Enterprise Strategy Group™ by TechTarget

The State of Hybrid, Multi-cloud Management Maturity in APAC:

Where the Region Trails, Where It Leads, and Why It's So Important to Improve

infoblox

This Enterprise Strategy Group eBook was commissioned by Infoblox and is distributed under license from TechTarget, Inc.

CONTENTS

"There are **specific, actionable steps every organization can employ** to improve their hybrid, multi-cloud operations and associated business outcomes."

Introduction

Objectives

Recently completed primary market research executed by TechTarget's Enterprise Strategy Group and Infoblox validated that there are specific, actionable steps every organization can employ to improve their hybrid, multi-cloud operations and associated business outcomes.

The goal of this eBook is to go a level deeper and inspect how responses from individuals and organizations based in the Asia-Pacific (APAC) region compared to their peers in the rest of the world. Additionally, we seek to understand if the benefits of becoming a hybrid, multi-cloud Leader are as pronounced in the APAC region when we compare those Leading organizations to their less-mature counterparts in the region.

Highlighted Findings

Organizations with more mature hybrid, multi-cloud operations in APAC significantly outperform their peers:

Leaders are more efficient: They have reduced cloud costs by 20.5% more than Nascent organizations over the last year through better management.

Leaders get their products to market faster: 41% say they are typically first movers in their markets versus just 11% of Nascent organizations.

Leaders delight cloud users: They were 2.2x as likely to say they generally exceed their employee satisfaction goals related to cloud-hosted workloads (61% versus 28%) and were nearly twice as likely to say they generally exceed their customer satisfaction goals related to cloud-hosted workloads (61% versus 34%).

BACK TO CONTENTS

How APAC Organizations Differ From Their Peers on Hybrid, Multi-cloud Maturity

The Current State of Hybrid, Multi-cloud Management Maturity

To assess the state of the market, Enterprise Strategy Group created a survey focused on the people, processes, and technologies in place to enable organizations to manage their cloud environments. The answers to these questions enabled Enterprise Strategy Group to determine how well-aligned all participating organizations were to a range of best practices. The organizations that are most mature are designated as *Leading*, followed by *Converging, Emerging*, and *Nascent*.

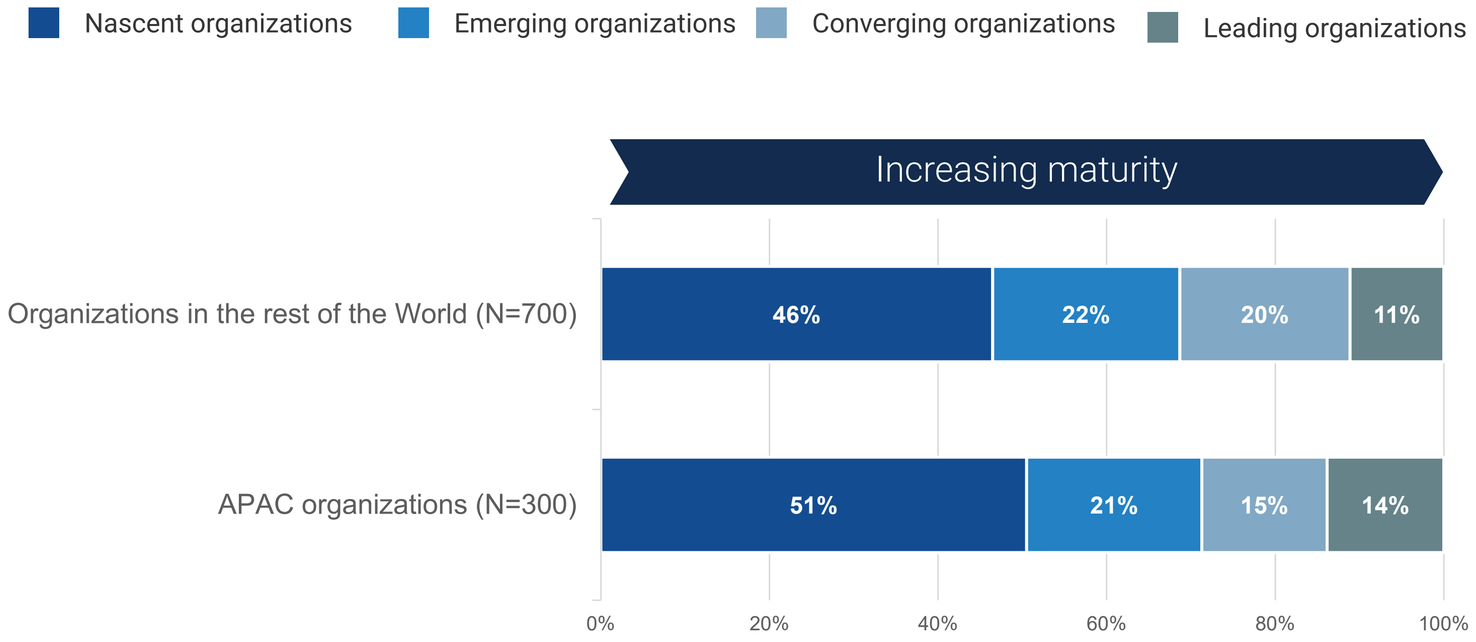
Enterprise Strategy Group's analysis employed a point-based scoring system in which organizations were evaluated as having (or not having) mature cloud management attributes and practices. They could then earn (or not earn) maturity points as a result. A maximum of 105 maturity points could be earned.

