VIEW POINT

A ROBUST CLOUD SECURITY ARCHITECTURE ALSO STRENGTHENS YOUR ENTERPRISE STRATEGY

Abstract

When you think of real-life cyberattacks, do you imagine Tom Cruise breaking into a secure data centre amidst much drama to steal that one file that could save his and his team members' lives? You cannot be further away from the truth. The real-life scene involves attackers sitting at their laptops scouring the internet for vulnerabilities to exploit. Enterprises need to have a complete understanding of the cloud threat landscape and be prepared with the right cyber security architecture if they have to thwart such attacks. So, what does having robust cloud security entail?

Infosys®
Navigate your next

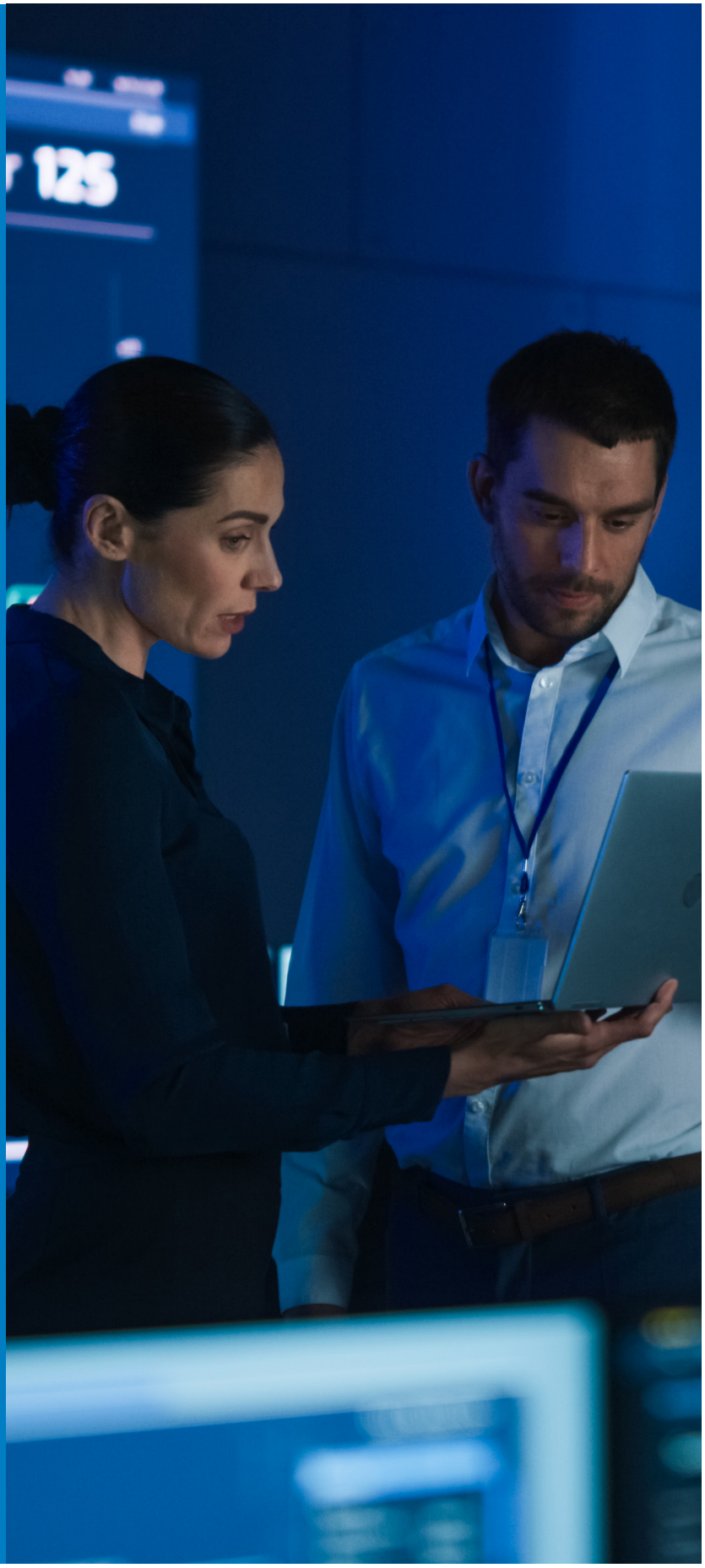
Cloud Security Architecture – An often overlooked but critical requirement:

With more of the world's computing needs moving to cloud-enabled services, organisations shifting their data and applications to cloud-based systems need to evaluate security layers and assess whether their cloud security requirements are met. The creation of cloud security architecture is a much-overlooked but critical task that needs to be performed to optimally leverage cloud technologies. According to Gartner, "by 2021, 50 % of organisations would have unknowingly exposed some IaaS storage services, network segments, applications, or APIs directly to the public internet".

Cloud security architecture involves a framework that helps understand how an enterprise defines its cloud security for each cloud-based service that it uses, and the technologies needed to create a secure environment. The architecture provides a written as well as a visual model of the structure of the security system. It provides information on how to configure and secure cloud-based activities and operations such as protecting applications and data, identity and access management, overall visibility into compliances and a window to the possible threats that the system may face.

The goal of developing cloud security architecture is to be able to detect and remove any security weaknesses from the cloud environment. There is a need to recognise the difference between cloud security controls and cloud security architecture before the move is made to cloud systems. While cloud security controls provide tactical solutions to reduce information security risks, a properly designed security architecture eliminates threats faced by the entire organisation.

Focusing on threats helps the organisation understand interrelationships between users, cloud environments, applications and service providers. It will then help in limiting redundancies in security control, thus reducing both capital and operational costs.



