APAC service providers must scale up and scale out security infrastructure to meet demands of distributed clouds, IoT and 5G

A new study by Ovum reveals that service providers are developing distributed clouds ahead of 5G deployments and security must keep up

Overview

Service providers are increasingly embracing distributed cloud technology, the Internet of Things (IoT), and 5G technology.

This creates a need for an architecture which can provide increased capacity and massively increased performance. As service providers adopt new architectures, they must ensure that their security posture is sufficiently agile to change with new requirements, and that security does not act as a bottleneck to network performance. Security infrastructure must be able to scale up to handle increased capacity requirements, and scale out to accommodate the increased signaling and session demands of edge distribution, combined with increasing volumes of IoT endpoints.

A growing number of service providers are implementing distributed clouds and IoT. These technologies create a much larger attack surface and make cybersecurity much more complex. Service providers often respond to these new challenges by investing in new security solutions. However, this creates additional challenges as a unified view of agile networks and numerous security tools, will become more difficult to achieve, yet more critical.

Against this background, Ovum research reveals that:

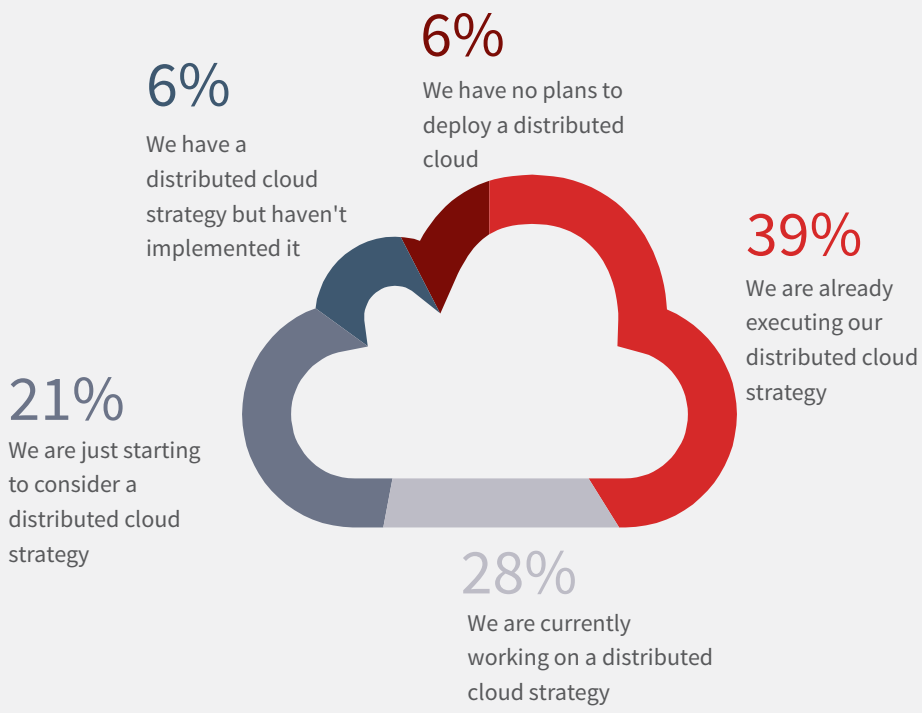
- Service providers are developing distributed cloud architectures ahead of 5G deployments.
- Distributed clouds and IoT lead to new security challenges.
- 5G use cases will add to security complexity, compounding the issues associated with distributed clouds and IoT.
- Service providers must ensure that they have a unified view of their evolving networks as distributed clouds, IoT and 5G are rolled out.
- Service providers state that they are secure, however, they need to ensure that their security posture accommodates distributed cloud, IoT and 5G roll-outs.
- Intrusion detection systems are a major area of focus for service providers.

Service providers are developing distributed cloud architectures ahead of 5G deployments

Service providers are transforming their networks to improve agility and operational efficiency. Distributed cloud architectures, in which compute, network, and storage resources are deployed in numerous locations outside of a centralized data center, will play an important role in the next generation of services that service providers wish to deploy. The distributed cloud will present some new challenges, but it will also offer the promise of a variety of benefits, including lower costs and increased revenue. Service providers are progressing in a similar way to enterprises, years ago, starting with open source and virtualization and moving on to the cloud and its attendant automation.

