GET DEEP OBSERVABILITY WITH GIGAMON AND DYNATRACE

Deep Observability for More Secure and Reliable Cloud Applications

IT organizations managing hybrid cloud deployments face a difficult challenge as these 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 this with metadata to eliminate blind spots and identify issues such as expiring TLS certificates, rogue applications, and data exfiltration attempts.

Here's where Gigamon Deep Observability Pipeline integrated with Dynatrace Software Intelligence Platform comes in – to help you deliver secure, compliant, and reliable cloud applications.

Gigamon accesses traffic from any cloud and/or data center and extracts valuable L2–L7 network and application metadata attributes using Gigamon Application Metadata Intelligence (AMI) and sends this network-derived intelligence to Dynatrace for visualization and analysis.

Gigamon augments traditional metrics, events, logs, and traces (MELT) data with over 7,000 applications and security-related attributes.

Dynatrace then visualizes, analyzes, and alerts the intelligent metadata and processes it with advanced AI and machine learning (ML) to provide comprehensive observability. The multidimensional dashboard provides extensive and highly granular views into network operations, security, and application performance. IT can then analyze, troubleshoot, and optimize the entire software stack and accelerate bringing valuable services to market.

Key Joint Solution Features

- Access to over 7,000 L2–L7 attributes that can be forwarded to Dynatrace to solve new security and performance use cases
- Out-of-the-box integration with Gigamon expands Dynatrace's visibility into managed and unmanaged hosts, including BYOD, IoT, and even containers
- Visibility into East-West and North-South traffic across multi-cloud and on-premises
- Visualization of all applications running on your network
- Notifications on HTTP response code changes and anomalous traffic patterns to get ahead of potential performance or security issues
- Traffic optimization capabilities, including packet de-duplication, application filtering, and flow/packet slicing to fine-tune traffic going to tools without sacrificing data fidelity

