Gigamon®

See what matters.™

The top 3 reasons
you need a visibility platform.

This is not an equation.

It is an illustration of the network data and business challenges you face, without visibility. **See what matters.™**

Gain 20/20 network insight.

To manage, secure, and understand your network data, first you have to be able to see it.

Digital transformation is driving every workplace, creating advantages in collaboration, speed, and innovation. Along with that transformation, the enormous increase in the volume of data and devices attaching to corporate networks adds complexity and introduces new risks. At the same time, network speeds are increasing well ahead of software tools' ability to perform needed compute functions to ensure control and safety. And threats have become "democratized," making it easier for bad actors to find ways to penetrate networks and cause disruptions that have both organizational and human costs.

What's the best strategy to protect your organization's data, systems, and people? A visibility platform that allows you to manage all traffic flowing across your network, deliver the right information to the right tools at the right times, and gain insights that drive better decisions. You must have visibility across your extended network—including your own data centers, remote offices, private and public clouds—to manage complexity and control costs, secure your critical data and assets, and understand what's going on across your organization. Read on to understand how a visibility platform allows you to do this.

Four problems solved with visibility.

1. Network blind spots.

According to Enterprise Strategy Group (ESG) research, 90% of organizations have limited visibility into what's happening across their extended networks. Network blind spots create myriad problems that can reverberate throughout the enterprise. It's impossible to achieve consistent deployment of security measures when you have network blind spots. An enterprise network is highly complex, requiring numerous, disparate management, monitoring, and analytics tools that are not synchronized and can be difficult to integrate across the network. The time and effort it takes to successfully monitor and execute all these moving parts inevitably leads to higher Capex and Opex costs.

2. Performance anxiety.

And then there is the performance of the network itself. A hodgepodge of traffic and a host of tools trying to determine when and whether something is a threat creates inevitable lags and interruptions in network service. Beyond the annoyance factor, these disruptions affect productivity, and that's costly for any organization.

3. Heightened vulnerability.

An inability to see all your network data can leave your company even more vulnerable to security breaches. Modern firewalls and malware detectors can't keep up with inspection of an ever-growing volume of traffic and network threats—often leaving companies exposed to new, advanced, and possibly encrypted attacks.

Once inside, malware can spread and go undetected for weeks or months until it rears its ugly head, potentially compromising proprietary data.

4. Customer "un"intelligence.

On the customer-facing front, network blind spots can diminish your ability to deliver the best possible services and solutions to your customers. When awareness of and intelligence about how your customers are connecting with your business are missing, you have to rely on after-the-fact reporting and manual data manipulation to understand the customer experience. If your customers are trying to engage with you digitally, you need to know when, how, and where they are doing so, as well as who they are, so that you can ensure quality performance and service levels. Bad connections and experiences can lead to reduced loyalty and lower sales.

You can't manage, secure, or understand what you can't see. Visibility lets you take control.

We've collected the top ways a pervasive visibility solution addresses these key business problems in the following pages.

This is not a microscope.

It's a way to see relevant information clearly. In the same way a visibility platform identifies crucial data and routes it to the right tools in your network. **See what matters.™**

REASON 1:

Visibility cuts network complexity and cost.

It erases data contention.

Data contention is a problem that continually plagues networks that have blind spots. A basic way to enable both efficient network monitoring and stronger security is to implement a mirror/SPAN port, which is often used to analyze data. While this is a low-cost method that works well on less-trafficked networks, a SPAN port tends to drop packets when it is overloaded. This means you can lose critical data, which in a best-case scenario only causes downtime, but in a worst-case scenario costs you a fortune.

In the long term, poor reliability of SPAN data means you can lose important information about your customers that you could use to improve intelligence or streamline delivery of better services. And if your customers are affected by these packet losses, you can lose business and damage your reputation.

A visibility platform extends well beyond SPAN monitoring and analysis in capability and scale. It allows for real-time monitoring of all the traffic flowing across your network, and supports fast analysis and routing of the right traffic to the right tools and applications. By streamlining the flow of traffic to your monitoring and security tools, you eliminate contention, improve performance, and reduce cost and complexity.

It eliminates downtime during upgrades.

Software, hardware, and firmware are all in continuous need of updates, and delaying implementation can be dangerous (WannaCry, anyone?). System upgrades are also crucial, as they can boost compatibility and productivity across departments.

Ad-hoc deployment or upgrade of tools—while part of the system is down—can create network bottlenecks, leading to service delays and unexpected downtime. To compensate, you might resort to disabling certain network devices, which may increase throughput but degrade security inspection and analysis, thereby increasing your overall risk profile.

Use of the many varied management, security, and upgrade tools across the network leads to other complexities, too. Often, network speeds and tool capacity don't match, leading to oversubscription; devices with limited scalability can be quickly overwhelmed by traffic, causing dropped packets and degraded protection from threats.

An effective visibility solution streamlines network tool deployment and upgrades because it allows you to control resources and only implement where necessary, eliminating redundancy and overload.