Most service providers agree that cloud-based architectures and principles will be critical to managing the sustained growth of data traffic. A majority of respondents in a recent Heavy Reading survey of service providers indicate they had adopted or were planning to adopt a distributed cloud strategy. Distributed cloud deployment intentions are shown in Figure 1 below.

Figure 1: Distributed cloud deployment plans.



With the distributed cloud, service providers can offer Internet of Things (IoT)-ready services as well as position themselves to support third-party applications and potentially enter adjacent markets to create new revenue streams. Note that these new services can be delivered even before 5G is deployed. However, 5G will require a distributed cloud to be in place – accelerating network transformations. Low latency services, which require processing closer to the end user, are expected to be a significant part of service providers' 5G service portfolios.

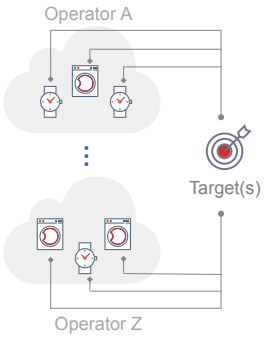
Distributed cloud and IoT lead to new security challenges

Distributed clouds and IoT implementations massively increase the attack surface available to malicious actors. Each IoT implementation will have different security policies and requirements associated with it. This adds to the complexity of securing these implementations.

Figure 2 shows the security threats posed by IoT and edge computing.

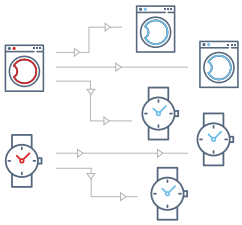
Figure 2: Security threats posed by edge computing and IoT

DDoS from Infected IoT devices



- Zombie army of monoculture “things”
- Compromised devices coordinate large attacks

IoT targeting peer devices

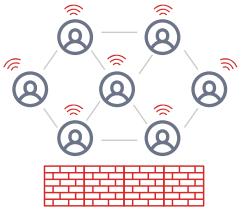


- Compromised devices hunt for vulnerable peers
- Infected device traffic affects network performance

Other malicious IoT events

- OTA request flood
- Device data exposure
- Target attacks
- IoT vandalism

Accidental IoT disruption



- Mass concentration of roaming devices
- Access network, gateway overload

This growing number of threats and the scale of the damage that they can cause typically leads service providers to purchase multiple security solutions to address the challenges.

In addition to using IoT devices as an entry point for a network, IoT devices are increasingly being used to launch DDoS attacks. The threat type emanating from IoT devices varies significantly, hence all these risks need to be managed.

To date, service providers have been able to address smaller DDoS attacks with their existing technology. Larger DDoS attacks have tended to force service providers offline and cause service interruptions. As DDoS attacks grow in frequency, scale and sophistication, new solutions are required. 5G and IoT will require service providers to be able to filter traffic on a much larger scale than before. For this to be effective, their protection will need to build in greater automation, intelligence and machine learning capabilities.