Attributes and practices assessed include:

- Has the organization established a cross-functional cloud platform team that combines network, security, and cloud operations practitioners?
- Is the organization leveraging enterprise-grade, cloud-neutral networking solutions?
- Does the organization take a defense-in-depth approach to security solutions, including using DNS for a broad range of security use cases?
- Is the organization intelligently automating a broad range of both NetOps and SecOps workflows in the cloud?

Comparing the maturity level of organizations in APAC to the rest of the world shows that a fair degree of consistency exists across the globe. However, organizations in APAC are more likely to be in the least-mature cohort (51% versus 46%) while also being slightly more likely to be Leaders (14% versus 11%), meaning organizations in APAC tend to be more sharply divided in terms of their hybrid, multi-cloud maturity level.

Organizations, by hybrid, multi-cloud management maturity.



BACK TO CONTENTS

What Distinguishes a Hybrid, Multi-cloud Leader From Its Peers?

Enterprise Strategy Group's hybrid, multi-cloud maturity model is multifaceted, spanning people, processes, and technologies. Below, key differences between Leading organizations and other maturity cohorts are summarized:

Establishment of a converged cloud platform team:
Converging network and security to be part of an organization's cloud operations center of excellence can yield significant benefits in terms of efficiency, agility, and security. By breaking down traditional silos between these two teams, the organization can foster better collaboration and alignment of goals, leading to streamlined processes and faster decision-making. In the context of the maturity model, questions to assess an organization's progress include specific steps taken to converge teams, like creating hybrid roles that span these disciplines or increasing the frequency of collaboration, the propensity of the organization to have deployed common tools used in both of these teams, and the establishment of a cross-functional cloud or platform engineering team focused on meeting the organization's requirements for scalability, reliability, security, and performance in cloud environments.

Use of enterprise-grade, cloud-neutral networking solutions:
These solutions, such as third-party-provided DNS, DHCP, and IPAM (DDI), provide robust management capabilities, enabling efficient provisioning, allocation, and tracking of network resources in dynamic cloud environments. By leveraging tools that are designed for multi-cloud operations, as opposed to cloud service provider (CSP)-provided tools that only work on a single provider's infrastructure, organizations can enhance cross-cloud consistency and attain greater agility, reliability, and performance. The centralized management and reporting capabilities provided by these solutions enable better visibility and control over network infrastructure, simplifying compliance efforts and reducing operational overhead.

Taking a defense-in-depth approach to cloud security solutions:
The maturity model advocates for an organization not to be solely reliant on the cloud security and monitoring tools provided by IaaS providers. This is because every organization has different specific security policies, regulatory obligations, and/or governance standards that may require additional security measures beyond what cloud providers offer. In particular, the use of DNS across a spectrum of security use cases—like enforcing acceptable use policies, detecting and blocking malware, and incident investigation or threat hunting—is an organizational attribute rewarded in the maturity model.

Automation of both NetOps and SecOps workflows in the cloud:
Automation increases operational efficiency by reducing manual effort and human error, enabling organizations to deploy, manage, and scale network infrastructure and security services more quickly and consistently. This agility enables faster response to changing business requirements and security threats and also improves productivity, both within technical teams and for stakeholders like developers.

