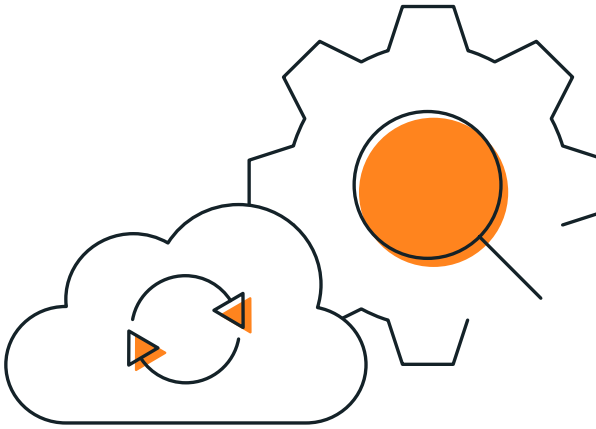
Gigamon® | New Relic

Hybrid Cloud Visibility and Observability with AI

Ensure Superior Software, Security, and Compliance



THE CHALLENGE

Organizations with hybrid cloud deployments require full-stack observability and artificial intelligence (AI)-driven insights to confidently ensure network security, compliance, and reliability. IT needs to discover assets including unmanaged devices with workload visibility and combine with metadata to eliminate blind spots and identify issues such as expiring TLS certificates, rogue applications, and data exfiltration attempts.

THE SOLUTION

New Relic One ingests multiple sources of telemetry, including metadata, logs, events, metrics, and traces and processes them with advanced AI and machine learning (ML) to provide comprehensive observability. The multi-dimensional dashboard provides extensive and highly granular views into network operations, security, and application performance. IT can analyze, troubleshoot, and optimize the entire software stack and accelerate bringing valuable services to market.

Gigamon Hawk ensures full visibility and expands sources of data with Application Metadata Intelligence. Over 5,000 L2–L7 attributes are generated and consumed by New Relic One to solve for a myriad of security and performance issues.

Introduction

Today's enterprise landscape spans on-premises, multi-cloud, and SaaS applications deployed on intricate networks involving tens of tools, hundreds of applications, thousands of servers with potentially millions of users, on a wide variety of devices spread around the world. As a result, IT teams, including CloudOps, NetOps, and SecOps, struggle with the complexity and cost of these infrastructures.

Cloud vendors can offer tooling for application performance and security, but they lack cross-platform visibility. They also are short on rich, digestible telemetry from the network layer, even though organizations are responsible for the security of intra- and inter-cloud networking traffic. With the move to the cloud, tools need to support any deployment scenario and should actually ease the migration.

To obtain comprehensive visibility and ultimately observability, IT needs to combine tools with an expanded view into all workload traffic of interest. These can include unmanaged devices, such as IoT/OT, VM-to-container, container-to-container, cloud-to-cloud, and cloud-to-on-premises. Visibility to network-level traffic data is paramount because this data is the "ground truth" of what is being communicated between infrastructure nodes. Only then can IT ensure security and compliance and exceed SLAs.

Simultaneously, IT teams are under pressure to ship new features faster, minimize downtime, and resolve issues before they ever impact customers. With ongoing digital transformation, the roles of software engineers and developers are more critical. They need a data-driven approach to observability to plan, build, deploy, and run robust software that delivers great digital experiences for their customers, employees, and partners.

Enter New Relic

New Relic One is an enterprise-grade SaaS observability solution that provides the knowledge of what is happening in the digital system and why, at any time, regardless of the environment. It visualizes the whole picture of everything that enables applications and devices to deliver value to customers, from the container running a microservice in the cloud to a mobile website's shopping cart button. This telemetry data platform is the single source of truth for all the operational data, empowering IT to ask and answer any question in milliseconds.

IT is empowered to collect, explore, and alert on all metadata, metrics, events, logs, and traces from any source with the world's most powerful, managed, open, and unified telemetry platform. Automatic integrations with Gigamon and open-source tools enable easy setup, eliminating the cost and complexities of hosting, operating, and managing additional monitoring systems or data stores. With all telemetry data in one place, organizations can investigate unknowns with confidence. With New Relic One, administrators benefit from:

+ 400+ agents and integrations, including Gigamon, enabling, ingesting, and storing all operational data
+ Full-stack observability to visualize, analyze, and optimize the entire software stack from one place
+ Eliminating telemetry data silos and instantly detecting, diagnosing, and resolving anomalies
+ Monitoring distributed services, applications, and serverless functions
+ Querying with lightning-fast response times and real-time alerts
+ Eliminating data silos and accelerating mean time to detection and resolution

