AWS Blueprint for Ransomware Defense

First published May 11, 2023
Last updated November 20, 2023

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

ABSTRACT
INTRODUCTION
GETTING STARTED
KNOW YOUR ENVIRONMENT (NIST CSF-IDENTIFY)
SECURE CONFIGURATIONS (NIST CSF-PROTECT)
ACCOUNT AND ACCESS MANAGEMENT (NIST CSF-PROTECT)
VULNERABILITY MANAGEMENT PLANNING (NIST CSF-PROTECT)
DATA RECOVERY AND INCIDENT RESPONSE (NIST CSF-RESPOND)
MALAWARE DEFENSE (NIST CSF-PROTECT)
SECURITY AWARENESS AND SKILLS TRAINING (NIST CSF-PROTECT)
DATA RECOVERY AND INCIDENT RESPONSE (NIST CSF-RECOVER)
CONCLUSION
CONTRIBUTORS
FURTHER READING

Table of Contents

Abstract

The Amazon Web Services (AWS) Blueprint for Ransomware Defense provides guidance and a mapping of AWS services and features to 40 recommended security controls from the Center for Internet Security Critical Security Controls (CIS Controls), designed to defend against ransomware events.

Introduction

In support of the Ransomware Task Force (RTF) initiatives and the Institute for Security and Technology (IST) Blueprint for Ransomware Defense publication, AWS developed the AWS Blueprint for Ransomware Defense to assist AWS customers in aligning with these controls. This artifact is complementary to the IST Blueprint, because we've aligned to the same 40 recommended controls that were carefully selected for their specific effectiveness in defending against ransomware events, as well as their ease of implementation. The AWS Blueprint for Ransomware Defense provides guidance and a mapping of AWS services and features as they align to aspects of the Center for Internet Security Critical Security Controls (CIS Controls), which provides the basis for the IST Blueprint.

Analysis by the CIS Community Defense Model found that implementing these 40 controls helped mitigate 70 percent of the techniques associated with ransomware. It should be noted that CIS has described these controls as "essential." Implementing these controls can help IT professionals with limited cybersecurity expertise in their efforts to defend against general and non-targeted ransomware events. These 40 controls are also aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) five security functions: identify, protect, detect, respond, and recover.

Although implementing these essential security controls, which are outlined in the CIS Implementation Group 1 (IG1), may not prevent all attacks, it can help protect you from many. These controls are targeted to organizations that might have gaps in their cybersecurity knowledge. In reviewing and taking action on the guidance in this publication, your organization can help improve your resilience against ransomware.

Ransomware is a business for threat actors, who are now commonly using ransomware-as-a-service models; however, ransomware events are typically a consequence of a lack of security hygiene. More than ever, it's become important to protect your environment from the challenges that come with non-targeted events in the form of ransomware.

Getting started

Before we move on to the controls, let's start with the basics. There are foundational services that we recommend customers use to help them manage their environment for scale and security. These services were built based on customer feedback about their experiences with managing their AWS environments securely at scale. Whether you are a small start-up or a large enterprise, we recommend that customers use these services. This includes using AWS Organizations, AWS Control Tower, and AWS IAM Identity Center (successor to AWS Single Sign-On). AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. By using AWS Organizations, you can programmatically create new AWS accounts, allocate resources, group accounts to organize your workloads, and apply policies to accounts or groups of accounts for governance. An AWS organization consolidates your AWS accounts so that you can administer them as a single unit. AWS Control Tower automates the creation of a landing zone with best-practices blueprints that configure Organizations for a multi-account structure; provide identity management by using IAM Identity Center; provide federated access by using the IAM Identity Center console; create a central log archive by using AWS CloudTrail and AWS Config; implement network configurations by using Amazon Virtual Private Cloud (Amazon VPC); and define workflows for provisioning accounts by using AWS Service Catalog and associated AWS Control Tower solutions. In AWS Control Tower, IAM Identity Center allows central cloud administrators and end users to manage access to multiple AWS accounts and business applications. AWS Control Tower uses IAM Identity Center to set up and manage access to the accounts created through AWS Service Catalog.

In each section that follows, we've highlighted the foundational AWS services and features that relate to each NIST CSF security function. In addition, we've provided a detailed mapping of the controls to many of the respective and relevant AWS features and services that can be used to implement those controls.

Know your environment (NIST CSF – Identify)

Establishing an inventory of systems and software in an ephemeral environment and across different resources is simpler in the AWS Cloud than in traditional environments. AWS has several services and features that can help provide transparency and visibility across your environment. Although there are several tools, such as the AWS Command Line Interface (AWS CLI) and AWS SDKs, that allow you to interact with the environment dynamically and can provide you with detailed information, including inventory, we recommend AWS Config as the primary service for this task. A fully managed service, AWS Config provides an AWS resource inventory, configuration history, and configuration change notifications for better security and governance. You can create rules that automatically check the configuration of AWS resources that AWS Config records.

In addition, for asset and software-level inventory across your Amazon Elastic Compute Cloud (Amazon EC2) instances, you can use Inventory, a capability of AWS Systems Manager. You can use Inventory to collect metadata from your managed nodes, store this metadata in a central Amazon Simple Storage Service (Amazon S3) bucket, and then use the built-in tools to query the data and quickly determine which nodes are running the software, the configurations required by your software policy, and which nodes need to be updated. You can also configure and view inventory data from multiple AWS Regions and AWS accounts.

There are many features and services that can help you identify and classify your data based on criticality and sensitivity in order to help you determine appropriate data protection and retention controls. Tagging your AWS resources allows you to organize your resources along technical, business, security, and compliance dimensions. This will help you classify your data, associate a data owner and applicable legal and compliance requirements, influence where the data should be stored, and specify the resulting controls that need to be enforced. This may include classifications to indicate if the data is intended to be publicly available, if the data is internal-use only (such as customer personally identifiable information (PII)), or if the data is for more restricted access (such as intellectual property, legally privileged, or marked sensitive), and more. Companies that are most effective in their use of tags typically create business-relevant tag groupings to organize their resources along technical, business, and security dimensions. In addition, you can use Amazon Macie to help you identify sensitive data, such as PII.