Taken together, these four organizational attributes determine where any given organization lands on the hybrid, multi-cloud maturity model. Organizations looking to increase their level of maturity should first and foremost seek to drive more alignment with these principles.

BACK TO CONTENTS

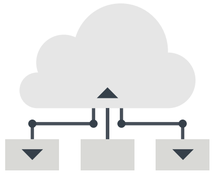
Network and Security Teams in APAC Collaborate Less on Cloud Strategies

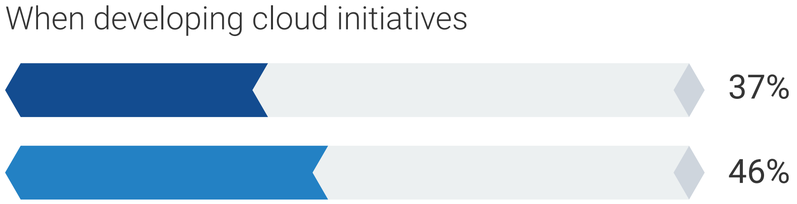
Inter-team collaboration is a component of Enterprise Strategy Group's maturity model. The reasoning is simple: If these teams work well together, it is easier for the organization to integrate security measures with network infrastructure, coordinate incident response when issues arise, and more efficiently share tools, processes, and knowledge, reducing duplication of effort and leveraging each other's strengths.

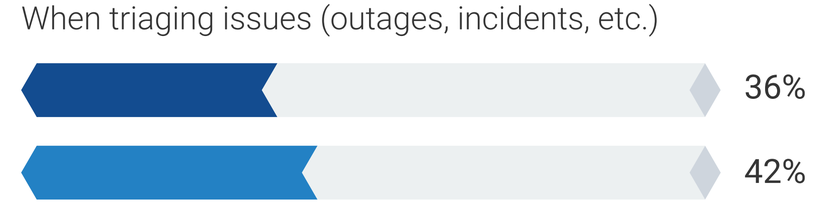
APAC organizations report that a less collaborative environment exists across their teams in a few key areas. First, just 37% of APAC respondents said that their teams are highly collaborative when developing cloud initiatives—a significant reduction compared to the 46% of respondents in the rest of the world. Next, respondents in APAC were less likely to say collaboration is highly collaborative when teams are triaging incidents and outages (36% versus 42%).

Given that both differences are statistically significant, organizations in APAC would be well served to carefully evaluate how their cloud networking and security teams work together today and if there are any steps they can take to foster improved collaboration.

How would you describe the communication between networking and security staff when undertaking the following tasks? (Percentage of respondents saying "highly collaborative")







APAC organizations

Organizations in the rest of the World

BACK TO CONTENTS

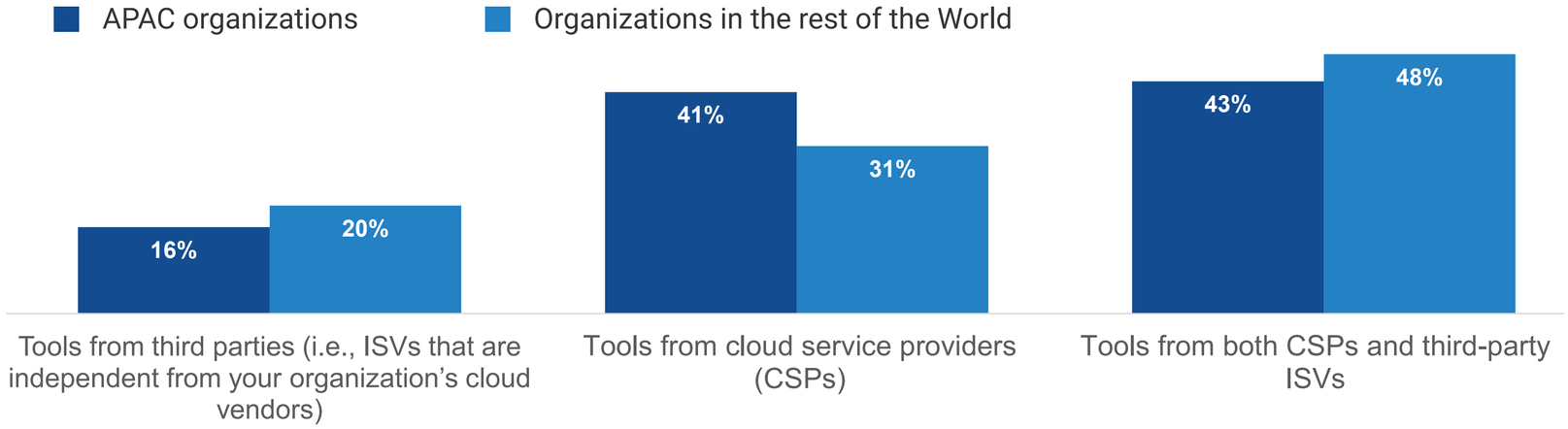
APAC Organizations Are More Reliant on CSP-specific DDI Tools

