Reduce tool proliferation and sprawl, and in doing so contain CapEx and OpEx costs • Rapidly deploy new security/operational tools with minimal network impact • Reduce time to PoC, evaluate, troubleshoot and deploy management and security tools

Positive Business Outcomes	<ul style="list-style-type: none"> • Maintain an IT infrastructure in line with business growth and expansion • The business is able to evolve faster and respond to competitive changes more effectively • Improved utilization of manpower and funding resources • Improved credibility and trust with business and customer stakeholders • Reduced risk of breach; protecting reputation, customers and revenue
Required Capabilities	<ul style="list-style-type: none"> • Advanced traffic selection controls that ensure the right network traffic is delivered to the right tool • Ability to load balance network traffic with full session- awareness across multiple tool presences • Integrated bypass capability to reduce maintenance windows by routing traffic around or through tools • Common platform to deliver traffic, metadata and flow records to SIEMs and network security tools • Pervasive reach across 1Gb to 100Gb physical networks, virtualized data centers and the public cloud
Metrics	<ul style="list-style-type: none"> • Time to rollout new infrastructure and deliver a business-ready environment • Time to plan and execute upgrade of a management or security tool (for example, during software upgrades) • Time to detect and resolve operational issues across the enterprise • Management and security tool ROI, utilization and effectiveness • Percentage of assets and network segments under surveillance

NetOps Value Driver: Access to and Control of Data for Improved Visibility Across Physical, Virtual and Cloud Infrastructure

Before	<ul style="list-style-type: none"> Limited visibility and lack of control across diverse environments (physical, virtual, cloud) Departmental friction makes it hard to access data Irrelevant data overloads management and security tools and requires unnecessary upgrades Ad hoc tool deployment creates silos of IT management and causes tool sprawl Suboptimal use of tools and personnel leads to process inefficiencies
Negative Consequences	<ul style="list-style-type: none"> Business impact and increased exposure due to stalled network and security initiatives Excessive, reactive, unplanned spending on management and security tools Inefficient use of enterprise IT tools creates overload and unnecessary expenditure Longer time to detect outages, incidents and threats and then remediate as appropriate Employee churn; loss of expertise and continuity in IT NetOps and SecOps teams
After	<ul style="list-style-type: none"> Consistent and rapid visibility across diverse environments (physical, virtual, cloud) Deliver only relevant data to the right management or security tool at the right time Adapt to infrastructure changes rapidly with an integrated approach to IT management and security Maintain security at the speed of the network to improve confidence in the enterprise security posture Meet internal and industry compliance requirements and pass appropriate audits with stakeholders

Positive Business Outcomes	<ul style="list-style-type: none"> Faster rollout of new business solutions and infrastructure to serve those solution Improved utilization of resources and management and security tools; reduced cost of infrastructure management Improved NetOps and SecOps productivity, teamwork and satisfaction Improved security posture with rapid detection of root cause of incidents or operational issues Attract and retain higher skilled talent
Required Capabilities	<ul style="list-style-type: none"> Single visibility solution across diverse enterprise environments (physical, virtual, cloud) Powerful network packet transformation capabilities (for example, decryption, NetFlow generation, deduplication) A common platform to deliver traffic, metadata and flow records to SIEMs and network management tools Ability to deploy visibility appliances at any speed (1Gb to 100Gb) inline and out-of-band Management and security tool agnostic solution to deliver the relevant network traffic to the right tools
Metrics	<ul style="list-style-type: none"> Time to rollout new infrastructure and deliver a business-ready environment Time to plan and execute upgrade of a management or security tool (for example, during software upgrade) Time to detect and resolve operational issues across the enterprise Management and security tool ROI, utilization and effectiveness Percentage of assets and network segments under surveillance

NetOps Value Driver: Reduce TCO of Monitoring During Network Traffic Growth and 40/100Gb Network Upgrades

(CISO, Head of InfoSec, Director of SecOps)

Before	<ul style="list-style-type: none"> • Network upgrades result in high-cost management and security tool investments • Challenging to simultaneously achieve high network availability, performance and security protection • Slow to rollout new or upgrade transformational technologies (public cloud, virtualization) • Compliance requirements (MIFID, GDPR, HIPAA) are increasingly hard to meet • Security tool upgrades to inline protection demand lengthy and business-impacting maintenance windows • Latency in IT response to business requests drives high-cost shadow-IT initiatives
Negative Consequences	<ul style="list-style-type: none"> • Higher cost associated with management and securing of infrastructure • Hidden costs of shadow-IT activities, public cloud expansion and network-upgrades due to tooling impact • Increased risk of breach; damaged reputation and lost customers • Reduced regulatory compliance and potential risk of compliance fines • Unable to manage and secure all network segments/traffic resulting in increased risk
After	<ul style="list-style-type: none"> • Lower cost of ownership of enterprise management and security infrastructure • Simplified integrated architecture for faster technology rollouts • Eliminate management and security tool overload and reduce tool sprawl • Ensure that management tools have access to the right network traffic to meet regulatory compliance • Network running at peak performance without compromising management or security