Configuration of access management to your AWS environment is an important step to verify that your environment is secure from the start. We recommend that you adhere to security best practices in IAM and use IAM Identity Center for centralized workforce access management, and managing access to your accounts and the permissions within those accounts. You can manage your user identities with IAM Identity Center, or manage access permissions for user identities in IAM Identity Center from an external identity provider.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Inventory and control of enterprise assets 1.1	AWS Cost and Usage Reports (CUR)	With AWS CUR, you can review, itemize, and organize the most comprehensive cost and usage data for your account.	AWS CUR is your one-stop shop for accessing the most detailed information available about your AWS costs and usage. Cost and usage reports can be generated at hourly, daily, or monthly granularity. You can enable AWS CUR from the cost and usage reports page in the AWS Billing console.	No cost associated.
	AWS Config	AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources.	AWS Config provides you with a mechanism for recording and detecting a wide range of actions on resources in your account.	AWS Config pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Inventory and control of software assets 2.1 2.2	AWS Systems Manager Inventory	Inventory, an AWS Systems Manager capability, provides visibility into your AWS computing environment.	You can use Inventory to collect metadata from your managed nodes. You can store this metadata in a central S3 bucket, and then use built-in tools to query the data and quickly determine which nodes are running the software, the configurations required by your software policy, and which nodes need to be updated. You can also configure and view inventory data from multiple AWS Regions and AWS accounts.	AWS Systems Manager pricing
Data protection 3.1	Tagging AWS resources	You can assign metadata to your AWS resources in the form of tags. Each tag is a label consisting of a user-defined key and value.	An effective tagging strategy uses standardized tags and applies them consistently and programmatically across AWS resources. You can use both reactive and proactive approaches for governing tags in your AWS environment.	No cost associated.
Data protection 3.1	Amazon S3 - Managing your storage lifecycle	An Amazon S3 Lifecycle configuration is an XML file that contains a set of rules with predefined actions that you want Amazon S3 to perform on objects during their lifetime.	When an object reaches the end of its lifetime based on its lifecycle policy, Amazon S3 queues it for removal and removes it asynchronously. There might be a delay between the expiration date and the date at which Amazon S3 removes an object.	Amazon S3 pricing
Data protection 3.1	Amazon Macie	Amazon Macie is a data security service that discovers sensitive data by using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks.	Macie automates the discovery of sensitive data, such as personally identifiable information (PII) and financial data, to provide you with a better understanding of the data that your organization stores in Amazon S3. If Macie detects sensitive data or potential issues with the security or privacy of your data, it creates detailed findings for you to review and remediate as necessary. You can review and analyze these findings directly in Macie, or monitor and process them by using other services, applications, and systems.	Amazon Macie pricing
Establish and maintain an inventory of accounts 5.1	AWS Identity and Access Management (IAM)	With IAM, you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.	IAM helps you securely control access to AWS resources. You can use IAM to control who is authenticated (signed in) and authorized (has permissions) to use AWS resources, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.	No cost associated.

Secure configurations (NIST CSF – Protect)

We recommend that you use AWS Control Tower to support a multi-account secure configuration (Note: Although highly recommended as an AWS best practice, AWS Control Tower is not required). AWS Control Tower offers a convenient way to set up and govern a secure, multi-account AWS environment. It establishes a landing zone and enables governance by using guardrails that you can choose from a prepackaged list. The landing zone is a well-architected, multi-account baseline that follows AWS best practices. Guardrails implement governance rules for security, compliance, and operations.

AWS customers can tailor, or harden, the configuration of an Amazon EC2 instance, Amazon Elastic Container Service (Amazon ECS) container, AWS Lambda function, or AWS Elastic Beanstalk instance, and persist this configuration to an immutable Amazon Machine Image (AMI). Then, whether invoked by AWS Auto Scaling or launched manually, the new virtual servers (instances) launched with this AMI receive the hardened configuration. EC2 Image Builder allows you to create images with only the essential components, reducing your exposure to security vulnerabilities. When a security patch is available, Image Builder can automatically patch your images. You can also apply AWS provided security policies (such as strong password enforcement, full disk encryption, and firewall enablement) or custom security policies to your images to help you meet your applicable internal compliance criteria. You can use Amazon Inspector to quickly discover vulnerabilities in compute workloads and notify the appropriate teams to take immediate action.

In AWS, you can use AWS Config to determine changes across the AWS environment. AWS Config also generates configuration items when the configuration of a resource changes, and it maintains historical records of the configuration items of your resources from the time you start the configuration recorder. By default, AWS Config creates configuration items for every supported resource in the Region. If you are using AWS Config rules, AWS Config continuously evaluates your AWS resource configurations for your desired settings. Depending on the rule, AWS Config will evaluate your resources, either in response to configuration changes or periodically.