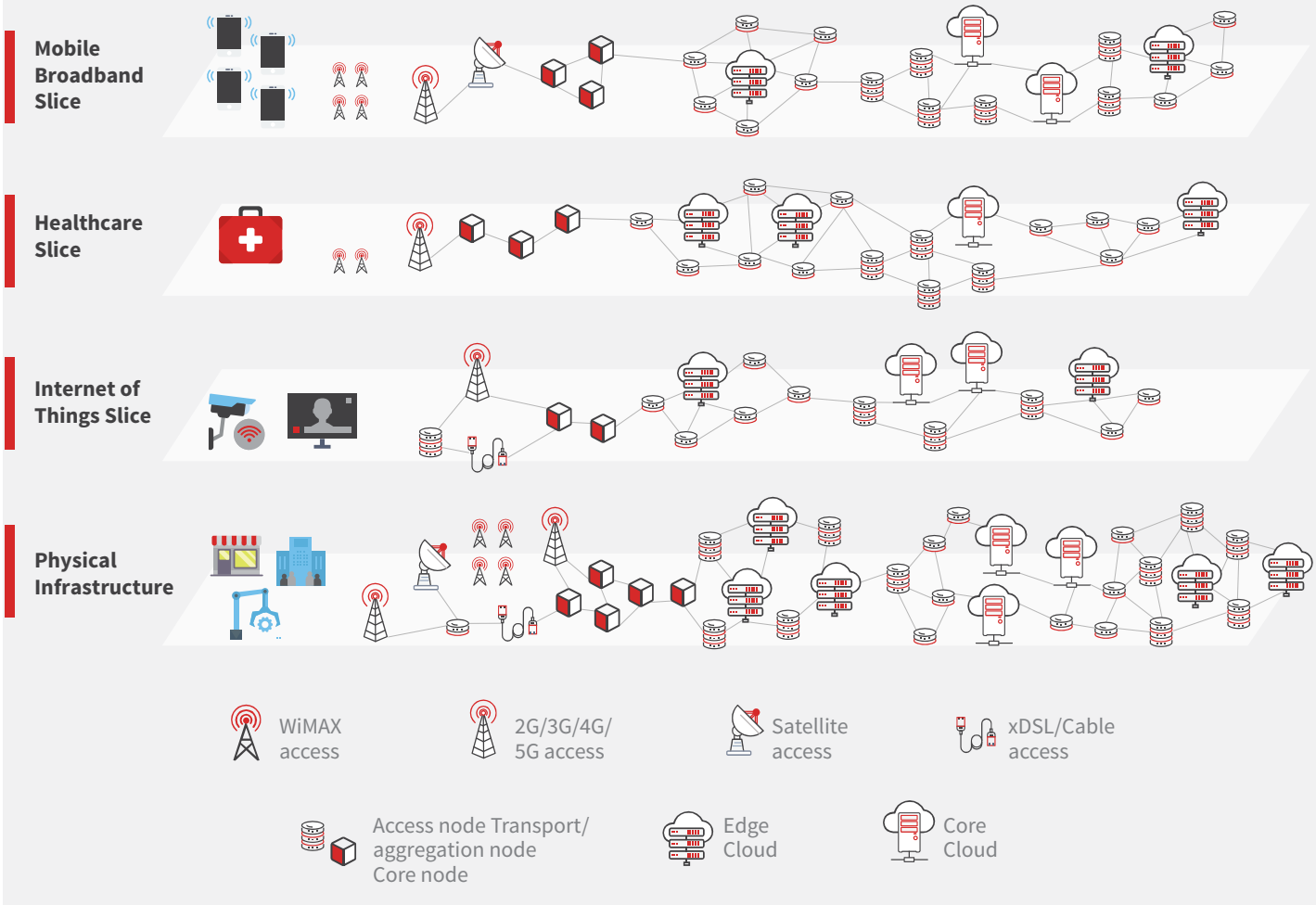
5G use cases will add to security complexity

5G is expected to allow mobile service providers to partition their network resources, to address a diverse set of use cases with differing performance and functional requirements from very different users. They can also multiplex these use cases over a single physical infrastructure.

These varying service performance profiles have a direct impact on security protocol choices and policy implementation. For instance, the service in one use case, such as a smart city application, may require extremely long device battery life, which constrains the security protocol in some other way (e.g., how often re-authentication is performed). In another example, the use case may be very privacy-sensitive, requiring unusually intensive security procedures (e.g., very frequent reallocation of temporary identities).

Figure 3 shows that 5G is expected to lead to the provision of multiple use cases or network slices.

