netskope

White Paper +

Five Key Considerations for Protecting Enterprise Data in AWS

Security in the public cloud is based on the concept of shared responsibility, which means the cloud service provider is responsible for the security of its infrastructure and the customer is responsible for the data and applications that run on that infrastructure.

Increasingly, enterprises are using Amazon Web Services (AWS) as part of their cloud strategy. According to the latest estimates from Synergy Research Group, Amazon's share of the worldwide cloud infrastructure market has risen to 34%, which exceeds the combined market share of its two largest competitors, Microsoft Azure (21%) and Google Cloud (10%).

AWS provides a secure platform for companies to store and process data, run existing applications, and develop new ones. But it's the customer's job to watch out for unauthorized access, security misconfigurations, data exfiltration, malware, and compliance violations.

Despite their best efforts, it's not always easy for enterprise IT and security practitioners to get their arms around everything that's happening in the cloud, particularly as business units rapidly (and sometimes surreptitiously) migrate applications to the cloud, and developers shift to a cloud-first model for new applications.

Most enterprises come to the realization that as the number of applications and amount of data in their cloud grows, securing cloud deployments may not be as easy as they had envisioned. This is when a third-party security vendor like Netskope can help to enhance visibility and strengthen security posture. Netskope offers a portfolio of tightly integrated security products aimed at securing cloud environments, protecting data, and maintaining compliance.

Here are the top five considerations that enterprises should focus on when protecting data and applications running on AWS:

1. Security Posture Management

By most estimates, 80% of enterprise data now resides in the cloud, so that's where attackers are focusing their attention. Forensic analysis of cloud data breaches often points to simple misconfiguration errors as the root cause. By deploying cloud security posture management (CSPM), organizations can discover which types of data assets are stored in which cloud-based accounts and evaluate how well those assets are being protected. CSPM can also detect malware or vulnerabilities, determine if policies are meeting compliance standards, identify what steps need to be taken to remediate any misconfiguration issues, and implement automated remediation where possible.

CSPM tools help to protect cloud resources by benchmarking configuration settings against corporate policies, regulatory compliance rules, and security best practices. They alert security teams to policy violations such as Amazon S3 buckets that are publicly accessible, or data at rest that is not properly encrypted. They can also help to prevent risky network exposures and simplify regulatory compliance activities. And crucially, CSPM tools provide continuous monitoring to spot any new configuration errors that can crop up in dynamic and rapidly changing cloud environments.

Organizations should look for cloud security posture management systems that have broad out-of-the-box capabilities and are easily customizable for specific use cases.

2. Data Security

The next step is drilling down into the data itself. A large organization will undoubtedly have data stored in several, or even hundreds, of AWS accounts. Organizations need to conduct comprehensive, continuous scans of all cloud data repositories to satisfy a wide variety of concerns, such as whether sensitive data is stored in properly configured S3 buckets, whether personally identifiable information data is encrypted, and whether there are systems in place to control data movement and block data exfiltration.

Other critical questions to ask include: Is my data being continuously protected against malware and ransomware attacks? Do my data storage practices meet compliance requirements? Are my cloud data security policies properly aligned with my on-premises data security policies?

To address these concerns, organizations need to deploy storage scanning and data loss prevention (DLP) tools that enable continuous data discovery and protection. Cloud access security brokers (CASBs) that offer both application programming interface and in-line protections tightly integrated with DLP technologies are ideal partners. Organizations should look for DLP systems with advanced features such as optical character recognition and machine learning that can identify and prevent all types of data from being exfiltrated, including images or screenshots of whiteboarded information. They should also look for threat protection systems that use sandboxing techniques to conduct deep malware scanning.

3. Shadow IT Discovery

Security teams have their hands full protecting data in the cloud they know about. But what about cloud provider accounts that IT isn't even aware of – those business-led cloud accounts, also known as shadow IT? Most of the time these accounts represent legitimate business uses that are being paid for with a company credit card. But business teams don't always go through the proper IT channels to get the cloud resources they need—for example, when strict security requirements might delay or complicate a crucial project. In other cases, a software developer might spin up their own account on a personal credit card. This creates the potential for abuse of the account, along with accidental or intentional data leakage.