You can also implement stateful and stateless packet inspection in AWS, either by using AWS native technologies or by using partner products and services available through the AWS Marketplace. You can use Amazon VPC to create a private, secured, and scalable environment in which you can define your topology—including gateways, routing tables, and public and private subnets. AWS native technologies that are available for you to control traffic between resources include Amazon VPC network access control lists (network ACLs), security groups, and AWS Network Firewall. AWS Firewall Manager allows you to centrally manage AWS Network Firewall policies, common security groups, and Amazon Route 53 DNS Resolver Firewall.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Secure configuration 4.1 4.2 4.4 4.7	AWS Config	AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources.	AWS Config provides you with a mechanism for recording and detecting a wide range of actions on resources in your account.	AWS Config pricing
	EC2 Image Builder	Image Builder simplifies the building, testing, and deployment of virtual machine (VMs) and container images for use in AWS or on-premises. Keeping virtual machine and container images up to date can be time consuming, resource intensive, and error-prone. Currently, customers either manually update and snapshot VMs or have teams that build automation scripts to maintain images.	Instead of having individual workload owners invest in security that is specific to their workloads, save time by using common security capabilities and shared components. Some examples of services that multiple teams can consume include the AWS account creation process, centralized identity for people, common logging configuration, Amazon Machine Image (AMI), and container base image creation. This approach can help builders improve workload cycle times and work to consistently meet security control objectives. When teams are more consistent, you can validate control objectives and better report your control posture and risk position to stakeholders.	Elastic Compute Cloud (Amazon EC2) pricing
	Amazon Inspector	Amazon Inspector is an automated vulnerability management service that continually scans Amazon Elastic Compute Cloud (Amazon EC2), AWS Lambda, and container workloads for software vulnerabilities and unintended network exposure.	Amazon Inspector continuously assesses your environment throughout the lifecycle of your resources by automatically scanning resources whenever you make changes to them. Events that initiate rescanning a resource include installing a new package on an Amazon EC2 instance, installing a patch, and the publication of a new common vulnerabilities and exposures (CVE) report that affects the resource. When an open vulnerability is detected, Amazon Inspector calculates an Amazon Inspector risk score by correlating up-to-date CVE information with temporal and environmental factors such as network accessibility and exploitability information to provide a contextual finding. Amazon Inspector is integrated with AWS Organizations and supports delegated administration.	Amazon inspector pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Secure configuration 4.1 4.2 4.4 4.7	AWS Firewall Manager	Firewall Manager is a security management service that you can use to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations. As new applications are created, Firewall Manager makes it simpler to manage resources by allowing you to enforce a common set of security rules.	Firewall Manager helps protect your network by simplifying your administration and maintenance tasks for AWS WAF, AWS Shield Advanced, Amazon Virtual Private Cloud (Amazon VPC) security groups, AWS Network Firewall, and Amazon Route 53 Resolver DNS Firewall across multiple accounts and resources. With Firewall Manager, you set up your AWS WAF rules, Shield Advanced protections, Amazon VPC security groups, AWS Network Firewall, and domain name system (DNS) firewall rule group associations only once. The service automatically applies the rules and protections across your accounts and resources, even as you add new resources.	AWS Firewall Manager pricing
	AWS Network Firewall	Network Firewall is a highly available managed network firewall service for your VPC. It enables you to deploy and manage stateful inspection, intrusion prevention and detection, and web filtering to help protect your virtual networks on AWS. You can also import rules you've already written in common open-source rule formats, and enable integrations with managed intelligence feeds sourced by AWS Partners.	There are multiple deployment models available with Network Firewall. The right model depends on your use case and requirements. Examples include the following: • A distributed deployment model where Network Firewall is deployed into individual VPCs. • A centralized deployment model where Network Firewall is deployed into a centralized VPC for east-west (VPC-to-VPC) or north-south (internet egress and ingress, on-premises) traffic. • A combined deployment model where Network Firewall is deployed into a centralized VPC for east-west and a subset of north-south traffic.	AWS Network Firewall pricing
	Amazon Route 53 Resolver DNS Firewall	With Route 53 Resolver DNS Firewall, you can filter and regulate outbound DNS traffic for your virtual private cloud (VPC).	Route 53 Resolver DNS Firewall lets you control access to sites and help block DNS-level threats for DNS queries going out from your VPC through Route 53 Resolver. With DNS Firewall, you define domain name filtering rules in rule groups that you associate with your VPCs. You can specify lists of domain names to allow or block, and you can customize the responses for the DNS queries that you block.	Route 53 Resolver DNS Firewall pricing
	Network access control lists (ACLs)	Network ACLs allow or deny specific inbound or outbound traffic at the subnet level.	Apply controls with a defense-in-depth approach for both inbound and outbound traffic. For example, for Amazon VPC this approach includes security groups and network ACLs.	Amazon VPC pricing
	Security groups	Security groups control the traffic that is allowed to reach and leave the resources that each security group is associated with.		

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Secure configuration 4.1 4.2 4.4 4.7	AWS Secrets Manager	Secrets Manager helps you manage, retrieve, and rotate database credentials, application programming interface (API) keys, and other secrets throughout their lifecycles.	Secrets Manager helps you protect the credentials (secrets) that you need to access your applications, services, and IT resources. You can replace hardcoded credentials in your code with an API call to Secrets Manager to retrieve the secret programmatically. This helps make sure that the secret can't be compromised by someone who is examining your code, because the secret no longer exists in the code.	AWS Secrets Manager pricing
	AWS Systems Manager Parameter Store	Parameter Store, a capability of AWS Systems Manager, helps provide secure, hierarchical storage for configuration data management and secrets management.	You can store data such as passwords, database strings, AMI IDs, and license codes as parameter values. Values can be stored as plain text or encrypted data. You can reference Systems Manager parameters in your scripts, commands, and configuration and automation workflows by using the unique name that you specified when you created the parameter.	AWS Systems Manager Parameter Store pricing
	AWS Identity and Access Management (IAM)	IAM is a web service that helps you securely control access to AWS resources. You can use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.	You cannot deploy AWS services without creating IAM principals and granting permissions first. A full explanation of IAM is beyond the scope of this document, but this section provides important summaries of best practice recommendations and pointers to additional resources. For IAM best practices, see Security best practices in IAM in the AWS documentation, IAM articles in the AWS Security Blog, and AWS Re:Invent presentations. The security pillar of the AWS Well-Architected Framework outlines key steps in the permissions management process: define permissions guardrails, grant least privilege access, analyze public and cross-account access, share resources securely, reduce permissions continuously, and establish an emergency access process. The AWS Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services in a multi-account environment. It can be used to help design, implement, and manage AWS security services so that they align with AWS recommended practices. The recommendations are built around a single-page architecture that includes AWS security services—how they help achieve security objectives, where they can be best deployed and managed in your AWS accounts, and how they interact with other security services.	No cost associated.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Secure configuration 4.1 4.2 4.4 4.7	AWS Identity and Access Management (IAM) Access Analyzer	IAM Access Analyzer helps identify resources in your organization and accounts that are shared with an external entity; validates IAM policies against policy grammar and best practices; and generates IAM policies based on access activity in your AWS CloudTrail logs.	Use IAM access advisor, AWS CloudTrail, IAM Access Analyzer, and related tooling to regularly analyze historical usage and permissions granted, and then remediate over-permissions.	No cost associated.
	AWS Shield	Shield is a managed distributed denial of service (DDoS) protection service that helps safeguard applications running on AWS.	There are two tiers of Shield: Shield Standard and Shield Advanced. AWS customers benefit from the automatic protections of Shield Standard at no additional charge. Shield Standard provides protection against the most common and frequently occurring infrastructure (layer 3 and 4) events. Shield Standard uses deterministic packet filtering and priority-based traffic shaping to automatically mitigate basic network layer unauthorized events. Shield Advanced provides more sophisticated automatic mitigations for unauthorized events that target your applications running on protected Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 resources.	AWS Shield pricing
	AWS WAF	AWS WAF helps you protect against common web exploits and bots that can affect availability, compromise security, or consume excessive resources.	You can use our preconfigured template to quickly get started with AWS WAF. The template includes a set of AWS WAF rules that can be customized to best fit your needs, and that are designed to block common web-based events. The rules help protect against bad bots, SQL injection, cross-site scripting (XSS), HTTP floods, and attempts by known bad actors. Once you deploy the template, AWS WAF begins to block the web requests to your CloudFront distributions that match the preconfigured rules in your web access control list (web ACL). You can use this automated solution in addition to other web ACLs that you configure.	AWS WAF pricing

Account and access management (NIST CSF – Protect)

Account and access management in AWS can be categorized into three main categories: developer and operator access to the AWS console, AWS CLI, and SDKs; consumer access to workloads hosted in AWS; and resource-to-resource access within the AWS environment.