Figure 3 – Network slicing and 5G use cases

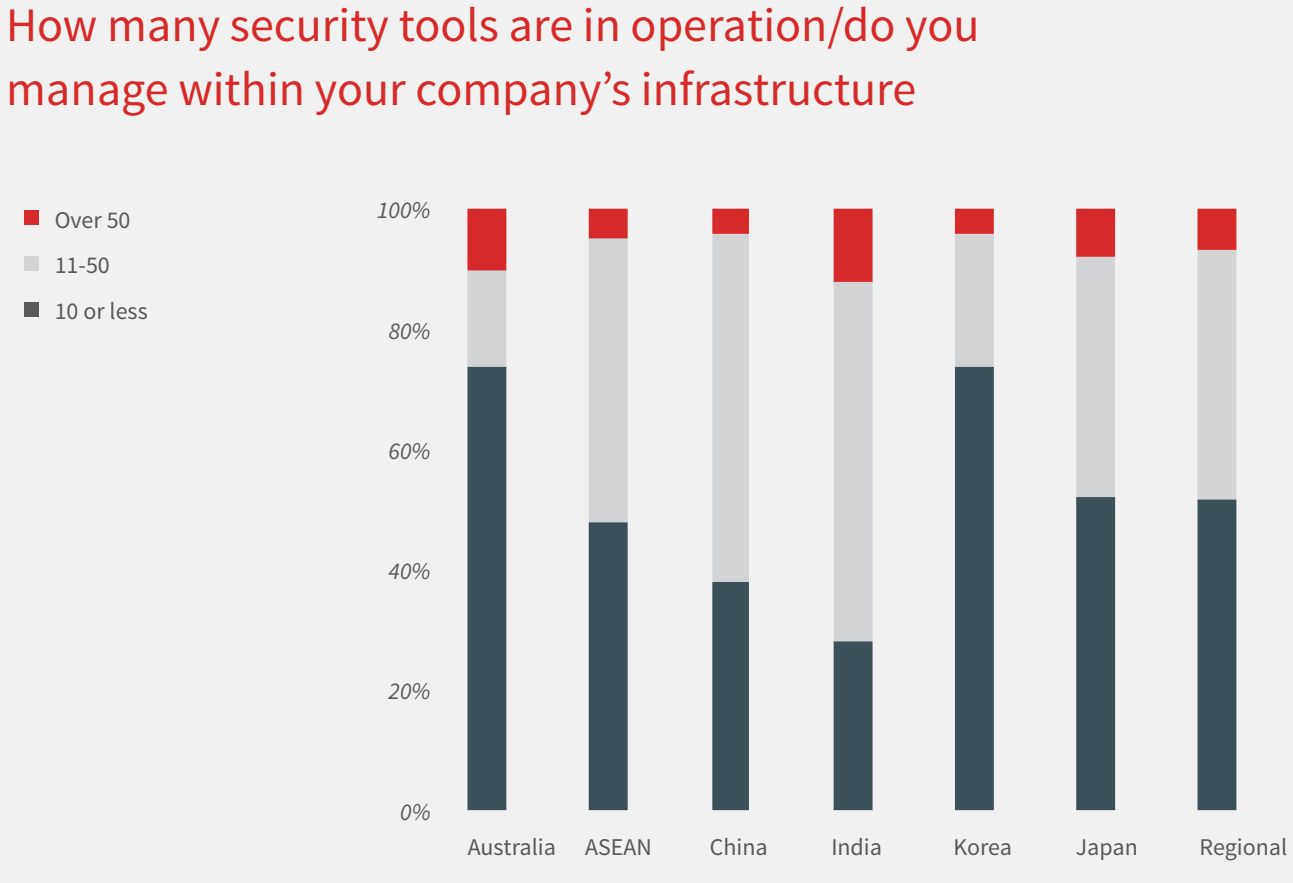


Service providers must ensure that they have a unified view of their evolving networks

A common response by service provider decision-makers to the increasing complexity of their distributed cloud and IoT environments – where existing tools cannot always detect new and emerging threats – is to deploy brand new security solutions. Over time, however, this creates an estate of siloed security products, sometimes reporting to their own dashboard. Although service providers are addressing this management challenge, typically with SIEMs, they must continually ensure that there is provision for the centralization of security alerts, so as cybersecurity staff do not face the challenge of monitoring multiple consoles and cross-referencing between disparate screens and information formats. Additionally, applying security policy changes is a laborious and time-consuming task in a multi-dashboard environment, which represents a security threat in its own right.

Figure 4 shows how the number of tools that are used by APAC organizations including service providers.

