

Mind the Cloud Visibility Gap

**The Structural Deficiency in Your Digital
Infrastructure and How to Close It**



The Challenges of Managing a Hybrid Cloud World

Today's enterprises and government agencies are living in a more complex IT world than ever before. On-premises, private cloud, public cloud, and now hybrid and multi-cloud environments are the new normal for almost every organization.

Complexity is one issue, but there's another major issue: IT has to hit a continually moving target to ensure security and business continuity in an already complex environment that's changing all the time.

The result is a hybrid IT environment where legacy infrastructure, applications, and databases have to interact with applications built on new technologies like containers and service meshes and deployed using IaaS, PaaS, and SaaS models.

The challenge for IT is how to gain — and retain — visibility into an ever-changing world of network assets and data in motion across a hybrid



Having a visibility strategy is going to be key to customers having a successful hybrid implementation”

SCOTT WARD, PRINCIPAL SOLUTIONS ARCHITECT AT AWS²

landscape. It is a challenge that can easily become a complex and costly proposition. In this whitepaper, we examine this challenge, including its root cause and impact on organizations, and how visibility plays a key role in helping IT teams successfully overcome this issue.

The Cloud Visibility Gap: The Structural Deficiency in Your Digital Infrastructure

By early 2020 in most enterprises, IT already had a plan to migrate their datacenters and infrastructure to the cloud. With the onset of the global pandemic, however, these well-considered, multiyear plans were most likely disrupted, and organizations had to accelerate cloud migration as face-to-face interactions were replaced by the switch to an online, cloud-based business model.

Faced with this challenge and the need to prevent new applications becoming fragmented or siloed off from the core enterprise infrastructure, IT has to ensure that all of their applications and assets work together to provide a secure, resilient infrastructure to support their mission-critical services and provide a positive customer and user experience.

The problem at the heart of this challenge is that the tools needed to monitor, manage, and secure this hybrid environment were not designed to work together. Network monitoring and security tools were designed for an on-premises world and typically lack visibility into cloud environments, applications, and services. Equally, cloud-based tools, designed around log-based monitoring, don't provide on-premises visibility or the level of detail into network health that enterprises have come to rely on in their on-premises and private cloud environments. This is the cloud visibility gap. This gap leaves organizations without a clear, complete, and consistent view of their networks, applications, and data in motion across their digital infrastructure. And it's a gap that continuously morphs and evolves. It is, in every sense, a moving target.



Because traditional network monitoring tools struggle with visibility into cloud activity, increasing cloud adoption will heighten the presence and criticality of network blind spots. Here, cloud visibility and control problems can best be solved by next-generation cloud visibility solutions like those from Gigamon.”

SCOTT WARD, PRINCIPAL SOLUTIONS ARCHITECT AT AWS¹

Mind the Gap: The Business Impact of the Cloud Visibility Gap

+

“The cloud visibility gap is what happens while you’re busy making other plans.” (with apologies to John Lennon)

As noted earlier, most enterprise-level organizations were already engaged in multiyear projects to move some, or all, of their workloads to the cloud to take advantage of the agility and elasticity it provides. The double-punch of the pandemic and subsequent global economic slowdown, however, has forced organizations to accelerate their cloud migration plans. In some cases, this means accelerating already agreed upon migrations, but for most organizations it has meant:

- + Adopting SaaS-based applications to provide tools to enable remote working for employees or enhance partner communication and collaborations

- + Developing PaaS or IaaS applications to support partner and customer interaction as organizations have been forced to move to a predominantly online business model

In many cases, the adoption of SaaS, PaaS, and IaaS-based applications has been driven by operating units in parallel — and sometimes, even in conflict — with enterprise IT and security teams. This pattern of cloud adoption is the so-called accidental hybrid model, a model that is now common to many organizations across all industries.

One of the problems inherent in this model is that the proliferation of these different platforms can cause organizations — either deliberately or accidentally — to revert to a siloed application infrastructure with islands of visibility that gives rise to the cloud visibility gap.