As noted, Enterprise Strategy Group's maturity model advocates for the use of cloud-neutral networking solutions that can span multiple cloud environments and provide more complete visibility, while giving administrators a unified experience.

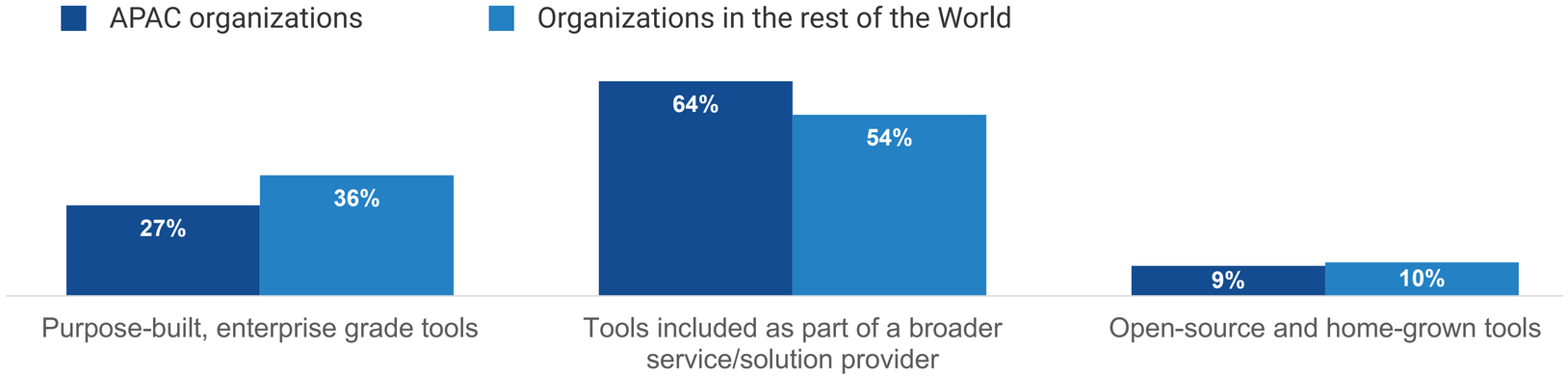
In contrast to their peers across the globe, APAC respondents more often report the DDI technologies they use are using tools provided by CSPs (41% versus 31%). Moreover, while the plurality of APAC respondents say they use both third-party and cloud-provided tools, when asked which they are **most reliant on**, they more often (64% versus 54%) indicate they are beholden to tools that are "bolted on" and provided as part of a broader service (as opposed to providing true enterprise-grade functionality).

Once again, the implication of these data points is that APAC-based organizations should inspect their current cloud network tooling with an eye toward adapting their approach.

Which best describes your organization's current DNS, DHCP, and IP address management solutions for cloud environments?



Which best describes the DNS, DHCP, and IP address management solutions your organization is <u>most reliant</u> on in its cloud environments?



BACK TO CONTENTS

APAC Organizations Less Fully Embrace DNS as a Security Enabler

Integrating DNS as a primary security control is a logical cybersecurity strategy due to its potential to thwart a wide array of threats. By leveraging DNS for security use cases, organizations can effectively detect and block malicious activities at the network perimeter, including malware infections, data exfiltration attempts, and phishing attacks. Additionally, DNS provides valuable insights into network traffic patterns and anomalous behavior, enabling proactive threat hunting and rapid incident response.

However, the data shows that organizations in APAC trail their peers in terms of utilizing DNS for security use cases. Specifically, they were significantly less likely than respondents in the rest of the world to say they use DNS extensively to detect ransomware (46% versus 54%) and as a tool in incident investigations (44% versus 53%).

