

When Networks Meet The New Tomorrow

**A Work-from-Home Model, Borderless Security
and Shrinking Budgets. Here's How to Cope.**



Introduction

The world just changed. Within a short period of time, unforeseen global events have led to vast changes in our working and everyday lives.

In the context of network operations and information security, this means supporting a newly distributed workforce and digital processes with a shrinking budget. Most organizations' networking infrastructure and tools were designed to support a predominantly office-based workforce. Overnight, IT has had to retool to support a remote workforce that is two to three times larger than was ever planned. On top of that, security needs to be maintained as network traffic has turned from the inside, out. Rapid network and tool modifications are raising new security, resilience and performance concerns. Similarly, the applications we depend on, whether custom, packaged or web-based, are all being pushed to previously untested limits.





Overview

This paper looks at IT priorities that organizations will need to address now and in the new tomorrow:

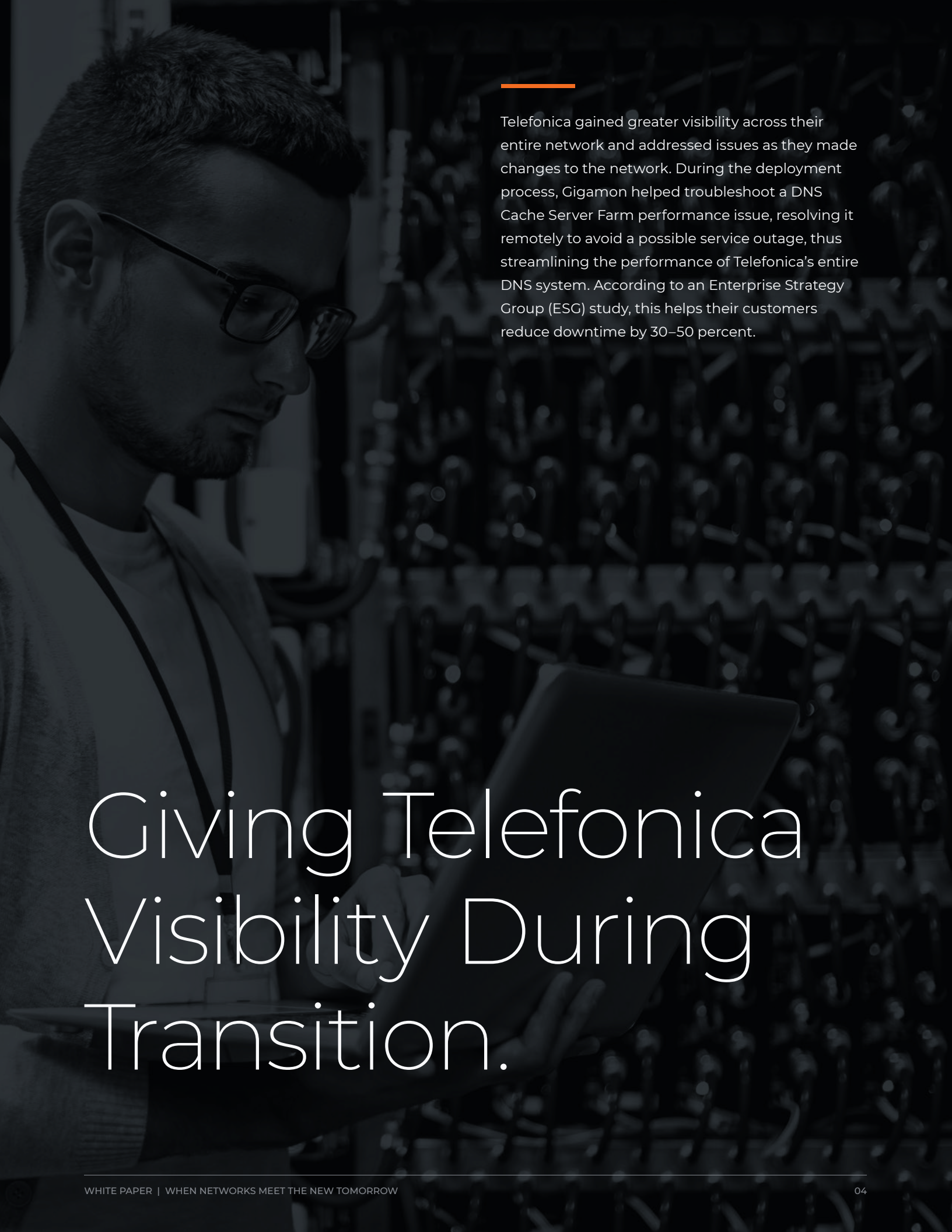
+ TODAY

The imperative is to ensure security and continuity of operations in this new inside out environment while redeploying network resources to maintain the highest level of customer and internal user experience

+ THE NEW TOMORROW

Faced with uncertainty at all levels from capital markets, supply chains, government policy and consumer sentiment, organizations need the agility to respond quickly and cost-efficiently to new and unforeseen challenges and opportunities

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

A man with glasses and a beard is looking at a tablet in a server room. The background is filled with server racks. The image is in grayscale with a dark overlay.

