A GUIDE TO AWS SECURITY & COMPLIANCE

How to get started using nOps to solve AWS security challengers

nOps

nOps

A Guide to AWS Security & Compliance

As businesses continue the COVID-accelerated process of moving operations into the cloud, they are grappling with security and compliance issues for their cloud-based services. Users of Amazon Web Services (AWS), one of the premier cloud providers, have access to a wide assortment of security and compliance tools.

AWS employs five pillars to ensure their frameworks are optimized and aligned with industry best-practices, and so can you and your business. We will provide an overview of AWS security and compliance efforts to teach you how to effectively monitor risk and compliance in your business operations.

AWS SECURITY

AWS has a comprehensive suite of tools that ensure the security of data and systems from central servers to user endpoints. Selecting, configuring, managing, and monitoring these services can be a time-consuming task. Fortunately for AWS users, there are third-party services available to help optimize the AWS experience and **ensure proper monitoring of your cloud infrastructure solutions.**

IDENTITY AND ACCESS MANAGEMENT

Because users are one of the primary vulnerabilities of any cloud-based application ecosystem, **AWS Identity and Access Management (IAM)** provides several identity authentication and permissions policy controls. IAM allows security and compliance personnel to assign user identities and access levels.

IAM can apply access policies, including least access privileges, which are critical in the enforcement of zero-trust policies for businesses. AWS users can also strengthen user security by requiring strong passwords, setting expiration dates, and employing multi-factor authentication where appropriate.

AWS administrators can ease sign-on burdens for users with **AWS Single Sign-On (SSO)** when security allows. SSO allows users to access multiple services, including both AWS and external services, from a single login.

AWS Organizations allows AWS users to create enterprise-level organizational units with specific roles and permissions based on service control policies. IAM and Organizations work together to ensure enforcement of proper security measures when users attempt to access company resources.

Figure 1: AWS Organizations process (from https://aws.amazon.com/organizations/)

AWS Secrets Manager provides management of identities such as database credentials, API keys, and OAuth tokens. Secrets Manager can work in conjunction with IAM policies to provide finely tailored control of roles and permissions.

NETWORK AND ENDPOINT SECURITY

AWS also has several options for securing network resources and endpoints. **AWS Firewall** Manager is a centralized console for managing firewall deployment in accordance with AWS Organizations policies. Within AWS Firewall, security personnel can apply both **AWS Network Firewall** rules and **AWS Web Application Firewall (WAF)** rules as needed.

AWS Firewall also works with **AWS Shield** to protect against distributed denial of service (DDoS) attacks. These types of attacks are becoming increasingly common, and there are important tips every organization should follow to prevent them.

CERTIFICATES AND ENCRYPTION

AWS has a suite of tools for deploying security certificates and encryption keys. **AWS Certificate Manager** oversees deployment, management, and renewal of public and private SSL/TLS certificates to help secure network communications and verify website identities. Security certificates are also an important factor in ensuring compliance with data privacy laws that have data-in-transit security restrictions.

As its name implies, **AWS Key Management Service (KMS)** helps secure data by associating permissions with cryptographic keys. KMS is a hardware-based solution, relying on FIPS 140-2 validated modules. KMS works with CloudTrail (see below) to generate key usage logs, allowing for identification and notification of anomalous or non-compliant usage.

AWS CloudHSM is a cloud-based hardware security module for deployment and management of encryption keys. CloudHSM is particularly useful when organizations are using multiple cloud service providers. These types of functions are encryption 101 for businesses, so if you're not using them, you should start today.

VULNERABILITY AND THREAT DETECTION

AWS provides tools for continuous threat monitoring and vulnerability identification. **AWS GuardDuty** monitors network activity and uses sophisticated machine learning tools to identify anomalous activity and assess potential threats. GuardDuty users can also define rules for automated threat response, minimizing potential damage and decreasing response and recovery times.