To what extent does your organization leverage DNS to protect users for each of the following security use cases? (Percentage of respondents saying "extensively")

Detection/blocking of malware/ransomware

APAC organizations

Organizations in the rest of the World

Security incident investigation/response/ threat hunting

BACK TO CONTENTS

APAC Organizations Have Fewer Siloed Cloud Networking and Security Controls

One aspect of team convergence the maturity model evaluates is the use of common tools across network and security teams. By sharing common tools, networking and security teams can streamline communication and enhance overall efficiency, as they are able to reference the same data and view it through a common interface. Additionally, leveraging integrated management solutions allows for better visibility and control, enabling more effective monitoring and responses to security incidents and network issues.

In this regard, APAC organizations lead their peers globally, as they were much less likely to report their security and network teams use their own management tools and that there is no overlap (16% versus 22%).

While there is certainly still room for all organizations to improve on this aspect of hybrid, multi-cloud management maturity, APAC organizations lead the world.

With which of the following statements do you most agree as it relates to the tools in use across your organization's network and security teams to manage cloud resources?

BACK TO CONTENTS

Why APAC Organizations Should Focus on Increasing Their Hybrid, Multi-cloud Maturity

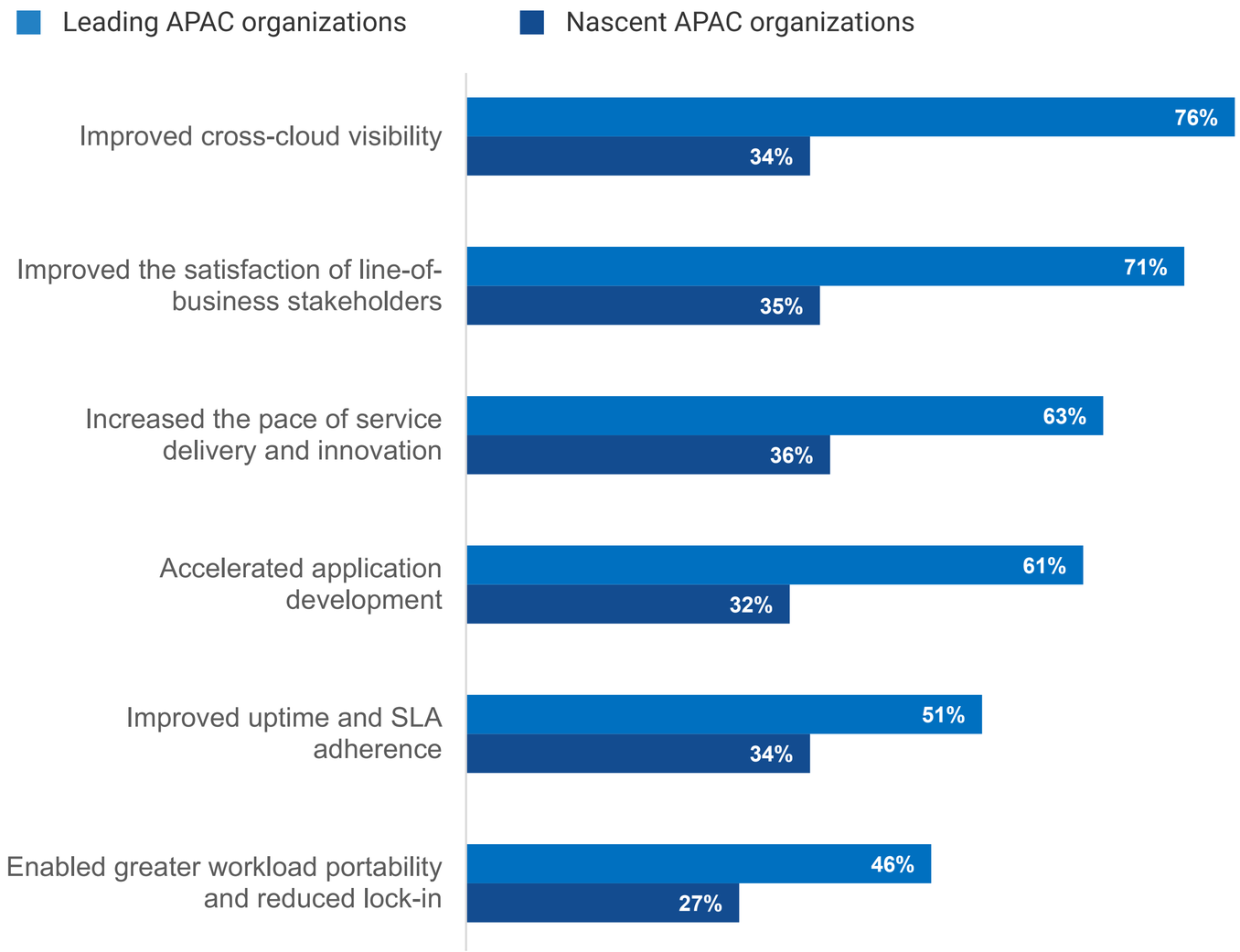
Leaders' Technology Investments Have a Bigger Payoff