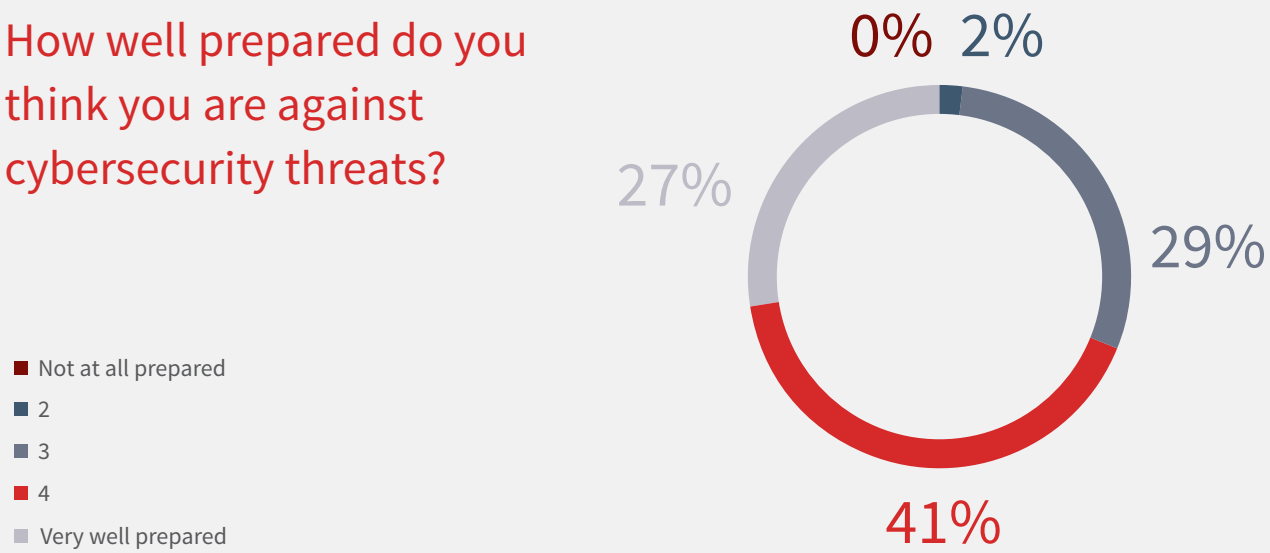
Figure 4: Number of security tools used by large APAC organizations



Service providers must ensure that their security postures accommodate distributed cloud, IoT and 5G roll outs.

When interviewed, service providers state that they are well-prepared against cybersecurity threats. When asked how well-prepared they believe they are against cybersecurity threats, on a scale of 1 to 5, more than two thirds of service providers express the view that they are well or very well prepared against cybersecurity threats. Figure 5 below illustrates service provider perceptions.

Figure 5: Perceived preparedness against cybersecurity threats



As service providers embrace distributed cloud, IoT and 5G technology, security will require upgrades to physical infrastructure to scale up, and virtual infrastructure to both scale up and scale out. Without this investment in additional performance, security will become a bottleneck to overall network performance.

5G adoption will increase available bandwidth, providing an even more robust network for generating attack traffic from compromised connected devices. As volumetric DDoS attacks grow in terms of frequency, magnitude, and sophistication, traditional defenses such as out-of-band scrubbing centers and manual interventions have become inadequate and cost-prohibitive.

In the case of large volumetric attacks, redirecting suspicious traffic to a scrubbing center adds latency and imposes a significant financial burden, since mitigation costs are directly tied to the volume of the data traffic. Service providers should consider adopting new DDoS protection approaches that incorporate AI, real time analysis, and telemetry to automate a more intelligent and cost efficient detection and mitigation process.

