SECURITY

Reducing the cloud security overhead

Why creating a layered defensive strategy that includes security by design can help address cloud challenges

Robin Birtstone

Wed 13 Mar 2024 // 08:51 UTC

SPONSORED FEATURE The world is filled with choices. Whether it's the 20 different types of shampoo on offer at the grocery store, or the dozens of Linux distros you can try for free, you can have it all.

The same goes for cloud service providers. Increasingly, companies are spreading the love between multiple cloud services when offloading workloads to public cloud infrastructure. But that choice brings a big security headache, because it makes your infrastructure harder to see and control.

A recent study by 451 Research found that 98 percent of enterprises have now adopted a multi-cloud infrastructure strategy. They're doing it for several reasons. The one that might first spring to mind - redundancy and disaster recovery - is the least pervasive, at 21 percent. Instead, companies are more focused on data sovereignty (the need to keep certain data in your national borders), and cost optimization, which are primary multi-cloud drivers for around four in ten companies.

Lack of security skills a problem

Cloud solutions might help companies to manage costs and data location more effectively, but securing these fragmented infrastructures takes some maturity. Unfortunately, cloud strategies are often immature, growing organically like weeds.

Cloud computing can offer significant advantages to enterprises in terms of scalability, cost-effectiveness, and flexibility. But the ability to fully realize its benefits often depends on whether the organization possesses the requisite security and collaboration skills. Without that expertise, enterprises may struggle to implement sufficiently robust measures to properly safeguard sensitive information, leaving them vulnerable to breaches and compliance violations, for example.

Moreover, managing the risks inherent to cloud environments demands continuous monitoring and adaptation, necessitating close cooperation between IT, security, and operations teams. The integration challenges which often occur between cloud and on-premises systems further underscore the importance of collaboration between these different functions.

This organic cloud growth frequently puts those tasked with protecting the organization on the back foot, warns Gurmail Singh, Cloud Security and Alliances Director at Trend Micro™.

"As the digital horizon expands, security, cloud and ops teams have to redefine their role, not just as protectors, but as architects of a new era, where cloud adoption and success are inseparable companions to help embed digital trust into cloud initiatives," he says.

Cloud security worries can exacerbate existing challenges facing security departments, with skills often a factor. In April 2023, job vacancies in cybersecurity stood at 3.5 million, according to industry watcher Cybersecurity Ventures, up 350 percent in a decade.

"In the early stages of public cloud adoption, we supported lots of organizations struggling to build the right security posture in their cloud landing zone," Singh recalls. "This was down to a number of critical factors. Skills, a unified platform approach and stakeholder alignment were some of the most important areas when it came to realizing a stronger security baseline."

"Organizations that don't prepare and collaborate with the right stakeholders for cloud projects often become vulnerable to higher risk posture."

Division of responsibilities

Even now, almost two decades after AWS first spawned the modern cloud market, some companies are still struggling to understand the shared security model that governs the cloud.

"The key to building resilience in the public cloud is through customers understanding their shared responsibility for security, what is the responsibility of the cloud provider versus the customer's role in securing data, application and OS layers," says Singh. "Within the cloud's expanse, even the smallest human error can cast a shadow of insecurity, underscoring the critical importance of vigilance and education in safeguarding organizational digital estates."

Oracle and KPMG found while over 95 percent of CISOs said they were familiar with the term, only eight percent said they fully understood it for all kinds of cloud services. Now, factor in those resident multiple cloud environments and you have a potentially disastrous outcome.

"Often if an organization is new to the cloud, they're more vulnerable to misconfiguring their network topology," says Singh. "Or maybe misconfiguring a publicly open S3 bucket. Those human errors lead to a very vulnerable attack surface."

For examples of said misconfigurations, just check the headlines. Here's one from Toyota, which has repeatedly exposed its customers' data in cloud storage that shouldn't have been viewable. Other misconfigurations are also common, from excessive permissions through to

unrestricted open network ports, the use of default credentials, and cloud networks that aren't properly segmented.

The danger of no cohesion

Using multiple clouds exacerbates these problems. In its 2023 Cloud Security report, (ISC)2 found that 58 percent of companies felt they lacked the skills to deploy and manage a complete solution across all environments. Over half also found ensuring data protection and privacy for each environment to be their biggest challenge, and roughly the same number had problems understanding how different security solutions fit together.

A lack of cohesive visibility and control across all these clouds makes managing basic security hygiene even more difficult. There are plenty of problems that multiply, introducing new dangers for admins.

Vulnerability and patch management can be tricky enough in one cloud environment, adding more strains admins even further. It takes time to review API vulnerabilities in one cloud environment, but now imagine doing that across different internal groups for applications in different clouds.

Some companies evolve and have mature processes and technology to manage security in a multi-cloud infrastructure, says Singh: "As more projects arise, you build a team and address repeatable questions." These companies will often create templated governance policies and standard security measures. They might even formalize consistent enough policies to follow them, but it's a big ask for many.

