

Optimize and Secure your Hybrid Network

Four steps to overcome disruption in the new tomorrow for an agile, secure and scalable network.

Introduction

The world just changed. Disruption is sweeping the global economy and, like every economic disruption, this provides the opportunity for agile, innovative organizations to turn disruption into a competitive advantage. This paper looks at the network and security priorities that organizations need to address today, in the Return to Work transition and in The New Tomorrow.





Overview

+ TODAY

The imperative is to ensure continuity of business operations and the highest possible level of customer and internal user experience while ensuring organization-wide security, and to do so with frozen budgets and resources.

+ RETURN TO WORK

Organizations were forced to transition to Work from Home (WFH) in a matter of days, but the Return to Work (RTW), or more precisely, Return to Office, will be a process that takes place over several months and requires a new, fluid working environment for many workers.

+ THE NEW TOMORROW

Faced with global disruption, uncertainty and challenges, organizations have the opportunity to reimagine their business models and accelerate or launch digital initiatives that will enable them to emerge stronger. They must develop models that cover a number of possible future states and build an agile networks and security infrastructure to support these models.

We would like to share our thoughts on how organizations can best navigate these unprecedented times, based on what we are seeing across our customer base of leading organizations in every industry.

Today

Now that the immediate impact of the Work-from-Home shift has settled and the future is coming into focus, IT is faced with a new set of challenges driven by four business imperatives.

Deliver the Best Possible Customer Experience

Delivering the best possible customer experience is an essential mandate regardless of whether an organization is in healthcare, banking, home shopping, food delivery or any of the myriad services on which home-based consumers now depend.

Providing this level of customer experience will mean some combination of accelerating digital transformation initiatives, redeploying existing applications to more scalable cloud-based architectures or bringing new SaaS-based applications online. Most organizations had these initiatives underway before the present crisis, but many are now looking at how they can accelerate these initiatives or launch new initiatives that reimagine their business built on a new digital platform.

Do More with Less

One of the challenges of delivering the best possible customer experience by accelerating digital transformation initiatives is that most organizations must operate with frozen or reduced budgets and limited resources, whether they were immediately hit by the economic downturn or caught up in the general slowing of the economy.

In response to this, many CIOs are working with their organizations' financial teams to drill into CapEx and OpEx costs and reprioritize these investments to ensure that critical security and digital initiatives can be delivered. In parallel with reprioritizing project spending, IT organizations must also optimize their existing infrastructure, tools and applications to

free up OpEx and resources that could be better spent on higher-impact customer-focused or digital transformation initiatives.

Support the Fluid Workspace

For many organizations across all industry and government sectors, the Work-from-Home model will not only become part of their long-term planning, it will become the basis of a "fluid" workplace that seamlessly merges WFH and office-based working.

This means that capabilities that were put in place to support WFH without detailed planning, such as increased reliance on SaaS-based video conferencing and collaboration applications, now need to be integrated with office-based systems so that workers can transition between these environments without losing productivity.

Secure the New Network

Bad actors moved quickly to exploit the prevailing atmosphere of paranoia and uncertainty in the immediate aftermath of the pandemic and unleashed a wave of phishing, malware and ransomware attacks. These attacks often occurred as many organizations struggled with the Work-from-Home challenge, including VPN capabilities and BYOD laptop, phones and home networks with inadequate endpoint security.

Because these security issues were such a high priority, most organizations responded decisively and increased security spending and resources to address them. However, as organizations move to a fluid workplace model, there will be new challenges that will require InfoSec teams to have full visibility and control over a wider range of devices, users, applications and data than ever before.

Return to Work

Just as the timing of the shift to Work from Home varied from country to county and state to state, so will the Return to Work (RTW) or, more precisely, the Return to Office.

Most organizations are now planning the Return-to-Work process and have formed cross-functional teams, with IT being a key part of those teams and process. But while these plans are being developed, what should IT, NetOps and InfoSec teams focus on? Looking at Gigamon customers, we see that they are focusing on projects that fall into three broad areas.

Plan the Return to Work

Many organizations are planning a future in which significant number of their employees will continue to work from home, either on a permanent basis or for an extended period of time as part of a mixed onsite/offsite model that is now being described as “the fluid workplace.”