Adding Visibility to Observability

GigaVUE® Cloud Suite, a key part of Gigamon Hawk — the visibility and analytics fabric for hybrid cloud, brings a network and application perspective to New Relic with its comprehensive visibility solution. Cloud Suite acquires all desired traffic via agents or built-in mirroring services, including East-West between virtual machines and containers, and within and between on-premises, public, and private clouds. It captures traffic from unmanaged IoT/OT devices where agents are difficult to deploy. The monitored traffic is partially filtered, encrypted, and tunneled to a virtual cloud-based visibility node (GigaVUE V Series) where it is aggregated and processed. (See Figure 1.)

GigaSMART® Application Filtering Intelligence (AFI) configured on the visibility nodes identifies over 3,500 applications and their underlying protocols. Applications can be filtered to enable IT to concentrate on pertinent traffic and ignore others. For workloads of interest, these nodes leverage Application Metadata Intelligence (AMI) to generate over 5,000 metadata attributes, many at Layers 4–7, which are far more revealing than basic NetFlow/IPFIX from the network infrastructure. (See Figure 2.)

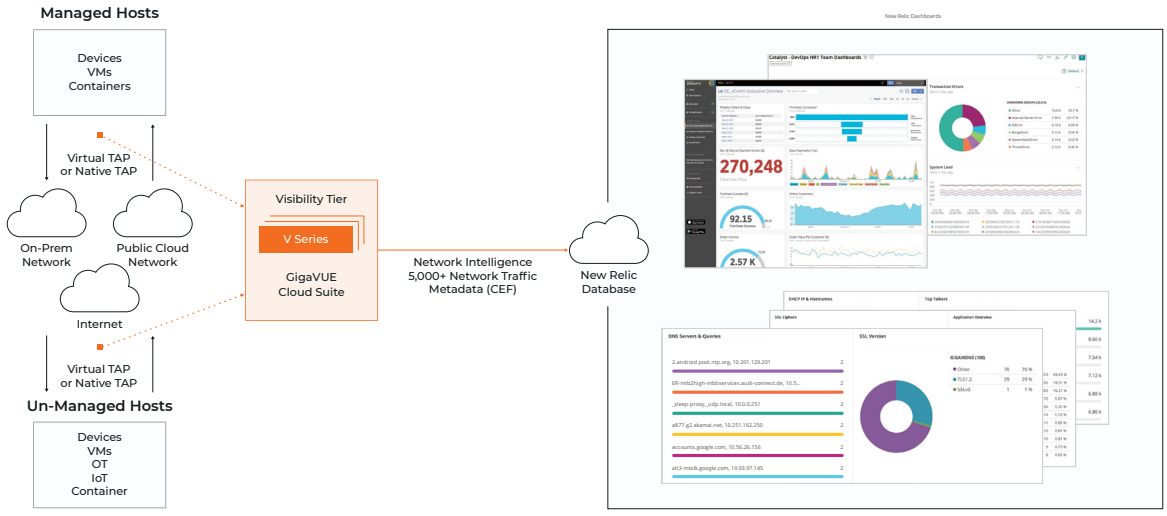


Figure 1: Strengthening security with the network perspective to New Relic

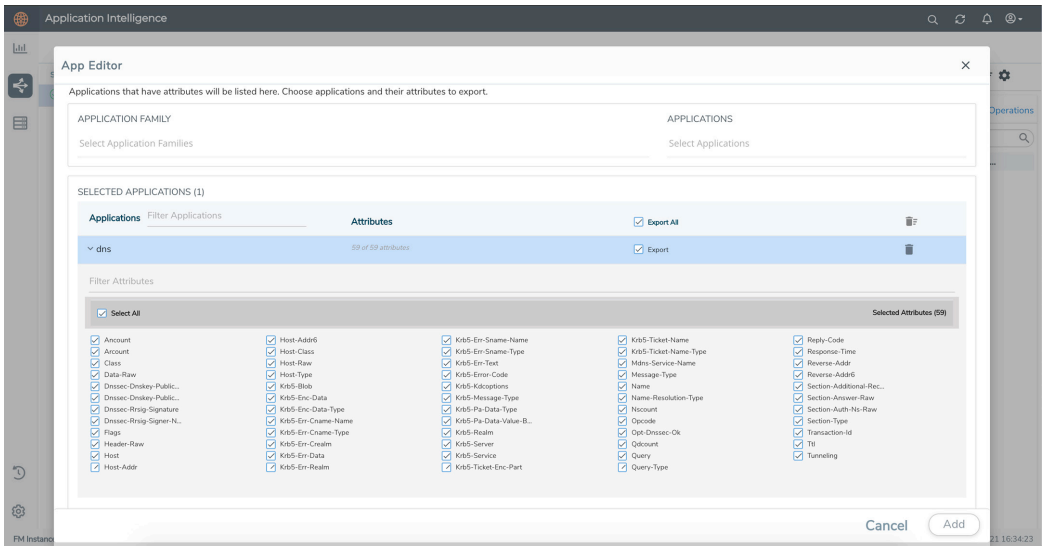


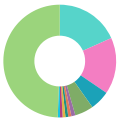
Figure 2: Fabric Manager dashboard allows granular selection of numerous metadata elements on a per app and protocol basis. Here DNS attributes are shown.

AMI utilizes deep packet inspection to provide summarized and context-aware information about raw network packets, augmenting a comprehensive approach to obtain application behavior. Organizations can acquire critical details pertaining to flows, reduce false positives by separating signals from noise, identify nefarious data extraction, and accelerate threat detection through proactive, real-time traffic monitoring as well as troubleshooting forensics.

Powerful Synergistic Combination

AMI complements the metadata attributes provided by New Relic agents. These added app-aware attributes are exported from the Gigamon Cloud Suite to New Relic One in various formats, including CEF and IPFIX, which can be consumed to provide reports in the New Relic dashboard. (See Figure 3.)

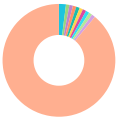
Application Overview



GIGAMONS (1.23 K)

Other	610	49.43 %
dns	226	18.31 %
dhcp	200	16.21 %
https	70	5.67 %
tcp	66	5.35 %
Classification-unknown	14	1.13 %
ssl	11	0.89 %
gtp	10	0.81 %
apple_location	10	0.81 %
facebook	9	0.73 %
google	8	0.65 %

DHCP IP & Hostnames



GIGAMONS (200)

