Publication date:
November 2020
Author:
Jeff Wilson

The Power of Integrating Security and Networking in Service Provider Networks

APAC Edition

Brought to you by Informa Tech

Contents

Introduction

Massive increases in traffic for business and consumer applications are forcing service providers around the Asia/Pacific region to rethink how they architect networks and deploy security for them at scale. Traffic growth is easy to observe but measuring growth in terms of threats can be difficult; 68% of the respondents in this study said they have seen a moderate to significant growth in the volume of threats in the last year, and 78% expect a moderate to significant increase in the next year.

The COVID-19 pandemic in 2020 has only accelerated traffic growth and put a strain on both network and security capacity as countries around Asia/Pacific take mitigation measures to slow the spread of the virus. Technology providers in networking and security have long looked for ways to create meaningful integrations in networking and security in order to improve both scale and efficacy, and service providers around the globe are starting to look seriously at integrated solutions as a way forward.

In August 2020 Omdia surveyed 77 purchase decision makers and practitioners at Tier 1 and 2 service providers is Asia/Pacific to understand their real networking and security challenges, and to ask about their plans to integrate networking and security at both technology and organizational levels, and we present the highlights of those surveys here.

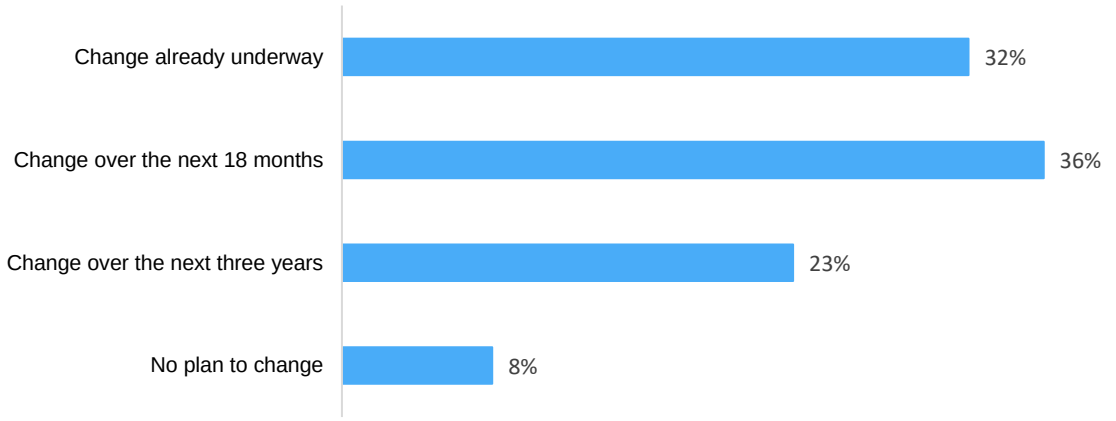
Dynamic networks drive integration of networking and security

The single key takeaway from the survey is that integration of networking and security is a critical goal for large service providers, and most of those providers are in various stages of integrating in three key areas:

- Technology: Looking at meaningful integrations of routing or switching with security in the core, at the edge, and in the data center
- IT organization: Looking to merge or increase communication between networking and security operations
- Technology suppliers: Looking for vendors that can deliver pre-integrated solutions.

These integrations all serve one primary goal: to deploy effective security at scale. Providers are in the middle of massive changes in how networks are built, such as shifting to edge networking and deploying virtual or cloud-enabled networking elements, and this impacts all areas of infrastructure. We asked respondents if these changes were impacting security architecture, and the answer was a resounding yes: 68% already have changes under way or will make changes within the next 18 months. Only 8% said they had no plan to change, and in some cases that was because they are ahead of the curve and have already rearchitected security, as shown in Figure 1.