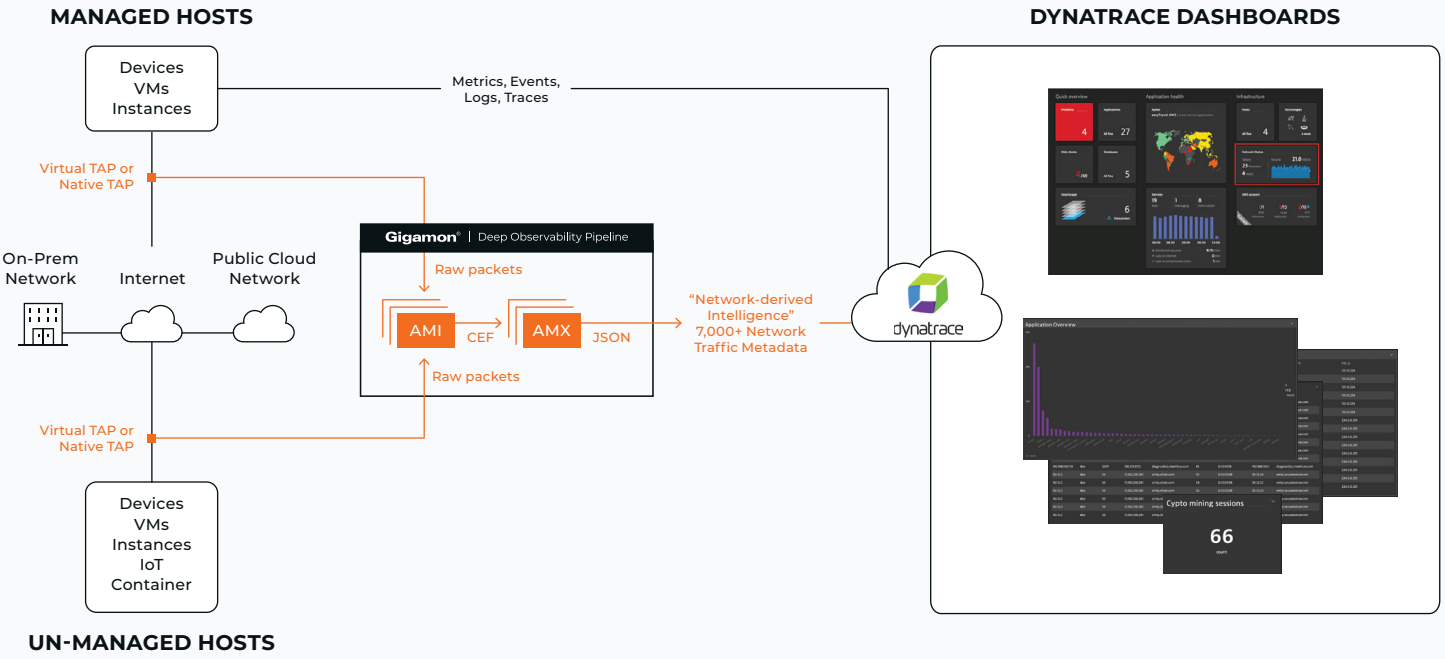


Figure 1. Gigamon accesses traffic from all sources, extracts network-derived attributes, and sends this traffic to Dynatrace.

Problem and Solution

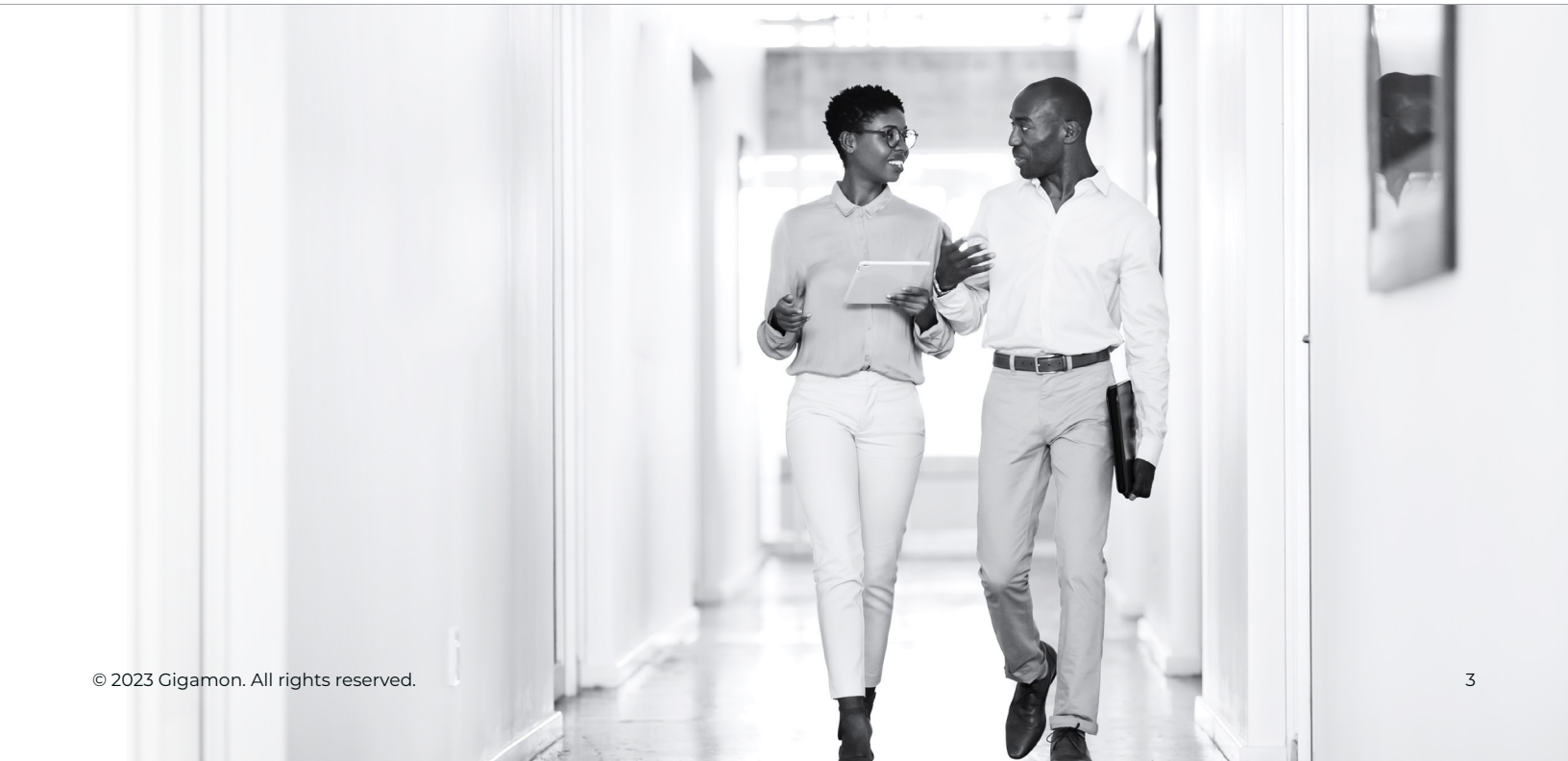
Organizations with hybrid cloud and even multi-cloud environments are becoming the norm. However, moving applications to public clouds or developing cloud-native applications bring new challenges, such as:

- Decreased visibility and control, raising security and compliance risks
- Multi-cloud "silos" that make it nearly impossible to maintain a consistent security posture and quickly pinpoint the root causes of performance issues
- New tools and processes — which could vary by cloud — for teams to invest in and learn

All of the above can slow your cloud initiatives and make life harder for your teams. But what if Gigamon and Dynatrace could address these critical hybrid cloud challenges? Gigamon Deep Observability Pipeline gives you complete network visibility, and together with Dynatrace, the power to see deeply into what is happening in your cloud deployments.

Here are just a few examples of security and compliance use cases enabled by the joint Gigamon and Dynatrace solution:

- **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.



How the Joint Solution Works

AMI complements the MELT data collected by Dynatrace OneAgent. These added app-aware attributes are exported from GigaVUE® Cloud Suite™ to Dynatrace Software Intelligence Platform in various formats (including CEF, IPFIX, and JSON) which can be consumed to provide reports in Dynatrace dashboards.

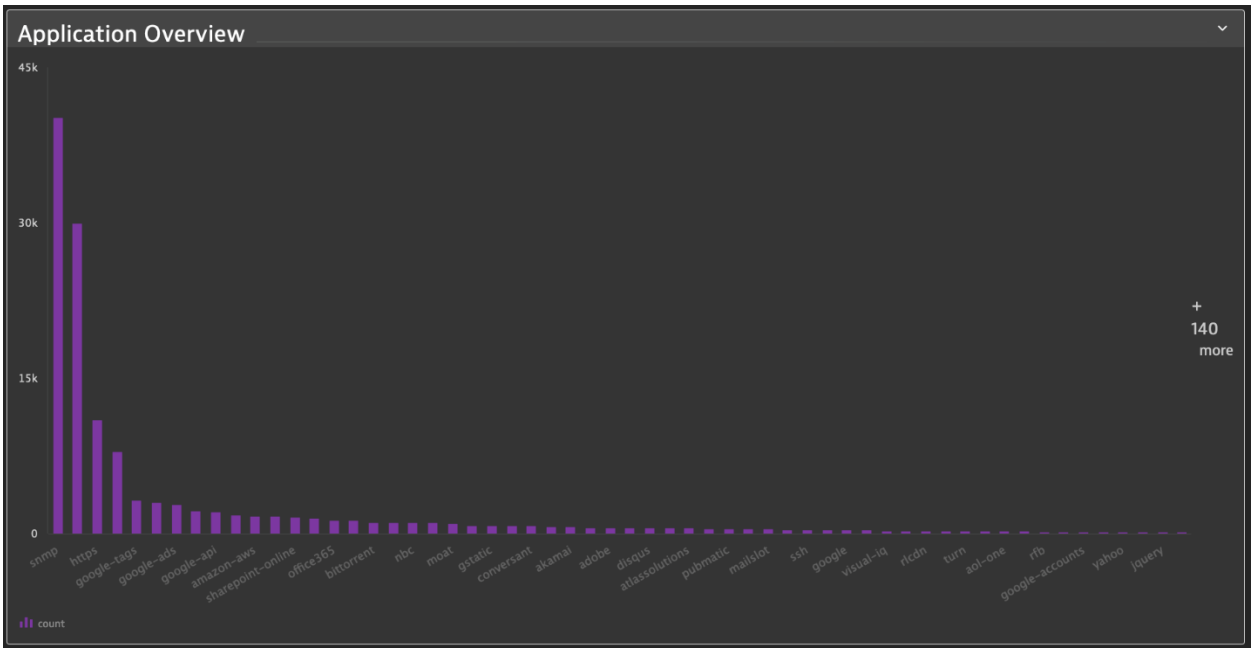


Figure 2. Gigamon AMI through the Dynatrace dashboard shows all applications running on a network.

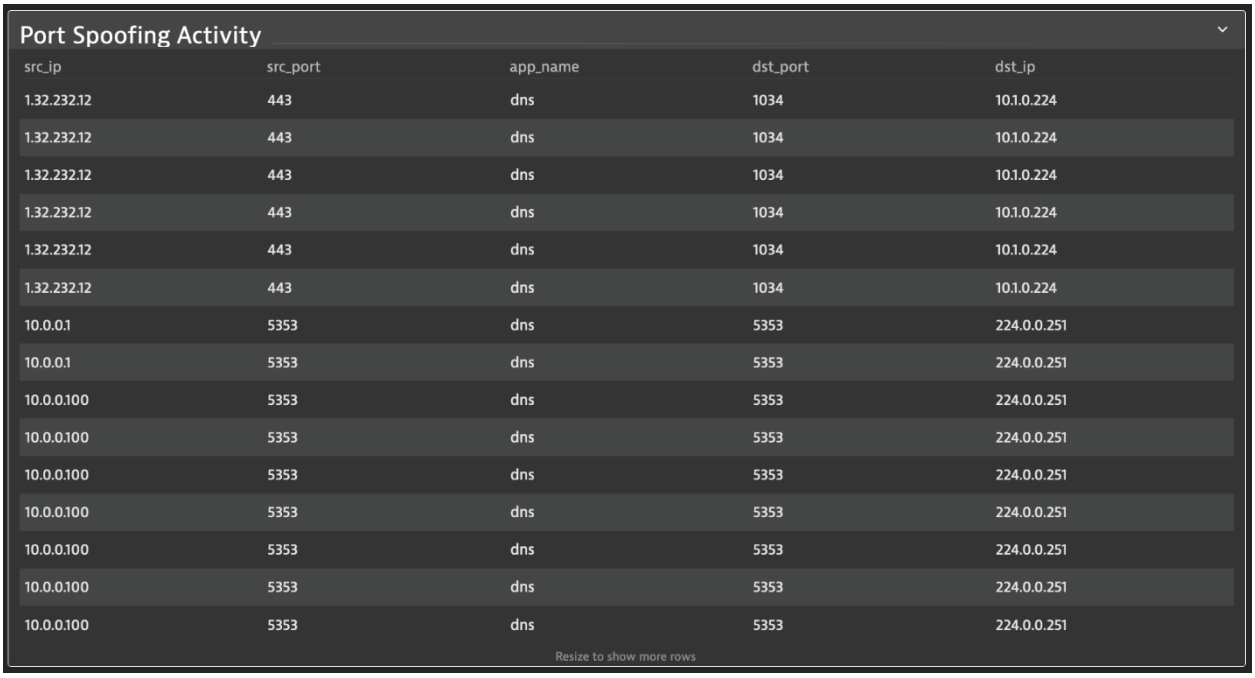


Figure 3. Gigamon AMI exposed through the Dynatrace dashboard shows all port spoofing activities.

