connectria

The Healthcare Leaders Guide to Architecting for HITRUST CSF in AWS

Table of Contents

Overview 02

What Is HITRUST CSF? 03

HITRUST Certification 04

HITRUST CSF Controls 05

AWS Shared Responsibility Model 07

AWS Services with HITRUST Certification 08

AWS Tools to Support HITRUST-Compliant Architecture 09

HITRUST Expertise and Support 12

Overview

Public cloud adoption has been a driving force behind innovation, cost efficiencies, and improvements in care across the United States health system in recent years.

It has provided the platform for advancements in healthcare, such as faster diagnostics, the development of new treatments and therapies, and remote consultations. It offers highly scalable storage, making it a better alternative to the on-premises data center for large volumes of patient data. It is a distributed infrastructure, which offers an easier and more secure way to share patient data across the healthcare ecosystem. It's also a more resilient environment for your data, helping you to maintain the optimum availability of critical health information.

However a move to the cloud raises questions about the security of sensitive patient data and compliance with regulations affecting the industry-in particular, the data protection provisions of the Health Insurance Portability and Accountability Act (HIPAA).

However, the HIPAA stipulates only general requirements on how to protect healthcare information. This makes sense because every computing environment is different. And so it cannot mandate a one-size-fits-all set of rules for information security.

The HITRUST Alliance, which was established in 2007, set out to address the problem of HIPAA compliance by creating a framework that gave organizations a robust and comprehensive system for protecting their data, ensuring they had all bases covered whatever the IT environment.

The purpose of this guide is to help organizations that manage protected health information (PHI) but are unsure how to meet HITRUST requirements in the cloud. It focuses specifically on deployments hosted on the leading cloud platform Amazon Web Services (AWS) and runs through the most important things you need to consider before you embark upon your HITRUST compliance journey.

Healthcare in the Cloud

According to a forecast published in a recent report by B2B market research company Markets and Markets, the global healthcare cloud computing market is set to skyrocket from USD 39.4 billion in 2022 to USD 89.4 billion by 2027. This epresents a compound annual growth rate (CAGR) of 17.8%.

The company attributed much of the growth to wider use of electronic health records (EHRs), greater emphasis on technology following the coronavirus pandemic, and increasing adoption of big data analytics.

What is HITRUST CSF?

HITRUST CSF is a framework, known as the Common Security Framework (CSF), that was originally developed by the Health Information Trust Alliance to help protect sensitive personal data. It is intended for use by organizations in any industry but is primarily aimed at the US healthcare sector.

It aids compliance with HIPAA requirements concerning the handling of PHI. Although it doesn't replace or prove HIPAA compliance, it nevertheless provides a widely accepted mechanism for achieving it.

Furthermore, HITRUST CSF incorporates more than 40 other regulations and standards, such as the following:

- ISO/IEC 27001 and 27002
- NIST 800-53 and NIST 800-171
- PCI DSS
- COBIT
- CCPA
- GDPR

It can therefore streamline compliance as a whole-through an assess once, report many approach that reduces duplication of the work and effort needed to meet other sets of data protection requirements.

At the same time, it may open up new business opportunities to those that serve the healthcare sector but would like to break into other market segments.

