C&W Business

Deciphering the future of cloud security

Security is a key consideration whenever a company deploys a network application, as they may open themselves up to possible intrusions. Even if the cloud security architecture seems reliable internally, there are still some issues when it comes to multiple accesses, cloud interconnectivity, APIs, and new DevOps strategies. With all these new possible backdoors, managers struggle to keep consistent policies across all platforms and maintain full visibility and control of the data. Let's review emerging trends, evolving risks, and strategic solutions for the future of cloud security.

We compiled some insights gleaned from a recent Cloud Security Alliance (CSA) report[1]. CSA is a not-for-profit organisation on a mission to encourage the adoption of best practices for providing security assurance in cloud computing, and its corporate members include companies like Microsoft and Fortinet. C&W Business partners with both companies to bring top-notch cloud and security solutions to our customers.

Insight 1
Filling new cloud security holes

While recognising their challenges, leaders are still optimistic about their cloud security postures. Organisations have "moderate confidence" (42%) or "a lot of confidence" (31%) in their ability to defend against threats and vulnerabilities. They feel that technological evolution has been the key to their defense and will continue to play a major role in safeguarding their information.

Insight 2
Companies use many tools

Most enterprises combine tools from their primary supplier and third parties to secure their data. Cloud service providers are the preferred solution for "access management and vulnerability identification" (47%). Businesses turn to third parties for "detecting network threats" (46%) and "preventing data leakage" (35%).

Insight 3
Security holes exist

However, enterprises still have blind spots. For instance, among security products, data loss prevention tools (13%) were the least preferred investment for businesses. The hesitancy could reflect the difficulty of implementing such solutions.

Insight 4
Visibility continues to be a challenge

Another challenge stems from the process of consolidating information and correlating events from different solutions should a company come under attack. Typically, they need to triage their solutions to recognise what is happening, but such integration becomes more difficult as they add more tools. As a result, 68% of respondents state that the number one reason their organisations have security incidents is a "lack of visibility".

[1] Cloud Security Alliance - "SaaS Security and Misconfigurations Report" . 2022

Insight 5

Security needs to be a cross-functional responsibility

Organisations consistently struggle to overcome basic security challenges due to internal organisational shortcomings. Employees assume that security is only a problem for the security team. Firms could gain a stronger security posture by extending security responsibility from their IT operations and security teams to application engineering and DevOps for their own platform management. Responsibility should also be extended to HR for staff training, the internal communication of all policies and best practices, and creating awareness about the increasing number of threats.

Insight 6

Lack of knowledge and experience adversely affects security teams

Security experts are hard to find. Knowledge gaps and limited hands-on experience are well-known issues within the information cybersecurity industry[2].

Knowledge gaps and inexperience account for:

62%
of misconfigurations

And are the top barrier to implementing:

Cloud security strategies	Prevention and proactive monitoring tools	Automated troubleshooting solutions
59%	**59%**	**56%**

Insight 7

DevSecOps strategies are immature

DevOps has become the enterprise application development foundation. Incorporating strong security processes (DevOpsSec) into development is an emerging goal for a growing number of organisations.

This strategy results in stronger, more secure, and more resilient applications. It requires strong collaboration among development, security, and operations groups. Many organisations struggle to implement such policies. They even have trouble reaching an interdepartmental agreement on corporate security policies and how to implement those policies. In fact, less than a third of businesses have been successful in this regard, according to the Cloud Security Alliance.

Usually, this problem starts with the leaders and extends to their teams. The lack of alignment among departments could be due to organisational differences, like varying priorities among corporate managers. Another possible explanation is a lack of practical knowledge. Departments do not know enough about DevSecOps strategies and best practices to start implementing them or aligning their enterprises to adhere to them.

Insight 8

Better coordination is needed

Businesses have technical tools capable of closing security gaps at their disposal. What is largely missing is coordination among different environments. With the right alignment, companies are able to work together and focus their teams on common goals. Enterprises then need to select, deploy, and prioritise tools that provide:

- Improved visibility
- Effective risk governance
- Automation

[2] Cloud Security Alliance - Survey Report: "Cloud Security Posture Management and Misconfiguration Risks". 2021

Insight 9

Progress is being made, but it needs to be aligned

Corporations can achieve coordination among their departments and move towards an effective DevSecOps approach. In fact, some businesses have taken that step, which has proven effective in dealing with missteps like configuration errors. The organisations that have implemented DevSecOps and are aligned on security policies and enforcement among their departments ar more likely to detect and remediate configuration issues[3]:

Of the organisations that find configuration errors within a day:

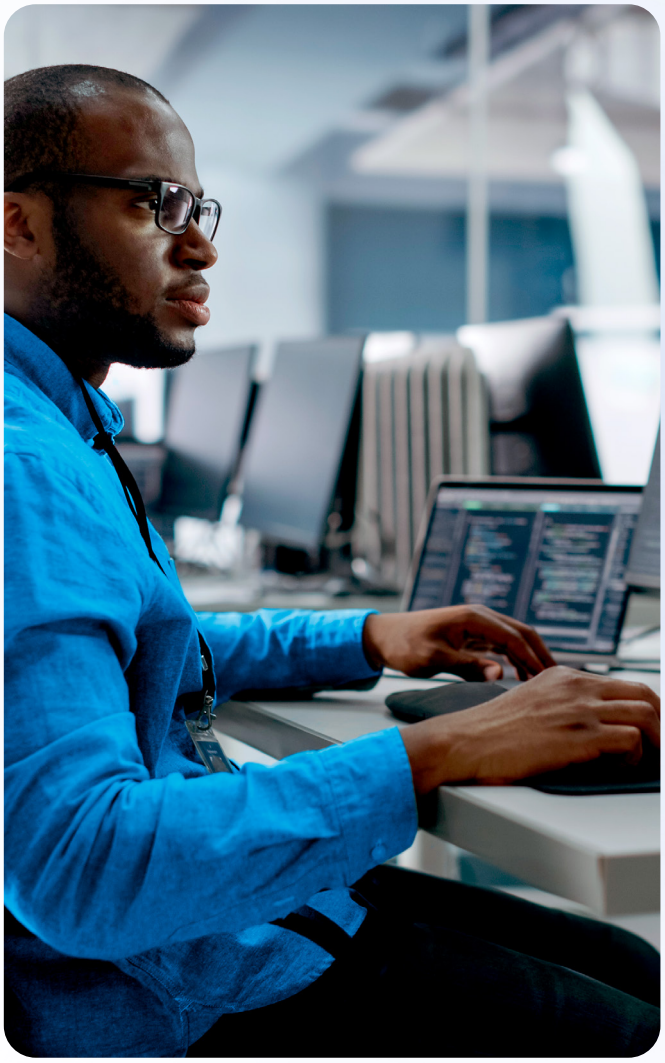
56%
Have fully aligned teams

31%
Have no aligned teams

Of the organisations that fix configuration errors within a day:

51%
Have fully aligned teams

19%
Have no aligned teams



With the right alignment, companies are able to work together, develop teams that focus on common goals, and implement the tools needed to deliver adequate levels of visibility and management into their cloud environments. As a result, they protect their cloud workloads.

In summary, although companies feel good about their security posture, they recognise the limitations of their approach and the necessity of bringing more dispersed groups together in order to gain the needed visibility. Only then will their security be as strong in practice as they perceive it to be.

[3] Cloud Security Alliance - "The State of Cloud Security Risk, Compliance, and Misconfigurations".2021