Telefonica gained greater visibility across their entire network and addressed issues as they made changes to the network. During the deployment process, Gigamon helped troubleshoot a DNS Cache Server Farm performance issue, resolving it remotely to avoid a possible service outage, thus streamlining the performance of Telefonica's entire DNS system. According to an Enterprise Strategy Group (ESG) study, this helps their customers reduce downtime by 30–50 percent.

Giving Telefonica Visibility During Transition.

Today

IT is being asked to deploy additional capacity and services faster than ever before, but also to balance this new capacity with three critical requirements:

A New Work-from-Home Model

Certain aspects of infrastructure and applications are facing scaling challenges, perhaps at unprecedented levels. The sudden and rapid shift to working from home (WFH) has left IT teams with little time to scale their remote access infrastructure for employees. As they scramble to bring remote working capacity online quickly, by repurposing older or existing infrastructure, issues such as failures and bottlenecks can arise in the new network segments and infrastructure. Detecting these issues in a timely manner is critical. But with already stretched resources, these issues becomes a truly significant challenge.

In addition to supporting internal users, IT is faced with an upsurge in usage of external apps. Customers are now engaging with companies mostly through mobile applications or online.

Our clients in the financial services, healthcare, entertainment and retail industries are seeing a significant increase in the number of users and frequency of use for their consumer apps. As new application containers, microservices and virtual machines are being stood up rapidly to meet sudden growth in user demand, IT and infrastructure teams risk being left behind by fast-working DevOps and applications teams. This mismatch in alignment can have serious consequences. While application capacity may ramp up, infrastructure capacity may lag and network bandwidth issues, reduced user experience, and application and data access or usage may not be monitored adequately for threats.

Borderless Security, Beyond the Network

Any additional network user activity in new network segments can become a source for threats, such as data leakage or ransomware. Bad actors are quickly exploiting the prevailing paranoia and uncertainty in an effort to compromise users' systems. These threats use droppers, which are then used to download additional malware on user's systems to compromise credentials, ultimately leading to ransomware attacks, and potential data exfiltration. (See examples [here](#)¹ and [here](#)².)

Compounding the inside out challenge is that remote workers use their home network and/or personal devices for work. And it's not certain that every worker is following recommended security protocols. Even the mandated use of VPNs may not solve the problem, especially if endpoints have not been recently patched. As an example, vulnerabilities are being found and reported in various VPN and firewall manufacturers, which allow [Mirai botnet-type variants to take control](#)³. In an effort to ramp up capacity, enterprises need to make sure that if they are using older gear, these are fit for purpose and can be patched and secured.

Working with Reduced Budgets

As many sectors of the economy start to slow down, organizations are already planning for a potential recession. Travel, entertainment and service industries are all being severely impacted. The trickle effect of this on the broader economy is something that organizations are planning for in the form of budgets cuts, hiring freezes and spending constraints. IT and applications teams are particularly feeling the impact as they are being asked to scale up without scaling their resources — the need to do more with less has never been more pressing.

¹ <https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#37bf4a0a75fd>

² <https://www.businessinsider.com/hackers-are-using-fake-coronavirus-maps-to-give-people-malware-2020-3>

³ <https://krebsonsecurity.com/2020/03/zxyel-flaw-powers-new-mirai-iot-botnet-strain/>

The New Tomorrow

Stay Focused While Assessing Your Options

As the economy absorbs the shock of recent weeks, many organizations are already planning for a potential recession. Global supply chains were initially disrupted in Asia and these effects are now compounded and amplified by the dramatic changes in the European and U.S. economies. These changes deeply impact travel, hospitality, retail, entertainment and service industries. And, for those not directly affected by forced closures, the trickle effect of closures on the broader economy is causing almost all IT organizations to review spending priorities and budgets.


As business and IT organizations assess their priorities, they are faced with uncertainty: How long will the crisis last? What additional network bandwidth, applications and services will need to be added? How should they cope with both the challenges and in some cases, the opportunities of this crisis? Will work-from-home become a permanent model for their organizations?

One approach to addressing many of these challenges is to leverage network information-in-motion for application, user and device discovery, troubleshooting, application performance, user experience monitoring, and security.

Network data is the single source of truth about the performance and security of your network. If this data is reliable and up to date, teams will not have to keep changing log levels on servers, reminding application developers to instrument applications or adding new applications for monitoring.

To ensure that this data is reliable enough to be classified as a single source of truth, it is imperative that it includes information-in-motion from physical, cloud and virtual environments, systems of record, log files and other data sources. A best practice is to use a wire once model, where all information-in-motion becomes immediately available to security and performance-monitoring tools as new network segments are brought online. Getting access to network data should be done quickly, with minimal intervention and little to no reliance on applications, DevOps and other teams.



A person wearing a dark hoodie and a jacket is crouching in a starting position. A smartphone is attached to their left arm. The background is dark and out of focus.

Under Armour needed complete visibility into the performance and security of their digital applications. This reliability was key to delivering on their customer expectations of user experience and trust. According to an ESG report, Gigamon enabled a 75 percent greater visibility of network traffic.