In the survey, respondents were asked if their organization's approach to cloud networking and security technologies was materially improving ITOps and SecOps outcomes in the cloud.

Respondents could answer with a range of responses, from "yes, significantly" to "not at all." When the maturity model is applied to the answers to this question, it quickly becomes clear that Leading organizations are getting much more benefit from their technology investments. Specifically, they more often say their approach to cloud network and security technology is significantly:

- Improving cross-cloud visibility (76% versus 34% of Nascent organizations).
- Improving the satisfaction of line-of-business stakeholders (71% versus 35%).
- Increasing the pace of service delivery and innovation (63% versus 36%).
- Accelerating application development (61% versus 32%).
- Improving uptime and SLA adherence (51% versus 34%).
- Enabling greater workload portability and reducing lock-in (46% versus 27%).

The percentage of respondents reporting their cloud networking and security solutions are significantly driving each benefit.



BACK TO CONTENTS

A Deeper Inspection of Application Development Outcomes

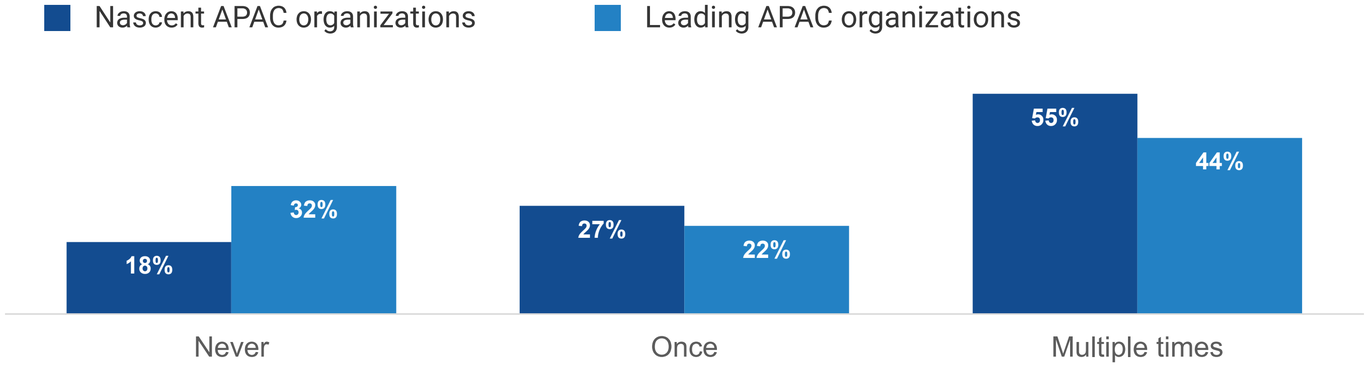
Not only did respondents at Leading organizations in APAC say their cloud networking and security solutions were helping improve application development outcomes, but their outcomes were also *objectively superior* to those of their less-mature counterparts.

Respondents were asked how often in the past year an application development project had been delayed due to the IT or security team's need for more time to inspect cloud services that underpin the project. 32% of Leaders said they have never delayed or disrupted the development team's progress on new apps or features because the IT or security team needed more time to inspect cloud services in use. Only 18% of Nascent organizations could say the same.

