Build an Effective Observability Posture with Gigamon and New Relic

Overview

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 struggle with the complexity and cost of ensuring security and performance of these infrastructures.

Disparate 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 intraand 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. This includes visibility into unmanaged devices, such as IoT/OT, VM-to-container, container-to-container, cloud-to-cloud, and cloud-to-on-premises communications. Visibility into network-level intelligence is paramount because this data is the "ground truth" of what is being communicated between infrastructure nodes. Only then can teams ensure security and exceed SLAs.

On top of securing their infrastructure and monitoring performance, 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 than ever. 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.

The Challenge

Organizations require complete visibility across their hybrid-cloud infrastructure and observability over their full stack to confidently monitor and secure their environments. To ensure success, teams need the ability to eliminate all visibility blind spots across their complex infrastructures and ensure efficient identification of issues such as expiring TLS certificates, rogue applications, and data exfiltration attempts.

The Solution

New Relic One ingests multiple sources of telemetry by combining metrics, logs, events, and traces with metadata provided by Gigamon to establish comprehensive full stack observability. The multi-dimensional dashboard provides extensive and granular views into network operations, security, and application performance. Teams can analyze, troubleshoot, and optimize their software stack and accelerate bringing valuable services to market.

The Gigamon Deep Observability Pipeline ensures complete visibility by providing New Relic a stream of intelligence that complements metrics, events, logs, and traces 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.

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.

Teams are empowered to collect, explore, and alert on all metadata, metrics, events, logs, and traces from across their infrastructure with a 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 now 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 the Gigamon Deep Observability Pipeline, brings network and application intelligence to New Relic with its comprehensive visibility solution. Gigamon acquires via agents all East-West traffic living within and between on-premises, public, and private clouds, and between virtual machines and containers. The intelligence captured includes traffic from unmanaged IoT/OT devices where agents are difficult to deploy. The monitored traffic is accessed and sent 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 teams 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.)

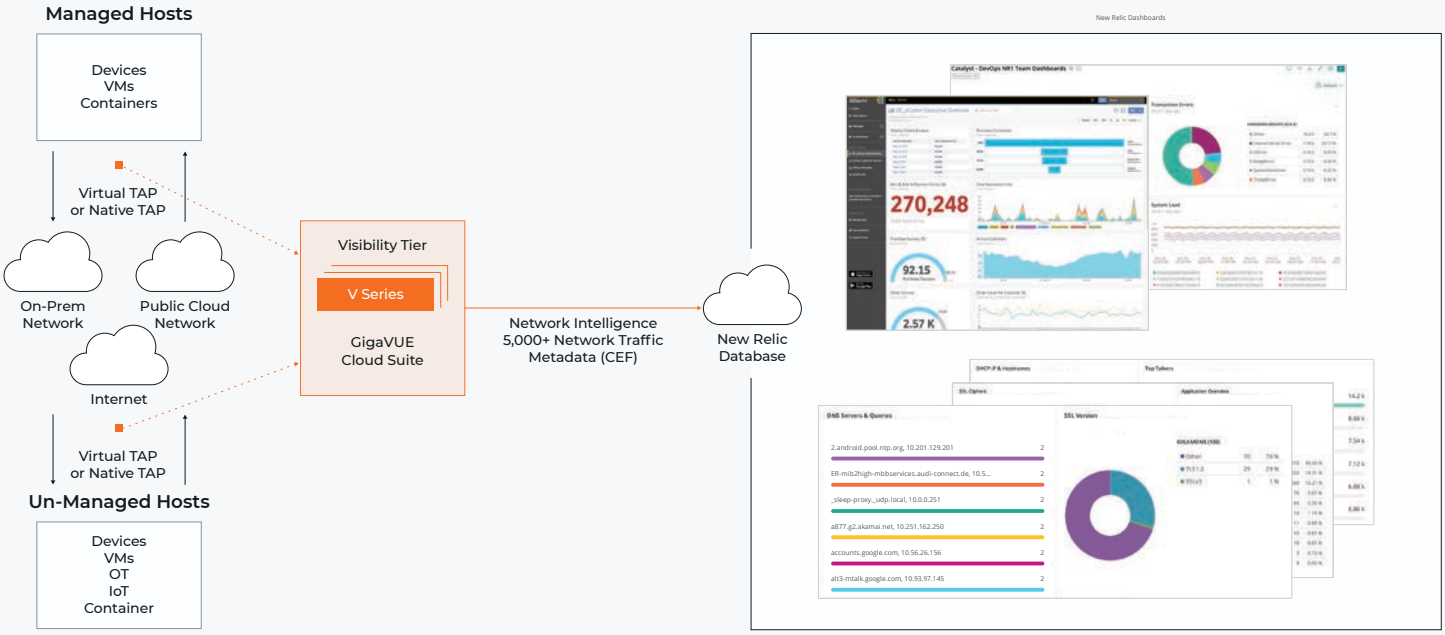

Figure 1. Strengthening security with the network perspective to New Relic.