HITRUST Certification

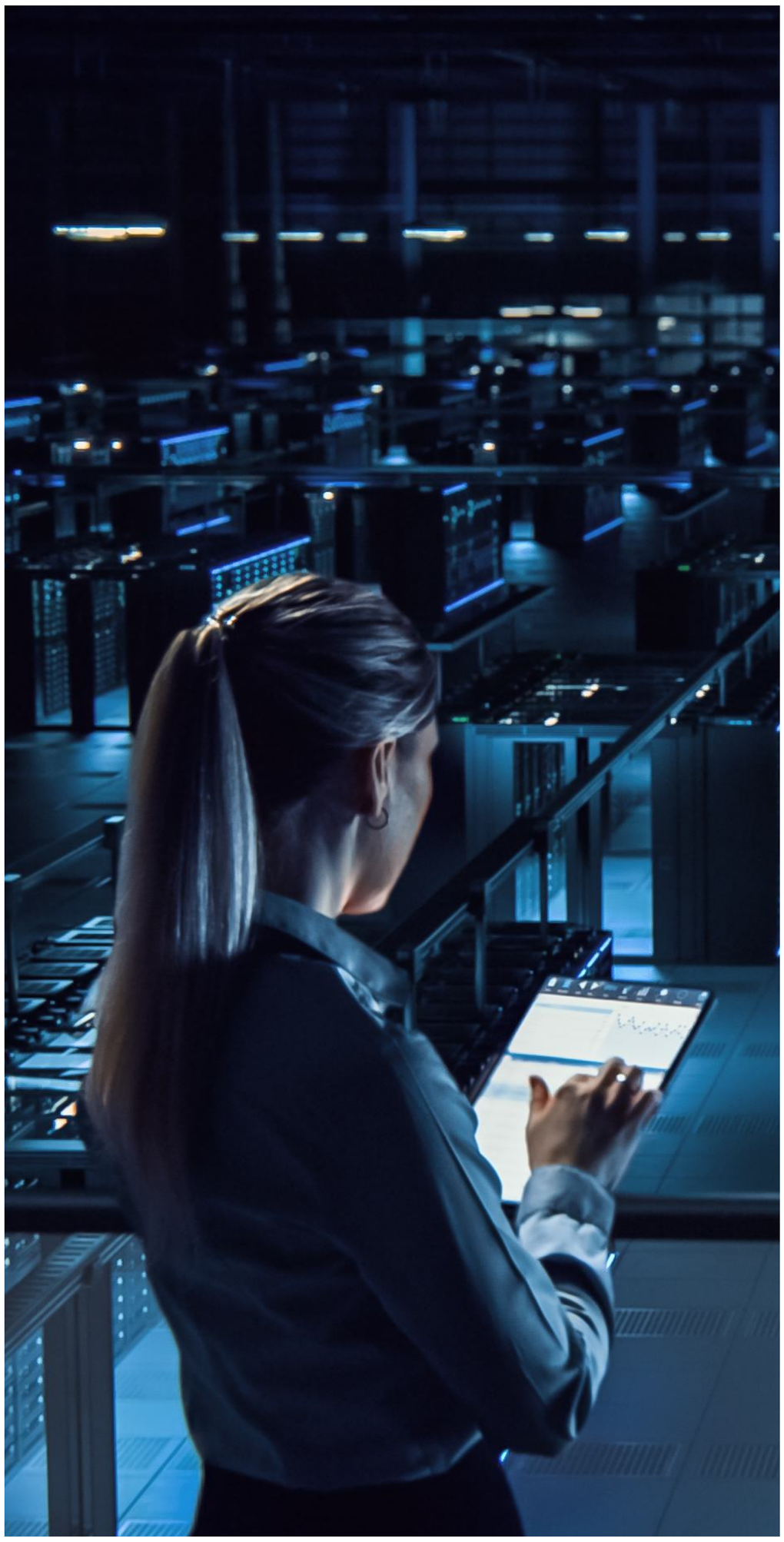
HITRUST certification involves an independent assessment over several weeks followed by a certification process, which takes an additional six weeks.

You can choose between three different assessment levels, each of which provides a level of assurance appropriate to the degree of risk to your data and the maturity of your cybersecurity activities.

e1 Assessment
A basic level of assessment suited to organizations that handle low-risk data.

i1 Assessment
An intermediate level of assessment that demonstrates you're implementing a comprehensive program of robust security measures and best practices.

r1 Assessment
The highest assessment tier is suited to organizations that handle a significant volume of sensitive data and need the utmost levels of protection to keep it secure.



HITRUST CSF Controls

The HITRUST CSF is organized into 14 control categories, 49 control objectives, 156 control requirements, and 19 assessment domains, where:

Control Categories draw upon the control sets used by ISO 27001 and form the basic structure of the framework.

Control Objectives are high-level goals, which you select based on what's most appropriate for your organization, such as the scale of your operation and level of risk to your data.

Control Requirements are the specific action steps you need to take to meet your control objectives. These can be policies, procedures, guidelines, or even organizational structures that you'll need to have in place to meet compliance.

Assessment Domains are curated sets of control requirements that are intended to align with a typical IT organizational structure. This approach makes assessment more efficient by mapping each grouping of controls to the responsibilities of a specific IT department.

Healthcare Top Targets for Cybercriminals

The Cost of a Data Breach Report 2023, published by IBM and the Ponemon Institute, revealed that the healthcare sector suffered the highest data breach costs of all industry verticals at an average of more than USD 10 million per incident. It was the twelfth year in a row that healthcare ranked worst in the survey.