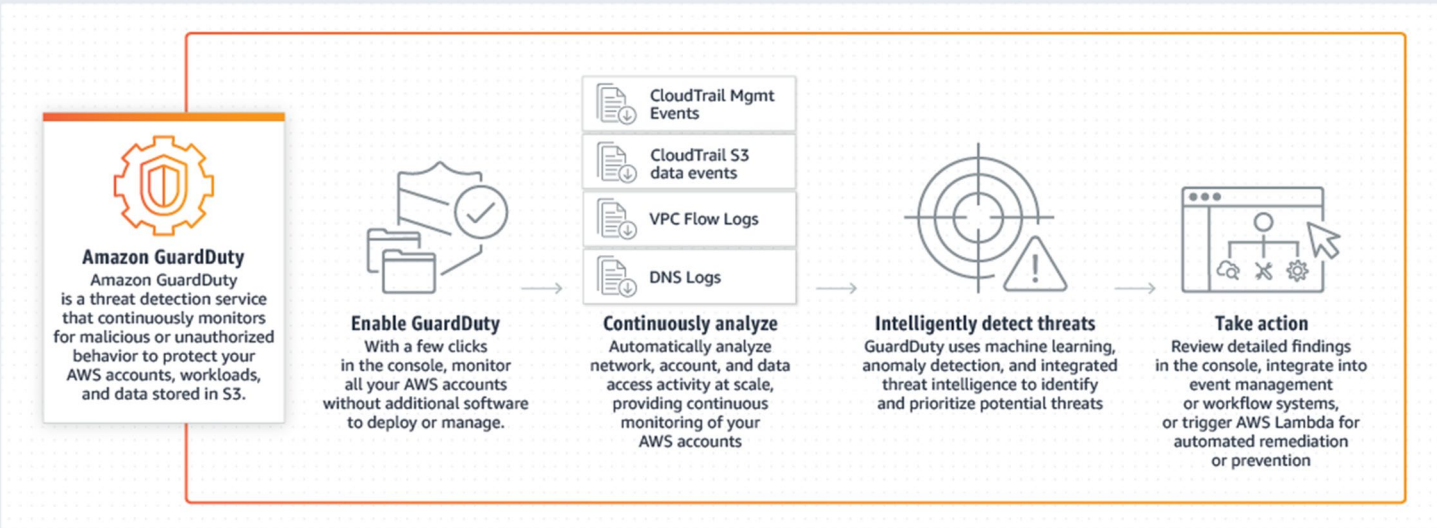


Figure 2: AWS Guard Duty Process (from https://aws.amazon.com/guardduty/)

For those using Amazon Elastic Compute Cloud (ECC), **AWS Inspector** is an agent-based tool that uses predefined rules packages to provide similar threat assessment capabilities as those in GuardDuty. There are numerous success stories about businesses using these types of systems to modernize their cybersecurity infrastructures.

SECURITY EVENT NOTIFICATION

Because of the sheer number of AWS security tools, event notifications could become burdensome with some degree of consolidation. **AWS Security Hub** aggregates notifications from many other AWS security applications - including GuardDuty, Inspector, IAM Access Analyzer, Macie (see below), and AWS Systems Manager - into integrated dashboards. Security and compliance personnel can then more quickly and easily identify issues and take appropriate actions.

AWS COMPLIANCE

A wide variety of laws and regulations, both in the United States and abroad, address data storage security and reliability in the cloud. To maintain compliance, AWS implements a shared responsibility paradigm between AWS and their customers.

This means AWS is responsible for the security of the cloud itself, i.e., the AWS infrastructure, including all hardware, software and networks. AWS users, in turn, assume responsibility for security and compliance of their own data maintained in the cloud.