The cloud visibility gap isn’t an abstract concept: It’s a real issue that can have negative impacts not just for IT, but also for your entire organization. Let’s look at four such issues that we often hear about from our customers.



POOR CUSTOMER AND USER EXPERIENCES

Optimizing customer and user experiences by maximizing application availability and performance are must-haves for success in the always-on digital world. Troubleshooting CX issues is challenging. Cloud tools can miss critical insights into the data in motion on the network, which can impact inter-component communication and lead to slow application performance.

SECURITY AND COMPLIANCE BLIND SPOTS

Ensuring continued security and compliance in a hybrid world is nonnegotiable, especially for organizations that must meet regulatory, compliance, and audit standards. Relying only on application logs and trace files can lead to an incomplete picture of security because instrumentation of logs can vary by developer, logs can be suppressed by bad actors, and logging is often switched off or minimized by CloudOps in a tradeoff between performance and security.

ESCALATING COST AND COMPLEXITY

Adopting a hybrid infrastructure creates complexity, and with complexity comes cost. Multiple teams, multiple tools, and multiple agents feeding those tools all generate unnecessary network traffic that uses expensive bandwidth and CPU capacity. Additionally, where cloud traffic moves across boundaries or is backhauled to on-premises tools or applications, organizations typically must pay data movement charges that can very quickly add up.

CLOUD MIGRATION RISK

Migrating or rebuilding workloads in the cloud is vital to digital innovation, yet also fraught with complexity and risk. Without the right level of visibility across the hybrid cloud network, many security, compliance, and performance challenges arise, leading to failed digital initiatives. Such failures not only reflect poorly on IT, but they also reflect poorly on the organization and, in commercial ventures, on the brand that these initiatives portray to perhaps tens of millions of customers.

Four Steps to Close the Cloud Visibility Gap

Regardless of how the cloud visibility gap has occurred, IT, security, and business teams must work in close collaboration to close the gap and re-establish visibility across all of the organization's applications and IT assets. This needs to be a pragmatic initiative driven by a sense of urgency to prevent the customer experience, security, and compliance issues identified earlier from become serious issues.

For IT, security, and business teams to be able to work together, all of these stakeholders must have access to the same data and make decisions based on that data. To achieve this, organizations need a solution that can capture, aggregate, optimize, and then distribute all of the data on the hybrid network to the tools that need to consume it to ensure that IT, security, and business stakeholders are aligned and have the data visibility they need.

1. CAPTURE

Capturing data in motion across a large-scale hybrid network can be a daunting task in terms of the variety and the sheer volume of data. This data is typically captured by either tapping or mirroring techniques that copy network traffic and route the copied traffic to a security or management tool for analysis. In designing these processes, follow best practices to ensure that only the required traffic is tapped or mirrored in order to avoid performance issues and the costs associated with CPU and bandwidth utilization.

2. AGGREGATE

Once captured, this data needs to be aggregated and visualized through what is commonly called "a single pane of glass." This visualization needs to show data sources and destinations and, ideally, to provide map sources to destinations. This process can be achieved manually, using, for example, a simple drag-and-drop user interface, but it's usually more efficient to use a rules-based approach to automate this process.

3. OPTIMIZE

As well as aggregating data, this data in motion needs to be inspected and analyzed to identify whether it contains duplicate packets of network data. Some level of duplicate traffic, maybe 15–20 percent, is normal on a large-scale network, so it's important to eliminate this duplicate traffic to ensure overall data accuracy. In addition to de-duplication, traffic flows can also be optimized by filtering out traffic from applications that have been classified as safe or low-risk or that are irrelevant to certain tools or destinations.

4. DISTRIBUTE

Finally, traffic must be distributed to the tools or destinations that need to consume this data. Again, you can apply optimization techniques to the network data to reduce the volume of data being transmitted. For example, where a performance monitoring tool is able to consume NetFlow metadata, this can reduce the amount of data transmitted to that tool by up to 95 percent without losing the contextual value of this data.