This should come as no surprise given the value of PHI, as it contains a wealth of information that can be exploited by criminals. For example, they can use it for:

- Bogus insurance claims
- Treatment under a false name
- Fake prescriptions of drugs (for personal use or resale on the black market)
- Ransom demands to individuals or healthcare organizations

Common tactics used as part of healthcare breaches include:

- Abuse of access privileges by insiders
- Phishing
- Compromised credentials
- Malware
- Ransomware
- Software supply-chain exploits
- Theft of laptops and other devices

High-Profile Breaches in Healthcare

The following is just a small selection of the countless number of cyberattacks on organizations operating in the US healthcare sector over the last 10 years.

Organization	Year	Tactics Used in Attack	Data Compromised	Scale of Data Affected
Anthem Blue Cross (Health Insurance Provider)	2015	Spear-phishing	Names, addresses, dates of birth, social security numbers, email addresses	78.8 million records
Premera Blue Cross (Health Insurance Provider)	2015	Phishing and advanced persistent threat (APT)	Names, addresses, dates of birth, email addresses, social security numbers, bank account numbers, claims details	10.4 million individuals
Managed Care of North America (Dental Benefits Administrator)	2023	Unauthorized access and malware infection	Names, addresses, telephone numbers, email addresses, dates of birth, social security numbers, driving license numbers, government-issued ID numbers, health insurance details, information relating to care provided	8.9 million individuals
OneTouchPoint (Healthcare Mailing Vendor)	2022	Ransomware	Healthcare member IDs, names, information provided during health assessments	4.1 million individuals
Medical Informatics Engineering (Healthcare Software Development)	2015	Compromised credentials	Names, addresses, email addresses, telephone numbers, login details, dates of birth, social security numbers, medical conditions, lab results, diagnoses, disability codes	3.9 million patients

AWS Shared Responsibility Model

A move to the cloud relieves you of many of the responsibilities involved in managing your infrastructure. And, likewise, many of the responsibilities for compliance and security.

However, cloud customers are often unsure as to which of those responsibilities come within their purview and which are the concerns of the cloud service provider (CSP).

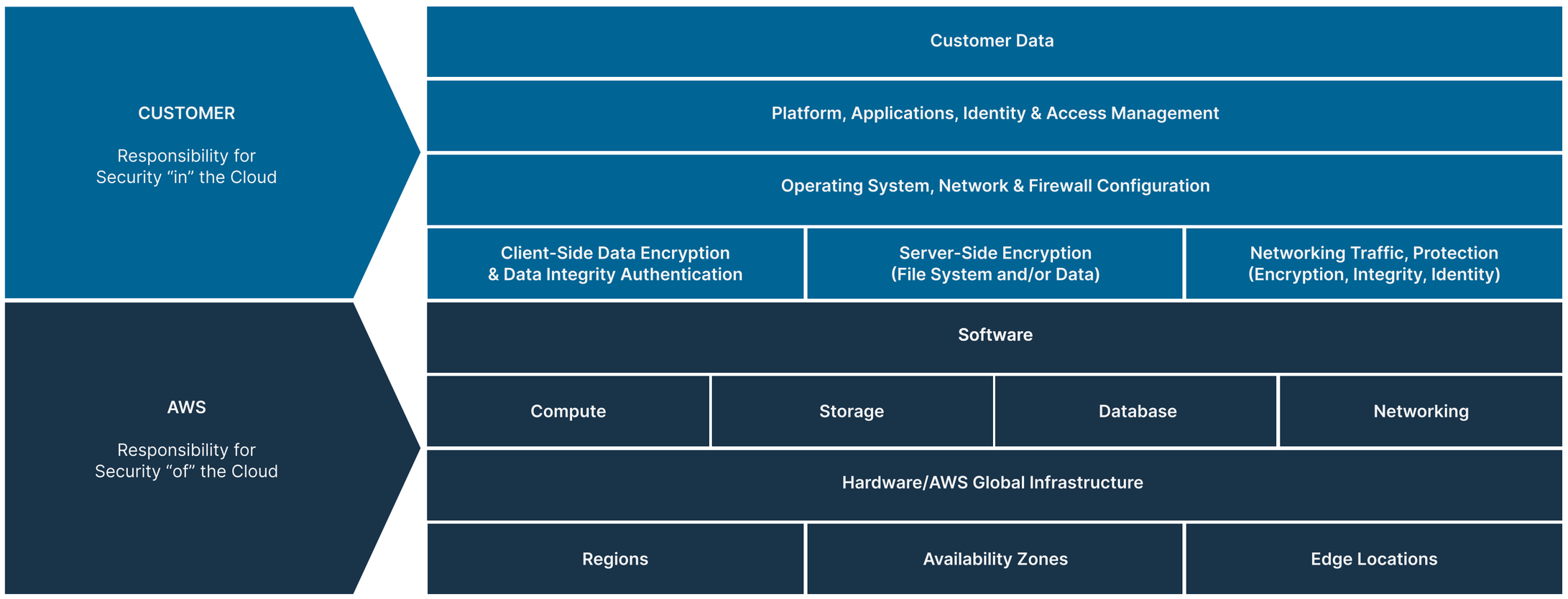
AWS uses a shared responsibility model to help customers understand individual party obligations. It does so by distilling it down into two basic concepts:

Security of the Cloud

Those aspects of compliance and security for which AWS is accountable. These cover its host operating system and hypervisor, the physical security of its facilities, and the integrity of the tools it makes available to customers.

Security in the Cloud

Your responsibilities as the customer. These depend on the AWS services you use. But, in terms of infrastructure-as-a-service (IaaS) offerings, they would include any applications you host on the platform, the security of your guest operating systems, and the configuration of your network and other IaaS components.



The model is a brilliantly simple approach to explaining how you should go about ensuring full compliance and security coverage for your cloud-based workloads. But it doesn’t give you the granular detail you need for meeting the specific requirements of compliance frameworks such as the HITRUST CSF.

However, HITRUST has published a shared responsibility matrix, which is available as a free download, to help clarify HITRUST requirements specifically in the context of AWS deployments. It has also produced similar matrices for other leading CSPs, such as Microsoft Azure and Google Cloud Platform.

AWS Services with HITRUST Certification

The starting point to ensuring your AWS deployments meet HITRUST CSF requirements is to select only those services that have been certified by an approved HITRUST auditor.

These include the following core AWS services:

- AWS Identity and Access Management (IAM)
- Amazon Elastic Compute Cloud (EC2)
- Amazon EC2 Auto Scaling
- Elastic Load Balancing (ELB)
- Amazon Elastic Container Service (ECS)
- Amazon Elastic Kubernetes Service (EKS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic File System (EFS)
- Amazon Relational Database Service (RDS)
- Amazon Simple Queue Service (SQS)
- Amazon Virtual Private Cloud (VPC)
- AWS Elastic Beanstalk
- AWS Lambda

Please note, that AWS documentation which services are currently included is updated regularly. Verifying the services on this list with your Cloud Services Provider (CSP) is recommended.

One of the unique features of HITRUST certification is the ability to automatically inherit assessment scores from your CSP's assessment. This saves time and money by reducing the work involved in demonstrating you've implemented the required controls - leaving you to focus only on those that fall within your remit.

You should refer to the AWS version of HITRUST's shared responsibility matrix to determine precisely which controls you can inherit as part of its shared responsibility and inheritance program.

AWS Tools to Support HITRUST-Compliant Architecture

With more than 150 control requirements, the task of meeting and maintaining HITRUST compliance is a complex and time-consuming manual undertaking.

However, AWS provides a way to streamline compliance through a range of tools that can help you meet HITRUST architecture principles. The following examples are all certified under HITRUST CSF requirements.

Amazon CloudTrail

A service that logs, monitors and records account activity performed through API calls. For example, when:

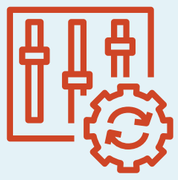
- Someone accesses a resource through the AWS Management Console
- A user issues a command in the AWS Command Line Interface (AWS CLI)
- An AWS resource receives aREST API call

CloudTrail aids compliance by providing an audit trail of resource management activity. In addition, you can integrate it with Amazon CloudWatch to create workflows that execute in response to HITRUST compliance violations.

Amazon CloudWatch Logs

A feature of Amazon CloudWatch through which you can centralize the capture and storage of logs from your systems, applications, and AWS services. By aggregating logs in a convenient central location, you can efficiently analyze and monitor your environment for any suspicious activity or non-compliant events.