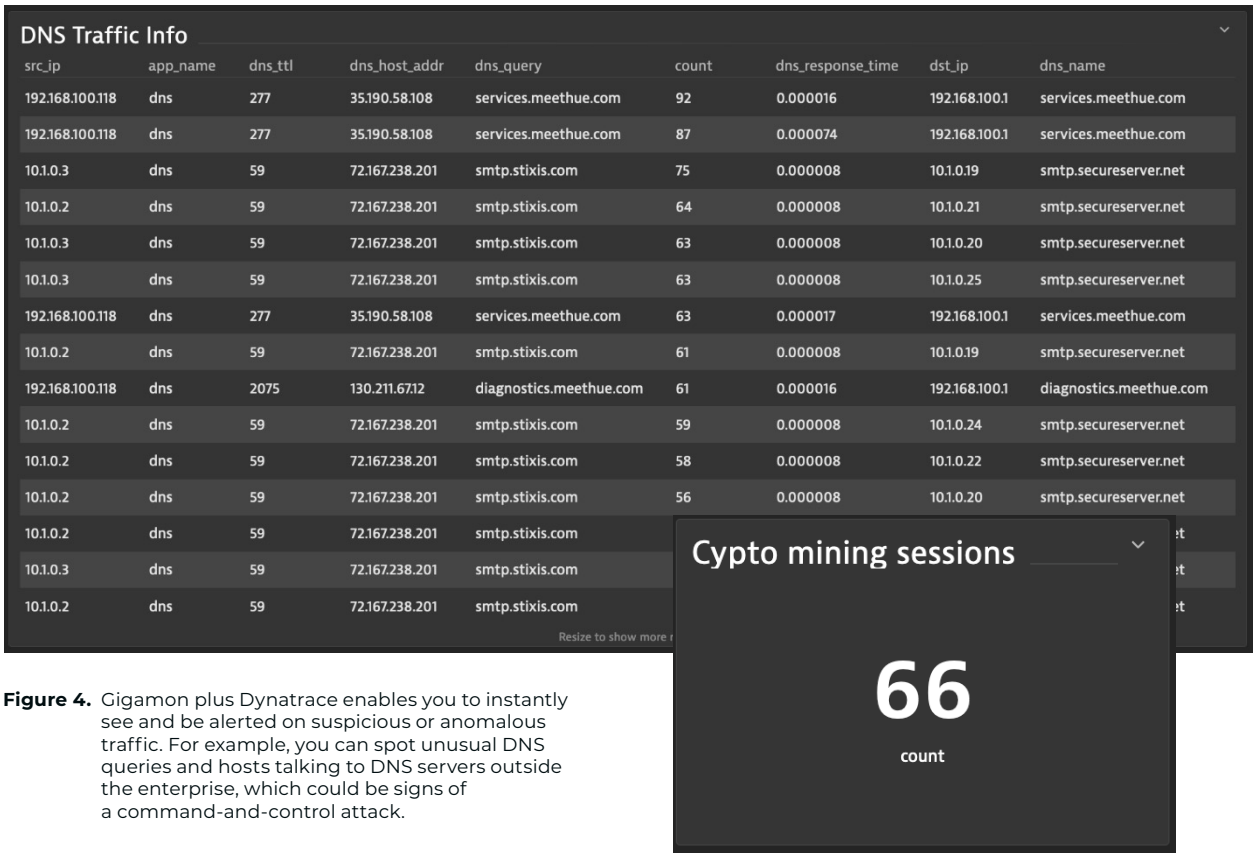


Figure 4. Gigamon plus Dynatrace enables you to instantly see and be alerted on suspicious or anomalous traffic. For example, you can spot unusual DNS queries and hosts talking to DNS servers outside the enterprise, which could be signs of a command-and-control attack.