Positive Business Outcomes	<ul style="list-style-type: none"> • Reduced tooling CapEx and OpEx following infrastructure upgrades • Faster rollout of business initiatives; IT as an enabler vs. an obstacle • Fewer operational and security incidents; faster time to resolution • Reduced compliance fines and remediation costs • Increased productivity and innovation within NetOps and SecOps teams
Required Capabilities	<ul style="list-style-type: none"> • Advanced traffic selection controls that ensure the right network traffic is delivered to the right tool • Ability to load balance network traffic with full session- awareness across multiple tool presences • Integrated bypass capability to reduce maintenance windows by routing traffic around or through tools • Common platform to deliver traffic, metadata and flow records to SIEMs and network security tools • Pervasive reach across 1Gb to 100Gb physical networks, virtualized data centers and the public cloud
Metrics	<ul style="list-style-type: none"> • Time to rollout new infrastructure and deliver a business-ready environment • Time to plan and execute upgrade of a management or security tool (for example, during software upgrade) • Time to detect and resolve operational issues across the enterprise • Management and security tool ROI, utilization and effectiveness • Percentage of assets and network segments under surveillance

Service Provider Value Drivers

Our Customers' Value Drivers

- **Scale infrastructure analytics and management to support evolution to 5G:**
Optimize tooling investment while delivering new subscriber performance and services
- **Access to and control of data for improved visibility everywhere:** Manage, monitor and control network communications across physical, virtual and distributed environments
- **Improve and differentiate through subscriber experience:** Reduce churn and increase subscriber adoption by optimizing quality, breadth and relevance of service

Defensible Differentiators

- One comprehensive platform accessing communications anywhere
- Scale, breadth and depth of traffic intelligence
- High quality and reliability of overall solution
- Strong and rapid ROI of subscriber-aware intelligence solution
- #1 Leader in Visibility to Information-in-Motion Market; singular focus of the company

Service Provider Value Driver: Scale Infrastructure Analytics and Management to Support Evolution to 5G

(VP Infrastructure Architecture/VP Service Assurance/VP or Director of Network Operations)

Before	<ul style="list-style-type: none"> Traffic volume is overwhelming analytic probe capacity, with 5G dramatically exacerbating the issue Control and user data separation (CUPS) demanding new virtualized infrastructure Excessive spend on infrastructure tooling and telemetry solutions Challenges rolling out new solutions and expanding existing solutions Multiple business units unable to share same data (network traffic)
Negative Consequences	<ul style="list-style-type: none"> Increased risk; potential for increased churn; unable to see and analyze all subscriber traffic Increasing spend; higher OpEx spend in future years Increased resources required to adopt, operate and evolve infrastructure Low level of leverage between operations and product marketing functions Delays in adoption and roll-out of next-generation solutions (5G)
After	<ul style="list-style-type: none"> Ability to respond to subscriber-impacting issues in a timely manner Reduce time to PoC, troubleshoot and deploy next-generation infrastructure and tooling/telemetry Increase cross-functional alignment between business units to deliver new, valuable subscriber features Deliver relevant network traffic to the right tools at the right time in both virtual and physical environments Satisfied subscribers; high-quality services and infrastructure; lower cost of ownership

Positive Business Outcomes	<ul style="list-style-type: none"> Architect, deploy and operate holistic analytic strategy that scales to 5G levels of performance Lower cost-of-ownership; lower OpEx Improved satisfaction of subscribers; improved competitive differentiation Faster and more agile organizational execution Reduced risk of security breach – protecting reputation, customers and revenue
Required Capabilities	<ul style="list-style-type: none"> Access to subscriber traffic across a distributed/CUPS architecture Tool agnostic platform with open integration capabilities with existing tools (for example, Tek, NetScout, BSS/OSS) Management through a single pane of glass across diverse environments (physical, virtual, cloud) Manage and control traffic-overload on service assurance tools Single platform that delivers subscriber-aware network traffic
Metrics	<ul style="list-style-type: none"> Project timeline to deploy new infrastructure, services and initiatives Analytic, management and telemetry tool and probe utilization and latency CapEx and OpEx expenditure on analytic probes Planned and unplanned downtime across broader range of network assets and segments Subscriber growth and churn

Service Provider Value Driver: Access to and Control of Data for Improved Visibility Everywhere