Cloud Security – A shared responsibility:

Before we get into the details of cloud security architecture, it is essential to acknowledge that cloud security in public clouds is a responsibility that is shared between cloud customers (the business enterprise) and cloud service providers. However, in the case of private clouds, management of security – in a comprehensive manner – can be handled by the cloud customer.

In a public cloud, it is the cloud service provider's responsibility to secure the infrastructure i.e., software, routers, switches, firewalls, storage networks, directory services, management controls, cloud API, etc. The customer is responsible for the overall protection of the stored data and its access. These responsibilities would differ slightly depending on which service is being deployed i.e., IaaS, SaaS, or PaaS.

The cloud security architecture type is key for the determination of the service model.

Since a lot of the threats and issues depend on the service model that is being used, the type of security architecture also needs to vary.

Software as a Service (SaaS):

In this model, the customer's responsibility is limited to the management of the security associated with accessing the software while the provider takes care of the security protocol at the backend. Salesforce and Microsoft 365 are prime examples here. In the case of SaaS applications, phishing is a significant threat where attackers try to gain access by stealing login credentials from customers. Similarly, credential exposure and insider threats are also concerns that come with using SaaS.

Infrastructure as a Service (IaaS):

Here, where infrastructure is purchased from a cloud computing services provider, e.g., Azure, the security threats are similar to any on-premises vulnerabilities like malware, insider threats, and credential exposure. Customers are responsible for the security associated with anything they install on the infrastructure which includes operating systems, applications and middleware. In this case an appropriate security strategy would be one where layers of security are created involving standard security tools, cloud-specific tools, access management, data encryption and network encryption.

Platform as a Service (PaaS):

Organisations use PaaS to acquire a platform from a cloud provider and only have to manage, run, and develop applications, without having to manage or develop the platform infrastructure required. Amazon Web Services (AWS) is a leading service provider in this sector. Threats, in PaaS, are mostly caused by customers themselves by either using defaults in application configurations that expose them to external threats or by giving permissions haphazardly leading to unauthorised access to the systems. Security requirements in this model involve cloud-style and non-standard security applications.

With all these service models, there are several cloud security challenges that exist:

- Identity and Access: Since cloud systems are not secured by default, it is easy to create and leave resources unattended. While all cloud providers offer robust identity and access management security systems, businesses need to set them up and apply them correctly across all resources.
- Unsecured APIs: APIs are either not secured enough or use weak authentication, leading to them being left wide open and allowing access to attackers to take over the environments.
- Misconfiguration: Cloud environments have a vast number of resources e.g., storage buckets, databases, serverless functions, etc. If these resources are misconfigured then they are vulnerable to attack through public networks leading to data being compromised and damage to critical systems.

- Compliance risks: The cloud provider and security architecture must allow for all relevant compliance requirements and fulfilment of compliance obligations.
- Invisible control plane: When it comes to PaaS, the control plane needs to be secured. While the provider offers management of the implementation of applications, identity infrastructure, etc., the customer is responsible for securely configuring the control plane.

The seven commandments to consider for an effective cloud security architecture:

Whether you are migrating already existing applications to the cloud or building them in a PaaS like Amazon Web Services, the design of the cloud infrastructure needs to include robust security architecture as well.

In order to do that, there are 7 key elements to be considered before embarking on a cloud journey:

1. **Build security at every layer:** Since there are several layers of individual security technologies that need to be selected and deployed, it would be best to ensure that each layer is "self-defending" so as to have an in-depth defence structure. This would mean automatic updates on operating systems, secure coding and monitoring logs.
2. **Centralised management of components:** This is the practice of taking multiple components and tools deployed in the cloud infrastructure and managing them through a centralised system of processes and personnel. This ensures a comprehensive and unified view of the cloud security status and also ensures efficiency.
3. **Design for redundancies in case of failures:** A disaster recovery plan is mandatory despite how robust we think our cloud security infrastructure is. It is critical especially given the increasing incidents of ransomware attacks and other security failures. This includes maintaining backups which can be used to resume full operational capacity. It also includes having resiliency built into all components, especially those that need to be online constantly.
4. **Design for elasticity and scalability:** While building the architecture, the design should be made keeping in mind scalability options in terms of the horizontal or vertical scale. Horizontal scaling and elasticity ensure that additional servers can be added as per business requirements. Vertical scaling allows for resizing of the servers. Increasing the capacity of hardware or software can be taken care of by increasing the number of resources.
5. **Alerting and notifications:** All cloud components need to be interacting precisely as intended with each other for alerts and notifications to function in an error-free manner. Should security events or operational issues arise, having information logs helps in tackling and mitigating them.
6. **Appropriate storage for deployments:** Choosing the right kind of storage options based on the organisations' needs is imperative while designing cloud security architecture. The type that is chosen has to take into consideration the organisation's data security strategies and policies.
7. **Centralisation, Standardisation and Automation:** Last, but not least, integrating tools into a single dashboard to provide visibility to those managing cloud resources, standardising consistent security models across all services and automation of security controls are all needed to be able to run a robust cloud security system.

In Conclusion:

Designing and developing robust cloud security architecture systems is no easy task. As with any new technology, there are several challenges to be overcome. However, once the organization's security policies, compliance guidelines and best practices are taken care of, the benefits to the security strategy and overall organisation strategy are well worth the effort.

* For organizations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed on organizational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive, yet modular suite of services is doing exactly that. Equipping **organizations with intuitive decision**-making automatically at scale, actionable insights based on real-time solutions, anytime/anywhere experience, and in-depth data visibility across functions leading to hyper-productivity, Live Enterprise is building connected organizations that are innovating collaboratively for the future.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next