ARTICLE

Automating Cloud Security

Netmagic multicloud security environment helps to create a strong, durable and scalable security state for the enterprise. In a multi-cloud world, enterprises are struggling to ensure security. Here's how automation can help

Rishikesh Kamat
Vice President Product Management
NTT Global Data Centers and
Cloud Infrastructure, India
(erstwhile NTT-Netmagic)

In a multi-cloud world, enterprises are struggling to ensure security. Here is how automation can help

In a multi-cloud world, many enterprises are finding it difficult to monitor and secure different cloud-based systems, as there is no single point of control to monitor security and compliance. Many enterprises also make the mistake of assuming that the existing system and application-centric security controls that are prevalent for the on-premise infrastructure, will be applicable for the cloud too. This creates risks and makes organizations vulnerable, as the same solution may not work in a cloud-based world. Additionally, patching and configuration management across different systems is hence extremely challenging.

When multiple cloud-systems are used, human errors can go up significantly. One of the most common forms of human errors that can expose organizations to security risks is misconfiguration.

In a recent report on cloud security, Trend Micro said that on an average, 230 million cloud misconfigurations were found each day.

Misconfiguration is just one component of inadequate cloud security. Besides misconfiguration, the Cloud Security Alliance, lists ten more threats to cloud computing. These include: data breaches, lack of cloud architecture and security, Insufficient Identity, Credential, Access and Key Management; Account Hijacking; Insider Threats; Insecure Interfaces and APIs; Weak Control Plane; Metastructure and Applistructure Failures; Limited Cloud Usage Visibility and Abuse and Nefarious Use of Cloud Services.

While most public cloud providers have robust security measures, the customers are responsible for securing applications or databases that they put on top of the cloud platform. For example, misconfiguration happens when cloud computing assets are unsecured. This could mean default credentials left unchanged or excessive permissions being granted. In addition, many organizations make the mistake of assuming that assuming that the same settings that work onsite will work in a cloud environment. Gartner has hence, rightly, put the onus of security on the customer. Gartner says that, “Through 2022, at least 95% of cloud security failures will be the customer’s fault.”. Hence, it is necessary for organizations to take a proactive approach towards cloud security.

An automated approach to cloud security

Given the scale and pace of cloud deployments, many enterprises feel overwhelmed to manage and secure dynamic cloud deployments. This is where automation can help. Cloud automation can help in enforcing best practices and compliance, so that any human errors that may have inadvertently resulted in the infrastructure being insecure are corrected. This also means that security engineers do not have to manually configure different firewalls, access points, networks etc.

Ensure continuous checking of security vulnerabilities

In this age of zero day vulnerabilities, it is common to find organizations scrambling to patch their servers or virtual instances across thousands of servers. Traditionally, this would mean a software or systems engineer working frantically to patch each and every server across many hours or days. For example, when the Heartbleed vulnerability was discovered way back in 2014, it left many engineers scrambling to update SSL across thousands of virtual servers. In such cases, automation can help in updating servers quickly by simply running an automation script. This makes it possible for even a small team or security engineers to quickly respond to a security threat.

Improving visibility across multiple clouds

Automation tools can help in bringing in an unified approach for monitoring multiple clouds. Enterprises can also visualize on how a small configuration change can increase the security risks for all associated elements. With a complete 360° view of multiple clouds, enterprises can use cloud automation tools to automate reporting, detect intrusion attempts and use governance features to stay compliant with respect to different regulatory requirements.

Ensuring secure access

Identity is the core foundation for all security controls, and hence automation is extremely crucial in enabling secure access across multiple clouds. An automated cloud management tool can help in enforcing and configuring permissions based on roles rather than individual users.

Enforce security best practices

Cloud automation tools can be used to define custom security policies and compliance rules specific to unique business, cloud environment, or application needs.

Address misconfigurations with automated actions

Organizations can reduce security risks by auto-remediating new violations with alerts that help developers avoid critical mistakes. Developers can also understand application security in a better way by gaining access to cloud misconfiguration insights within their development platforms. Automated reporting can help developers get a better understanding of security risks, and help them be more compliant with different regulations and security practices.

In summary, cloud security automation can make a huge difference in three important aspects, **Standardization** (Automation can help in ensuring security in a streamlined and consistent manner); **Efficiency** (Cloud security automation can help organizations scan and test multiple server instances for security vulnerabilities with high accuracy rates) and **Scalability** (Automation can help organizations scale up security tests and patch updates without an appropriate increase in manpower).

For organizations looking to automate cloud security, identity and access management (IAM) is one of the key areas where automation can provide a lot of value and reduce security risks. The other big use case can be seen in the case of patching, where automation can help in patching a lot of servers without manual intervention. Using behavioral analysis tools, automation can also help in analyzing the network and responding to an attack quickly -- this is extremely useful in the case of detecting zero-day attacks. More importantly, automation can also help in quickly bringing up another site as part of a disaster recovery plan, if the first site is hit by ransomware or cyberattacks.

Cloud security automation can also help in detection, alerting key people, remediation, taking counter measures and forensics. For example, using an automated cloud security tool, you could run a bot that does continuous compliance monitoring, compliance reporting and security automation. The insights discovered by the bot can be validated against a set of pre-defined policies to confirm policy adherence.

As one can see, cloud automation tools can help in driving alignment across teams and build a shared understanding of security risks and violations. Cloud automation helps in ensuring continuous security and compliance and using real-time insights to proactively fix security vulnerabilities in a scalable and accurate manner.