Taken together, these four approaches ensure clear, complete, and consistent visibility into your data in motion. This enables IT, security, and business teams to gain visibility into all of their data to align around the common goals of ensuring the best possible customer and user experience, optimizing security, and reducing the complexity and cost of network and security operations.

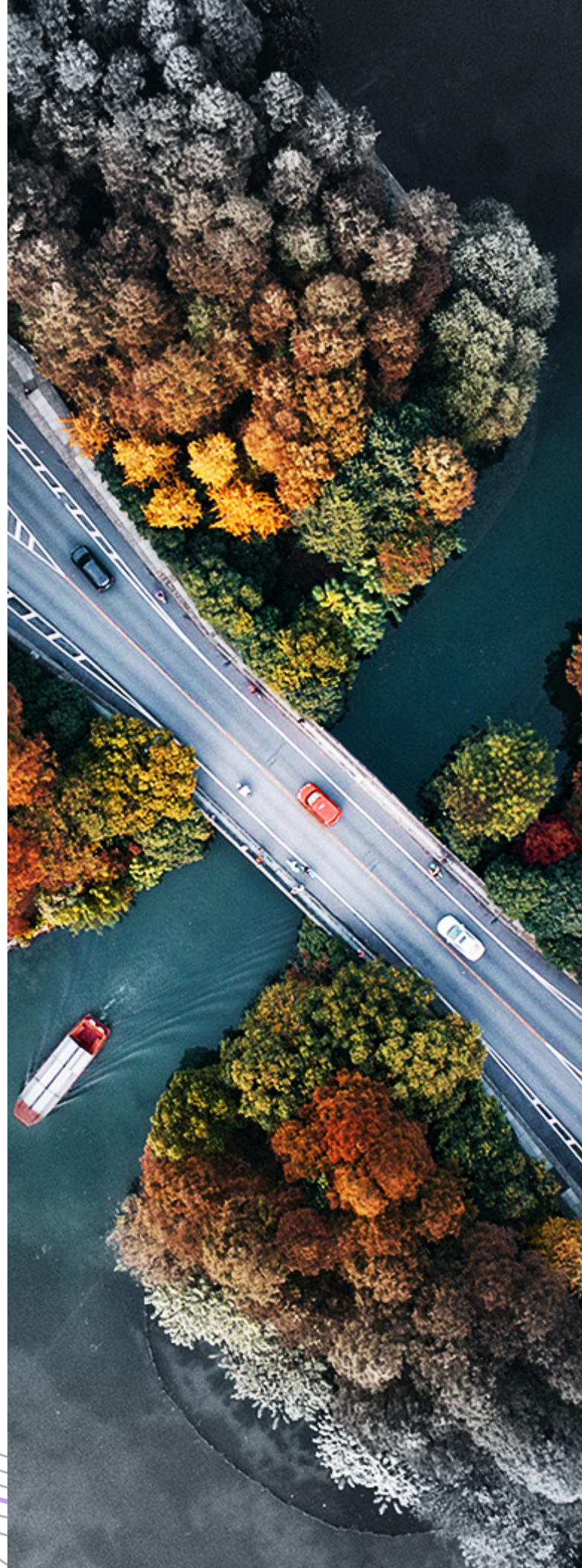
Gigamon Hawk — Closing the Cloud Visibility Gap

What if you could see everything — including the moving targets — across the entire landscape of your hybrid network and could close this visibility gap? That is precisely what [Gigamon Hawk](#) is built to do. Leveraging over a decade of investment in the market-leading Gigamon Visibility and Analytics Fabric™, Hawk extends this capability to the hybrid cloud to provide critical visibility and context for exactly what's happening across your entire infrastructure.