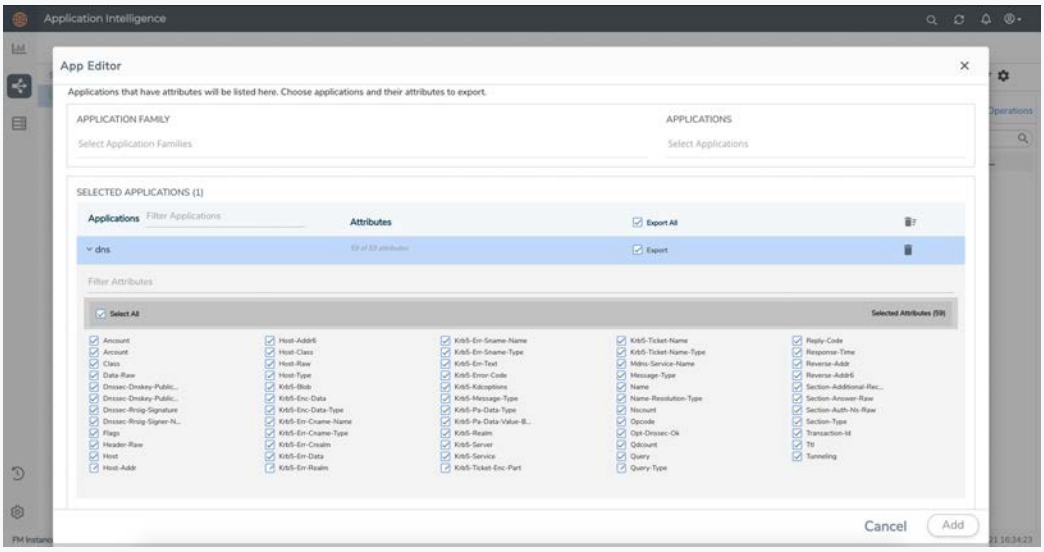

Figure 2. Fabric Manager dashboard allows granular selection of numerous metadata elements on a per app and protocol basis. Here DNS attributes are shown.

AMI utilizes deep packet inspection to provide summarized and contextual 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.)

Teams can use this combination of intelligence 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.

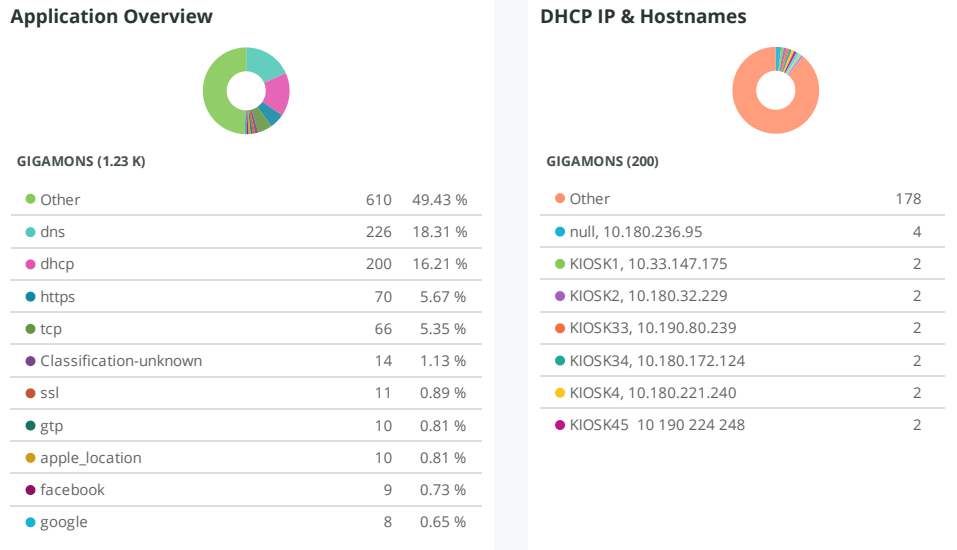

Figure 3. Sample New Relic dashboards based on Gigamon AMI and AFI.

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 offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide.

To learn more, please visit gigamon.com.

For more information on Gigamon and New Relic please visit
gigamon.com | newrelic.com

Gigamon®

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

06.23_03