We recommend that you manage developer access through federation to an existing identity provider (IdP), such as Active Directory, Okta, PingOne, or others. You can use IAM Identity Center to centrally manage or federate users to your existing IdP. You can also use IAM Identity Center to manage workforce permissions across your AWS accounts within an organization in AWS Organizations.

You can use Amazon Cognito to enable and manage access to workloads that you build, and to store consumer identities and manage permissions centrally for access to your workloads hosted on AWS. You should define clear processes for signup and sign-in flows, as well as offboarding flows, so that unique and strong passwords are enforced and accounts that are no longer needed are promptly removed.

See Security best practices in IAM for more details.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Account and access management 5.2 5.3 5.4 6.1 6.2 6.3 6.4 6.5	AWS Identity and Access Management (IAM)	IAM is a web service that helps you securely control access to AWS resources. You can use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.	You cannot deploy AWS services without creating IAM principals and granting permissions first. A full explanation of IAM is beyond the scope of this document, but this section provides important summaries of best practice recommendations and pointers to additional resources. For IAM best practices, see Security best practices in IAM in the AWS documentation, IAM articles in the AWS Security Blog, and AWS re:Invent presentations. The security pillar of the AWS Well-Architected Framework outlines key steps in the permissions management process: define permissions guardrails, grant least privilege access, analyze public and cross-account access, share resources securely, reduce permissions continuously, and establish an emergency access process. The AWS Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services in a multi-account environment. It can be used to help design, implement, and manage AWS security services so that they align with AWS recommended practices. The recommendations are built around a single-page architecture that includes AWS security services—how they help achieve security objectives, where they can be best deployed and managed in your AWS accounts, and how they interact with other security services.	No costs associated.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Account and access management 5.2 5.3 5.4 6.1 6.2 6.3 6.4 6.5	AWS IAM Identity Center	IAM Identity Center (successor to AWS Single Sign-On) helps you securely create or connect your workforce identities and manage their access centrally across AWS accounts and applications. IAM Identity Center is the recommended approach for workforce authentication and authorization on AWS for organizations of various size and type.	Identity and access management are key parts of an information security program, helping you to make sure that only authorized and authenticated users and components are able to access your resources, and only in a manner that you intend. For example, you should define principals (that is, accounts, users, roles, and services that can perform actions in your account), build out policies that are aligned with these principals, and implement strong credential management. These privilege-management elements form the core of authentication and authorization. IAM Identity Center can help centralize user and access management. If you have an existing identity provider (IdP) that you'd like to federate with, IAM Identity Center can support this. By centralizing your user and access management, you can make sure you have visibility and least privilege for your users.	No cost associated.
	AWS Config	AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources.	A foundational practice is to establish logging and monitoring at the account level. This base set of mechanisms is aimed at recording and detecting a wide range of actions on the resources in your account.	

Vulnerability management planning (NIST CSF – Protect)

Vulnerability management is another area within security that is different in the cloud compared to a traditional, more static, environment. In the cloud, you need to do more than assess the operating systems and software vulnerabilities—you also need to assess your cloud resources for risky configuration. In addition, many organizations adopt a shared responsibility model when addressing these findings, as opposed to having a central security team, and use a distributed approach where application or developer teams are responsible for resolving the findings within the workloads they build and operate.

In order to determine the security posture of your environment, we recommend that you use AWS Security Hub. Security Hub provides a comprehensive view for security findings across your AWS environments and Regions. You can configure findings aggregation, and your teams can use Security Hub as a central tool to review, investigate, and remediate security findings. Security Hub can also be used to distribute security findings to downstream tooling such as SIEM, alerting, and ticketing systems.

AWS Config can help you identify misalignment with policies, compliance frameworks, or industry best practices at the cloud layer.

AWS Systems Manager works with other tools to manage patching for the compute resources of the organization at the operating system and application layers, even when some of these resources reside in the on-premises environments that support an array of operating systems.

Amazon Inspector can aid an organization's vulnerability management capabilities by providing continuous scanning and patching of operating system and application layer vulnerabilities on EC2 instances, AWS Lambda functions, and container images. It uses the widely deployed AWS Systems Manager Agent (SSM Agent), so it is not necessary to deploy another independent agent.

