Point of View

Better together

Six reasons to keep the procurement of network and security services together.

verizon business

Network + security

The business and technical benefits of procuring and managing them as one.

David Bailey
Global Solutions Executive

David has over 20 years of experience working with large global enterprises and public sector organisations to define and meet their infrastructure and security needs. This has included wired and wireless networks for Internet of Things (IoT) applications and agile, intelligent infrastructure to support demanding applications like artificial intelligence (AI).

As cyberthreats continue to evolve and network infrastructures become more complex, organisations must adapt by breaking down silos and fostering greater integration between cybersecurity and networking. By doing so, they can build more resilient, secure, and efficient systems that support their business objectives and protect their critical assets. This need has been given fresh impetus by the rapid growth of AI workloads and the huge volume of data that they require.

As well as being a highly regarded Tier-1 network provider that operates one of the world's most expansive IP networks, Verizon is a leading provider of cybersecurity services. This includes advisory, threat intelligence, incident response, compliance auditing and forensics. We also produce what is probably the most comprehensive data-based annual report on data breaches, the Verizon Data Breach Investigations Report (DBIR)—now in its 18th edition. All this experience gives us a unique perspective on designing, managing and securing infrastructure.

Whether it's our global backbone, our networks for consumer Broadband and telephony or the thousands of WANs we manage for global enterprises, we believe that network and security management are inextricably linked. This paper will explain the benefits of procuring and managing these services together.

1 Strengthen defences

When managed separately, cybersecurity and networking teams often operate in silos, leading to gaps in communication and strategy. This can create vulnerabilities as configurations may not always align.

> Security and networking teams operating separately can lead to blind spots and communication issues, leading to gaps in defences and hampering incident response.

Combining these functions facilitates continuous monitoring and near-real-time threat detection across network layers. The configuration of devices, such as routers and switches, can be managed and policies enforced consistently throughout the organisation. This cohesive strategy allows for a more proactive stance against potential threats, reducing the risk of breaches and helping quickly identify and mitigate vulnerabilities.

- **Improve the operating model**
  This unified approach can drive a more resilient cyber posture while delivering cost savings through greater efficiency in the operating model—including reduced duplication of activities, staffing efficiencies, reduction of communication overhead and simplification of systems and licensing. It can also help reduce the integration and interoperability challenges of multiple technology silos.

- **Reduce downtime and third-party risk**
  These improvements can extend to helpdesk operations, where they can help improve service to staff, reducing lost time and boosting productivity. It can also help identify gaps and problems in processes with both employees and partners that attackers have been known to exploit to gain access.

- **Make controls more effective**
  Combined management can help improve the detection of vulnerabilities—when managed independently, aspects of infrastructure management may be overlooked and vulnerabilities slip through the net. More thorough and timely identification and remediation of vulnerabilities helps close the window for attackers to strike.

- **Improve use of data and threat intelligence**
  Threat intelligence is critical to effective cybersecurity strategies. When security and networking are managed together, organisations can leverage threat intelligence more effectively. Integrated solutions can analyse network traffic and security events in real time to identify indicators of potential threats. This can help mitigate attacks

2 Improve efficiency and cost-effectiveness

Procuring and managing cybersecurity and networking separately often results in inefficiency and unnecessary costs. Unifying these services can help:

- **Reduce costs**
  Managing these functions together can simplify budgeting and financial planning, provide a clearer overview of technology expenditures and generate savings.

- **Alleviate resourcing challenges**
  Breaking down siloes can also help alleviate resourcing challenges. Cybersecurity and networking professionals often require overlapping skills, and a unified approach facilitates more effective training programmes that cover both domains. Having staff able to perform both network and security tasks can help improve utilisation. This is especially important when you need to provide round-the-clock services around the world. It can also enhance employee satisfaction and retention, as professionals are given opportunities to expand their skill sets and take on diverse roles within the organisation.

3 Securely integrate multi-clouds and accelerate digital transformation

Cloud-based services are central to most digital transformation initiatives. Successful transition of applications to the cloud requires robust integration of networking and security. As companies' cloud maturity grows they often find that they need a multi-cloud environment, often incorporating hybrid cloud. A unified approach to network and security can help organisations manage these more complex environments:

- **Manage multi-cloud environments more effectively**
  By connecting cloud infrastructure with intelligent networking, teams can get greater visibility into workloads, performance and usage patterns. This can help simplify management and expedite troubleshooting.

- **Apply security policies consistently across on-premises and cloud-based resources**
  Unified controls help ensure that compliance and protection standards follow data wherever it resides, reduce configuration errors and avoid security gaps.

- **Simplify the management of hybrid and multi-cloud environments**
  Integrated solutions that enable IT teams to orchestrate services and policies from a single platform instead of managing disparate systems can streamline operations and enable greater automation, efficiency and agility.

4 Increase scalability and flexibility

Organisations must be adaptable to address rapidly changing customer needs and the technological landscape. Failure to stay agile can lead to reduced competitive advantage and missed opportunities, and eventually irrelevance and obsolescence.

- **Maintain the integrity of defences as network infrastructure changes**
  An integrated approach to cybersecurity can help businesses to respond to events more quickly. As organisations grow or adopt new business models, a cohesive network and security strategy helps maintain the robustness of defences as changes are made to the network infrastructure.

- **Avoid duplicated effort and technology**
  Siloed teams may invest in separate tools/services when a single solution may be more cost-effective and easier to manage. Integrated teams can collaborate more effectively, reducing the time and resources spent on deploying new services and resolving issues.

