Cloud security in no man's land

wipro

Cloud technology has carved its way into executive level business conversations and has seen acceptance as an essential element in strategic decisions. Safe to say, the Cloud is becoming a foundational pillar of business innovation and most promising innovations see success when the ecosystem provides the required and apt technology platform.

However, the recent past has borne witness to multiple data breaches affecting enterprises, industries and government agencies. A common attribute of these data breaches is a direct or indirect reference to the Cloud platform. This raises critical questions about the viability of innovations on Cloud platforms.

The crux of the problem lies in the perception of security for Cloud computing. In principle, Cloud security is beyond traditional security and slices across all layers of software-defined network (virtual memory, virtual storage, virtual computing power, and virtual interfaces). Here we highlight 10 Cloud security specific principles.

- **The Cloud security role is amalgamated** – In data breaches, many times fraudsters can download data stored in the Cloud storage, due to a slip from the resource administrator during access restriction configuration. Cloud platforms do not have a separate role for security administration. The Cloud security role is an amalgamation of multi-functional roles. The security configuration in the Cloud is designed to be part of different functional roles like firewalling, identity, access control, audit logging, encryption, and other policy.

  Therefore, Cloud admins should adapt and begin performing security configurations.

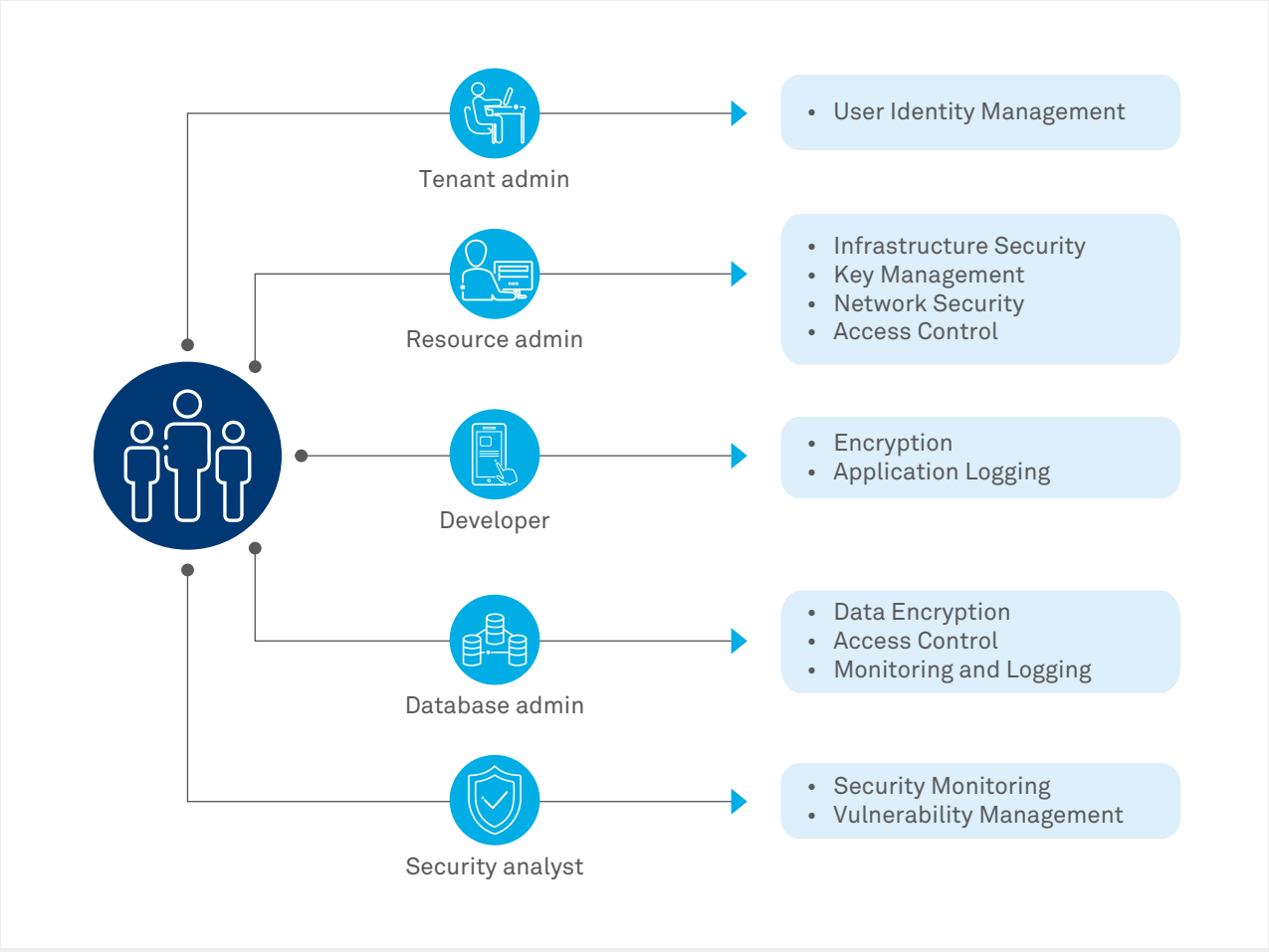

Figure 1: Security roles played by different administrators in the cloud

Any resource deployed in the Cloud is available to anyone on the Internet unless the resource is logically segregated with appropriate access restriction and permissions.