If you want to use partner tooling, a convenient way to consume this is through AWS Marketplace. The Marketplace helps with the procurement, provisioning, and governance of third-party software, services, and data.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Vulnerability Management Planning 7.1 7.2 7.3 7.4 12.1	AWS Security Hub	Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner offerings.	Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices. Security Hub collects security data from across AWS integrated services, supported third-party products, and other custom security products that you might use. It helps you continuously monitor and analyze your security trends and identify the highest-priority security issues.	AWS Security Hub pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Vulnerability Management Planning 7.1 7.2 7.3 7.4 12.1	AWS Config	AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources.	AWS Config provides you with a mechanism for recording and detecting a wide range of actions on resources in your account.	AWS Config pricing
	AWS Systems Manager Patch Manager	Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes with both security-related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications. You can use Patch Manager to install service packs on Windows nodes and perform minor version upgrades on Linux nodes. You can patch fleets of Amazon EC2 instances, edge devices, or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Amazon Linux, Amazon Linux 2, CentOS, Debian Server, macOS, Oracle Linux, Raspberry Pi OS (formerly Raspbian), Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Ubuntu Server, and Windows Server. You can scan instances to see only a report of missing patches, or you can scan and automatically install the missing patches that are detected.	Patch and vulnerability management is a shared control from the AWS Shared Responsibility Model—controls that apply to both the infrastructure layer and customer layers, but in separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications. You are also responsible for patch management for your AWS resources, including Amazon EC2 instances, AMIs, and many other compute resources. For Amazon EC2 instances, you can use Patch Manager to automate the process of patching managed instances with both security-related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications.	AWS Systems Manager pricing
	Amazon Inspector	Amazon Inspector is an automated vulnerability management service that continually scans Amazon EC2, AWS Lambda, and container workloads for software vulnerabilities and unintended network exposure.	Amazon Inspector continuously assesses your environment throughout the lifecycle of your resources by automatically scanning resources whenever you make changes to them. Events that initiate rescanning a resource include installing a new package on an Amazon EC2 instance, installing a patch, and the publication of a new common vulnerabilities and exposures (CVE) report that affects the resource. When an open vulnerability is detected, Amazon Inspector calculates an Amazon Inspector risk score by correlating up-to-date CVE information with temporal and environmental factors such as network accessibility and exploitability information to provide a contextual finding. Amazon Inspector is integrated with AWS Organizations and supports delegated administration.	Amazon Inspector pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Vulnerability Management Planning 7.1 7.2 7.3 7.4 12.1	Elastic Container Registry (Amazon ECR) image scanning	Amazon ECR image scanning helps in identifying software vulnerabilities in your container images. Amazon ECR uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project. With basic scanning, you can configure your repositories to scan on push, or you can perform manual scans and Amazon ECR will provide a list of scan findings.	Amazon ECR provides basic image scanning that can help you identify software vulnerabilities on your container images stored in Amazon ECR.	Amazon ECR pricing
	AWS Security Bulletins	AWS makes public notifications in the form of security bulletins, which are posted on the AWS Security website. Individuals, companies, and security teams typically post their advisories on their own websites and in other forums, and when relevant, AWS includes links to those third-party resources on the AWS Security Bulletins site.	Monitor the AWS Security Bulletins site to make sure you receive the latest public notifications about security related vulnerabilities.	No cost associated.
	AWS Marketplace	From the AWS Marketplace, you can quickly launch preconfigured software and choose software solutions in AMIs, software as a service (SaaS) format, and other formats. Additionally, you can browse and subscribe to data products. Flexible pricing options include free trials, hourly, monthly, annual, and multi-year pricing, and a bring your own license (BYOL) model.	If you are running a third-party network infrastructure, such as a vendor AMI from the AWS Marketplace within your AWS environment, we recommend that you regularly check the vendor's website for security bulletins and monitor for security-related updates. Roll updates out in accordance with your patch and vulnerability management policy and procedures.	Refer to the AWS Marketplace listing for vendor-specific pricing.

Data recovery and incident response (NIST CSF – Respond)

Logs provide auditability and traceability and allow for technical troubleshooting and investigation of security events. AWS offers a number of services that can help you collect, aggregate, manage, and analyze logs. There are three key planes of logging: the control plane, the data plane, and the networking plane. The control plane includes access to the AWS service APIs, CLI, and management console, while the data plane refers to access to specific objects within services, such as objects stored within Amazon S3 or /var/log/messages on a Linux based EC2 instance. The network plane refers to logging network level activity within the virtual private cloud (VPC).

Logs are indispensable for incident response, because they provide answers to the who, what, where, and when of changes made to your environment. It is important to provide least privilege permissions to the logs, because they contain important information about how your system works, and to protect the logs from unauthorized or accidental deletion. We recommend that you store your logs in a dedicated AWS account such as a log archive account. This provides you with a centralized dedicated account to aggregate, manage, and apply protective controls to your log data. Managing logs in a central account can simplify permissions and monitoring activities. There is no cost associated with the creation of an AWS account; however, there are costs for the associated data storage. To help with costs, you can use an Amazon S3 Lifecycle configuration to manage the lifecycle of logs that are stored in S3, while helping protect them from accidental deletion. Amazon S3 Lifecycle uses transition policies to move objects to more cost-effective storage for logs that are not frequently used or needed for compliance, and expiration actions can delete data that is no longer necessary, freeing up budget for other initiatives.

You can enable an AWS CloudTrail trail for accounts within your AWS Organizations organization, which can provide you with improved visibility. This visibility can include actions taken by a user, role, or AWS service on AWS resources through the console, AWS CLI, or the AWS SDKs and APIs. AWS Control Tower automatically creates a log archive account and enables critical logging services such as AWS CloudTrail and AWS Config, and it records them in Amazon CloudWatch.

CloudTrail also allows you to enable data events logging for Amazon S3, AWS Lambda, Amazon Cognito, Amazon DynamoDB, and other services, which can provide valuable visibility into the data (distinct from operations on the configuration of the service), which is especially important for buckets that contain sensitive information. For additional data plan logging, many services support publishing logs to Amazon CloudWatch Logs. You can use this feature to collect logs for other resources, as well as non-API logs for AWS services, and manage retention of those logs by using CloudWatch log data retention.

AWS recommends that customers who are using a VPC enable network traffic flow and DNS logs by using, respectively, VPC Flow Logs and Amazon Route 53 Resolver query logs. These logs can be streamed to either an S3 bucket or a CloudWatch log group. You can create a VPC flow log for a VPC, a subnet, or a network interface. You can be selective regarding how and where you enable VPC Flow Logs to reduce cost.

AWS CloudTrail logs, VPC Flow Logs, and Route 53 Resolver query logs are three core components that provide data for security investigations. Other AWS services can generate logs and findings that are not captured by this basic logging trifecta, such as Elastic Load Balancing logs, AWS WAF logs, AWS Config recorder logs, Amazon GuardDuty findings, Amazon Elastic Kubernetes Service (Amazon EKS) audit logs, and Amazon EC2 instance operating system and application logs. Amazon Security Lake automatically collects logs for AWS CloudTrail, Amazon Virtual Private Cloud (VPC), Amazon Route 53, Amazon Simple Storage Service (S3), and AWS Lambda. It also collects security findings through AWS Security Hub for AWS Config, AWS Firewall Manager, Amazon GuardDuty, AWS Health, AWS Identity and Access Management (IAM) Access Analyzer, Amazon Inspector, Amazon Macie, and AWS Systems Manager Patch Manager. You can also add data from third-party security solutions that support the Open Cybersecurity Schema Framework (OCSF) and your custom data. This data includes logs from internal applications or network infrastructure that you have converted into OCSF format. For more guidance related to logging, see the recently updated AWS Security Incident Response Guide. Refer to Appendix A: Cloud capability definitions in the Security Incident Response Guide for the full list of logging and monitoring options.

In AWS, there are several services you can use to query logs, such as CloudWatch Logs Insights for data that is stored in CloudWatch log groups; Amazon Security Lake; and Amazon Athena and Amazon OpenSearch Service for data that is stored in Amazon S3. You can also use third-party tools such as a security information and event management (SIEM) solution.