Singh describes what the market calls the ratio of doom. "For every 100 developers shaping the digital frontier, there are usually only 10 ops personnel and a lone security guardian," he says. "Yet, in this ratio of doom, lies the clarion call for shared ownership, where every line of code, every deployment, becomes a collective responsibility in fortifying our digital citadels."

For security to work in cloud environments, companies will need security to transcend the confines of siloed responsibility, weaving a collective response across the human chain insists Trend Micro. That chain links everyone from vigilant SOC analysts to diligent ops teams, innovative developers, sturdy infrastructure stewards and steadfast legal and compliance teams right the way through to the prudent stakeholders in finance and procurement, says the company. Across this united front, organizations can fortify digital programs to safeguard not just data, but establish trust and resilience across its digital estate.

"Each of these groups have a vested interest in security if they can be persuaded to see it," adds Singh.

Development teams that focus on designing secure architecture, testing early for security issues, and using safe coding practices can reduce the cost of security remediation, for example. Operations staff that follow best practice security can deploy consistent, security-audited cloud instances that operate more reliably and minimize downtime.

A technical layer for cloud security

Sharing responsibility this way across varied stakeholders creates an organizational platform which better supports mature security processes. It's a springboard from which companies can mature their cloud security posture. But this is just the beginning, because now they face some difficult tasks and challenging choices.

Finding, prioritizing, and then mitigating risk is where a technology layer for cloud security can make the security operations center (SOC) team more effective.

"The SOC is often left behind on cloud projects," explains Singh. "The SOC team can face a relentless battle to tame the volume of events, to weave coherence from chaos, and to extract value from the labyrinth of data. Amidst these challenges, prioritizing correlation becomes the beacon, guiding their efforts to safeguarding and ensure resilience against the ever-evolving threat landscape. Getting value out of the SIEM platform is a big data science conundrum."

Trend Micro Vision One is designed to serve as the cornerstone of cloud extended detection and response, unifying disparate elements of cloud security landscape into a single, cohesive platform. By seamlessly integrating the management experience for cloud builders, infrastructure, DevOps, and SOC teams, it illuminates the path forward, empowering organizations to navigate the complexities of cloud security with clarity, efficiency, and organizational security productivity for cross-functional teams, says the company.

Vision One operates at three separate layers. At the top is its attack surface risk management layer, which helps explain the enterprise's risk score and helps the SOC to map its vulnerable assets. It predicts the impact of a potential compromise so that they can prioritize the most pressing cyber risks. These include software vulnerabilities, misconfigured assets, and account compromise. It takes a quantitative approach to these tasks, using indexes to measure risk, attack severity, and exposure.

After quantifying a risk in the cloud using Vision One, the security team can identify the asset owner and then communicate with them, along with any other relevant stakeholders, to work out a risk mitigation strategy. Vision One will also recommend risk mitigation tactics to help shape their approach to the issue.

The attack surface risk management tool draws on the platform's XDR capability, which is the part that enables the SOC to gain a single, cohesive view of all its assets in context. It provides a contextual view of the security situation across the cloud, endpoint, email,

network, and operational technology, monitoring behaviors and identifying activities across cloud and other infrastructure that could be malicious when viewed together.

Vision One can also automate some responses to security gaps as the XDR layer surfaces them, using playbooks to execute pre-defined mitigation activities.

Drawing on threat intelligence

This understanding of how infrastructure behavior maps to cyber risk comes from Trend Micro's global threat intelligence network. The company harvests threat data from its Zero Day Initiative, along with local Trend Micro threat intelligence centers around the world.

That includes delivering network-level patches for bugs that vendors are unlikely to handle themselves, such as flaws in end-of-life products. These all get pushed out across its Global Smart Protection Network, which keeps customers up to date on the latest available patches for assets in the cloud and beyond.

Analysts rate Trend Micro as a pacesetter when it comes to this type of cyber security. Research company IDC estimates the company accounted for the single largest share (16 percent) of the global cloud workload security market in 2022 while the Trend Vision One - Endpoint Security product was recognized as a leader in endpoint protection platforms by Gartner's Magic Quadrant methodology in 2023.

Trend Micro also partners with AWS to integrate with its services, tightly coupling Vision One policies with cloud security services, explains Singh. At AWS's re:Invent conference in November, Trend Micro announced new capabilities for Vision One including cloud infrastructure entitlement management and container security risk visibility. Trend continues to be a launch security partner with AWS to help organizations reduce cloud risks as they leverage more AWS capabilities.

The number of cloud service providers in the average company's portfolio is unlikely to decrease any time soon. They're likely to increase the distribution of workloads around different cloud providers as they become more astute at cloud economics and as the functionality options from different providers increase.

Sponsored by Trend Micro.