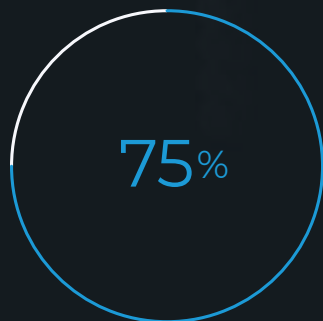
A survey by 451 Group taken in March¹ suggested that 38 percent of survey respondents expected this to become the new normal for their organization; however, a poll taken during a recent Gigamon healthcare webinar² suggested this could be as high as 75 percent. Moreover, many organizations are reporting that home-based employees are actually more productive than office-based workers, contrary to many people’s expectations.

This productivity is largely achieved through the effective use of easy-to-use, secure and scalable SaaS-based applications, such as video conferencing and collaboration, that leverage high-bandwidth internet and cellular networks and are quickly replacing older desktop-based applications. IT organizations must ensure that they can secure and support this fluid workplace and provide a seamless experience for employees in both WFH and office environments.

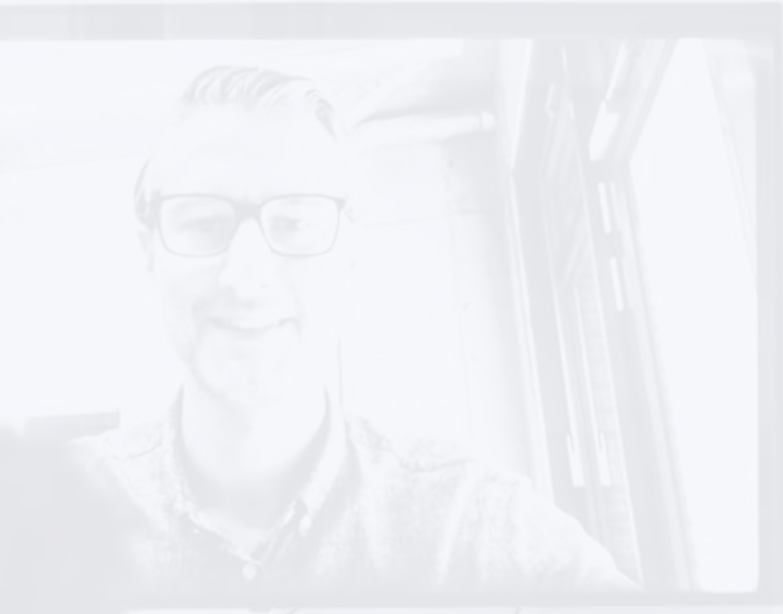
Use the Cloud to Accelerate Digital Transformation

Digital transformation initiatives are inherently cloud-based because the cloud enables the fastest deployment of new applications and digital services. However, in order to deliver the richest functionality and customer experience, these cloud-based apps often span physical, virtual, cloud and multi-cloud networks.