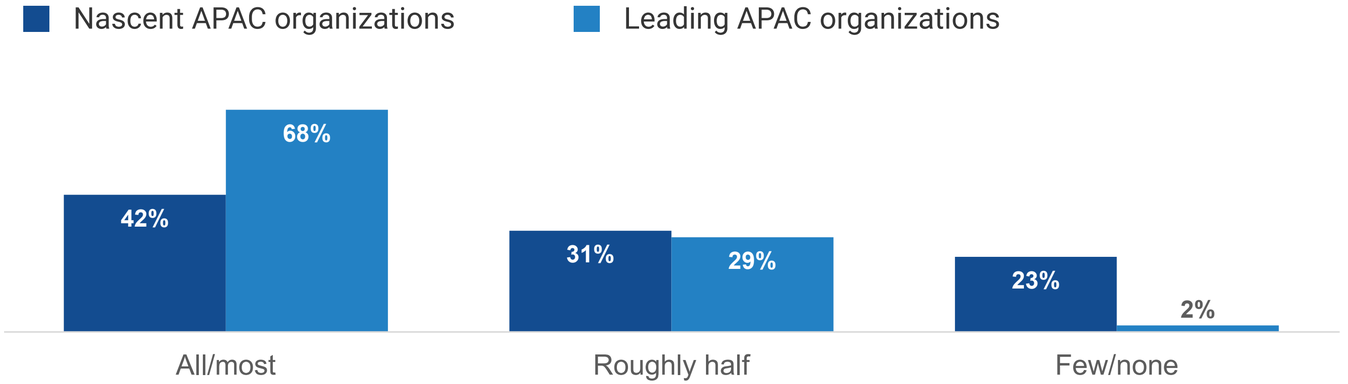
Respondents were also asked to consider all of their organization's internally developed applications and estimate the proportion for which code was able to be pushed to production "on demand." 68% of Leaders said that developers can push code to production for most or all of their applications (versus 42% of Nascent organizations).

Both proof points show just how much more prepared Leaders are to enable their development teams.

In the past 12 months, how often has an application development project been delayed due to the IT or security team's need for more time to inspect cloud services that underpin the project?



Considering all of your organization's internally developed applications, for what proportion is code able to be pushed to production "on demand"?



BACK TO CONTENTS

Leaders Have More Efficient and Resilient Cloud Environments.

Leaders also reported dramatically different results relating to the cost effectiveness, reliability, and security of their cloud environments:

Cost efficiencies

20.5% larger reduction

All respondents were asked to estimate how much their cloud monitoring and visibility solutions were helping them reduce their cloud costs (relative to if those solutions were not in place), and Leaders reported a 20.5% larger reduction.

Improved resilience:

25% fewer instances of downtime

All respondents were asked to estimate how many times in the past year cloud-hosted, business-critical workloads had gone down or seen severely degraded performance. Here, Leaders reported roughly 25% fewer incidents. When things do go down, Leaders are able to resolve issues faster: They were 4.8x as likely to say they are able to restore service in a matter of minutes instead of hours or days (29% versus 6%).

Agile security:

>2x as likely to be significantly accelerating security workflows

From a security perspective, Leaders were much more likely to say that over the last year they've significantly accelerated the time it takes to detect suspicious activity (54% versus 21%), investigate those anomalies (51% versus 20%), and respond to actual attacks (59% versus 29%).

BACK TO CONTENTS

Leaders Get to Market Faster With Solutions That Delight Users

Finally, the research shows that Leaders' advantages in agility and resilience are helping them succeed as businesses in a quantifiable and material way.

All respondents were asked how their organization performs in terms of time to market. Leaders in APAC were much more likely than their less-mature peers to report success: 41% said they are typically first movers in their markets versus just 11% of Nascent organizations.

And the solutions brought to market are meeting users' expectations:

- Leaders were 2.2x as likely to say they generally exceeded their employee satisfaction goals related to IT-managed, cloud-hosted workloads (61% versus 28%).
- Leaders were nearly twice as likely to say they generally exceeded their customer satisfaction goals related to IT-managed, cloud-hosted workloads (61% versus 34%).

Generally speaking, how does your organization perform in terms of employee end-user satisfaction with IT-managed cloud workloads?

Generally speaking, how does your organization perform in terms of customer satisfaction with IT-managed cloud workloads?

BACK TO CONTENTS

Conclusion

Evaluating the data from APAC-based respondents provides two clear learnings. First, on balance, organizations in APAC have a moderate amount of catching up to do relative to their peers across the globe. While the gap is not insurmountable, it is consistent across areas like inter-team collaboration, DDI solutions that can provide more consistency and complete visibility across clouds, and the use of DNS to improve security operations. Second, the effort to close these gaps will pay off for organizations in the region. Leaders in the region consistently report dramatically better technical and business outcomes associated with their cloud environments. Cloud strategists in APAC would do well to prioritize investments and establish processes that are aligned to the hybrid, multi-cloud management maturity model discussed in this eBook.