Considered as one of the top 10 security items to improve in your AWS account, we recommend that you regularly check and update your AWS account and security contact information, which provides AWS with the necessary points of contact to share information, collaborate, and orchestrate a response if needed. Review this section of the AWS Security Incident Response Guide for more information about updating your AWS account contact information.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Incident response and management 8.1 8.2 8.3 17.1 17.2	AWS CloudTrail	CloudTrail is an AWS service that helps you enable operational and risk auditing within your AWS account. Actions taken by a user, role, or AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS CLI, and AWS SDKs and APIs.	Use AWS Organizations and enable the organization trail. This setting will enable CloudTrail in both existing and new AWS accounts within an organization in AWS Organizations. This also simplifies configurations to send logs to the dedicated Log Archive account.	AWS CloudTrail pricing
	Amazon S3 data events	Data events provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities.	Amazon S3 data events should be enabled on S3 buckets that contain objects that an organization considers to be sensitive, such as business critical data, regulated data (for example, protected health information (PHI) or personally identifiable information (PII)), or other classifications deemed sensitive to an organization.	AWS CloudTrail pricing
	AWS services and log destinations	Although many services only publish logs to Amazon CloudWatch Logs, some AWS services can publish logs directly to Amazon S3 or Amazon Kinesis Data Firehose. If your main requirement for logs is storage or processing in one of these services, you can have the service that produces the logs send them directly to Amazon S3 or Kinesis Data Firehose without additional setup.	There are several models to help meet this requirement. You could leverage AWS Security Hub, Amazon Security Lake, or an existing SIEM tool in your security suite. You could also leverage a custom Centralized Logging on AWS solution. This solution contains a suite of infrastructure services that deploy centralized logging to collect Amazon CloudWatch Logs from multiple accounts and AWS Regions. It uses Amazon OpenSearch Service and Kibana, an analytics and visualization platform that is integrated with Amazon OpenSearch Service, to create a unified view of log events.	Centralized logging solution pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Incident response and management 8.1 8.2 8.3 17.1 17.2	Amazon S3 Lifecycle policies	To manage your objects so that they are stored cost effectively throughout their lifecycle, you can configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects.	There are two types of actions: Transition actions define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-Infrequent Access (IA) storage class 30 days after creating them, or archive objects to the S3 Glacier Flexible Retrieval storage class one year after creating them. Expiration actions define when objects expire. Amazon S3 deletes expired objects on your behalf.	Lifecycle policies do not themselves accrue a cost; the transition to different storage does.
	Amazon CloudWatch and CloudWatch log data retention	Amazon CloudWatch monitors your AWS resources and the applications you run on AWS in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications. The unified CloudWatch agent enables you to collect internal system-level metrics from EC2 instances across operating systems, collect system-level metrics from on-premises servers, and retrieve custom metrics from your applications or services. By default, log data is stored in CloudWatch Logs indefinitely. However, you can configure how long to store log data in a log group. Data older than the current retention setting is deleted. You can change the log retention for each log group at your convenience.	Use CloudWatch to collect logs from other resources, in addition to non-API logs for AWS services. Data retention should be configured to the requirements of the organization.	Amazon CloudWatch pricing
	AWS account and security contact information	You can store contact information about the primary account contact for your AWS account. You can also add or edit contact information for the alternate security account contact, which receives security-related notifications, including notifications from the AWS Trust and Safety Team.	Modify the account name, email address, or password for the AWS account root user. Update the alternate security contact across your AWS accounts for timely security notifications.	No costs associated.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Incident response and management 8.1 8.2 8.3 17.1 17.2	VPC Flow Logs	VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to the following locations: Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. After you create a flow log, you can retrieve and view the flow log records in the log group, bucket, or delivery stream that you configured.	Flow logs can help you with a number of tasks, such as: • Diagnosing overly restrictive security group rules • Monitoring the traffic that is reaching your instance • Determining the direction of the traffic to and from the network interfaces Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. You can create or delete flow logs without risk of impact to network performance.	VPC Flow Logs pricing (select Logs and scroll to Vended Logs)
	CloudTrail Lake	AWS CloudTrail Lake is a managed data lake that lets organizations aggregate, immutably store, and query events recorded by CloudTrail for auditing, security investigation, and operational troubleshooting. This new service simplifies CloudTrail analysis workflows by integrating collection, storage, preparation, and optimization for analysis and query in the same product. With this, you won't need to maintain separate data processing pipelines that span across teams and products to analyze CloudTrail events.	CloudTrail Lake does not require you to move and ingest CloudTrail logs elsewhere, which helps maintain data fidelity and decreases dealing with low-rate limits that throttle your logs. It also provides near real-time latencies, because it is fine-tuned to process high-volume structured logs, making them available for incident investigation. Also, CloudTrail Lake provides a multi-attribute query experience with SQL and is capable of scheduling and handling multiple concurrent queries.	AWS CloudTrail Lake pricing
	Amazon Security Lake	Amazon Security Lake automatically centralizes security data from cloud, on-premises, and custom sources into a purpose-built data lake that is stored in your account. With Security Lake, you can get a more complete understanding of your security data across your entire organization.	You can use Security Lake to help you improve the protection of your workloads, applications, and data. Security-related data includes service and application logs, security alerts, and threat intelligence (such as known malicious IP addresses), which are the source of truth for detecting, investigating, and remediating security incidents. Security best practice requires an effective log and security event data management process. Security Lake automates this process and facilitates solutions that perform streaming analytics detections, time-series analytics, user and entity behavior analytics (UEBA), security orchestration and remediation (SOAR), and incident response.	Amazon Security Lake pricing

Malware defense (NIST CSF – Protect)

There are several AWS native solutions and partner products and solutions available to help you perform malware detection and protection in your AWS environment. One AWS native solution you can use is Amazon GuardDuty Malware Protection. With Malware Protection enabled, whenever GuardDuty detects suspicious behavior on an Amazon EC2 instance or a container workload, GuardDuty Malware Protection automatically initiates an agentless scan on the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the impacted EC2 instance or container workload to detect the presence of malware.