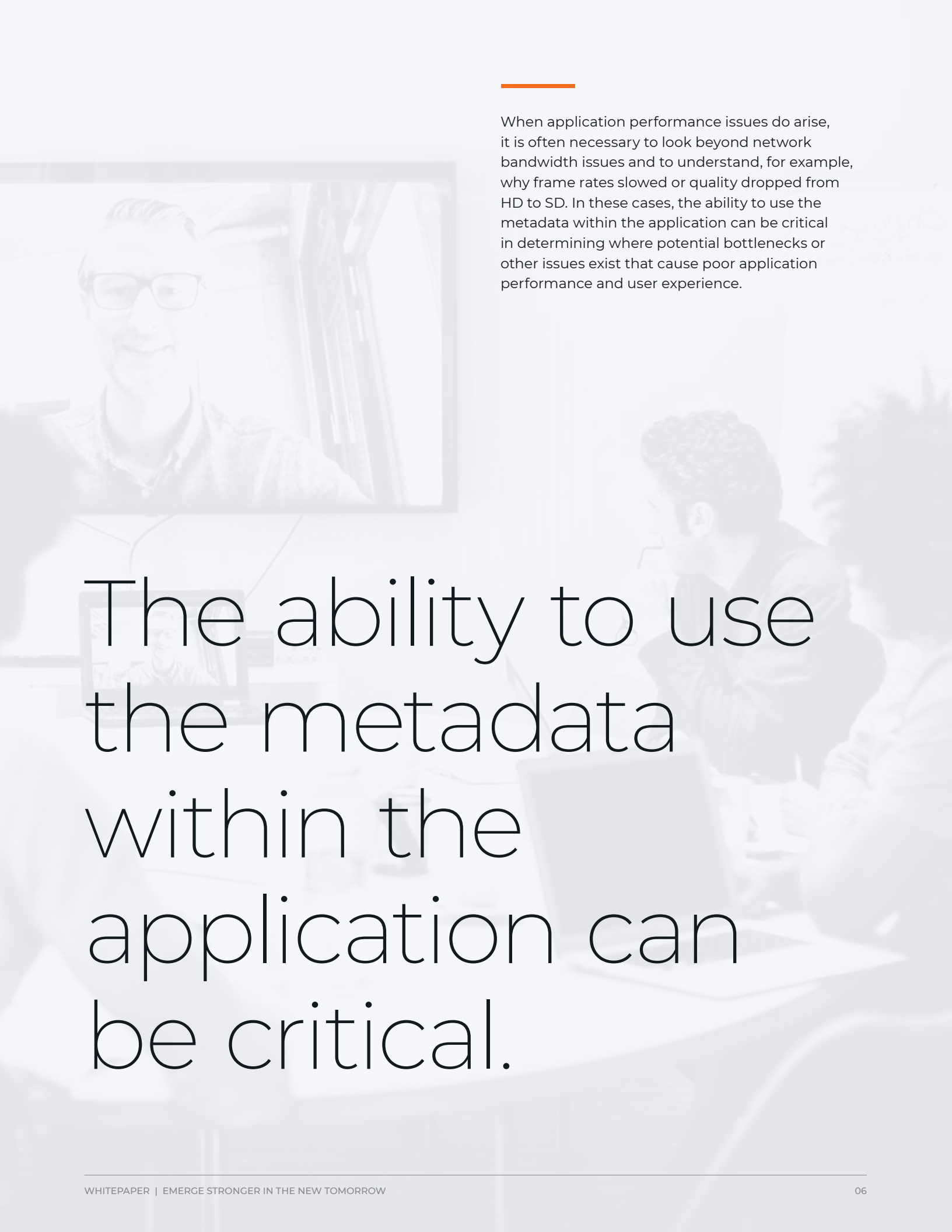
These initiatives may be based on SaaS-based applications or they may be based on custom applications designed by internal IT organizations and deployed on cloud- and container-based platforms for rapid scalability. To achieve this, there must be visibility into all data — both encrypted and unencrypted — as it traverses the distributed tiers of the application, including inter-container communications.



A poll taken during a recent Gigamon healthcare webinar suggests that 75 percent of survey respondents expect WFH to be the new normal.



When application performance issues do arise, it is often necessary to look beyond network bandwidth issues and to understand, for example, why frame rates slowed or quality dropped from HD to SD. In these cases, the ability to use the metadata within the application can be critical in determining where potential bottlenecks or other issues exist that cause poor application performance and user experience.



The ability to use the metadata within the application can be critical.

Reevaluate Security

Now is the ideal time for InfoSec teams to evaluate the lessons learned in responding to this crisis and to apply these to a review of their existing security models, procedures and tools. These models were likely under stress even before the COVID-19 crisis as a result of:

- + Understaffed InfoSec and SecOps teams³
- + Rapid growth in encrypted North-South and East-West traffic
- + Massive growth in traffic and attack surface often as a result of OT and IoT adoption

These issues have now been compounded by the additional stress that the crisis has placed upon security staff, tools and budgets.

While the exact security model will vary by organization, key building blocks for a successful, agile model are ensuring end-to-end visibility into all network traffic; AI and ML-based analytic tools that detect and prioritize anomalies and threats; and automation tools that handle mundane tasks, freeing security teams to focus on the highest priority issues.

For some organizations, this security review may include an evaluation of adopting a Zero Trust model. In a world where the fluid workplace model is the new normal, moving toward a Zero Trust architecture not only makes sense, it is close to an imperative. At the simplest level, because the network is under constant attack from a huge array of external and internal threats, all users, devices, applications and resources must be treated as being hostile. These users and devices need to be rigorously authenticated, and data and other network assets need to be protected at a much more granular level than perimeter-based security models allow.

Optimize Bandwidth

The combination of supporting the Return to Work while driving digital transformation and ensuring enterprise-wide security means that all organizations need to maximize network bandwidth and network traffic visibility. Increasing network bandwidth can be achieved either by upgrading or replacing the existing network infrastructure or by optimizing existing bandwidth. Often optimizing existing bandwidth is a short-term measure that organizations need to take while they plan a network upgrade in the medium term.