5 Expedite incident response and reduce downtime

In the event of a security incident, a unified approach to cybersecurity and networking enables a more robust and coordinated response.

- **Mitigate the impact of security incidents**
  By managing these functions together, organisations can create more aligned incident response procedures so that teams can work together more seamlessly. This can expedite response and mitigate the impact of attacks.

- **Identify and isolate threats more quickly**
  With unified services, companies can take a more proactive stance, continuously monitoring the network for vulnerabilities and threats. This can enhance security and reduce the likelihood of disruptions.

- **Automate and accelerate incident response**
  An integrated approach facilitates the deployment of automated response mechanisms, which can reduce the time it takes to contain and remediate incidents. Unified management also enables more effective post-incident analysis, helping organisations to learn from incidents and improve their security posture.

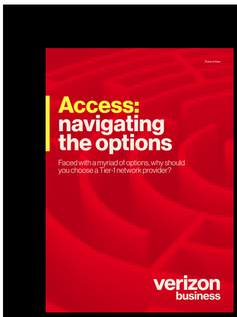
6 Simplify compliance and reporting

Compliance is often associated with industries like finance and healthcare, but increasingly most companies face strict data protection rules. Any company that handles card payments or personally identifiable information (PIII) is likely to have to be able to demonstrate compliance with minimum cybersecurity standards. This can be a time-consuming and expensive task, made even more challenging by complexity in the IT environment.

- **Improve consistency of security controls**
  Managing cybersecurity and networking as one can help simplify compliance efforts by ensuring that security controls and network configurations are consistently applied and documented.

> Automated reporting tools can be more effective when cybersecurity and networking are managed as one.

- **Create a single point of accountability**
  Unified management provides a single point of accountability for compliance-related activities, making it easier to track and report on adherence to legislation and regulation such as:
  - The General Data Protection Regulation (GDPR)
  - The Health Insurance Portability and Accountability Act (HIPAA)
  - The Payment Card Industry (PCI) Data Security Standard (DSS)
  - The California Consumer Privacy Act (CCPA)



Point of View

Access: navigating the options

Faced with a myriad of options, why should you choose a Tier-1 network provider?

verizon business

Navigating the options for enterprise access

This other paper from this series gives insight into how the choice of provider can have a huge impact in terms of performance and outcomes for your business. This is especially important for latency-sensitive applications, such as many AI use cases.

15-minute read

Why Verizon?

Simple: We are the network. Our million miles of fibre underpins much of the internet's core. That means we can offer visibility, performance and reliability that other providers can only dream of.

But it's not just about pipes. We've also got one of the world's largest and most experienced security teams, covering threat intelligence, incident response, digital forensics, compliance and more. Each year they carry out over 1,000 governance, risk and compliance engagements.

It's borderline weird how much we love data and keeping it secure. We've analysed over half a million (542,678 to be precise) security incidents—a combination of our own engagements and submissions from over 60 contributors from law enforcement and the security industry around the globe—to produce our annual Data Breach Investigations Report (DBIR). We also process trillions of security events from our networks and our clients' networks each year, providing a staggering amount of data to feed our predictive artificial intelligence (AI) models.

Enough numbers? What really sets us apart is our network and our people. When it comes to connecting your business, keeping it secure and delivering rock-solid application performance—we have the expertise to deliver.

Why settle for anything less?

23T+

We process an average of 23 trillion security events each year.

550K+

We manage over half a million network, hosting and security devices.

1K+

We carry out over 1,000 governance, risk and compliance engagements each year.

Let's talk

From IoT to real-time analytics and AI, Verizon can help you stay at the forefront of using technology to monitor, manage and improve operations. If you still have questions after reading this paper, get in touch with us at: verizon.com/business/en-gb/contact-us

The Network Procurement series

This paper is one of a series exploring the growing demands on enterprise networks and important questions companies should ask during the procurement process to help ensure that the solution they chose are truly enterprise-grade and will meet their current and needs.

Something big is coming

Data IoT AI

This paper explores some of the key drivers behind the explosive growth in the volume of data enterprises are gathering and what that means for network planning.
verizon.com/business/resources/articles/iot-genai-data-explosion.pdf

Access: navigating the options

Performance

There are many decisions to make when buying networking. Understanding the three tiers of the internet is critical to thoroughly evaluating the options. This paper explains what they mean for network performance and security.
verizon.com/business/resources/articles/tier-1-isp-enterprise-connectivity.pdf

Network peering

Cloud Performance Reliability

Peering is fundamental to network performance and consequently enterprise applications, particularly ones based in the cloud. Despite this, it’s rarely discussed during procurement. Read this short paper and put that right.
verizon.com/business/resources/articles/network-peering.pdf

Are you in the dark about performance?

Data Performance Manageability

Read this paper to learn how the decision to split the procurement of physical (underlay) and logical (overlay) networks can affect network performance, visibility and manageability.
verizon.com/business/resources/articles/overlay-underlay-network-procurement.pdf

Better together

Security Performance Manageability

Cyberthreats continue to grow in volume and sophistication. This short paper offers six reasons to consider greater integration between cybersecurity and networking to improve protection while reducing workload and cost.
verizon.com/business/resources/articles/unified-network-security-services.pdf

Supercharge your AI applications

AI Performance

Artificial intelligence (AI) promises to be the most disruptive technology since the internet became mainstream around 30 years ago. This paper explains why network performance is critical to the performance of many AI applications and realising the anticipated benefits.
verizon.com/business/resources/articles/network-infrastructure-ai-platforms.pdf

verizon business