You can also enable Amazon Route 53 Resolver DNS Firewall to filter and regulate outbound DNS traffic for your VPC. To do this, you create reusable collections of filtering rules in DNS Firewall rule groups, associate the rule groups to your VPC, and then monitor activity in DNS Firewall logs and metrics. Based on the activity, you can adjust the behavior of DNS Firewall accordingly.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Email and browser protections 9.1	AWS Systems Manager Inventory	Inventory, a capability of AWS Systems Manager, provides visibility into your AWS computing environment.	You can use Inventory to collect metadata from your managed nodes. You can store this metadata in a central Amazon S3 bucket, and then use built-in tools to query the data and quickly determine which nodes are running the software and configurations required by your software policy, and which nodes need to be updated. You can also configure and view inventory data from multiple AWS Regions and AWS accounts.	AWS Systems Manager Pricing
Email and browser protections 9.2	Amazon Route 53 Resolver DNS Firewall	Resolver DNS Firewall, a capability of Amazon Route 53, provides protection for outbound DNS requests from your VPCs.	With Resolver DNS Firewall, you can filter and regulate outbound DNS traffic for your VPC. To do this, you create reusable collections of filtering rules in DNS Firewall rule groups, associate the rule groups to your VPC, and then monitor the activity in DNS Firewall logs and metrics. With DNS Firewall, you can monitor and control the domains that your applications can query. You can deny access to the domains that you know to be malicious and allow other queries to pass through. Alternately, you can deny access to all domains except for the ones that you explicitly trust.	Amazon Route 53 Resolver DNS Firewall pricing
Malware defenses 10.1 10.2	Amazon GuardDuty Malware Protection	Malware Protection, a capability of Amazon GuardDuty, scans and detects malware on Amazon Elastic Block Store (Amazon EBS) volumes attached to your potentially compromised Amazon EC2 instances and container workloads.	With Malware Protection enabled, whenever GuardDuty detects suspicious behavior on an Amazon EC2 instance or a container workload, Malware Protection automatically initiates an agentless scan.	Malware Protection in Amazon GuardDuty pricing

Security awareness and skills training (NIST CSF – Protect)

Security awareness programs and training have proven to increase security consciousness among the workforce and improve the skills needed to address cybersecurity risks. Security awareness training should be implemented annually, at a minimum, in order to keep your workforce up-to-date on identifying security-related risks. Training programs like AWS Skill Builder can help your workforce learn how to interact with enterprise assets and data in a secure manner. AWS Workshops provides hands-on labs for you to educate your workforce on AWS services, including in security-related focus areas. The AWS Well-Architected Tool helps guide cloud architects in building a secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Security awareness and skills training 14.1 14.2 14.6	AWS Skill Builder	AWS Skill Builder offers digital training for over 500 on-demand courses and learning plans so you can build the skills you need.	Through the use of Skills Builder, your team can learn core concepts and the application of AWS tools in a lecture-style program. This helps team members bridge gaps in skill areas that are specific to their role or learn AWS tools at a higher level.	AWS Skill Builder pricing
	AWS Workshops	Workshops are hands-on events designed to teach or introduce practical skills, techniques, or concepts.	Your team can use workshops to get a better hands-on understanding of AWS tools and services in scenarios that follow real-world use cases. Workshop content can help customers ramp up in their job area and be more successful.	The costs associated with workshops varies depending on the details for each workshop. In many cases, you can delete or clean up the resources created after the workshop with few associated fees.
	AWS Well-Architected Tool	AWS Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. Built around six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—AWS Well-Architected provides a consistent approach for customers and partners to evaluate architectures and implement scalable designs.	The AWS Well-Architected Framework includes domain-specific lenses, hands-on labs, and the AWS Well-Architected Tool. The AWS Well-Architected Tool, available at no cost in the AWS Management Console, provides a mechanism for regularly evaluating workloads, identifying high-risk issues, and recording improvements.	No costs associated.

Data recovery and incident response (NIST CSF – Recover)

It is important for organizations to have processes in place to restore systems to their last known good configuration in cases when a security event cannot be stopped or absorbed. We recommend that you have a plan and solution in place and perform regular recovery exercises so that you can quickly recover from an incident and return to the normal operation baseline.

AWS Backup is a fully-managed backup service that centralizes and automates the backup of data across AWS services. AWS Backup provides an orchestration layer that integrates Amazon CloudWatch, AWS CloudTrail, AWS Identity and Access Management (IAM), AWS Organizations, and other services. This centralized AWS Cloud native solution provides global backup capabilities that can help you achieve your disaster recovery and compliance requirements. By using AWS Backup, you can centrally configure backup policies and monitor backup activity for AWS resources. In addition, Amazon EBS Snapshots provide a way to copy an EBS volume and store it using Amazon S3 features, including lifecycle, data protection, and access to protection mechanisms. Two of these mechanisms are S3 Object Lock and AWS Backup Vault Lock, which can provide you with additional security and control over your backups. Clear separation of duties and access should be managed for backups. Backups should be isolated at the account level to maintain separation from the affected environment during an event.

For organizations that need a full recovery solution for cloud-based or on-premises applications, AWS Elastic Disaster Recovery can help you quickly and reliably recover applications while using affordable storage, minimal compute, and point-in-time recovery.

Finally, we recommend that you build your AWS environment and resources with infrastructure-as-code solutions like AWS CloudFormation. With CloudFormation, you can define your resource in code and use mappings and parameters to deploy your resources in different AWS accounts and AWS Regions, which can help you test your disaster recovery processes and make it simpler to build out test environments. AWS CodeCommit is a secure and highly scalable, managed source-control repository that provides backup and restore capabilities for configuration files, including CloudFormation templates. Organizations can use CodeCommit in combination with CloudFormation to quickly deploy infrastructure as code for testing, or in case of an event.

