NTT DATA
Trusted Global Innovator

Evolving Security to Meet the Challenges of the Cloud

September 13, 2022

The widespread move to the cloud has forced organizations to restructure themselves to be more flexible, scalable, and adaptable in various ways. However, these advancements have posed new challenges to cybersecurity experts. Cloud security requires a different approach to managing risk and designing security controls because it is a shared responsibility model, and cloud service providers constantly release new features and services. The industry has had to redefine what it means to build a strong security posture. The challenges of the cloud are new, and the solutions are also. However, the structures of those solutions are familiar to anyone who's been in the cybersecurity industry for any length of time. No single technology or process will solve today's problems, but rather it's the time-tested combination of people, process, and technology.

The race for best practices is on

Hackers defeating complex security isn't the most significant enterprise risk. Misconfigurations and improper setups remain the largest contributors to cloud data breaches. The Capital One breach, for example, was primarily due to misconfigurations and excessive permissions.

And it's not simply initial misconfigurations that are the problem; configuration drift is also a significant issue. Configuration drift is usually down to changes made in production workloads without proper consideration given to security. Businesses are usually mostly focused on enabling their critical use cases. Modern businesses react quickly. They're flexible and adaptive. This means deploying new features and software in the cloud environment as quickly as possible to maintain their edge. Security can, at times, become a

secondary consideration. Ultimately this is about the balance between innovation and security. The risk is we move so slowly we stifle innovation, or we move so quickly and don't effectively mitigate risk.

In the wake of such challenges, there has been a race to develop a set of best practices that can account for such egregious oversights. The stable security perimeter of legacy institutions is being replaced by an amorphous multi-cloud environment subject to constant change. Attempts to extend traditional security approaches have caused an increase in complexity and lack of visibility. How, then, do we proceed?

Process: shift left and continually improve

As with every other enterprise-level system connected to the internet, cloud instances must be built with security in mind. Rushing to set up an enterprise cloud and planning on returning to develop the security later is planning for failure. Retroactive security measures are never as effective, and organizational friction often slows or prevents implementation.

All major cloud providers provide robust best practices and implementation guides and wizards to help set things up correctly. In the race for cloud adoption, sometimes implementations are rushed to meet business objectives, but this is not a corner that can be cut safely. Cloud architects and security teams must take the time to set things up with security in mind from day one — and keep it in mind as they move forward.

Software companies will be well aware of the CI/CD pipeline — continuous improvement and continuous development. The CI/CD pipeline enables developers to build, test, and incorporate changes to code more frequently, producing better quality code that can be deployed automatically. However, creating this pipeline only works if the software/service architecture is built in a way that supports iterative releases and makes it critical that precautions are taken during the initial stages of the software development process. Infrastructure as Code (IaC) is a prime example. IaC is designed to make cloud provisioning simpler, faster, and predictable. However, misconfigurations are practically unavoidable if security is not applied at the IaC layer. And this can all be foreign territory for organizations outside the software development industry, but it's critical to building robust cloud security.

At the heart of modern cloud security lies automation. Things move too fast in the cloud to react to all breaches manually. Of course, human monitoring and response are critical. Still, safeguards must be in place to trigger response actions immediately — in some cases, even a few minutes (or seconds) can mean the difference. Paradoxically, that need for automation drives a need for skilled people.

Cloud security can't truly work without some degree of automation. You have to be able to write code for everything.

If a conflguration drift happens at N:LL AM, we don't want the actual remediation to happen at T:LL AM when the IT administrators or cloud security lead wakes up. The automation needs to begin right away. Human monitoring and intervention are still needed, but the automatic response is critical.

Security experts need to have some degree of coding knowledge and to be able to work within the CI/CD pipeline. The profile of cloud cybersecurity expert must go beyond cybersecurity. They must understand the CI/CD very well, and they must be able to write code.

A greater emphasis on defining these traits within cloud security positions is a key component but not the end of the story. The processes and people still need that third leg: technology.

Technology: make the most of what's available

Ideal cloud security posture management is not just securely con gured at the onset: it must continuously search for risk and con guration drift. Typically, cloud workload protection platforms and posture management tools have worked separately. However, a tandem approach has provided maximum visibility, adaptability, integrated security, and better deployment options.

Tools like Microsoft's Azure Defender for Cloud, Prisma Cloud, and Orca do just this. Thanks to the progress made in machine learning, it's now possible to leverage large data sets to assess system threats across the entire cloud. The outcome is increased visibility across data points and fewer miscon gurations. Combining these with data analytics results in more automated threat detection responses, thus lifting the burden off security teams.

The major cloud service providers recommend that users not only follow their con guration best practices but also activate automatic procedures to prevent and correct potential miscon gurations. For example, the top three CSPs (Amazon, Google, and Microsoft) each have native cloud security tools to detect changes in the de ned con gurations and can then automatically launch procedures to correct that misconfiguration.

The Holy Trinity: people, processes, and technology working together

People with the right know-how, processes that keep security at the forefront while allowing exibility, and technology that makes it all easier are all critical. But without each other, none of those three pillars is su cient. One NTT DATA customer, a large bank in Spain, demonstrates this.

One of our banking customers in Spain has fully implemented the best practices and automated tools within their cloud, they've implemented a CSPM tool, and they have de ned the framework with many controls. But in addition, their security team had to write and maintain custom code that enforces controls thanks to their unique requirements.

This is an example of security-first cloud architecting: it involves developing a strategy from the onset that considers security and builds it into the development and maintenance workflow, takes advantage of the technology available, and leverages the skills and talents of the people to fill the gaps in that technology.

The world is constantly changing, and our global movement to the cloud is a critical component. The modern enterprise needs to embrace this change and subtly rethink its security programs accordingly. That means applying time-tested fundamental principles within this new arena.

If you're interested in learning more, check out our panel discussion, Continuous Security in the Cloud, and find out how industry experts from NTT DATA, Microsoft, and Cloud Security Alliance are tackling the complexities of cloud security, cloud security posture drift, automation, and risk mitigation measures.

Raul Neagoe

Senior Cybersecurity Product Manager

Raul coordinates the Cloud and Application Security Services product offerings at NTT DATA. Previously, Raul has served end cybersecurity program. He has more than 15 years of experience in cybersecurity and a proven track record of success in design, delivery and management, of cybersecurity solutions and services across multiple industry sectors.

Raul is deeply passionate about technology — especially cloud, security automation and AI. In his spare time, he is a guest professor of Incident Management and Cloud security at a Romanian university that's focused on empowering the new generation of cybersecurity specialists.