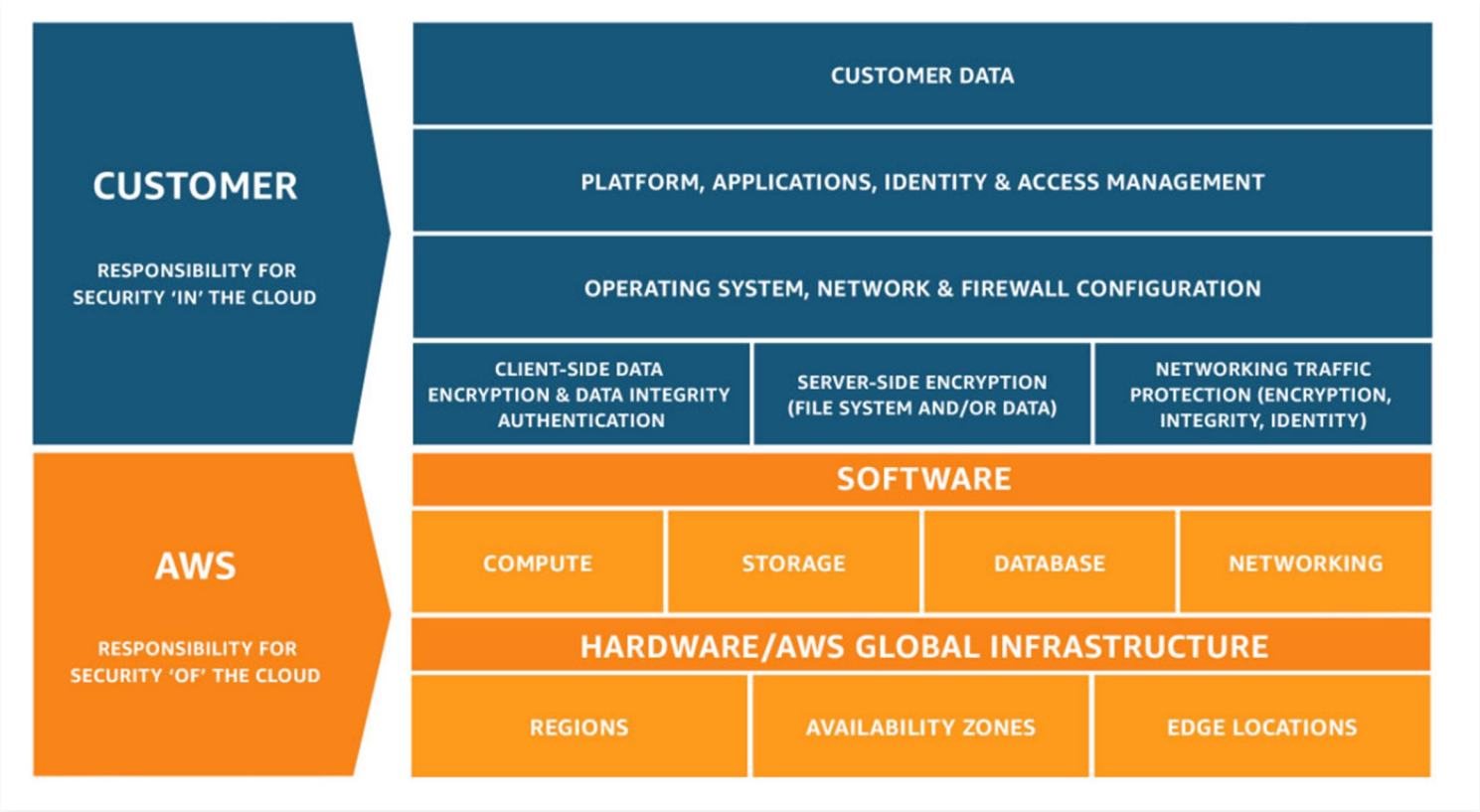


Figure 3: The AWS Shared Responsibility Model (from https://aws.amazon.com/compliance/shared-responsibility-model/)

AWS divides compliance standards into Certifications and Attestations; Laws, Regulations, and Privacy; and Alignments and Frameworks.

CERTIFICATIONS AND ATTESTATIONS

AWS has obtained numerous certifications and accreditations from a range of international organizations for its compliance efforts. A third-party auditor verifies each of AWS's certifications and accreditations.

At a high level, AWS is certified under International Standards Organization (ISO) 9001 (Global Quality Standard), 27001 (Security Management Controls), 27017 (Cloud Specific Controls), and 27018 (Personal Data Protection). AWS also holds a certification from the Cloud Security Alliance.