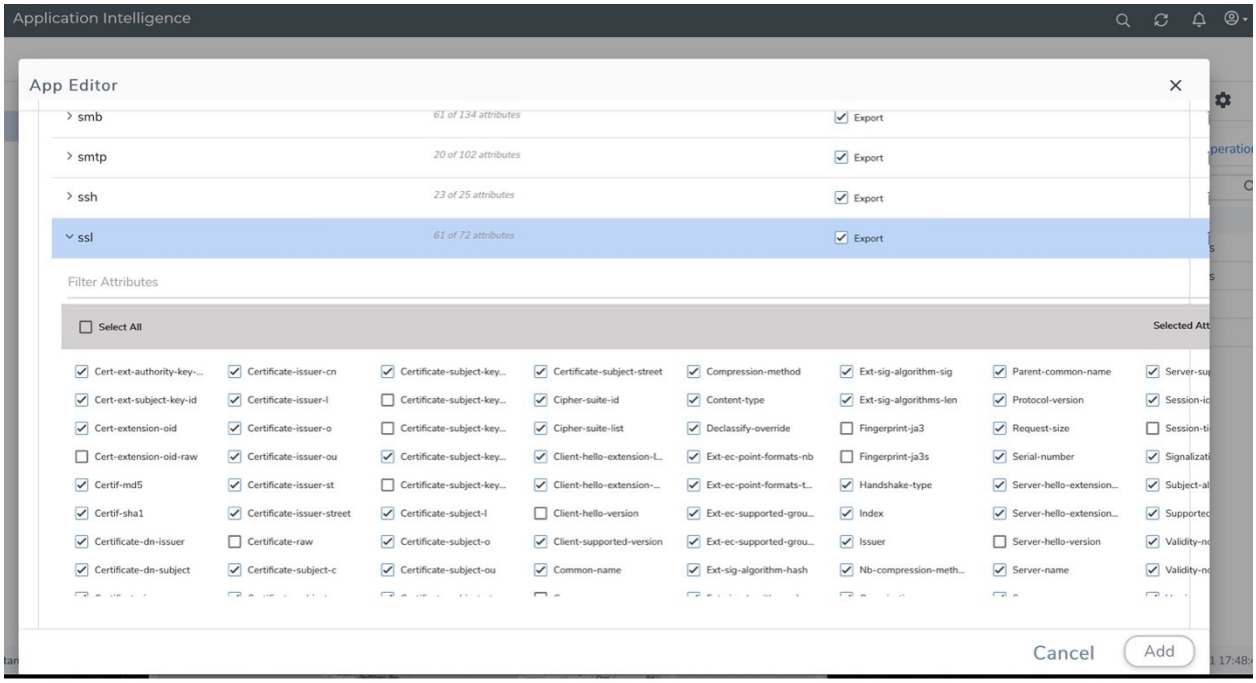


Figure 5. With GigaVUE-FM fabric manager, you can see the list of available SSL/TLS attributes that may be selected and sent to Dynatrace for analysis.

Conclusion

Gigamon Deep Observability Pipeline plus Dynatrace Software Intelligence Platform lets you detect critical security and compliance issues across your hybrid cloud, identify threats before they do damage, and get to the root of performance issues before large groups of users are affected. Gigamon and Dynatrace put you back in control even as applications and environments continue to evolve.

For more information on the Gigamon Deep Observability Pipeline and Dynatrace, please visit gigamon.com/partners/technology-partners.html#dynatrace.

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**.

Gigamon®

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

01.23_01