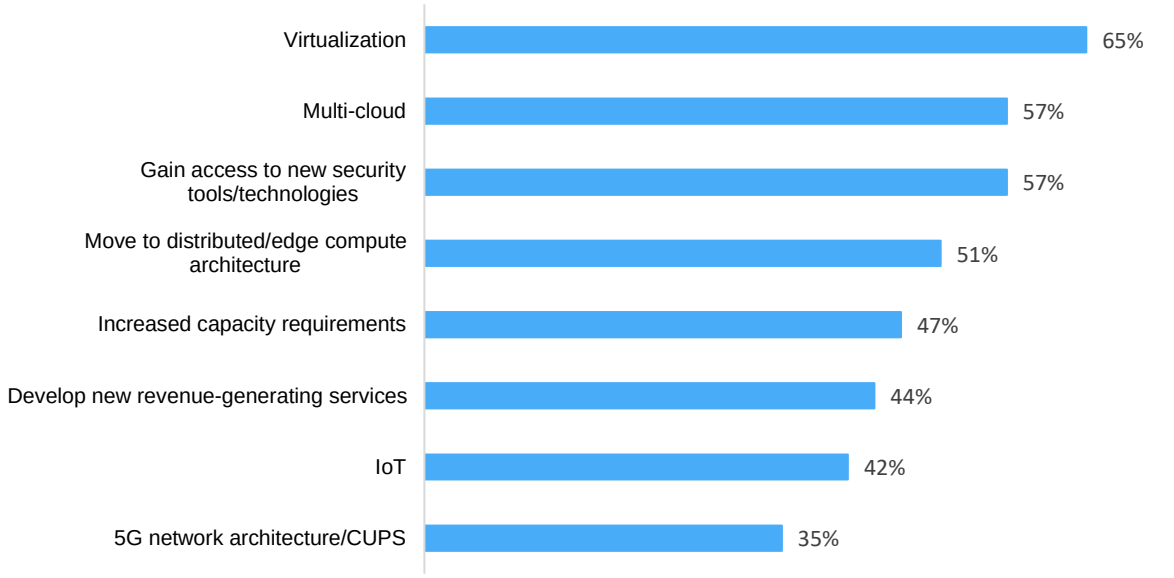
Figure 1: Timeline for evolving infrastructure



Source: Omdia

As a follow-up, we asked respondents what exactly is driving this change – virtualization (65%), multi-cloud (57%), gaining access to new security tools/technologies (57%), and the move to distributed/edge architecture (51%) top the list. Three of the top four are obvious architectural drivers but gaining access to new tools is an attempt to increase security efficacy, especially in cases where security needs to move into virtualized or cloud infrastructure. There are a host of new security challenges in virtual and cloud environments (and distributed service edge, which is often virtual as well) that in many cases cannot be addressed with existing security tools and architecture. Security architecture is a critical issue, and as networks go virtual, security must follow, as shown in Figure 2.

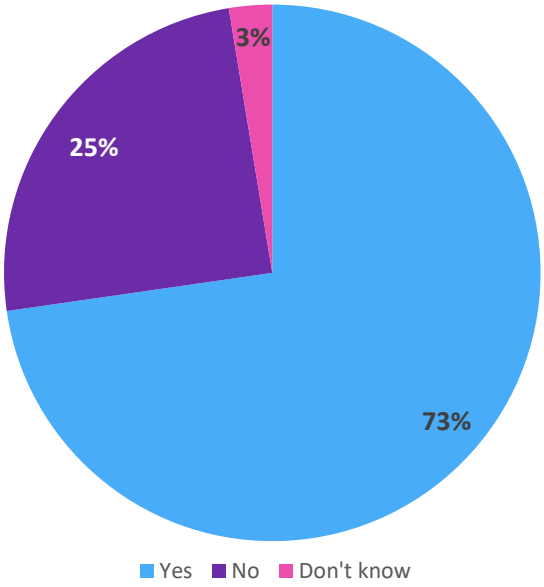
Figure 2: Drivers for evolving infrastructure



Source: Omdia

Another obvious and significant issue is overall security capacity. Tier 1 and 2 providers move mountains of customer and consumer traffic and are subject to a wide range of regulations and oversight. The move to distributed edge networks is both a response to historical traffic growth and an attempt to improve performance and make future growth more manageable. Omdia asked respondents if they are increasing security capacity in response to traffic and architecture and 73% said yes, as shown in Figure 3.