AWS also has more issue-specific certifications, including Systems and Organization Controls (SOC) 1, 2, and 3 from the American Institute of Certified Public Accountants (AICPA). SOC generates five reports detailing audits by Ernst & Young of AWS's achievement of key compliance goals. The five SOC reports cover all three levels of SOC certification. The AWS SOC certification page contains detailed descriptions of the purposes and contents of the various SOC reports and the applicable compliance standards, as shown in the Figure below:

	SOC 1	SOC 2: Security, Availability & Confidentiality	SOC 2: Privacy	SOC 3: Security, Availability & Confidentiality
What is the report?	A description of the AWS control environment and external audit of AWS defined controls and objectives	A description of the AWS controls environment and external audit of AWS controls that meet the AICPA Trust Services Security, Availability, and Confidentiality Principles and Criteria	A description of the AWS controls environment and external audit of AWS controls that meet the AICPA Trust Services Privacy Principle and Criteria	A public facing report demonstrating AWS has met the AICPA Trust Services Security, Availability, and Confidentiality Principles and Criteria
Under what Standard is the Audit Report Performed?	SSAE No. 18, Attestation Standards: Clarification and Recodification (AICPA, Professional Standards), which includes AT-C section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting. AICPA Guide, Service Organizations: Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)	SSAE No. 18, Attestation Standards: Clarification and Recodification, which includes AT-C section 105, Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy(SOC 2®) TSP section 100A, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, 2017 Trust Services Criteria)	Same as SOC 2: Security Availability & Confidentiality	SSAE No. 18, Attestation Standards: Clarification and Recodification, which includes AT-C section 105, Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements TSP section 100A, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, 2017 Trust Services Criteria)
What's the Primary Report Purpose?	To provide information to customers about AWS' control environment that may be relevant to their internal controls over financial reporting To provide information to customers and their auditors for their assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR)	To provide customers and users with a business need with an independent assessment of AWS' control environment relevant to system security, availability, and confidentiality	To provide customers with an independent assessment of AWS' systems and the suitability of the design of AWS' privacy controls. The SOC 2 Privacy Trust Principle, developed by the American Institute of CPAs (AICPA), establishes criteria for evaluating controls related to how personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.	To provide customers and users with a business need with an independent assessment of AWS' control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information
Who is the Primary Report Audience?	Customer management and their auditors	Users with business need	Users with business need to understand the AWS controls relevant to privacy	Publicly available **here**
What Period does the AWS Report Cover?	6 Months: 10/1-3/31 and 4/1-9/30	6 Months: 10/1-3/31 and 4/1-9/30	Point of time (as of report date)	6 Months: 10/1-3/31 and 4/1-9/30

Figure 4: SOC compliance reports (from https://aws.amazon.com/compliance/soc-faqs/)

SOC reports issue twice a year. The SOC Levels 1 and 2 reports are available in AWS Artifact, AWS's central repository for compliance reporting. Those interested in the Level 3 report (Security, Availability & Confidentiality Report) can find it in whitepaper form on the AWS website.

For e-commerce businesses and any others that accept online payments, AWS is compliant with the Payment Card Industry Data Security Standard (PCI-DSS).

LAWS, REGULATIONS, AND PRIVACY

Compliance with data privacy laws and regulations can be overwhelming, but data privacy is of the utmost importance in today's digital world. Stolen personal data like US passport information can go for up to $2000 on the dark web, making this a big business for hackers.

Privacy laws vary from country to country, and within some countries (like the US), from state to state. AWS has built-in tools to maintain compliance with various privacy regulations across more than 190 countries worldwide.

One of the most significant and strict privacy regimes globally is the European Union's General Data Protection Regulation (GDPR). AWS services are GDPR-ready, and AWS also helps customers assure GDPR compliance so you can earn your customers' trust with strong data integrity.

In addition to compliance with general national privacy laws, companies must also consider compliance with issue-specific privacy laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Fair Credit Reporting Act (FCRA). While certifications for these are not available, AWS provides tools that help customers meet specific laws and regulations like HIPAA, Internal Revenue Service Publication 1075, and more.