(VP Infrastructure Architecture/VP Service Assurance/VP or Director of Network Operations)

Before	<ul style="list-style-type: none"> Limited visibility and lack of network-traffic control across diverse environments (physical, virtual, cloud) Multiple business units unable to share the same network- traffic and subscriber data Analytic probes failing to keep up with growth in traffic; focused on low-value (irrelevant) network-traffic Ad hoc tool deployment creates monitoring silos vs. single integrated architecture Suboptimal use of tools and personnel leads to process inefficiencies
Negative Consequences	<ul style="list-style-type: none"> Competitive disadvantage due to delayed or stalled infrastructure upgrade and transformation initiatives Stalled subscriber growth and increasing churn due to inability to determine revenue profile across service offerings Inefficient use of network resources causes excessive, reactive, unplanned CapEx and OpEx expenditures Protracted time to identify and remediate operational and quality issues Employee churn due to burn-out leads to a loss of expertise and organizational continuity
After	<ul style="list-style-type: none"> Network monitoring and service assurance at the speed of today's and tomorrow's network Consistent and high-quality visibility across diverse and distributed environments (physical, virtual, cloud, CUPS) Delivery of subscriber-aware network-traffic to the appropriate analytic probes Rapid adaption to infrastructure changes and evolution with an integrated visibility platform Attract and retain higher skilled talent

Positive Business Outcomes	<ul style="list-style-type: none"> Improved ability to embrace LTE and 5G/CUPS network architectures Faster rollout of new subscriber services and product offerings; faster time to value Improved utilization of resources, reducing cost of infrastructure Reduced subscriber-churn and ability to attract new subscribers with differentiated offerings Increased organization agility and stability
Required Capabilities	<ul style="list-style-type: none"> Tool-vendor agnostic subscriber-aware traffic intelligence delivering relevant network-traffic to the appropriate analytic tools and probes Single pane-of-management of visibility platform across diverse environments (physical, NFV, virtual, cloud) Packet transformation and subscriber-aware intelligence capabilities Common platform across centralized and/or distributed subscriber control and user traffic Ability to deploy analytics both inline or out-of-band
Metrics	<ul style="list-style-type: none"> Project timeline to deploy new infrastructure, services and initiatives Analytic, management and telemetry tool and probe utilization and latency CapEx and OpEx expenditure on analytic probes Planned and unplanned downtime across broader range of network assets and segments Subscriber growth and churn

Service Provider Value Driver: Improve and Differentiate Through Subscriber Experience

(VP Infrastructure Architecture/VP Service Assurance/VP or Director of Network Operations)

Before	<ul style="list-style-type: none"> Subscriber product needs unclear; incomplete understanding of network usage Challenging to keep up with evolving competitive landscape and emerging technology Transformational technologies (cloud, NFV-SDN, 5G-CUPS) are limiting visibility and insight Traffic growth causing service assurance and management tools to be inundated and overloaded Cross-department demand for insights from network- traffic causing increased inefficiencies and conflicts
Negative Consequences	<ul style="list-style-type: none"> Increasing costs associated with adapting and operating analytics platforms Increasing risk of denial of service attacks causing service disruptions Increasing resources (CapEx, OpEx, personnel) required to manage evolving environment Risks of failing to maintain regulatory compliance Increasing blind spots across physical and virtualized infrastructure
After	<ul style="list-style-type: none"> Simplified integrated visibility architecture enabling faster technology rollouts Security at the speed of the network for timely response to subscriber and service delivery issues Eliminated traffic-loss due to probe overload; reduced probe proliferation Greater confidence regarding regulatory compliance Infrastructure performing in line with business requirements and subscriber expectations

Positive Business Outcomes	<ul style="list-style-type: none"> Improved customer experience and adoption of new service offerings Increased infrastructure uptime and quality of services Improved subscriber, service-quality and business metrics Reduced end customer churn; improved brand reputation Proactive development of differentiated services; stronger understanding of consumer demand
Required Capabilities	<ul style="list-style-type: none"> Tool-vendor agnostic subscriber-aware traffic intelligence delivering relevant network-traffic to the appropriate analytic tools and probes Single pane-of-management of visibility platform across diverse environments (physical, NFV, virtual, cloud) Packet transformation and subscriber-aware intelligence capabilities Common platform across centralized and/or distributed subscriber control and user traffic Ability to deploy analytics both inline or out-of-band
Metrics	<ul style="list-style-type: none"> Project timeline to deploy new infrastructure, services and initiatives Analytic, management and telemetry tool and probe utilization and latency CapEx and OpEx expenditure on analytic probes Planned and unplanned downtime across broader range of network assets and segments Subscriber growth, satisfaction and churn and associated carrier ranking

