Gigamon®

Optimizing Application Performance and Troubleshooting with Deep Observability

Eliminate Blind Spots, Reduce Downtime, and Accelerate Troubleshooting Across Hybrid and Multi-Cloud Environments

Modern enterprises face application performance degradation, security blind spots, and slow troubleshooting processes as they migrate to hybrid and multi-cloud environments. Identifying the root cause of performance issues—whether from the network, application, or infrastructure—remains a major challenge due to limited visibility, encrypted threats, and tool sprawl. This can lead to increased downtime, security vulnerabilities, and operational inefficiencies.

Challenges

IT teams are constantly putting out fires when it comes to slow applications, security gaps, and frustrating blind spots across hybrid cloud infrastructure. The biggest headache? Figuring out whether an issue is caused by the network, application, or infrastructure which can lead to prolonged troubleshooting and finger-pointing between teams.

Visibility is another major problem. As businesses move to hybrid and multi-cloud environments, analyzing traffic across on-prem, virtual, containerized, and cloud workloads gets tricky. Blind spots in east-west traffic and encrypted communications mean security threats — like rogue applications, expired SSL certificates, and unusual DNS activity—can slip through unnoticed.

And then there is the issue of too many tools. With a myriad of different security and performance monitoring tools deployed across the IT stack, teams struggle with siloed data, redundant tools, and skyrocketing costs. Instead of a clear, unified view, they are left with a patchwork of partial insights, leading to a “best effort” approach that’s slow, reactive, and inefficient.

At the end of the day, without the right visibility and intelligence, businesses face longer downtime, weaker security, and an overall frustrating IT experience, all of which hurt productivity and customer satisfaction.

Solution

The Gigamon Deep Observability Pipeline efficiently delivers network-derived telemetry to security and performance monitoring tools, providing IT teams with the intelligence and insights they need to eliminate blind spots, optimize performance, and strengthen security posture.

Deep Observability Across Hybrid Cloud Infrastructure

- **Complete Visibility**
  Gigamon enables granluar visibility into application traffic across on-prem, virtual, containerized, and cloud workloads, eliminating silos and blind spots.
- **East-West Traffic Inspection**
  Gain insights into lateral (east-west) traffic across hybrid cloud environments, allowing teams to track application flows and identify anomalies.
- **Decryption and Encrypted Traffic Analysis**
  Detect threats hidden in encrypted traffic by inspecting TLS/SSL flows without compromising data privacy.
- **Cloud-Aware Network Intelligence**
  Optimize performance and security with real-time insights into cloud workload traffic across AWS, Azure, and Google Cloud.

Accelerated Troubleshooting & Root-Cause Analysis

- **Instantly Identify Performance Bottlenecks**
  Determine whether issues stem from network congestion, slow links, expired SSL certificates, TCP retransmissions, or application slowdowns.
- **Automated Issue Detection**
  Get proactive alerts for SSL certificate expirations, weak ciphers, DNS anomalies, and TCP errors before they impact users.
- **Reduce mean time to identification (MTTI) and resolution (MTTR)**
  By integrating with SIEM, observability, and APM tools, Gigamon accelerates incident response and reduces downtime.

Security Enhancement & Threat Prevention

- **Detect Rogue Applications and Shadow IT**
  Identify unauthorized or misconfigured applications consuming network resources.
- **Prevent Encrypted Threats**
  Gain visibility into malicious encrypted traffic, expired certificates, and suspicious TLS handshake activity.
- **Identify Lateral Movement and Unusual DNS Activity**
  Detect hidden threats that bypass perimeter security by analyzing lateral traffic patterns and DNS requests.

Tool Consolidation & Operational Efficiency

- **Integrate Network-derived telemetry with SIEM and Observability Tools**
  Enrich Splunk, Datadog, and SIEM tools with network-derived metadata and enhanced visibility.
- **Eliminate Tool Sprawl and Visibility Gaps**
  Consolidate monitoring with the Gigamon Deep Observability Pipeline for stronger security, faster troubleshooting, and better performance.
- **Improve IT Efficiency and Cost Savings**
  Enable faster diagnostics and proactive issue resolution, reducing operational overhead and minimizing cloud egress costs.