Fundamental to optimizing network bandwidth is understanding what applications and traffic are running on the present network and how this is likely to grow in the future. To achieve this, visibility is needed into all of the users and applications on the network, whether it is in the data center, in remote or WFH environments, or in the cloud. Once this visibility has been gained, it is possible to understand the network traffic that they generate and consume.

In the short term, this understanding enables traffic to be optimized using techniques such as de-duplication, filtering, slicing and use of metadata. This same process will provide a solid basis for planning the capacity that will be needed to meet the organization's future networking needs. Projecting network capacity for tomorrow's networks is not an easy task, but having detailed visibility into today's hybrid network traffic is an essential first step.



Moving toward a Zero Trust architecture not only makes sense, it is close to an imperative.

The New Tomorrow

Every economic disruption provides the opportunity for agile, innovative organizations to turn that very disruption into a competitive advantage. Today, this means using digital technologies to transform the way that organizations interact and transact business with their customers more quickly, conveniently and cost-effectively than their competitors.

Most organizations had digital transformation initiatives underway before the present crisis, but those organizations who emerge strongest from this situation will be those that double down on these initiatives, or even start over by reimagining their business built on a new digital platform. One of the challenges in doing this today is that many organizations must operate with frozen budgets and limited resources.



VISIBILITY

As recent events have shown, agility doesn't just mean handling the pressures of growth and innovation; it also means handling unforeseen and unprecedented change. In this situation, it is critical that organizations' networks and security capabilities can support continued changes in working practices and new tools deployment.



AGILITY

You can't manage what you can't see, and gaining visibility into all network traffic will become a survival issue for many organizations. The physical, virtual and cloud-based visibility into both encrypted and unencrypted data that Gigamon provides is already trusted by many of the world's most demanding organizations, including leading global banks, healthcare, service providers, SaaS companies and government agencies.



GROWTH

Organizations that display and operationalize these characteristics of agility, visibility and innovation will emerge stronger from the present situation and will be poised for rapid organic and acquisition-based growth. To achieve this, they will need agile, scalable networks and tools like the Gigamon Visibility and Analytics Fabric™ that provide full visibility in the applications, users and data spread across physical, virtual, cloud and multi-cloud networks.



CLOUD

Most IT organizations in the world of The New Tomorrow are facing budget uncertainty. More than ever, being agile and running lean is critical not just for legacy systems but also for new cloud operations. Gigamon allows IT to get more out of existing investments, thereby generating additional discretionary budget within the current fiscal year. For example, by removing duplicate traffic, filtering out low-risk application traffic and allowing teams to redeploy shelved tools, Gigamon immediately increases monitoring and security tools' capacities by up to 70 percent.



Final Thoughts

The COVID-19 crisis has set off a chain reaction of events that will profoundly affect our society and economy. Organizations and their IT teams have responded successfully to the initial shock of the crisis, but the hardest challenges — and greatest opportunities — lie ahead. To survive those challenges and take advantage of those opportunities, organizations will need resilience, agility and visibility into every aspect of their operations. Gigamon is uniquely positioned to help our customers overcome these challenges and take advantage of this by accelerating their digital journey while allowing them to do more with less.

¹ Scott Crawford, Dan Kennedy, Fernando Montenegro, Eric Hanselman, Garrett Bekker and Aaron Sherrill. "COVID-19 and Beyond: Will the Work-From-Home Explosion Revolutionize Enterprise Security Architecture?" April 2, 2020. 451 Research. <https://go.451research.com/2020-mi-covid-19-will-work-form-home-revolutionize-enterprise-security-architecture.html>.

² Poll taken during a HIMSS Gigamon webinar on April 22, 2020.

³ "2020 Cyberthreat Defense Report." March 2020. CyberEdge Group. <https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf>.

About Gigamon

Gigamon provides network visibility and analytics on all traffic across your physical, virtual and cloud networks to solve critical security, performance and business continuity needs. The Gigamon Visibility and Analytics Fabric delivers optimized network and security performance, simplified management and accelerated troubleshooting while increasing your tools' return on investment. Our comprehensive solutions accelerate your organizations' ability to detect and respond to security threats, including those hidden in encrypted traffic. Trusted by 83 percent of the Fortune 100 and 4,000 organizations worldwide, Gigamon ensures that your business can run fast and stay secure in The New Tomorrow.

©2017-2020 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.

Gigamon[®]

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