Secure, Efficient and Agile: Hybrid Multicloud Security Defined

AN IDC INFOBRIEF | APRIL 2021

Sponsored by Red Hat, Intel, and IDC
Executive summary

The future of digital innovation is arriving way ahead of schedule, especially as accelerated by new COVID-19 realities. A strong hybrid multicloud security strategy lets enterprises boldly meet that future.

Transformation
By 2025, two-thirds of Asia/Pacific enterprises will have to transform themselves into bona fide software factories

Cloud-native
By 2025, net new production-grade cloud native apps will increase to 70% from 10% of apps in 2020, due to the adoption of technologies such as microservices, containers, dynamic orchestration, and DevOps

Third-party code
The reuse of third-party code in apps and digital solutions will increase from 35% in 2023 to 75% in 2024, leading to a corresponding increase in the number of applications produced each year by 1.5 times

Sources: FutureScape 2021 Asia/Pacific Implications (January 2020), N=989; Becoming a High-Performance Software Producer and the Future of Digital Innovation, IDC. #US46056620
The race is on

Applications are employing these methodologies or practices:

What percentage of your enterprise’s new applications are employing the following methodologies or practices?

<table>
<thead>
<tr>
<th></th>
<th>Now</th>
<th>Next Year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Less than 25%</td>
<td>26% to 50%</td>
</tr>
<tr>
<td>Agile</td>
<td>35%</td>
<td>43%</td>
</tr>
<tr>
<td>API management</td>
<td>26%</td>
<td>38%</td>
</tr>
<tr>
<td>Cloud-native development</td>
<td>28%</td>
<td>36%</td>
</tr>
<tr>
<td>Containerization</td>
<td>31%</td>
<td>36%</td>
</tr>
<tr>
<td>Continuous integration and design</td>
<td>27%</td>
<td>39%</td>
</tr>
<tr>
<td>Continuous testing</td>
<td>25%</td>
<td>35%</td>
</tr>
<tr>
<td>DevOps</td>
<td>21%</td>
<td>42%</td>
</tr>
<tr>
<td>Microservices</td>
<td>29%</td>
<td>38%</td>
</tr>
</tbody>
</table>

To achieve efficient and secure software development, Asia/Pacific organizations now rely on an array of advanced software development methodologies and practices across public and private clouds. A thoughtful hybrid multicloud security strategy lets them manage it all.
Effective digital innovation means secure digital innovation. Overall cloud security is a critical part of avoiding nightmare breaches and hacks.

The nightmare scenario

These are some recent examples of high-profile cloud security breaches resulting in customer data being compromised:

- **Errors in cloud configuration**
  Involving 106 million Capital One customers in the US and Canada, this giant breach in history arose from errors in cloud configuration and setup.

- **Improperly secured cloud server**
  Some 540 million Facebook member records were exposed as a result of a third-party partner operating within an improperly secured cloud server.

- **Hacking of cloud and supply chain software**
  One of the largest cyberespionage events in history, a massive eight-to-ten month cyberattack exposes US federal agencies via SolarWind’s cloud and supply chain software.
Connecting the dots

To reach new customers and optimize resources, enterprises are leveraging containers, microservices and an array of public and private cloud services. A well-considered hybrid multicloud security strategy is critical to managing all that complexity.

**The connected cloud**

Asia/Pacific enterprises face mounting challenges around application modernization, data integration and security across cloud silos. In response, IDC expects leading Asia/Pacific organizations to adopt well-connected cloud architectures and strategies.

**Policy driven**

Connected cloud strategies allow teams to take advantage of advanced cloud specific capabilities while maintaining security, compliance, and performance requirements via automated governance. The idea is easy and quick access to new services and innovation in edge, cloud, and datacenter resources.

**Data first**

Data is an all-important asset. The cloud empowers Asia/Pacific organizations to become more data-centric but privacy and security concerns loom. Enterprises need flexible, holistic hybrid multicloud security strategies to face them head on.

What IT activities will your organization prioritize over the next 18 months?

- Big Data & analytics: 20%
- Modernization of enterprise apps: 19%
- Reduction in total cost of IT: 17%
- Integration of enterprise apps: 14%
- Inhouse training upskilling & talent recruitment: 13%
- Security, licensing, governance, risk & risk & compliance: 11%
- Dev and IT Ops team alignment: 5%
Security at the speed of software

Automation powers the best hybrid multicloud security strategies. It lets enterprises continually address misconfigurations and errors, and helps them integrate security throughout their applications and processes.

**Offensive and defensive security**
Faster agile and DevOps-fueled development push old methods of securing software past the breaking point. Asia/Pacific enterprise leaders are coming to realize that continuous automated security testing – from planning to development, delivery and deployment – greatly improves their offensive and defensive security stance.