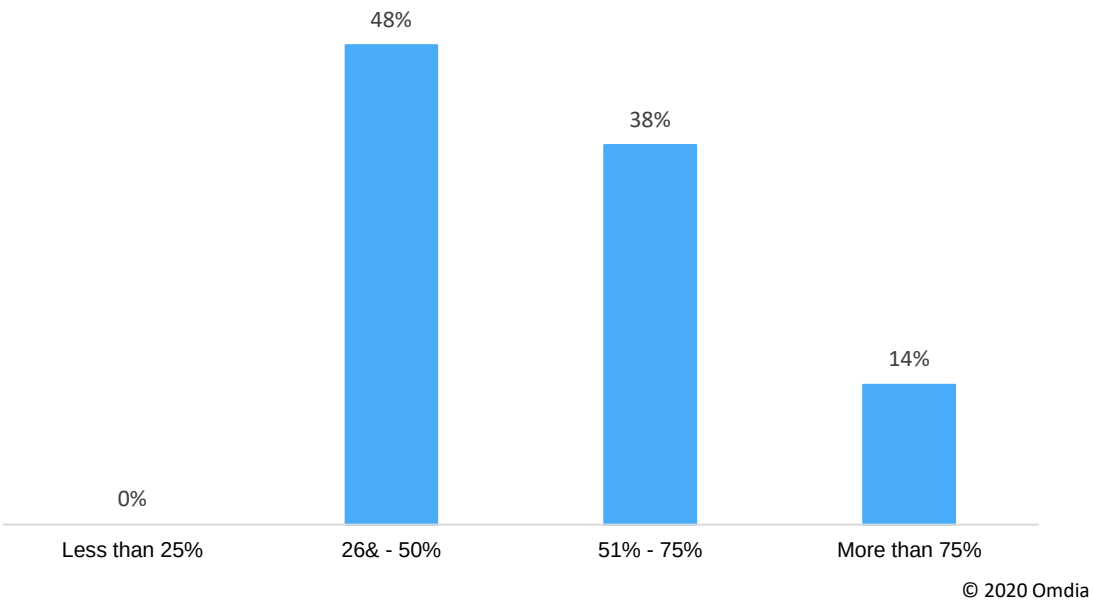
Figure 3: Plans to increase security capacity



Source: Omdia

We followed up by asking how much they planned to increase overall security capacity in the next year and the answer was significant: 52% of respondents plan to increase capacity by 50% or more, and 10% (not shown in the chart) essentially plan to double capacity.

Figure 4: Projected security capacity increase



Source: Omdia

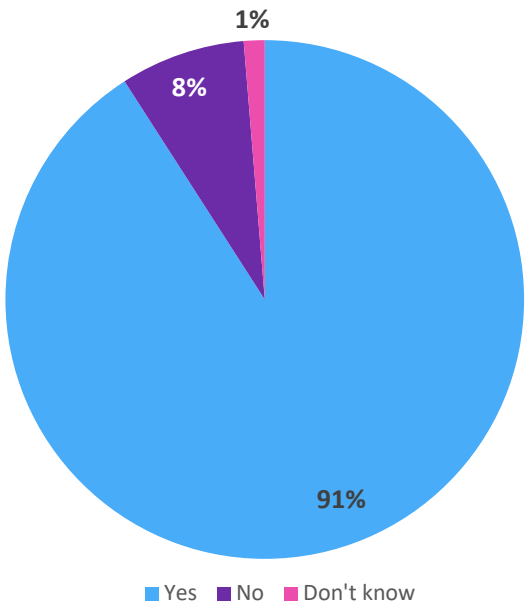
We also asked how security budgets are changing in this same time frame; only 10% of respondents are expecting a significant increase (over 10%) in their budget for security technology, and most are dealing with a flat to slightly increasing (less than 10%) budget. How can they possibly achieve these capacity increases under current capex and opex constraints that have only become tighter as a result of the pandemic?

