Oracle Perspective: The Rise of the Cloud Security Architect

Greg Jensen, Senior Principal Director - Security, Oracle Corporation

Organizations often look for where they can make the single greatest impact to improve their organization's security posture. As organizations are adjusting their priorities around a cloud-centric strategy, one position has stood out as one of the most central and strategic in meeting security and compliance milestones—the Cloud Security Architect (CSA).

So, what are CSAs, and how do they compare to a security architect? Traditional security architects often focus on broad-reaching security topics that impact the on-premises, mobile, and even cloud world. Over the years, this role has become a bit of a "Jack of all trades" role. The CSA was created to be the "master of cloud security" who understands every possible security and compliance related challenge that a line of business (LoB) owner or infrastructure, platform, or app team could run into when deploying new cloud services. This has led us to a point where we are seeing the role of the CSA surpass the security architect in popularity, according to the *Oracle and KPMG Cloud Threat Report, 2018.*

In the most generalist terms, an *architect* plans, designs, and constructs structures. In Information Technology terms, it is very similar when applied to cloud security. The CSA is responsible for:

- Reviewing the security posture of all SaaS, PaaS, and IaaS projects for industry best practices.
- Identifying risks where security requirements cannot be fully addressed in the timeframe of a project.
- Looking for opportunities where security can be optimized and enhanced.
- Ensuring policies and mechanisms are in place to meet compliance requirements across the cloud.

CSAs are facing increased pressure to balance LoB requirements with corporate security guidelines, and those goals often clash due to time pressure, resources, or budget. Organizations are in a rush to roll out more applications and workloads to the cloud, often with multiple cloud service providers, each with their own SLAs. Every cloud service provider responds to vulnerabilities and incidents differently. The CSA can play an important role in identifying shortcomings from each vendor to understand points of risk, and then develop plans to address them with the provider or internal teams.

ORACLE

The Cloud Security Architect Toolkit

The CSA is under intense pressure to have constant visibility and metrics behind organizations' use of sanctioned cloud resources, as well as visibility into user behavior with unsanctioned applications.

Every day, more organizations are being infected with cryptocurrency malware, turning unsuspicious application servers or cloud applications into hosted platforms for cryptocurrency mining attacks. Few are aware of this unless they see the traffic impacts on Network Performance Monitoring (NPM) tools or Application Performance Monitoring (APM) tools feeding into the Security Operations Center. Forty-eight percent of respondents in the *Oracle and KPMG Cloud Threat Report, 2018* cited that they are now using APM/NPM event feeds to identify threats.

CSAs also are reaching for tools such as Cloud Access Security Brokers (CASB) to help identify all the cloud applications in use, apply a risk score on users, and recommend remediation plans when suspicious activities are identified.

For more information on ways Oracle can enable your CSA or IT security strategies, visit us at www.oracle.com/security

One of the key challenges is balancing the security and compliance needs between an organization's hybrid and multi-cloud environments. One approach that some organizations are focused on is the single vendor model that uses a tightly integrated framework across the full stack of cloud services (DaaS, SaaS, PaaS, and IaaS), which many argue reduces risk and points of exposure. The single vendor approach often lends itself to the challenges of securing an organization once, and enabling them to scale as they need. Key criteria CSAs should look for in a cloud service provider include:

- **Comprehensive** – Secure users, apps, data, and infrastructure across the full cloud stack (DaaS, SaaS, PaaS, and IaaS).
- **Automated** – Detect, prevent, predict, and respond to the latest security threats with AI and machine learning.
- **Data-centric** – Control access to sensitive, regulated data using encryption, masking, and user access controls.
- **Unified** – Collect security and operational data in a single data set to correlate and analyze cyber threats.
- **Integrated** – Developed, architected, deployed, and maintained to securely work together.

The role of the CSA is as strategic as the cloud vendors chosen to underpin and secure that cloud architecture. Oracle and KPMG have a longstanding history of supporting our customers with solutions that meet the very challenges facing today's CSA.

For more information on Oracle security solutions, please visit **www.oracle.com/security.**