Reducing risk in a hybrid cloud model is the key to fueling growth

Tim Moody, Head of Portfolio & Strategy at Fujitsu

Security outages can kill brands

Cyber security is the number one concern for organizations when managing their hybrid cloud environments. This is hardly surprising when you consider that nine out of 10 companies have suffered data breaches in the last 12 months. Damages due to digital crime represent the most significant transfer of economic wealth in history, according to researchers at Cybersecurity Ventures.

Part of the challenge is that IT infrastructure is increasingly complex and harder to protect; ESG reports that 30-40% of a company's attack surface is unknown to the IT professionals tasked with protecting it. The problem has been compounded by the rise of IoT, the use of public cloud services, APIs and distributed workforces, leading to attack surfaces expanding and becoming more decentralized.

The damage can be catastrophic. The Cost of a Data Breach Report 2021, compiled by the Ponemon Institute, puts the average cost of a data breach in hybrid cloud environments at $3.61 million per incident. The study also found that it takes on average 287 days to identify and contain a data breach.

Cloud insecurity is overstated

Public cloud is one aspect of IT that was once considered a cause of greater cyber-insecurity. But over the two decades of its existence, that reality has changed. Where once users were ill-prepared for the additional risks of cloud connectivity, today's hyperscale public cloud providers offer levels of cyber security sophistication and investment that few organizations can match.

In a recent meeting with US President Biden, Google, for example, committed to spend $10 billion on security over the next five years and train an extra 100,000 people in relevant skills in the US alone. Microsoft says it has spent $1 billion per year on cyber security since 2015 and upped that commitment to $20 billion to deliver more advanced security tools over five years.

Leading the pack

Pretty much all the business world uses the public cloud today, to a greater or lesser extent. But few companies are operating in a 100% public cloud environment. The proportion today probably stands in single-digit percentages.

Most organizations also operate on-premises infrastructure, often delivering a private cloud service for its users. This public and private cloud combination is what we mean by "hybrid cloud".

In the context of extreme — and still-escalating cyber threats — recent research from Fujitsu identified a small group of companies that have already used its hybrid cloud infrastructures to build resilience and accelerate business transformation goals.

These hybrid cloud leaders, representing a third (33%) of the sample, were better at managing risks than the other, the hybrid cloud followers. Leaders, the research shows, evolved their hybrid cloud management to facilitate growth and reduce risk. They were 60% more confident than the followers they could manage security and 75% more confident about managing compliance across their hybrid environment.

However, while they were significantly more confident than the followers, the leaders were far from complacent. Not even a third believed that they were completely on top of compliance or security.

Trust no-one

If security creates such a challenge for companies, how can they improve?

Taking a "zero-trust" approach is essential, especially with a more significant proportion of the workforce working remotely. COVID-19 has pushed forward the question of how to secure an organization that has a globally distributed workforce.

Zero trust refers to a strict identity-verification process that treats every attempt to access networks, applications and data as a potential threat. When it comes to hybrid cloud environments, this can be a crucial security measure in maintaining integrity across public and private areas and multiple devices.

Zero trust models can help customers make sure they have a secure operating environment and, as a result, are becoming more prevalent.

Innovate with security in mind

The cautious, systematic approach required to build an effective security system is often contrasted sharply with the fast-paced world of innovation.

However, it's essential to reconcile the two. Innovation with security at its heart is crucial to protecting the enterprise, but there is a real challenge in balancing these two factors. The key is to build security from the bottom up. So, for every new capability developed using hybrid services, security should be a part of the underlying platform that's being delivered, not simply applied at the end of the production cycle.

The need for innovation is underscored by Fujitsu's research, which found that organizations' top transformation priority was to innovate and create seamless digital experiences. The third priority was to grow revenue from emerging technologies.

It turns out that the hybrid cloud leaders can also unlock these goals more effectively than the rest. For example, almost half (49%) of the leaders have enhanced their product innovation in the past year, compared to just 39% of the followers.

Generating growth

For companies that can improve their systemic security, the benefits go beyond protection against external threats. The Fujitsu research shows that 37% of the Hybrid Cloud Leaders believed enhancing security through a hybrid model would facilitate business growth.

The overall message is clear: Being proactive on security creates a solid competitive advantage, generating unmissable business outcomes. In the hybrid cloud ecosystems where most companies operate today, that means investment in promoting a collaborative, secure-by-design culture and in automated security tools and processes.

Want to know more? Read the full report "Unlocking the Secrets of Hybrid Cloud Leaders" and take your business to the next level.

Tim Moody, Head of Portfolio & Strategy at Fujitsu

Tim is a collaborative and enthusiastic technology leader with a depth of experience designing and delivering enterprise class services across both public and private sector. As a Fujitsu Fellow and Fujitsu Distinguished Engineer, he has a demonstrable record of accomplishment, delivering business innovation as both an individual contributor or leading large teams across a broad range of leading-edge technologies.