AWS Tools to Support HITRUST-Compliant Architecture



AWS Config

A fully managed auditing, benchmarking, and inventory discovery tool for monitoring configuration changes to your AWS infrastructure.

It checks your resources against a set of predefined and custom rules, notifying you whenever they deviate from the specified settings. In addition, it can automatically remediate a resource in response to a rule violation.

You can therefore use the service to support compliance by setting rules to align your resources with HITRUST CSF control recommendations.

AWS Inspector

A vulnerability scanning and management tool that continuously monitors your AWS environment for software vulnerabilities and network configuration issues.

The service provides comprehensive details about its findings to help you prioritize remediation activity and manage the patching cycle quickly and efficiently.

Amazon Macie

A fully managed service that uses machine learning and pattern matching to detect and help protect sensitive data stored on Amazon S3.

The solution automatically builds and maintains an inventory of your S3 buckets and continuously scans new data for potential security and privacy issues as it's added to the object storage service.

Amazon Macie performs several functions to aid compliance. For example, it can discover different types of sensitive data, such as access credentials, financial information, and personally identifiable information (PII), providing you with a detailed report of its findings.

Most importantly, it can identify PHI, helping you to keep track of the data you need to protect under HITRUST CSF and HIPAA requirements.

In addition, it provides several data security capabilities, such as the ability to identify buckets that are unencrypted, publicly accessible, or shared with AWS accounts outside of your organization.

AWS Services for US Healthcare

AWS offers many HIPAA-compliant solutions that are specifically designed for customers operating in the healthcare sector.

These include:

- AWS HealthScribe uses speech recognition and generative artificial intelligence (AI) which automatically transcribes conversations between clinicians and their patients.
- AWS HealthLake allows healthcare analysts to import large volumes of health data from different sources into a secure central repository to help get the insights they need.

AWS Tools to Support HITRUST-Compliant Architecture

AWS GuardDuty

An intelligent threat detection service that analyzes data sources, such as CloudTrail event logs and DNS logs, for signs of malicious activity.

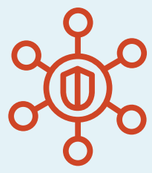
It uses machine learning and anomaly detection to identify potential threats and generates findings that can help you understand the nature of the threat and take appropriate action. The service also integrates with proprietary issue tracking and automated workflow platforms, such as PagerDuty, Jira, and ServiceNow.

AWS CloudFormation

An infrastructure-as-code (IaC) service for configuring, deploying, and managing resources based on infrastructure templates.

CloudFormation supports your HITRUST objectives through its ability to ensure consistent and compliant configuration of resources across your AWS environment.

You can also use it in conjunction with AWS Config to track configuration changes to CloudFormation stacks, thereby reducing the risk of configuration drift and non-compliance.



AWS Security Hub

A centralized cloud security posture management (CSPM) tool that continuously monitors your AWS deployments for deviations from security best practices.

It ingests security data from a range of sources, including AWS Config, Amazon Inspector, Amazon GuardDuty, and supported third-party services, and delivers its findings through a single consolidated dashboard.

You can also use Security Hub to generate findings by specifying rules for the controls you wish to enforce. Furthermore, it offers automated remediation capabilities.

Security Hub can help streamline HITRUST CSF compliance by providing a holistic view of your security posture and reducing the complexity and effort of managing controls.

HITRUST Expertise and Support

HITRUST compliance can be a formidable undertaking and a complex and time-consuming ongoing commitment. That's why many organizations call upon the expertise and support of an AWS managed service provider (MSP).

AWS MSPs like Connectria are trusted partners with a deep understanding of data protection regulations and standards. But they also have highly detailed knowledge of AWS infrastructure and tooling. This means they know exactly how to align your AWS setup with compliance requirements.

At Connectria, we can help ensure you have full compliance and security coverage with no gaps in requisite controls. Connectria will also help you minimize the risk of exploits by taking care of updates and vulnerabilities patches for you.

Additionally, we have the resources to stay on top of the latest threats and monitor your deployments 24 hours a day, 7 days a week. This means you always have coverage to respond to compliance and security issues before they escalate into more serious problems.

And above all, Connectria can guide you through every stage of your HITRUST journey and beyond.

Visit connectria.com to learn more.

connectria