Be sure to choose inline cloud protection tools that have the ability to scan all traffic moving in and out of cloud accounts and differentiate between corporate and personal accounts.

In the case of legitimate business use cases, visibility allows IT to apply proper security controls. In the case of personal accounts, IT can block movement of sensitive data from managed accounts and resources and require the developer to comply with company security policies.

The result is that the security teams gain visibility into everything happening in the AWS cloud and can ensure data protection policies are applied across all accounts and resources.

4. Intelligent, Layered Defenses

Most organizations recognize the value of a security posture based on defense in-depth—the idea that there is value in having multiple, complementary tools working together to prevent attacks, as long as they can be managed from a single console. In addition to security posture management, data and threat protection, and shadow IT controls, organizations should adopt specific systems to limit access to data and applications by unauthorized users and to prevent movement of sensitive data to unmanaged cloud infrastructure and accounts.

In this scenario, there might be a contractor who needs access to specific applications or data sets. But how do you make sure the contractor doesn't access other accounts, leak data, or make unauthorized lateral movements to adjacent infrastructure and resources?

Organizations need to implement and enforce strict data movement and data access policies for all cloud-based accounts. This provides another layer of protection to help identify if there are any gaps in cloud-based identity and access control systems.

Netskope protects against insider threats such as data exfiltration, compromised credentials, and malware with its advanced user and entity behavior analytics service. Netskope's advanced threat protection capabilities can identify and prevent bulk downloads and mirroring of data from managed to unmanaged accounts via the AWS console.

5. Private Application Protection

When companies develop new applications in the AWS cloud, it's important to apply granular access controls to make sure only authorized users can gain access. By implementing zero trust network access (ZTNA) principles, access is denied by default, and all users need to successfully authenticate before they can gain access to private applications. Authorized employees are only able to access the apps and data necessary to do their jobs.

Organizations seeking to address these five important considerations should consider one vendor who can provide a comprehensive cloud security platform, rather than deploying point products that need to be managed separately.

HOW NETSKOPE HELPS

Netskope can assist organizations at all levels of cloud usage and security maturity with cloud security, data protection, and compliance needs. It can help enterprises discover misconfigurations and policy violations in more than 270 AWS services, detect malware and sensitive data in S3 buckets, and block data exfiltration and threats such as malware and lateral movement in real-time.

For example, Zip, a fintech firm based in Australia, was looking for a platform to centralize security management, protect sensitive data in the cloud, and improve the user experience for its remote workers.

Zip selected Netskope to provide a comprehensive solution that included an inline CASB with built-in threat detection and DLP, a secure Web gateway, and ZTNA, all delivered as a cloud-based security service edge (SSE).

Netskope has enabled Zip to replace disparate security tools with a single platform and to provide secure access to AWS resources for remote workers, which proved critical during the recent pandemic.

CONCLUSION

To secure data and applications in the AWS cloud, organizations need to know the location and exposure level of sensitive data, identify misconfigurations and threats, and take quick action to protect critical data and services.

This may sound straightforward, but implementation can rapidly become complex for companies managing hundreds of AWS accounts with thousands of resources. Third-party vendors with specific knowledge and expertise with AWS can help to quickly improve visibility, identify any security gaps, and maintain compliance.

Netskope has been named a leader in Gartner's first-ever Magic Quadrant ranking of SSE vendors. Gartner reports that Netskope's strengths are its strong service-level agreements for uptime and latency, its advanced data security capabilities, and its "modular cloud-native platform hosted on its in-house built cloud infrastructure."

The Netskope Security Cloud is an SSE architecture designed to provide secure access to IaaS, SaaS, web, and private applications, whether running on-premises or in AWS. The Netskope Security Cloud delivers secure access to AWS for remote workers, detects and mitigates threats, and identifies and protects sensitive data. By directing traffic from any location and any device through the Netskope Security Cloud for processing and forwarding, Netskope provides a single point of control for both data and threat protection for security admins and analysts.

To learn more about securing your AWS environment or purchasing Netskope products please visit Netskope in AWS Marketplace.

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything, visit netskope.com.