Figure 5: A selection of AWS compliance standards in the Americas (from https://aws.amazon.com/compliance/programs/)

ALIGNMENTS AND FRAMEWORKS

Many government and private organizations have created frameworks for implementing effective cybersecurity controls and constructing associated compliance efforts. While certifications are not always available under these frameworks, AWS ensures that it complies with the recommendations and requirements of various frameworks across the world.

Some of these frameworks include:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework and Publication 800-53: sets out a general cybersecurity framework for implementation and monitoring of requirements and controls
- EU-US Privacy Shield: a framework allowing United States companies to qualify as having equivalent protections to the GDPR
- UK Cloud Security Principles: a 14-point framework for assessing the security of cloud services
  Japanese financial and medical information protection frameworks: industry-specific applications of Japan's Personal Information Protection Law

COMPLIANCE TOOLS

AWS includes robust compliance tools to help customers ensure business data is protected so your employees and your customers can feel secure.

AWS Config is the primary tool for helping users meet their portion of shared security and compliance responsibilities. AWS Config monitors and tracks resource configurations and assures compliance with corporate governance policies.

Users can monitor all changes to resource configurations across the AWS platform, and Config can send out notifications when resources are outside of acceptable parameters. Config also monitors resource dependencies and helps users make configuration changes with minimal impacts on the rest of the system.

AWS CloudTrail tracks user activity across all AWS services and allows organizations to assess any activity that may be against governance rules. CloudTrail users can configure alarms and events to notify relevant compliance personnel of non-compliant or anomalous activity.

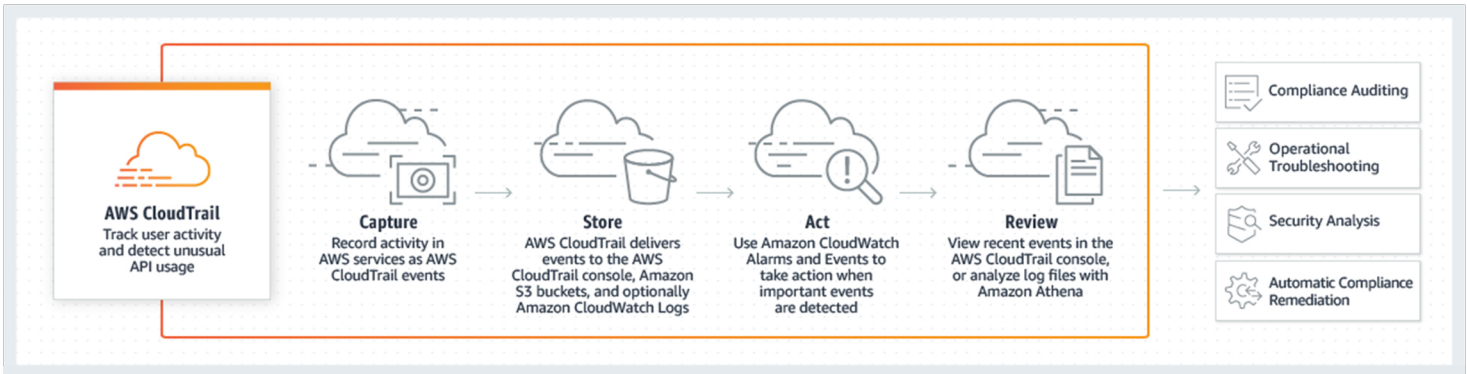
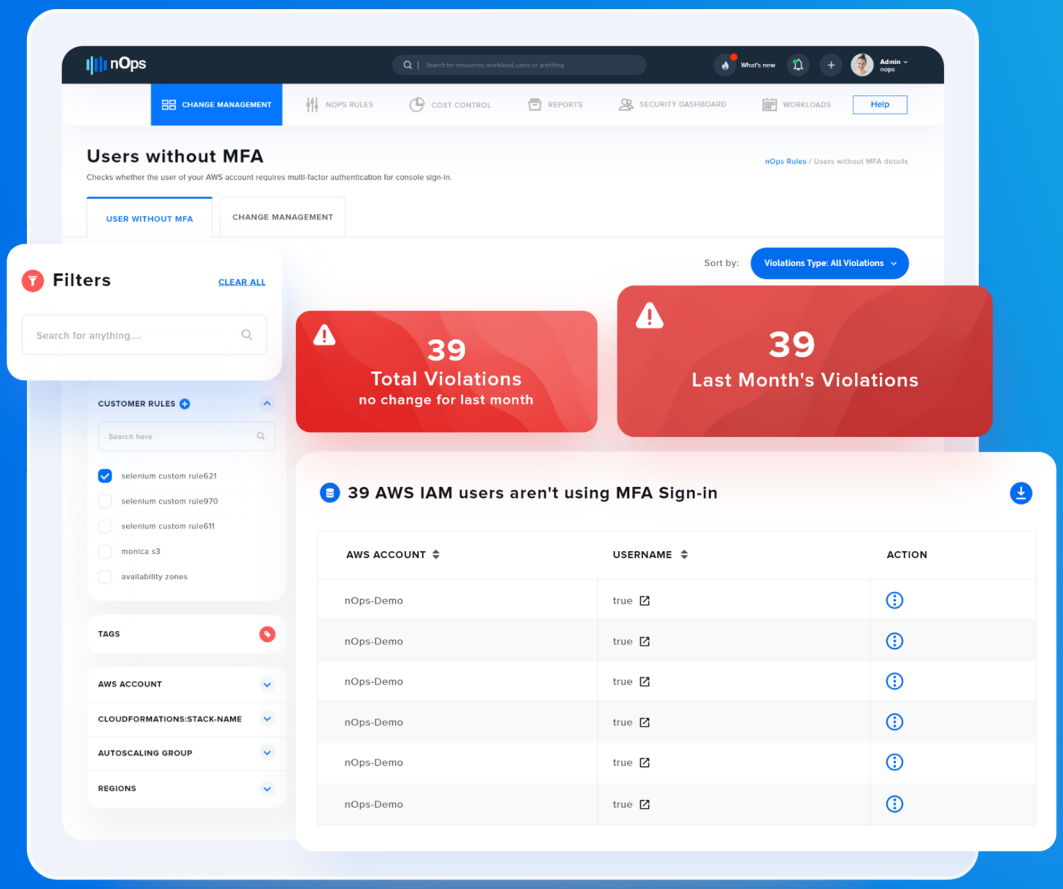


