Building Secure Digital Environments with AWS

How AWS Security Services Help State & Local Governments and Educational Institutions Build Secure Cloud Environments

There are a variety of dynamic security and compliance considerations that state, local and educational (SLED) organizations must meet when they build digital environments and services, including StateRAMP and the Federal Information Security Management Act (FISMA). How can these organizations design secure and scalable cloud architectures that help them adhere to these mandates?

Here are a few ways state and local governments and educational institutions can leverage secure, scalable, low-cost IT solutions from Amazon Web Services (AWS) to build compliant cloud architectures.

1. Launch a multi-account framework with AWS Control Tower

For organizations that need to establish multiple AWS accounts, customers can deploy a multi-account framework on AWS with AWS Control Tower, which can help provide resource and security isolation for customers' AWS accounts. AWS Control Tower deploys a landing zone - a well-architected, multi-account AWS environment that is designed to be scalable and secure. This landing zone acts as the starting point from which an organization can quickly launch and deploy workloads and applications with confidence in its security and infrastructure environment.

2. Set up a scalable organization foundation with Landing Zone Accelerator

SLED customers can deploy AWS security best practices by default using Landing Zone Accelerator (LZA), an open-source project developed by AWS and available on GitHub. LZA extends the functionality of AWS Control Tower by adding additional orchestration of networking and security services within AWS. Customers can also deploy LZA independently of AWS Control Tower to support regions and partitions that are currently not yet supported by AWS Control Tower.

3. Design and maintain guardrails with service control policies

Service control policies (SCPs) help customers place preventative guardrails inside their AWS organizations to enforce policies. For example, an agency may be required to operate only within the United States. In that case, customers can apply an SCP to deny access to or from regions for an account to ensure it only uses authorized regions. Even the root principal user inside of that account cannot override actions deployed at the organizational level with an SCP. In general, customers should use SCPs for situations that are security binaries—instances of strict either/or categories. For example, customers can create and deploy an SCP that prevents users or roles in any affected account from changing the configuration of Amazon Elastic Compute Cloud (Amazon EC2) virtual private clouds (VPCs) to grant them direct access to the internet.

4. Manage access privileges with identity federation—not local IAM users

Identity and Access Management (IAM) users are considered long-term static credentials that can pose security risks. To reduce this risk, customers can establish identity federation, in which an identity provider can automatically grant or revoke access to resources based on a user's group membership. Many SLED customers already use some form of centralized identity provider, like Okta. Identity federation can allow these organizations to provide SAML-based access to their AWS environments. AWS IAM Identity Center (successor to AWS Single Sign-On) also lets customers link a federated identity source like Azure AD into a service that provides just-in-time, IAM-role-based, timebound access to important AWS resources.

Additionally, AWS IAM Access Analyzer can help reduce the risk of accidental public exposure by making sure that resources and principals can't do more than they're supposed to do. This is increasingly discussed in the context of Zero Trust. IAM Access Analyzer helps identify resources in organizations and accounts that are shared externally, validates IAM policies against best practices, and can generate more appropriate IAM policies based on access activity in AWS CloudTrail logs.

5. Develop a strategy to identify and solve for sensitive data storage requirements

As an operational best practice, state and local governments and education entities may create a strategy to identify what, where and how sensitive data - such as personally identifiable information (PII) - is stored. Customers can use Amazon Macie, a data security service that uses machine learning (ML) and pattern matching to discover and help protect sensitive data. For example, Macie can help identify sensitive data stored in an Amazon S3 location that isn't authorized to store PII. In this way, Macie can provide visibility into data security risks, enable automatic protection against those risks and help customers in maintaining their data storage compliance programs.

6. Monitor and audit for compliant configurations

- AWS offers multiple services that support customers in monitoring and enforcing compliance in their AWS environments.

- AWS Config continuously monitors and records an AWS environment's resource configurations and relationships, and evaluates these against the desired configurations.

- Customers can incorporate event-driven functions with AWS Lambda or AWS Systems Manager to facilitate immediate alerts to relevant teams, or even automatically attempt to remediate resources that deviate from the desired configuration. Plus, AWS Config rules can now support proactive compliance.

- AWS Security Hub provides a comprehensive view of the security state of an AWS environment. It can also verify the environment against security industry standards and best practices, including the Center for Internet Security (CIS) and the Payment Card Industry (PCI) Security Standards Council. Additionally, Security Hub can help identify the highest priority events that may need remediation, can aggregate alerts across all AWS accounts within multiple regions and can automatically attempt remediation on those findings.

- Customers using infrastructure as code (IaC) can use open source tools like Cfn-lint, which help detect common errors within AWS CloudFormation templates.

- Similarly, Cloudformation-Guard is an open source policy-as-code tool to enforce compliance policies for IaC deployments. For example, a customer can set up Cloudformation-Guard to detect in their CloudFormation templates that Amazon Simple Storage Service (Amazon S3) server-side encryption isn't enabled by default, before deploying the code into production.

- For customers that must meet multiple compliance standards, AWS Audit Manager helps continuously audit AWS usage to make sure it maps to established or customizable compliance requirements. AWS Audit Manager can generate reports that provide evidence of compliance to internal and external auditors.

7. Create a detection and alert strategy for effective remediation

Once a robust monitoring framework is in place, it's important to create an effective alerting system to elevate issues through the appropriate remediation channel. Managed services like Amazon GuardDuty and Amazon Inspector can help improve an environment's security posture with threat detection and automated vulnerability management capabilities, respectively—but they can also facilitate sending immediate alerts for identified events through a ticketing system, messaging channel, email address monitored by an organization's security team and more. Alerts can be sent to multiple locations based on use case.

Note that to optimize security monitoring operations for your AWS environment, it may be important to reduce the noise. The reality of security tooling is that they can generate false positives, so tune services like GuardDuty to suppress findings that aren't relevant to you.