ANOMALIX

ANOMALIX WHITE PAPER

Why IAM and Network Security are Critical for Cloud Applications

Why IAM and Network Security are Critical for Cloud Applications

Credential theft attacks are the number one attack vector that malicious internet actors use to compromise cloud resources such as applications and data, according to the 2018 Verizon Data Breach Investigations Report.1 These attempts to gain access include phishing campaigns and botnets targeting organizational customers, employees, contractors, and partners that compromise personal devices with malware to capture login details for authenticated networks, applications and resources.

Due to this increasing credential theft threat activity by hackers, Identity and Access Management (IAM) is quickly becoming a critical component of all security programs to ensure the safety and integrity of applications as well as public or private cloud resources.

And considering today's cyber-threat landscape overall, Microsoft has recently defined "Identity as the new perimeter" stating that the adoption of decentralized corporate networks and cloud computing combined with the popularity of bring-your-own-device (BYOD) to work makes the idea of a traditional corporate network perimeter relatively obsolete.

Managing cyber risk in the cloud today necessitates IAM as a primary focus of any modern application migration strategy so that organizations can establish a secure, identity-driven perimeter to protect employees and ensure business productivity and continuity.

The Evolution of Application Security and Security DevOps

Traditional application security encompasses web application firewalls, enterprise application security, database security, email security, web browser security, and mobile app security. When adding public cloud application security, VM security, microservices security, and IoT security to the mix, the application security landscape appears more complex than ever. Not to mention server-less and containerized app development within hybrid environments adds additional layers of security concerns. Furthermore, when migrating workloads to the cloud, legacy applications must also be upgraded or re-factored to meet public or hybrid cloud security requirements.

Application Developers and DevOps personnel are granted more flexibility in public cloud operating models than within a traditional on-premise model. Applications and Data are fluid and often unrestricted in terms of replication and movement. The integrity of resource access and permission configuration is often unchecked and not subject to a zero-trust standard.

According to McKinsey, “existing applications will need to be refactored at the infrastructure and application layers to align with the security and capacity requirements of the public cloud. Security must be baked into these applications, and they must work in a more automated fashion. This requires significant attention from application teams, which can be hard to get.”

The security risk and impact of cloud computing models and a fluid workforce has upended traditional application security paradigms forcing organizations to re-think and re-engineer their technology environments. The application perimeter is now anywhere an access request is made from anywhere and on any device.

To mitigate the security risks created by this new work environment, organizations are beginning to adopt IT architectures that move access control decisions from the network perimeter to individual devices, users, and applications, where business-driven security policies and access controls are best enforced. The model must continue to support total visibility into access that is business or compliance relevant.

Identity Management Best Practices

Adopting modern IAM solutions offer many security benefits when migrating applications to the cloud. Many cloud providers such as Amazon Web Services, Microsoft Azure and Google Cloud provide IAM service functionality that makes it easier to provide secure access to employee applications either on-premises or in the cloud. However, there is still a lack of central visibility into all resource access a given account may have. The use of external authentication/authorization via directories and group memberships can compound the complexity of correlating all the access objects (and ultimately resource access) that a given account has access to directly or indirectly.

At the center of Microsoft’s cloud-based identity and access management service, for example, is Azure Active Directory (Azure AD). Azure AD helps organizational users sign in and access both protected external resources such as Microsoft Office 365, the Azure portal, and third-party SaaS-based applications as well as internal or on-premises applications and resources on corporate networks and intranets. Many public cloud consumers rely heavily on Azure AD to grant access to cloud resources in AWS.

Public cloud providers also lack the ability to graphically display access relationships, such as “Who Has Access to What?” and “Who’s Communicating with my Resources?” AWS, Azure and Google Cloud do not provide the ability to see and manage access across public cloud platforms. A better approach is needed to establish central visibility, control and monitoring of access to resources and data within a public cloud operating model.

Identity and Access Management in the Public Cloud

In addition to IAM best practices, identity automation management and governance provide methods for provisioning, deprovisioning, and compliance throughout the identity lifecycle. Governance utilizing IAM provisioning and deprovisioning based on policies such as Azure AD Conditional Access is key for compliance with regard to identity and privacy regulations such as GDPR in Europe, for instance.

Additional examples of automated IAM provisioning and de-provisioning include revoking access privileges for employees leaving a company or on-boarding new employees. Reporting an employee's departure from a company and then having the IT department automatically deprovision their access across all apps, services, and devices increase organizational productivity as well as security.

Defining security conditions with regard to both devices and applications that can access information from a network through conditional access policy enforcement in an automated fashion helps organizations scale their security and compliance needs when dealing with thousands or even tens of thousands of users.

Because large organizations today may spend thousands or even tens of thousands of IT staff hours for manual access provisioning and deprovisioning, deploying IAM solutions are increasingly becoming critical for not only enterprise security but also productivity.

Automated IAM provisioning and deprovisioning can also enable IT managers to reallocate their time to other value-added IT responsibilities to ensure organizational security.

Real-time Network Security and Compliance Management

Knowing who or what is communicating with your applications and data is extremely critical to identify normal and outlier behavior. Within Public Cloud infrastructures, the autonomy afforded to application developers and DevOps personnel is unprecedented.

Understanding who and what is communicating with your applications, resources, and data is challenging to identify and manage within public cloud environments. Establishing a baseline of communication patterns is essential to identify new and suspicious connections, whether it's potential lateral movement or access from blacklist IPs.

A real-time analysis and action plan are required to identify and remediate the real threats as they emerge. Network access administration is also primarily tied to the least privileged infrastructure configuration standards. Locking down non-essential ports and restricting access by IP has helped to reduce backdoor loopholes that can be easily exploited to gain access to business and customer information.

Conclusion

idGenius public cloud protection enables threat defense and continuous compliance assurance. idGenius Total Cloud Protection Platform leverages next-generation AI and machine learning to identify, correlate, and monitor and audit security and compliance activity. With idGenius, organizations are empowered to govern security and enable security operations across public cloud environments such as AWS, Microsoft Azure, and Google Cloud Platform.

idGenius is a cloud native Software-as-a-Service (SaaS) solution that addresses cloud security scenarios relating to Visibility, Security Governance, Compliance Assurance. The business value derived from idGenius includes reduced financial risk due to security breaches, reduced cost of compliance reporting as well as reduced security operations associated with manual and redundant activity.

ANOMALIX

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

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