Comprehensive network visibility can also accelerate your upgrades, and allow for both independent and simultaneous upgrades of tools. You maintain complete operation of your existing tools during the upgrade as well as afterwards.

It strengthens your weakest link.

In your data center or at your network's edge, failure of even one inline security tool can be devastating. Because network operations and security operations teams have different responsibilities that may not be coordinated, these problems can compound quickly. For example, upon discovery of a new threat or breach, a lack of coordination across NetOps and SecOps can lead to the loss of critical hours trying to contain the damage and implement fixes.

A visibility platform empowers you to close coordination gaps between network and security operations so that you maximize efficiency and increase the scale of both your network and security monitoring efforts. This, in turn, lets you maintain a highly available, highly resilient, and highly economical network. Effectively, a visibility platform aligns both teams around a shared view across the network.

It protects you from costly compliance violations.

To detect network threats and maintain security, it's essential to be able to see all network traffic. But merely accessing certain sensitive information can lead to possible litigation and costly penalties. In the United States alone, there are more than 8,500 federal, state, and local regulations regarding data management, including the Gramm-Leach-Bliley (GLB) Act for financial institutions and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 for safeguarding medical information.

SPAN ports were once a viable monitoring option, but monitoring and filtering ever-increasing volumes of network traffic moving at higher speeds demands more intelligent solutions that support compliance mandates.

A visibility platform lets you set policies for monitoring and analyzing traffic that support your compliance mandates so that you can quickly access, filter, and route content of interest/concern for further risk analysis. A visibility platform must allow you to mask sensitive information within network packets, as well as establish policies restricting decryption of personally identifiable information (PII) based on IP address, VLAN tags, URL categories, domain names, and more—all of which ensures that you avoid compliance conflicts and potentially heavy fines.

This is not a mirror.

It is your defense against dangerous blind spots. Just as a visibility solution can be for your network. **See what matters.**™

REASON 2:

Visibility mitigates network risk.

It filters out noise (like streaming media), freeing tools to focus on real threats.

Video, voice, and streaming media files tend to be very large and hog a lot of bandwidth; however, in terms of security threats, they represent very low risk.

Nevertheless, in a legacy network, all media is treated the same way as other data. The sheer size and volume of audio and video files can overwhelm your security and monitoring tools with needless processing and inspection. Ultimately, your tools just can't keep up.

A visibility platform boosts your efficiency by automatically avoiding processing of low-risk data types. You can steer media streams and audio only to relevant network tools, and ensure that video traffic only flows to and from video servers.

This means your security tools and applications can focus on identifying and neutralizing truly malicious traffic. Your tools can analyze suspicious packets contextually and in parallel by application, user, and content type, resulting in greater accuracy and reduced risk.

It helps you secure encrypted traffic.

The encryption of traffic with SSL/TLS cryptographic protocols has become pervasive in enterprise networks to provide communication security, but has also created dangerous blind spots for security operations teams. Advanced malware hidden within this traffic can propagate—undetected—throughout the network. And SSL-based Command & Control (C&C) traffic can easily exfiltrate data without raising an alert. Major security breaches can go undetected for weeks, months, or years. In fact, according to the 2015 *Trustwave Global Security Report*, the mean number of days from intrusion to detection is 188.

One option is to enable SSL decryption in your existing tools; however, there is a huge downside as systems experience up to 80% performance degradation. So, it may make you more secure, but it dramatically reduces productivity and that increases costs.

Outside examination.
A visibility platform examines select SSL/TLS traffic automatically—without complex configuration—to assess risk. Performing this essential task outside of your security tools removes a huge burden from your existing infrastructure without downgrading performance.

Using simple yet comprehensive policies, a visibility platform routes suspicious payloads to appropriate security tools for further analysis. Visibility policies also help ensure privacy compliance by not exposing sensitive network data, which helps further strengthen your security posture.

It helps reveal malware through metadata.

Monitoring threats using DNS is a common method of exposing rogue actors attempting to access the network. However, the resources that DNS log generation requires can significantly degrade performance. Moreover, monitoring for threats in SSL-encrypted connections may not be feasible due to bandwidth and processing limitations. Essentially, there is too much data and too few resources to process it.

A visibility platform tackles the data volume problem by generating metadata for smarter analytics and enhanced efficiency without compromising security. Monitoring and analyzing metadata on domain lookups is much more efficient than generating and analyzing DNS logs. It can reveal endpoints communicating with nefarious C&C servers. Metadata analysis can spot weak cryptography ciphers commonly used in SSL malware and suspicious servers that are using self-signed or disreputable digital certificates.

Metadata generation and analysis can also help point to other common hacking efforts, such as SQL injections, which seize databases and/or initiate internal network attacks; networked computers that have visited blacklisted sites; and Denial of Service (DOS) attacks.

It enhances security at remote sites.

Remote sites and branch office networks are significantly susceptible to security risks. A lack of strong security may be due to a lack of on-site security personnel, and corporate budgets rarely allow replication of security tools to remote locations.