Figure 6: AWS CloudTrail process(from https://aws.amazon.com/cloudtrail/)

AWS Macie uses advanced machine learning algorithms to help organizations identify and protect sensitive data. By doing so, Macie helps users ensure compliance with applicable data privacy laws and regulations. These types of tools can be especially essential for small and mid-size businesses who may lack the budgets and comprehensive security teams common in larger organizations.



BUILD A BETTER AWS COMPLIANCE PROGRAM WITH NOPS

With so many AWS security and compliance tools available, each with a multitude of features, getting the right configuration can be overwhelming. **nOps** can help you streamline your AWS security and compliance experience with pre-built security rules templates and comprehensive, customized notification and monitoring dashboards.

nOps offers continuous, real-time monitoring of your system for potential security or compliance events. At the highest level, **nOps** analyzes the health and integrity of your AWS infrastructure to identify potential access points and vulnerabilities.

nOps monitors your AWS configurations for unauthorized changes, logging all changes so that you have an easy-to-follow audit trail. And nOps helps simplify management of users and monitor identities for anomalous activity such as unusual root account usage or AWS console logins.

With nOps, AWS users can consolidate security event monitoring and notifications in easy to use, customizable dashboards. Automated alerts based on predefined security rules templates keep AWS users up-to-date on threats and system activity in real-time.

If you think of AWS as the big toolbox you keep in the garage for when you need a special tool, then nOps is your trusted Swiss army knife you keep in your pocket to deal with everyday tasks.

TAKE ADVANTAGE OF YOUR OPTIONS

AWS users have an almost overwhelming range of options for protecting and securing their data and ensuring compliance with company policies and data protection regulations. Working with AWS consultants can help you make the most of your options, ensuring the best possible AWS experience.