With the Gigamon cloud visibility platform, we maintained very fine-grained control over monitoring in the cloud, allowing us to adapt at a moment's notice to increased monitoring or enhanced capability needs”

MIKE MCBRIDE, FOXTROT DIVISION,
SOFTWARE AND CYBERSECURITY
ENGINEERING



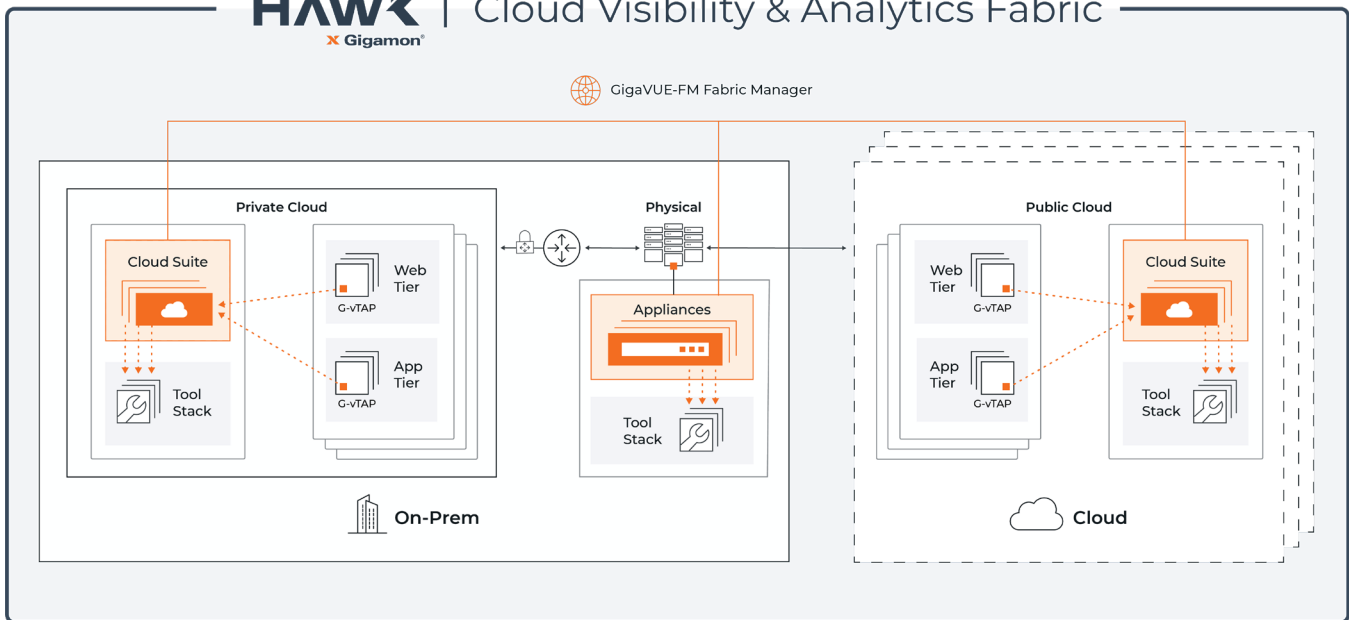


Figure 1. The Gigamon Hawk Cloud Visibility and Analytics Fabric provides visibility into all of the components of an organization's digital infrastructure closing the cloud visibility gap

Gigamon Hawk not only provides complete and consistent visibility across all of an organization's hybrid infrastructure components, it enables them to see, secure, scale, simplify and save on their digital initiatives.

SEE

Gigamon Hawk is a complete visibility solution that spans the entire hybrid cloud network. It provides NetOps, CloudOps, and InfoSec teams a clear, complete, and consistent view of what's happening across their hybrid infrastructure to help eliminate the blind spots that lead to performance and security risks.

SECURE

With a view from above, Gigamon Hawk can quickly detect vulnerabilities in data in motion across the hybrid network. Importantly, Hawk monitors not just North-South data in motion, but also East-West traffic within an individual platform or across multiple cloud platforms. And Hawk integrates with the Gigamon ThreatINSIGHT™ network detection and response application so that organizations can glean context and insight from all the data in motion on their network.