How Infoblox Can Help

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, Infoblox provides real-time visibility and control over who and what connects to an organization's network so that it runs faster and stops threats earlier.

LEARN MORE

infoblox®

RESEARCH METHODOLOGY AND RESPONDENT DEMOGRAPHICS

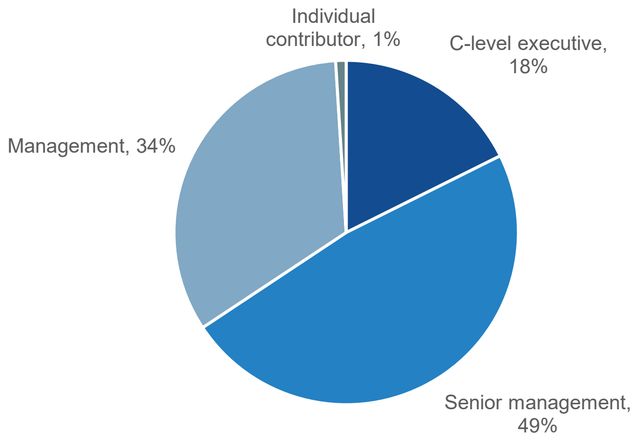
To gather data for this report, Infoblox commissioned Enterprise Strategy Group to conduct a comprehensive online survey of 1,000 networking and security decision-makers and influencers knowledgeable about their organization's public cloud environment.

Organizations represented span private- and public-sector organizations across the globe, including respondents based in North America (U.S. and Canada), Western Europe (France, Germany, Spain, and the U.K.), and the Asia-Pacific region (Australia, India, Japan, New Zealand, and Singapore). The survey was fielded between December 15, 2023 and January 17, 2024. The margin of error at the 95% confidence level for this sample size is + or - 3 percentage points.

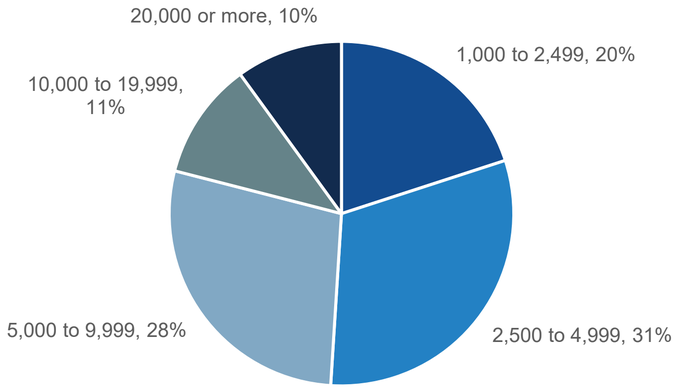
The demographics of the N=300 respondents based in the APAC region are displayed here.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

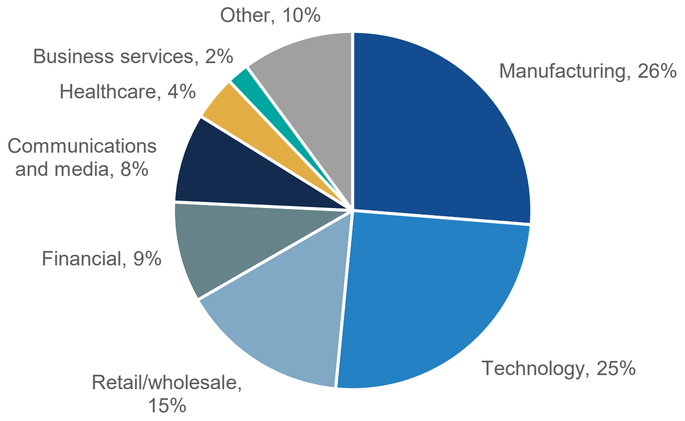
Which of the following best describes your current job title/level? (Percent of respondents, N=300)



How many total employees does your organization have worldwide? (Percent of respondents, N=300)



What is your organization's primary industry? (Percent of respondents, N=300)



BACK TO CONTENTS

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.