The technology integration imperative

One obvious way to scale security capacity and functionality while decreasing investments in new hardware is to look for solutions where networking and security work together and are tightly integrated. Switches and routers can use high-speed hardware functionality to stop attacks detected by specialized external threat detection software engines at wire speed without having to deploy a separate layer of security hardware. Solutions like this can quickly stop distributed denial-of-service (DDoS) attacks and/or east-west attacks in data centers. Threat intelligence feeds can be connected directly to switches and routers so they can drop or re-route attack traffic. Cloud-native security solutions that integrate with cloud networking and orchestration platforms can add a new layer of security in cloud environments (data center or edge) and help reduce the cost of threat mitigation significantly by eliminating the need for redundant hardware, while still running at the speed or scale that large providers require.

Omdia asked respondents if they viewed these types of integration as inevitable in their networks, and the answer was overwhelmingly yes – 91% of respondents assume that they will leverage integrated networking or security solutions as shown in Figure 5.

Figure 5: Integrating networking and security

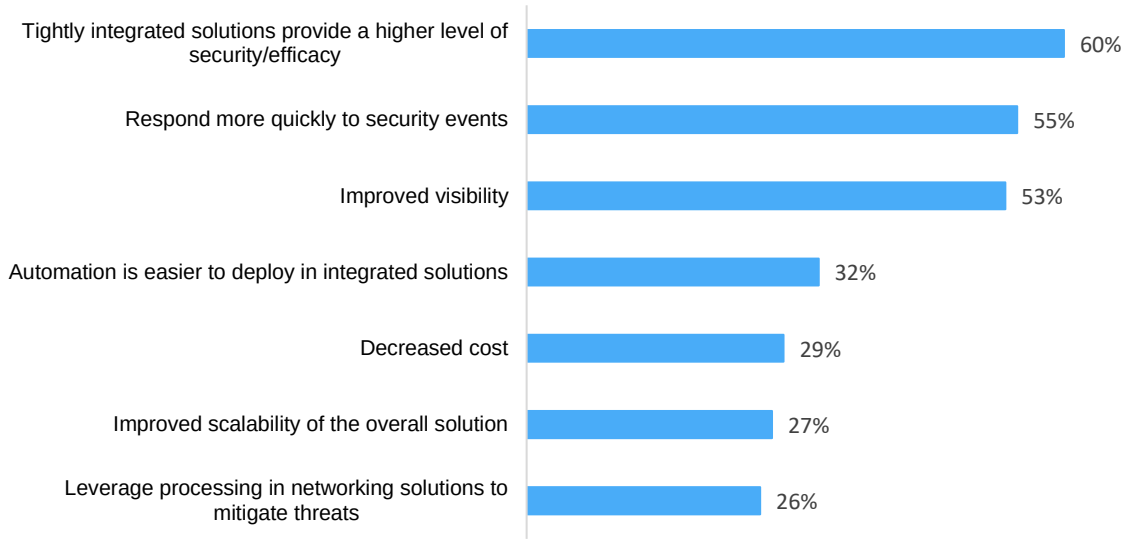


Source: Omdia

As a follow-on, we asked how important it was that networking devices directly participate in the mitigation of security events. This is the key advantage of integration; networking devices have the kind of high-speed hardware required to mitigate key threats; however, they lack the intelligence to do so. Seventy-four percent of respondents answered that it was either very important or imperative. The 29% that said it was "imperative" won't invest in new networking solutions that don't have security integrations.

The answer is clear but we wanted to understand the reasoning behind the answer, so we asked about the top benefits of investing in integrated solutions. The top three in the chart are focused mainly on security efficacy, not scale or performance, as shown in Figure 6. For many of these respondents the cost and scale benefits are fine, but the increased efficacy and visibility that integrated solutions enable is the real gem. This is a progressive point of view that recognizes the long-term value of security solutions; moving to these integrated solutions is not just a short-term stopgap for dealing with immediate scale and cost issues.