- **The Cloud is under continuous scrutiny** – Cloud providers publish their Cloud platform public IP subnet range to enable their Cloud customer's connectivity configuration and troubleshooting. However, this information is a treasure trove for fraudsters, bug bounty hunters and professional security research companies, who feed this information to automated BOTS, which continually scan Cloud platforms to identify resources with weak configurations, vulnerable software versions, open API and hard-coded credentials for different motives and vested interests for monitoring. Once fraudsters identify the object of interest, they attempt to gather information hosted in the Cloud resource and, based on the value of information, may choose a further course of action with the information owner.

- **The Cloud has zero-tolerance to errors and misconfiguration**s – An error or misconfiguration is what fraudsters are continuously perusing in the Cloud infrastructure. Once they find a suitable flaw, they exploit it as a passageway, resulting in a massive breach. In many data breaches, a simple misconfiguration of enabling public view in the Cloud storage has disclosed hugely sensitive information to an unauthorized entity. The administrator performing the task should be the subject matter expert in the platform and implement it as per the design. After configuration, the security analyst can use the Cloud Platform Security Risk Evaluator to check for any misconfiguration (example: Amazon AWS "Trusted Advisor" and Microsoft – "Azure Security Center").

- **The Cloud is ubiquitous** – Cloud technology is designed to be accessible to anyone via the Internet from any device. While designing the solution, the Security Architect should provide the highest consideration to manage this ubiquity. If not, this could prove costly later leading to security issues. Any resource deployed in the Cloud is available to anyone on the Internet unless the resource is logically segregated with appropriate access restriction and permissions.

- **The Cloud has inbuilt security features, sweat them all** – Cloud platforms provide adequate security features. However, in several instances, administrators fail to leverage these features due to lack of awareness. Non-usage of these features could become easy access for an attack. Only after exhausting all the features and if residual risk is higher than the acceptable appetite, administrators should look for additional security solutions. For example, if the application is hosted in IAAS server and is using Cloud storage for storing images, then Cloud storage bucket should have access enabled only from the application server and restrict all other access.

- **Death by password** – Account hijacking is one of the most prominent Cloud threats. If the Cloud resource is protected by a password alone, the data residing is highly vulnerable and could be a potential target. Identity and access control in the Cloud needs an additional layer of protection besides the traditional password-based control. The additional control could range from a simple access control to complex solutions such as Multiple Factor Adaptive Authentication.

- **Before deploying, know what you should be doing** – The Cloud is unforgiving if the administrator uses trial and error for configuring access, connectivity, privilege, etc. A hacker needs just a small window of time and a weak configuration to make a pathway inside your Cloud resource. All required security controls should be implemented before deploying the resources.

- **Cloud is plug-and-play, but Cloud security is not** – Application developers are spoilt for choice when it comes to the Cloud platform, components, functions from multiple providers for their requirements. However, Cloud security is not as simple plug-and-play—it is hence not necessarily considered when designing the solution, and must be incorporated ahead in the design cycle, and implemented in every individual element of the overall solution.

- **Cloud security gives no second chances, do it right the first-time** – Cloud resources deployed without the right security configurations will be gone in 60 seconds, leaving no room for a second time. Cybercriminals have developed innovative ways to exploit any weaknesses. Early this year criminals targeted unprotected MongoDB, wherein the attacker could excavate the entire data stored in the DB and demand ransom for data restoration. Cloud security needs a different thought process from conventional security.

- **Don't blink** – Cloud requires deeper and broader monitoring compared to traditional IT resources. The Cloud is a very dynamic environment; constant monitoring helps in understanding the environment better and provides insights into the tenant/subscription. Cyber threats perceived in the Cloud are very different from traditional IT resources. Constant monitoring is mandatory to ensure all vital signs are healthy and no control is relaxed for convenience.

Let us make Cloud security contiguous and breach a thing of the past. To make Cloud security contiguous, security practitioners should adopt new approaches such as building a federated model for Cloud security administration, strengthening roles & responsibilities for developers, system administrators, and business analysts, continually training all stakeholders for performing security roles, and revisiting existing processes to incorporate the new set of Cloud security principles. Doing so will ensure that business innovation can be secure, and at a lightning pace.

About the author

Sridhar Govardhan
General Manager and Head of Cyber Security, Wipro

His core competency accumulated over 18 years of professional experience are in the business critical domain of Cyber Defense, Information Protection and Regulatory Compliance. He has a proven track record of spearheading organizational initiatives in building self-defensible network, Cloud security and enabling employee mindset in security and productivity.

Sridhar acquired eleven industry-recognized certification in the domain of IT, information security, security framework and secure enterprise architecture (SABSA, CISA, CISM). He holds a Bachelor's engineering degree and M. Tech from BITS Pilani and has a two patents (pending) in the area of Cognitive Security.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/B&T/DEC2017-MAY2018