**Enterprise breaches**
Increased pipeline velocity overall and an increasing reliance on cloud technologies create a complicated set of challenges for enterprises. An automated, cohesive, and mature security policy addresses all these needs.

**Strategic freedom**
Automating security streamlines processes. It frees up teams from repetitive fixes and updates, which allows them to focus on the work that really matters.

---

**AUTOMATION**

By 2024, automation will accelerate software development, with 90% of new apps relying on policy-driven security and compliance.

**90%**

Now release code every two to three weeks (IDC 2019).

**19%**

now release code weekly

**16%**

of IT professionals told IDC they now release code weekly

---

Source: IDC PaaSView and the Developer

By 2024, automation will accelerate software development, with 90% of new apps relying on policy-driven security and compliance.

**90%**

Now release code every two to three weeks (IDC 2019).

**19%**

Now release code weekly

**16%**

of IT professionals told IDC they now release code weekly

An IDC InfoBrief | Secure, Efficient and Agile: Hybrid Multicloud Security Defined

Source: IDC PaaSView and the Developer
Team first!

Even the soundest hybrid multicloud security strategy won’t succeed without multidisciplinary, collaborative teams.

By 2023, 60% of Asia 1000 companies will shift security to earlier in the development process, allowing security teams and DevOps teams to fully engage.

Increased efficiency

Fail-forward, resilient organizations unite teams across the software development, operations, testing and security processes. Tighter collaboration among all stakeholders lets the team spot and fix vulnerabilities sooner. That, in turn, means the release of more secure software, faster.

Busting siloes

When organizations have separate siloes for development, testing and security, gaps result. Busting up such compartments is a best practice for hybrid multicloud security.

Starting small

Traditional Asia/Pacific organizations are not naturally set up for the collaborative, flat organizations that make software development hum. For optimal hybrid multicloud success, start with a project-by-project approach and advertise successes.
Continuous, automated and cycle-wide security is the urgent enterprise imperative

It is not surprising then, that enterprises are increasingly focused on integrating automated security tools in their cloud platform.

IDC Predicts:

20%  Through 2021, all enterprises will struggle with app modernization and data integration across cloud silos; 20% will adopt connected cloud architectures to overcome these concerns.

80%  By 2021, over 80% of enterprises evaluating cloud services for privacy-sensitive workloads will mandate maintenance of data sovereignty and data control capabilities across geographies.

Over 25%  By 2025, over a quarter of new cloud applications will use data-centric event-driven architectures rather than traditional code-centric ones, enabling better automation and business agility.

How far have you integrated security in your organization?

- 25%  of global enterprises tell IDC they have begun to deploy integrated DevSecOps security analysis tools and processes.
- 27%  tell IDC they are now evaluating and budgeting for the procurement of security analysis tools, dashboards, and platforms.
- 40%  plan to launch security analysis tools in the next year.

- Security is integrated throughout the SLDC as an ongoing activity
- Our developers involve security from the planning stages
- Security is rarely involved in the SDLC, if at all
- Security and testing are valuable parts of our DevOps teams

Source: Asia/Pacific 2021 DevSecOps Survey N-1112
IDC FutureScape 2021 Cloud Predictions: October 2020
Essential Guidance

Automate everywhere
Adopt automation across the enterprise. Streamline software development so processes and codes are tight and repeatable.

Hybrid cloud
Stability, security, and scalability are everything. Whether on-premises or on public or private clouds, applications and infrastructure must be readily available.

A mindset of experimentation
Agile, efficient organizations are able to pivot on a dime. Experiment with ways to more rapidly react to customer demands and efficiently deliver secure, quality software.

Collaborative culture
Bust up silos. Unite business, DevOps and security leaders. Build multidisciplinary, collaborative teams that are set up to rapidly iterate, bounce back from failure, and celebrate successes.

Copyright 2021 IDC. Reproduction without written permission is forbidden. This IDC Infobrief was produced by IDC Asia/Pacific Custom Solutions. The opinions, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC. Any information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval. For more information, visit: www.ap.idc.asia or email: ap.permissions@idc.com.
Message from the Sponsor

Helping organizations prepare for the digital future

Red Hat is a world-leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

Red Hat and Intel have co-developed deployable architecture solutions—including Intel® Select Solutions for Red Hat OpenShift® Container Platform—for more than 20 years with the goal of accelerating enterprise digital transformation. From the moment a feature is on a product roadmap, Intel and Red Hat work to create hardware and software that interact synergistically, so that customers can make full use of the latest technology as it becomes available. Intel further supports that synergy by being active in OpenShift Commons. These are just some of the reasons that many Fortune 500 companies use Red Hat Enterprise Linux and that the majority of the world’s data centers are powered by Intel® Xeon® processors. Know more: www.redhat.com/en/partners/intel