Figure 6: Benefits of integrated networking and security



Source: Omdia

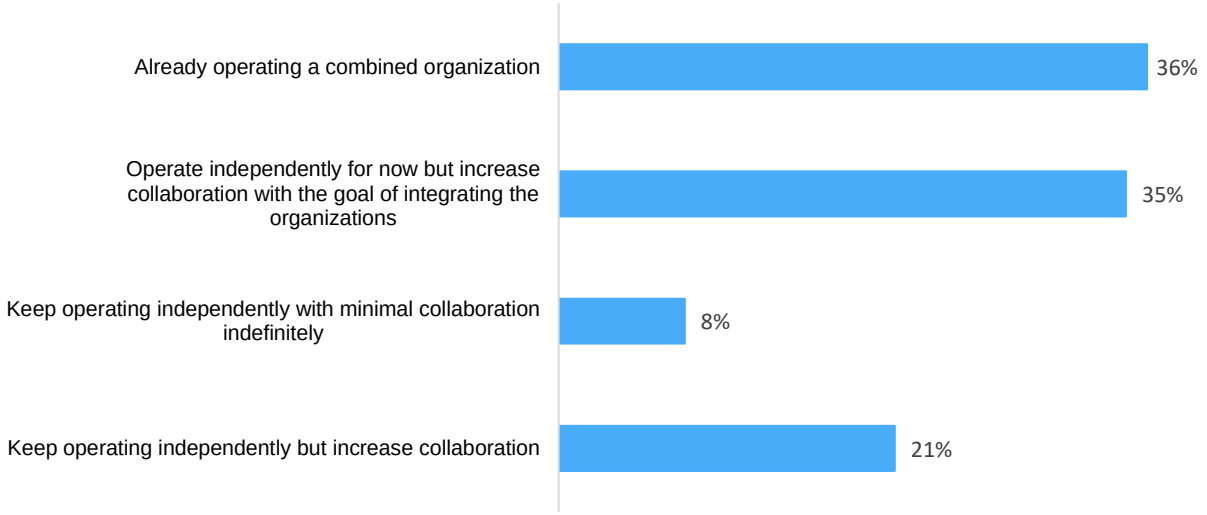
Enabling simpler automation falls in the middle of the list; automating network and service provisioning is a key part of the rollout of any new networks that service providers are currently working on, and anything that enables simplified automation of security rollout will be well received. Deploying automation solutions that work with both networking and security requires a new level of coordination between these two factions within the IT organizations of large service providers that have been separate historically.

Technology integration drives organizational integration

If networking and security are to be meaningfully integrated in the edge, core, and data centers, then it is likely that service providers will have to revisit how their teams operate and integrate. To understand the current structure of their IT organizations, Omdia asked respondents to give some insight into the current level of integration.

Thirty-six percent of respondents reported that security and networking are already operating as a single team, and 35% are separate but working toward complete integration. Many organizations have been moving in this direction for years, and the promise of integrated solutions is accelerating internal team integration, as shown in Figure 7.

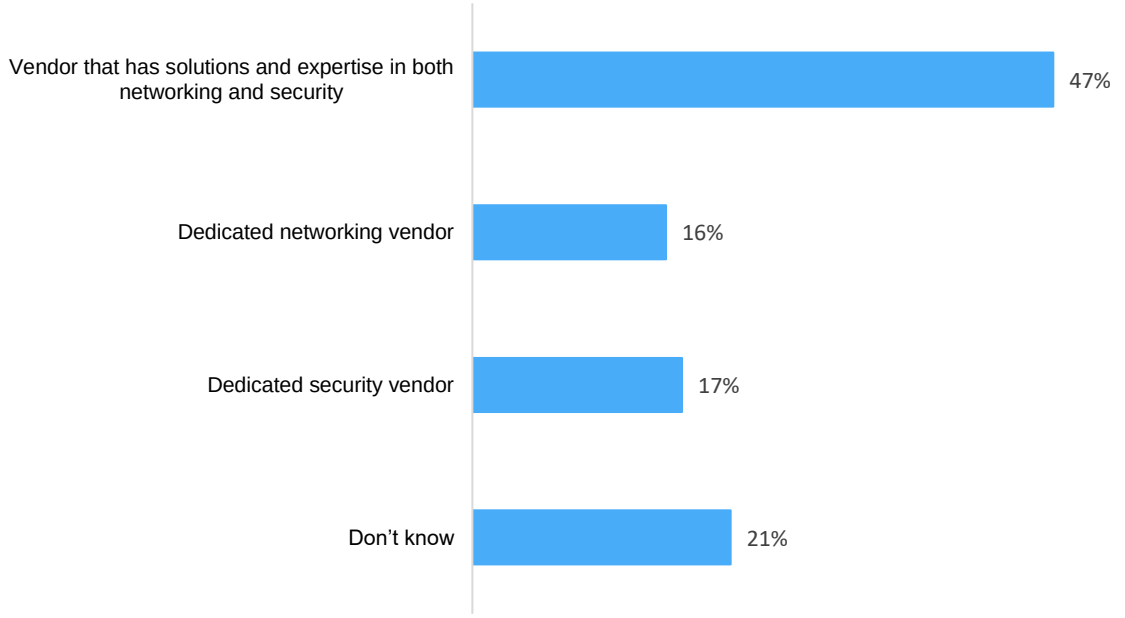
Figure 7: Drivers for integrating networking and security teams