Key Business Outcomes

- **Maximized Uptime and Service Availability**
  Detect and resolve performance bottlenecks before they impact users.
- **Faster Troubleshooting and Incident Response**
  Reduce mean time to identify (MTTI) and Mean time to respond (MTTR) with complete visibility.
- **Secure Hybrid and Multi-Cloud Operations**
  Gain insights into encrypted and lateral traffic to mitigate security risks.
- **Optimized Cloud Migration and Performance**
  Ensure seamless workload transitions with proactive monitoring.
- **Streamlined IT Tools and Cost Efficiency**
  Consolidate security and monitoring tools while reducing operational overhead.

Key Benefits

- **Complete Performance Visibility**
  Gain insights into traffic across cloud, virtual, and on-prem environments for faster issue resolution.
- **Proactive Troubleshooting and Root-Cause Analysis**
  Identify whether bottlenecks stem from network, application, or infrastructure layers.
- **Stronger Security Posture**
  Detect rogue applications, shadow IT, expired SSL certificates, and encrypted threats before they cause damage.
- **Reduced Tool Sprawl and Complexity**
  Optimize security and performance tools with network-derived telemetry, reducing traffic and lowering costs.

Today we are leveraging AMI capability to help us troubleshoot performance issues and safeguard our PCI environment as we move to PCI-DSS 4.0."

Corpay

By eliminating the noise from irrelevant data, our tools can now pinpoint critical information with greater accuracy. This leads to more reliable results and better decision-making. Today, we enjoy the peace of mind that the continuous uptime and reliability Gigamon delivers with a 100 percent ROI in less than 18 months."

RivCoNOW
COMMUNITY NOW. SERVICES NOW.

With Gigamon, we can place a magnifying glass on critical cloud environments, allowing traffic to be directed to any type of tool for a detailed and in-depth analysis."

LARGEST PRIVATE BANK IN LATIN AMERICA

Gigamon Application Metadata Intelligence Dashboards for Applications Performance and Troubleshooting Use Cases

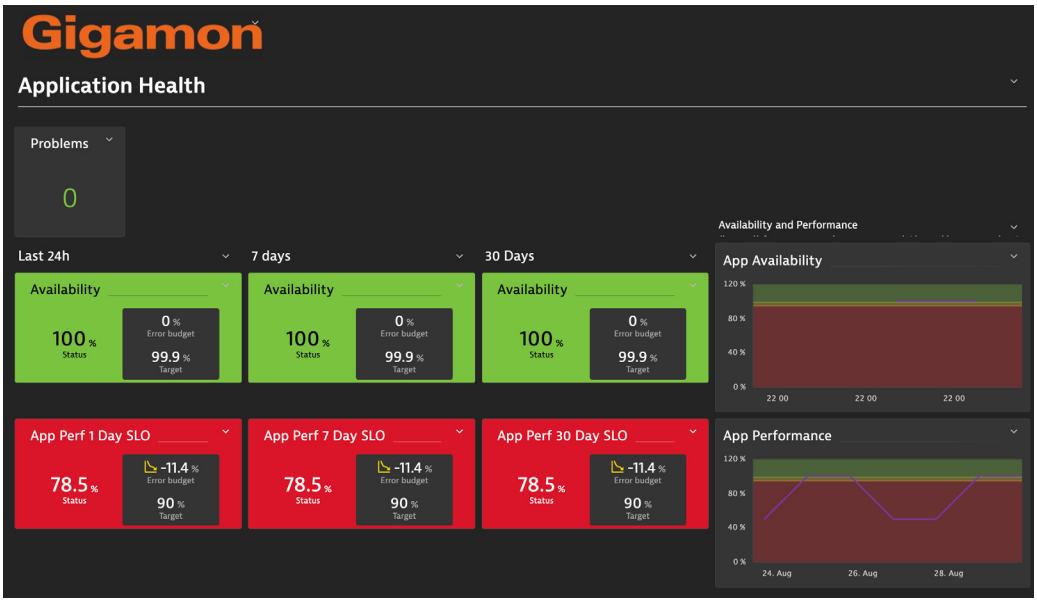


Figure 1. Comprehensive application performance monitoring.