U.S. Bank chose
Gigamon solutions
because it is a single
source of visibility across
our physical, virtual, and
cloud environments”

JAMES SCOLLARD, ENTERPRISE SOLUTIONS
ARCHITECT AT U.S. BANK

SCALE

Not only does Gigamon Hawk provide visibility into the entire hybrid network infrastructure, but it also enables organizations to maintain this visibility as the network scales up and scales out. Hawk provides visibility as code, enabling visibility to be embedded into cloud automation. This visibility as code, or elastic visibility, is vital for ensuring that visibility is maintained into the moving target of the ever-changing hybrid infrastructures.

SIMPLIFY

Gigamon Hawk taps the network once and can aggregate data from any cloud source, then transform and analyze it before sending it to any destination, whether that be a tool, data store, or other target. This not only optimizes the traffic and metadata sent to tools, but it also reduces the number of agents that need to be managed through an intuitive, single interface.

SAVE

Finally, while cloud costs are very complex to calculate and will be unique to almost every organization, reducing the number of agents

deployed across a hybrid network means reducing not only the complexity of managing the network, but also the bandwidth and CPU utilization for traffic mirroring to support those agents. Moreover, Gigamon Hawk traffic management features, such as de-duplication, application filtering, and metadata generation, can reduce the amount of traffic on the network. The exact reduction in traffic will vary from organization to organization. However, Gigamon has created Traffic Reduction and [Cost Calculator tools](#) to help identify and quantify possible traffic reduction savings.

In hybrid cloud environments, these savings can result not only from reducing bandwidth and CPU utilizations costs, but also from reducing data movement charges incurred when moving traffic across cloud boundaries, whether to other cloud instances or backhauled to tools in an on-premises datacenter.



“A large enterprise aerospace and defense company saw ROI with their investment in Gigamon solutions immediately, and confirms they saved \$1,000,000 or more.”²



Gigamon has stayed in lockstep with our environments as we've migrated from various architectures to include on-premises and the cloud. The consistency and reliability of traffic flows, due to the Gigamon solutions, enable us to make business-driven decisions without compromising IT security”

CHRISTOPHER EBLEY, CTO AT BLACKWOOD ASSOCIATES



Cloud migrations can be tough and confusing. Nothing lets you skip over the hard work, but learning the lessons of those who have already climbed the mountain can save costs, reduce frustration, and increase your odds for success”

RICH MOGULL, SECURORIS

Summary

The cloud visibility gap is a real issue that many organizations may not anticipate as they move to a hybrid infrastructure, either as part of a carefully planned migration process or from the need to adopt cloud applications to meet ever-changing organizational and customer needs in the so-called accidental-hybrid model.

For existing Gigamon customers, it is important to know that the visibility, security, and control they rely on can be seamlessly extended to any cloud. Equally, for organizations not yet using Gigamon, it is reassuring to know that a visibility solution trusted by 4,000 of the world's most-demanding IT enterprise and government organizations is available to close the cloud visibility gap.

Achieving hybrid cloud visibility is a complex issue and, due to the elastic and ever-changing nature of the hybrid cloud, it is also a moving target. To stay on top of this challenge and to close the cloud visibility gap, you need a solution that is as dynamic as the environment that you are trying to secure: Gigamon Hawk was designed to be that solution.

To learn more about Gigamon Hawk and see it in action, please visit gigamon.com or join our [Community Group](#) to discuss hybrid cloud issues and experiences with your industry peers.

About Gigamon

Gigamon helps the world's leading organizations run fast, stay secure and innovate. We provide 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 75 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. Headquartered in Silicon Valley, Gigamon operates globally.

For the full story on how Gigamon can help you to run fast, stay secure and innovate, please visit www.gigamon.com and follow us on Twitter [@gigamon](https://twitter.com/gigamon).

References

¹ Cloud Visibility and Analytics. Gigamon. Accessed April 6, 2020.
<https://www.gigamon.com/products/visibility-analytics-fabric.html#aws-451>

² Rich Mogull. "NetOps and SecOps Guide to Public Cloud Journeys." Securoris, 2021.
<https://www.gigamon.com/resources/resource-library/white-paper/wp-securosis-cloud-security-journeys.html>.

© 2020 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.