Source: Omdia

As service provider IT organizations and the technology they deploy move to integration of networking and security functions, they are likely to prioritize working with technology suppliers that also have solutions expertise in both security and networking. There are multi-vendor solutions, but 43% of our respondents are looking for a single vendor with integrated solutions, as shown in Figure 8. Over time, as respondents gain more experience purchasing and deploying integrated solutions, more of them are likely to look for vendors with strong expertise and product offerings in both.

Figure 8: Preferred vendor type for integrated solutions



Source: Omdia

Conclusion

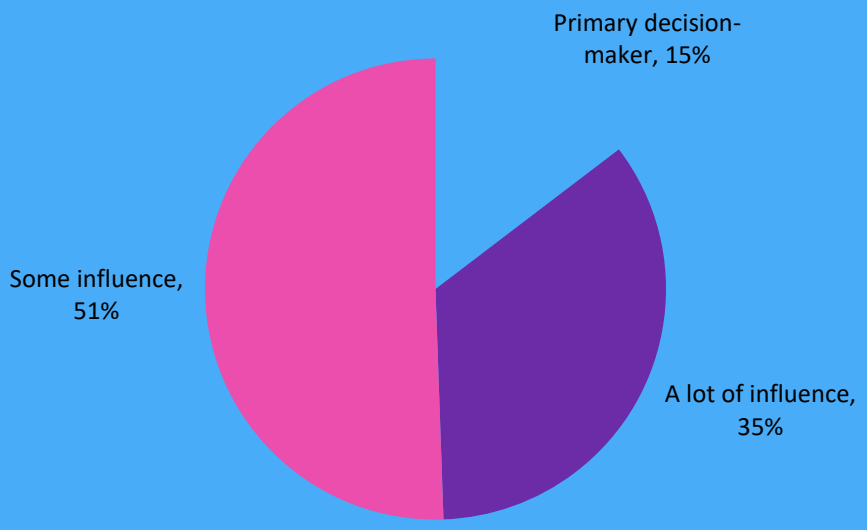
Tier 1 and 2 service providers in Asia/Pacific have seen record-high traffic driven by the COVID-19 pandemic while they have been in the middle of transforming their networks. This network transformation and the move to virtualized security and networking elements is only generating further threats and more potential security gaps in both their networks and security infrastructure. Based on the results of this survey, many are looking to technology solutions that integrate security and networking with a short-term benefit of helping them meet the scale and cost challenges they are currently facing, but also with the longer-term benefit of enabling more effective automated security and networking for their entire network: in the core, in the data center, and at the edge.

Appendix

Methodology

Using a panel of qualified networking and security decision makers, Omdia conducted a web survey in August 2020 with 77 Tier 1 and 2 communications service providers with a minimum of $50m in revenue. All respondents were from Asia/Pacific from countries representing the vast majority of population and service provider infrastructure in the region. To qualify, respondents needed to be responsible for managing or planning security deployments at their organizations. They also needed to have detailed knowledge of, and purchase decision influence over, their organizations' network security solutions. This was a key part of the screening process to ensure that we received responses from the knowledgeable decision makers that influence the buying process.

Respondents had to have at least manager-level positions in security or networking, with 64% of respondents having director (or higher) titles; 31% of respondents had architect or C-level titles. Respondents were given no incentives for completing the survey.



Source: Omdia

Author

Jeff Wilson
Chief Analyst, Cybersecurity Technology
askananalyst@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer