ANOMALIX

ANOMALIX
WHITE PAPER
Securing The Cloud

Securing The Cloud

Aggressive initiatives are in place across all industries to move as much functionality as possible from the data center to the cloud. IT departments are facing tight and cost-conscious stakeholders as they attempt to keep the business running while they "shift and lift" and develop net-new applications in the cloud. Unfortunately, this usually means security, governance, and compliance may not get the proper attention that they need. The dynamic nature of the modern cloud architecture limits the traditional agent and proxy-based solutions utilized by legacy security products.

Tools such as SIEM solutions don't support cloud infrastructure or API activity, leaving most organizations with a blind spot when it comes to cloud environment security. While Amazon, Microsoft, and Google take care of security for their data centers and the physical server hardware the virtual machines run on, there is a misconception that the cloud service provider bears the responsibility for fully securing the cloud environment. Customers are ultimately responsible for protecting the components, virtual machines, applications and data deployed in their cloud environments. Misconfiguration can present a greater risk of compromise than any other attack vector. Cloud Security Challenges Security begins with visibility. Most organizations struggle to create a holistic view into user access permissions, resource inventories such as servers and databases, API traffic and user activity within their public cloud infrastructure.

Other common issues customers face in the cloud include:

- **Managing outbound traffic** - common mistakes include failing to lock down resources, exposing workloads that can accept traffic from any IP or port
- **Limit your exposure** - a best practice is to ensure only load balancers and bastion hosts are exposed to the Internet
- **Limit SSH connections** – limiting SSH traffic from both external and internal sources is key to controlling a critical attack vector
- **Root/organization owner accounts** - these accounts should never be used directly; they should be used to create new accounts with assigned (least privilege) access

While cloud providers offer identity and access control tools, most organization lack the corresponding policies that determine the minimum set of privileges to job responsibilities. Furthermore, security groups are not typically built with the least privilege model in mind, as the access required is often wide ranging. Finally, turning on security logging and monitoring is imperative as it will provide visibility to unauthorized access attempts, access/permission usage, API call information, and configuration deployment events.

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144