“Having complete visibility into the performance and security of our digital applications is key to delivering on the expectations of user experience and the trust our customers demand.”

Helping Under Armour Protect Their Customers.

Stay Focused While Assessing Your Options

While the outcome of today's crisis remains unknown, here are our recommendations for how you can prepare your organization to succeed.

APPLICATION USER EXPERIENCE.

More than ever, it is apparent that digital applications are critical to organizations, and the need to ensure that they delivering the best possible customer and user experience has never been more important.

To achieve this, it is important to use tools that not only monitor and visualize application usage and user experience, but also are able to take action based on the performance and behavior of these applications.

For example, surges in video conferencing traffic due to the intensive use of applications like Cisco WebEx, GoToMeeting, Skype and Zoom can very quickly overwhelm out-of-band security tools such as intrusion detection. IT teams must be able to quickly visualize which applications are causing these traffic surges, decide whether to analyze this traffic and at what depth, and then filter out safe or low-risk traffic to preserve bandwidth for other applications.

BORDERLESS NETWORK SECURITY.

Against a backdrop of ever more frequent and sophisticated cyber-attacks, the COVID-19 pandemic has unleashed a new wave of bad actors seeking to take advantage of stretched InfoSec teams and users seeking information about the virus both at a global and local level. As such, having the right security tools and rich network data has never been more important.

Examples of the types of tools that can provide both short- and long-term assistance include:

+ THREAT DETECTION AND RESPONSE

With attack surfaces and vulnerabilities increasing as a result of the shift to WFH, on rapidly expanded VPN architectures, it is imperative that organizations have powerful tools to detect and respond to these new threats. For example, pointing tools at ingress/egress links and behind VPN concentrators provides a targeted approach to mitigating potential risks.

+ CENTRALIZED TRAFFIC DECRYPTION

While many tools can decrypt encrypted traffic, deploying a centralized solution to decrypt and inspect encrypted traffic is often the most efficient solution for many organizations. Centralizing TLS decryption capabilities allows traffic to be decrypted and inspected once before being re-encrypted and shared across multiple tools. The ability to look into encrypted traffic to and from applications can be important to realizing whether application and data access is legitimate or illegitimate. As application capacity is dynamically increased, applications are being quickly rearchitected and new applications are being spun up.

+ USE METADATA TO DRIVE SIEM EFFICIENCY

Where organizations are using solutions like Splunk or other SIEMs for active security monitoring, feeding both system and application metadata to these can be a powerful way to help ensure compliance while bringing new applications and capacity online. Organizations should strive to ensure that only precise and relevant metadata is sent to these tools in order to maximize the context being provided to them while minimizing the amount of data being sent to them. This is particularly important with SIEM tools where the billing model is based on the volume of data processed or stored.



+ ZERO TRUST

Many organizations were already in the learning, planning or implementation stages of a Zero Trust initiative. This crisis may prove to be the tipping point in accelerating these initiatives. The basic tenets of Zero Trust are to eliminate implicit trust associated with locality of access and to move an organization's defensive perimeter from the edge of the network to assets using the network, i.e., users, devices, data and applications.

In a world where a workforce, as a result of the COVID-19 crisis or planned changes in the business model, is shifting towards a "work anywhere, work anytime" model, moving towards a Zero Trust architecture simply makes sense. Visibility into all information-in-motion on the network is critical to supporting a comprehensive Zero Trust solution.

As is often said, Zero Trust is a journey that requires significant thought to ensure successful execution. Many organizations have been delayed in planning or starting this journey. But with the reimagining being forced upon us by the COVID-19 pandemic, the need to streamline and unify the security infrastructure has never been as urgent as it is now.

COST SAVINGS BY TOOL INVESTMENT OPTIMIZATION.

Most organizations have made significant investments in the network and security tools they use to manage and safeguard their networks and applications. As traffic shifts from LAN to WAN, it is critical that the data flow to these tools doesn't cause tool overload, visibility blind spots or other issues from the increased traffic.

In order to maximize the efficiency – and ROI – of an organization's tools, it is essential that network traffic from physical, virtual and cloud environments is optimized before it is delivered these your tools. Failure to do this can result in tools overload, teams having to manually intervene in otherwise automated processes and network availability, reliability and security issues.

The U.S. Department of Health and Human Services (HHS) upgraded their network to 10GBps, but many of their security tools had 1Gbps network interfaces. With Gigamon, the older tools were able to operate on traffic from the faster network. According to an ESG study, Gigamon provides the ability to right-size hardware and tooling for a savings of 40–50 percent.

Finding Speed and Savings for the U.S. Department of Health and Human Services.

Final Thoughts

The series of current global events has changed our reality overnight. NetOps and InfoSec teams have to manage a massive disruption as users work from home and prepare for an uncertain future. In this situation, visibility and infrastructure agility have become key success factors in an organization's ability to respond to these challenges.



About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all information-in-motion, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation.

Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including over 80 of the Fortune 100.

For the full story on how Gigamon can help you, please visit www.gigamon.com.

We invite you to join our online community and, specifically, our [Working from Home Collaboration Group](#), where you can share your concerns, thoughts and ideas with your industry peers and with Gigamon experts.

©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