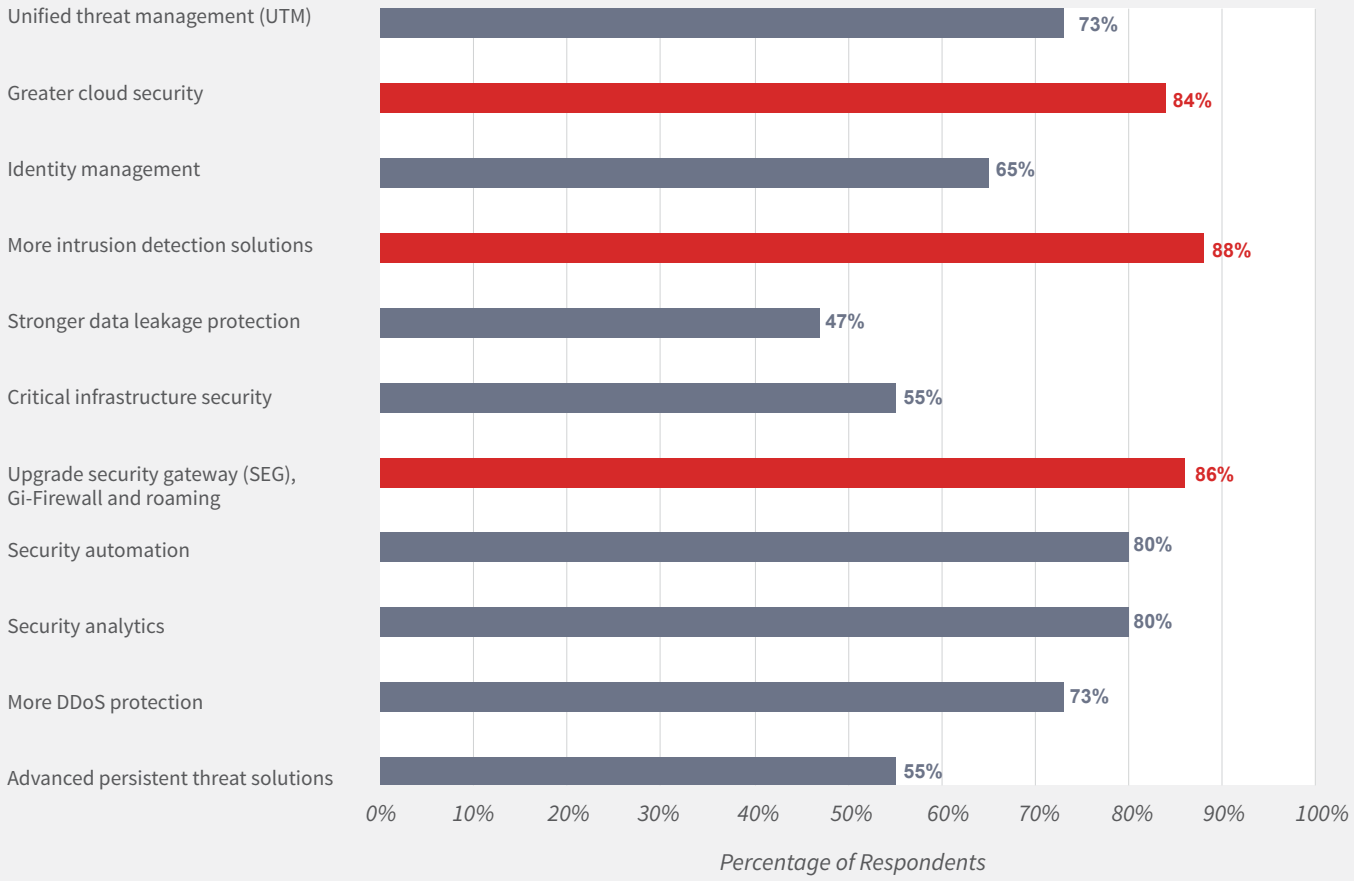
In addition to performance, security operations must also scale and support a distributed telco cloud environment with physical network functions (PNFs) and virtual network functions (VNFs). This requires a unified security management system that manages both physical and virtual domains and provides a unified view of these domains. In other words, security management needs to provide holistic system-wide visibility. Another component of this strategy is to leverage automated policy orchestration through programmable security policies to ensure a reliable and secure network that fulfills service-level agreements.

Intrusion detection systems are a major area of focus for service providers

In order to address new cybersecurity challenges posed by cloud, IoT and 5G technology, service providers are investing in multiple solutions. More intrusion detection systems, cloud security and firewall upgrades emerge as areas where focus is the greatest.

Addressing new cloud, IoT and 5G challenges

How do you expect to address new 5G, IoT and cloud threats?



Given the massively increased attack surfaces managed by service providers, artificial intelligence and machine learning need to be used to a greater extent. At present, service provider security systems are usually well equipped to handle known threats and comparatively small DDoS attacks. Only greater use of automation, artificial intelligence and machine learning can address much larger DDoS and sophisticated attacks, while minimizing service disruption.

Recommendations

The research shows that, service providers, need to manage risk associated with the roll out of new technologies. In particular, distributed cloud, IoT and 5G technology will require major changes to the security postures of today's service providers.

Service providers must take the following approaches to securing their assets as they adopt distributed cloud, IoT and 5G technology:

- Scale up and scale out security infrastructure in line with the move to distributed cloud, IoT/edge computing and 5G.
- Evaluate security performance to ensure that security solutions do not become a bottleneck to greater demands on network infrastructure.
- Ensure intrusion detection systems are up to date. Weak intrusion detection is leading to an increase in DDoS attacks. Use artificial intelligence and machine learning in your intrusion detection systems so as unusual network activity, that may come from an unknown threat, can be detected and addressed.
- Service providers must have a unified security management system that manages both physical and virtual domains and provides a unified view of these domains.

Methodology

Juniper Networks commissioned Ovum to conduct a survey of 50 IT decision makers from service providers in APAC. Data from this research was used together with data from a global survey of 100 service provider decision makers, conducted by Heavy Reading.

Author

Andrew Milroy
Head of Advisory Services, APAC
andrew.milroy@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

www.ovum.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo

900061-EN-001 Sep 2019