TCP Resets (aborts)

TCP Resets (aborts)

Session info that are experiencing an abrupt end to a tcp connection, due to some error

src_ip	dst_ip	tcp flag reset	Application
10.0.0.55	162.255.36.15		zoom
162.255.37.124	10.0.0.55		https
10.0.0.55	162.255.37.125		zoom
10.0.0.55	162.255.36.14		zoom
50.239.204.19	10.0.0.55		zoom
10.0.0.55	162.255.37.124		zoom
10.0.0.55	50.239.204.20		zoom
10.0.0.55	50.239.204.19		zoom
10.0.0.55	18.205.93.144		amazon-aws
10.0.0.55	161.199.139.254		zoom

Figure 2. Troubleshooting Application and Network Failures with TCP Reset Analysis.

Lost Data

Lost Data

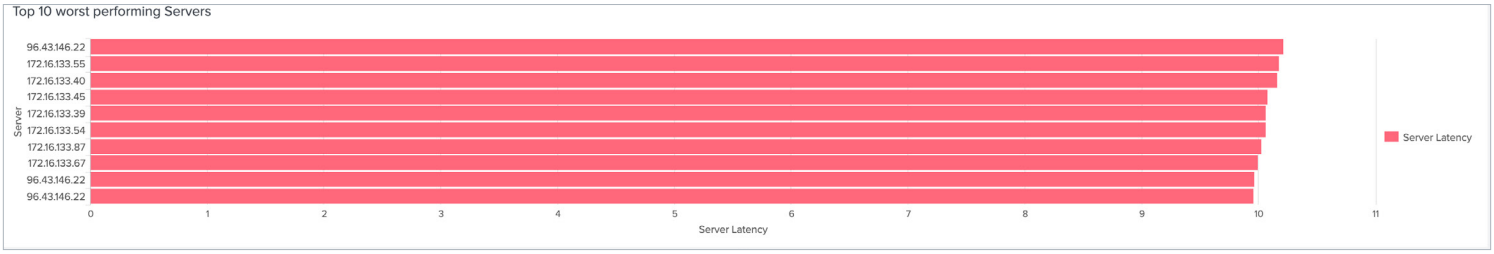
Session info that is experiencing lost data bytes

src_ip	dst_ip	Application	Lost Bytes
172.16.133.63	216.52.242.80	linkedin	1460
172.16.133.16	208.85.42.33	pandora	43800
172.16.133.12	157.56.242.198	https	45
172.16.133.67	23.66.230.80	xm-radio	1460
172.16.133.29	216.52.242.80	linkedin	1460
172.16.133.41	23.62.105.87	tripadvisor	681
172.16.133.132	199.27.208.55	http	388
172.16.133.54	12.130.48.51	http	716
172.16.133.28	208.111.160.6	http	1460
172.16.133.93	74.63.52.167	http	1460

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Figure 3. Identifying and Troubleshooting Lost Data in Application Sessions.

Top 10 Worst Performing Servers



Server Latency

Server Latency

Application response time of the server

Client	Server	Application	Server Latency
172.16.133.53	96.43.146.22	https	10.216352
96.43.146.22	172.16.133.55	https	10.179278
96.43.146.22	172.16.133.40	https	10.162212
96.43.146.22	172.16.133.45	https	10.079182
108.160.160.163	172.16.133.39	dropbox	10.066971
96.43.146.22	172.16.133.54	https	10.065842
199.47.218.150	172.16.133.87	dropbox	10.024448
96.43.146.22	172.16.133.67	https	9.999938
172.16.133.28	96.43.146.22	https	9.964887
172.16.133.93	96.43.146.22	https	9.963212