And if there is budget, a proliferation of tools at remote sites increases complexity of the overall security footprint, making it much more challenging to assess and manage all threats.

A visibility platform covers your remote sites and maximizes the reach of your security tools by giving you local ability to analyze data of interest and quickly detect anomalous activity. This boosts your security infrastructure ROI, and improves your corporate risk posture.

It enhances network protection of Software-Defined Networks (SDNs) and Data Centers (SDDCs).

Due to increases in their efficiency, scale, and economy, Software-Defined Networks (SDNs) have become the norm within modern data centers, usually controlled from a central location on top of existing hardware and software.

But as SDNs evolve and networks become more interconnected, it becomes much more difficult to see and secure all data as it moves across the organization.

One of the problems is virtual traffic. When you spin up new virtual machines (VMs) and scale out applications, traffic does not actually move through physical ports or switches, preventing traditionally effective monitoring. This creates a safe haven for hackers to hide and propagate their malware.

Another problem is accessing network data in legacy networks themselves: They consist of many different devices made by a variety of manufacturers and running third-party software, not all of which may be up to date. With a visibility platform, your legacy tools become more effective and can inspect new virtualized, overlay technologies with granular visibility and control, even in multi-tenant environments. You gain greater network insight and can filter protocol parameters such as specific VXLAN IDs and forward virtualized traffic to the appropriate application automatically. The end result is consistent access, visibility and security of the network data traversing your physical and virtual environments, which simplifies operations and reduces risk.

Additionally, a visibility platform can generate hi-fidelity NetFlow and metadata that permits both physical and virtual traffic analysis. You can use this information to identify and isolate rogue agents as well as route traffic more efficiently, which reduces both complexity and risk.

This is not an eye chart.

It is a tool to assess the accuracy of your vision. The same way a visibility platform can help you make smarter business decisions.
See what matters.™

REASON 3:

Visibility enhances decision-making.

It gives you greater customer insight.

More data, more devices, and more disparate traffic traversing networks introduces new challenges and opportunities. What do your most valuable customers—and employees and partners, for that matter—need from your network? Where and when do they need it? Can you tell? Monitoring and security tools can only do so much. With a visibility platform, you can see not only what is on your network, but who.

A visibility platform delivers user- or device-aware traffic intelligence, allowing you to optimize services delivery. For service providers and mobile operators, subscriber-aware traffic intelligence allows you to deliver the best Quality of Experience (QoE) across your entire subscriber base.

Plus, a visibility solution that efficiently routes the right traffic to the right tools at the right times can reduce costs across your extended network, boosting ROI even more.

It expands your vision into the cloud.

Cloud solutions can deliver unprecedented economies of scale, agility, and growth potential. But for all these benefits, both private and public clouds can also introduce challenges in managing, securing, and understanding what's happening across your entire business.

Private clouds.

Private clouds are comprised of software-defined clouds(SDCs), combining network, server, and storage virtualizations. All of these components have limited physical presence, rendering traditional monitoring and security tools ineffective. For example, if you're a tenant owner in an OpenStack-powered private cloud, your traffic visibility may be zero.

This means that lateral threat propagation within private clouds is nearly invisible, as IT administrators have a limited view into data traversing this virtualized environment.

A visibility platform gives you the necessary controls to gain insights into all of your virtualized traffic: east-west, north-south, potential bottlenecks, and more. You also gain consistent, centralized visibility and control in multitenant cloud deployments, including VMware.

Public clouds.

With public clouds such as Amazon Web Services (AWS), you gain scalability, agility, economy, and greater bandwidth in a pay-as-you-go model that is appealing to many organizations.

However, visibility into public cloud network traffic is more challenging than in private clouds or on-premise data centers. You may have log data, for example, but this is woefully insufficient for security operations. And with AWS, you don't have access to traffic at the packet level. The end result is limited visibility when you're lifting and shifting workloads to the public cloud and their internal VPCs.

With a visibility platform, you have the same access to public cloud traffic as you do with on-premise. In other words, you have a consistent view across your *entire* network that not only lets you access and monitor mission-critical workloads in a highly secure fashion, but even unblock workloads you may have delayed migrating because you wanted a better view into and understanding of network traffic. This level of visibility provides rich insight into content as well as the data inspection and protection capabilities you have been waiting for.

Ultimately, cloud is where your entire network and business are headed. Visibility across your entire organization is the end goal, giving you the insights you need to make the decisions that will keep you profitable.

This is not an ebook.

It is a tool for making your network a potential profit center.
See what matters.™

We hope you've started to see how pervasive visibility—achieved with a visibility platform—can help you:

- *manage, secure, and understand what's going on across your entire network*
- *cut network complexity and cost*
- *mitigate network risk*
- *and enhance your ability to make better business decisions.*

But what's next? To learn more about how visibility can enhance security, we recommend you also dig into our Security Delivery Platform ebook.

Partners complete the picture.

Gigamon enables data security and management solutions from a host of ecosystem partners.

Here are just a few:

Hewlett Packard Enterprise

paloalto NETWORKS

Symantec.

See what matters.™