Other	178
null, 10.180.236.95	4
KIOSK1, 10.33.147.175	2
KIOSK2, 10.180.32.229	2
KIOSK33, 10.190.80.239	2
KIOSK34, 10.180.172.124	2
KIOSK4, 10.180.221.240	2
KIOSK45 10 190 224 248	2

Figure 3: Sample New Relic dashboards based on Gigamon AMI and AFI

SecOps and CloudOps teams can use this unique combination to solve a wide array of security and performance problems including:

+ Identify expired TLS certificates. Utilize certificate expiry dates and notices of revoked or expired certificates to spot them.
+ Identify data exfiltration. Evaluate the volume and type of DNS requests received to reveal DNS tunneling in the network and help establish the legitimacy of domains.
+ Detect unauthorized remote connections used for data exfiltration. Evaluate suspicious SSH, RDP, and Telnet connections, by looking at bandwidth, connection longevity, IP reputation, and geolocation.
+ Monitor and control file access. Obtain insights into which clients are obtaining specified files. Generate lists of files involved and IP addresses of end users.
+ Locate weak ciphers. Metadata reveals all TLS connections with weak ciphers, along with the applications and systems hosting those apps, helping ensure security compliance.
+ Detect suspicious WAN activity. Identify command and control attacks. Determine whether a domain is legitimate or was generated using a botnet-controlled domain generating algorithm.

About New Relic

The world's best engineering teams rely on New Relic to visualize, analyze, and troubleshoot their software. New Relic One is the most powerful cloud-based observability platform built to help organizations create more perfect software. Learn why developers trust New Relic for improved uptime and performance, greater scale and efficiency, and accelerated time to market at newrelic.com.

About Gigamon

Gigamon helps the world's leading organizations run fast, stay secure and innovate. We provide Hawk, the industry's first elastic visibility and analytics fabric, which closes the cloud visibility gap by enabling cloud tools to see the network and network tools to see the cloud. With visibility across their entire hybrid cloud network, organizations can improve customer experience, eliminate security blind spots, and reduce cost and complexity. Gigamon has been awarded over 90 technology patents and enjoys world-class customer satisfaction with more than 4,000 organizations, including over 80 percent of the Fortune 100 and hundreds of government and educational organizations worldwide. Learn more at gigamon.com.

For more information on Gigamon and New Relic solutions visit: gigamon.com and newrelic.com.

Gigamon®

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