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Network Latency

Network Latency

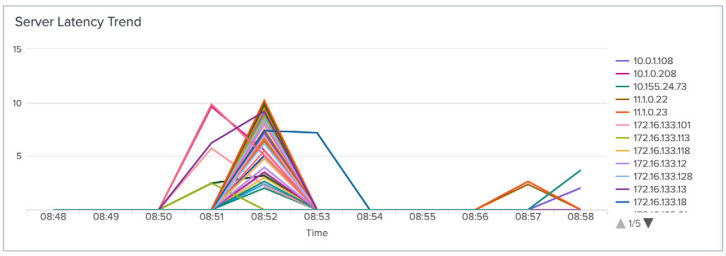
Sessions with respective TCP Rtt

Client	Server	Application	tcp rtt
10.1.0.208	208.51.221.18	facebook	9.052380
10.1.0.208	204.2.225.25	facebook	8.924756
10.1.0.208	205.234.218.80	facebook	6.331931
10.1.0.208	208.111.128.7	facebook	2.090564
172.16.133.60	172.16.128.169	symantec	1.563264
172.16.133.46	172.16.128.169	symantec	1.556455
172.16.133.75	172.16.128.169	symantec	1.555825
172.16.133.34	172.16.128.169	symantec	1.547001
172.16.133.132	199.27.208.20	http	1.433557
172.16.133.28	96.43.146.22	salesforce-chatter	1.204126

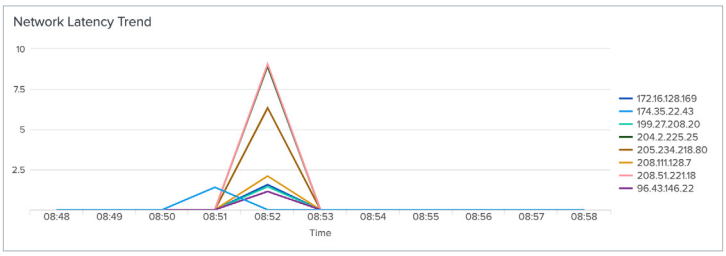
« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Figure 4. Pinpointing Latency Issues with Worst-Performing Servers and Network Delays.

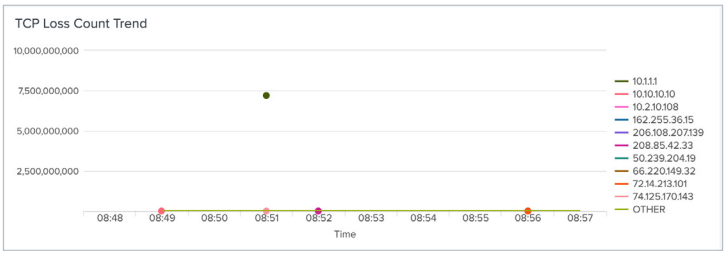
Server Latency Trend



Network Latency Trend



TCP Loss Count Trend



IP CRC Trend

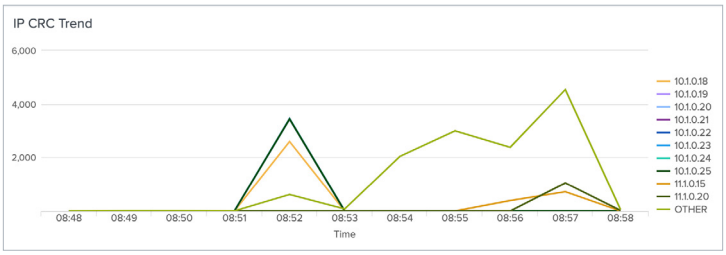


Figure 5. Tracking Performance Trends: Server Latency, Network Delays, and Packet Loss.

Conclusion

In today's fast-paced digital world, organizations can't afford slow applications, security blind spots, and inefficient troubleshooting. As IT environments become more complex—spanning on-prem, cloud, and hybrid cloud infrastructure—the ability to see, secure, and optimize network traffic has never been more critical.

Gigamon delivers deep observability that goes beyond traditional monitoring, providing real-time intelligence and insights into application performance, security threats, and network health. This helps IT team to eliminate blind spots, reduce mean-time-to-resolution (MTTR), and streamline tool sprawl, empowering IT teams to stay ahead of performance issues, proactively mitigate threats, and ensure seamless user experiences.

With Gigamon, organizations can achieve greater uptime, better secure and manage their hybrid cloud infrastructure, and troubleshoot issues faster than ever before, all while cutting operational complexity and costs. It's time to move from reactive firefighting to proactive IT excellence with the power of deep observability.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

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

03.25_01