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Data recovery and incident response 11.1 11.2 11.3 11.4	AWS Backup	AWS Backup enables you to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed policy-based service that further simplifies data protection at scale. Sample use cases include backup and restoration capabilities for systems, periodic backups of information, and immutable storage.	Regularly back up your data and test your backup files to enable recovery from both logical and physical errors. A key to managing failure is the frequent and automated testing of workloads to cause failure and then observe how they recover. We recommend that you do this on a regular schedule and test after significant workload changes. The objective is to thoroughly test your workload-recovery processes so that you are confident that you can recover all your data and continue to serve your customers, even in the face of sustained problems. Your recovery processes should be exercised as thoroughly as your normal production processes. You can use AWS Backup to schedule your backups of supported services.	AWS Backup pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Data recovery and incident response 11.1 11.2 11.3 11.4	AWS Backup	AWS Backup enables you to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed policy-based service that further simplifies data protection at scale. Sample use cases include backup and restoration capabilities for systems, periodic backups of information, and immutable storage.	Regularly back up your data and test your backup files to enable recovery from both logical and physical errors. A key to managing failure is the frequent and automated testing of workloads to cause failure and then observe how they recover. We recommend that you do this on a regular schedule and test after significant workload changes. The objective is to thoroughly test your workload-recovery processes so that you are confident that you can recover all your data and continue to serve your customers, even in the face of sustained problems. Your recovery processes should be exercised as thoroughly as your normal production processes. You can use AWS Backup to schedule your backups of supported services.	AWS Backup pricing
	Amazon EBS Snapshots	Amazon EBS provides the ability to create snapshots (backups) of EBS volumes. A snapshot takes a copy of the EBS volume and places it in Amazon S3, where it is stored redundantly in multiple Availability Zones.	You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. Each snapshot contains the information that is needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume.	Amazon EBS Snapshot pricing
	AWS Elastic Disaster Recovery	AWS Elastic Disaster Recovery minimizes downtime and data loss with fast and reliable recovery of on-premises and cloud-based applications by using affordable storage, minimal compute, and point-in-time recovery.	You can set up Elastic Disaster Recovery on your source servers to initiate secure data replication. Your data is replicated to a staging area subnet in your AWS account in the AWS Region you select. The staging area design reduces costs by using affordable storage and minimal compute resources to maintain ongoing replication. You can perform non-disruptive tests to confirm that implementation is complete. During normal operation, maintain readiness by monitoring replication and periodically performing non-disruptive recovery and failback drills. If you need to recover applications, you can launch recovery instances on AWS within minutes, using the most up-to-date server state or a previous point in time. After your applications are running on AWS, you can choose to keep them there, or you can initiate data replication back to your primary site when the issue is resolved. You can fall back to your primary site whenever you're ready.	AWS Elastic Disaster Recovery pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Data recovery and incident response 11.1 11.2 11.3 11.4	AWS CodeCommit	CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. It makes it simple for teams to securely collaborate on code with contributions encrypted in transit and at rest. CodeCommit reduces the need for you to manage your own source control system or worry about scaling its infrastructure. You can use CodeCommit to store anything from code to binaries. The service supports the standard functionality of Git, so it works seamlessly with your existing Git-based tools.	CodeCommit is a fully managed source control service that hosts secure GitHub-based repositories. It provides backup and restore capabilities for configuration files.	AWS CodeCommit pricing
	AWS Organizations	AWS Organizations lets you create new AWS accounts at no additional charge. You can allocate resources, group accounts, and apply governance policies to accounts or groups. The AWS account is an important means through which AWS enables security of your applications.	AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. By using AWS Organizations, you can programmatically create new AWS accounts, allocate resources, group accounts to organize your workloads, and apply policies to accounts or groups of accounts for governance. An organization consolidates your AWS accounts so that you can administer them as a single unit. It has one management account along with zero or more member accounts. Most of your workloads reside in member accounts, except for some centrally-managed processes that must reside in either the management account or in accounts assigned as delegated administrators for specific AWS services. You can provide tools and access from a central location for your security team to manage security needs on behalf of an organization.	There is no cost for creating an AWS account. Total cost is based on the usage within the account.
	AWS Control Tower	AWS Control Tower provides a simple way to set up and govern a secure, multi-account AWS environment, called a landing zone. It creates your landing zone by using AWS Organizations, bringing ongoing account management and governance as well as implementation best practices based on AWS experience working with thousands of customers as they move to the cloud.	AWS Control Tower offers a simplified way to set up and govern multiple accounts. It automates the setup of accounts in your AWS organization, automates provisioning, applies guardrails (which include preventive and detective controls), and provides you with a dashboard for visibility. An additional IAM management policy, a permissions boundary, is attached to specific IAM principals (users or roles) and sets the maximum permissions that an identity-based policy can grant to an IAM principal.	AWS Control Tower pricing

Capability and CIS mapping	AWS service	AWS service description	Configuration guidance	Cost
Data recovery and incident response 11.1 11.2 11.3 11.4	Amazon S3 Object Lock	With Amazon S3 Object Lock, you can store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use Object Lock to help meet regulatory requirements that require WORM storage, or to simply add another layer of protection against object changes and deletion.	Based on the criticality of your data, you may decide to enable Object Lock for some buckets, which provides you with an additional layer of deletion protection.	No associated costs.
	AWS Backup Vault Lock	AWS Backup Vault Lock enforces a WORM setting for the backups you store and create in a backup vault. With Backup Vault Lock, you can add an additional layer of defense that protects backups (recovery points) in your backup vaults from inadvertent or malicious delete operations and updates that shorten or otherwise alter their retention period. Backup Vault Lock helps you enforce retention periods, prevent early deletions by privileged users (including the AWS account root user), and helps you meet your organization's data protection policies and procedures.	Based on the criticality of your data, you may decide to enable AWS Backup Vault Lock as an additional layer of deletion protection.	No associated costs.
	AWS Cloud Formation	AWS CloudFormation gives you a convenient way to model a collection of related AWS and third-party resources, provision them quickly and consistently, and manage them throughout their lifecycles by treating infrastructure as code.	Use CloudFormation to deploy infrastructure as code to recover workloads quickly after an incident. Using infrastructure as code makes deploying and testing these processes fast and allows for automation.	AWS CloudFormation pricing

Conclusion

This blueprint is a resource that companies of all sizes and sectors can take advantage of to implement measures to defend against ransomware. Because data is often vital to the operation of mission-critical services, ransomware can severely disrupt business processes and applications that depend on this data. For this reason, many organizations are looking for effective security controls that will improve their security posture against these types of events. We hope you find the information in the AWS Blueprint for Ransomware Defense helpful and incorporate it as a tool to provide additional layers of security to help keep your data safe.

Contributors

Jeremy Ware – Security Specialist Solutions Architect, AWS

Kyle Dickinson – Senior Security Specialist Solutions Architect, AWS

Luis Pastor – Senior Security Specialist Solutions Architect, AWS

Megan O'Neil – Principal Security Specialist Solutions Architect, AWS

Further reading

AWS Well-Architected Framework – Security Pillar:
https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html
AWS Security Reference Architecture (AWS SRA):
https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html
AWS protecting against ransomware resource page:
https://aws.amazon.com/security/protecting-against-ransomware/
Security best practices in IAM:
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
Protecting your AWS environment from ransomware (e-book):
https://d1.awsstatic.com/psc-digital/2022/gc-200/security-ransomware-ebook/Security-Ransomware-eBook.pdf
Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF):
https://docs.aws.amazon.com/whitepapers/latest/ransomware-risk-management-on-aws-using-nist-csf/ransomware-risk-management-on-aws-using-nist-csf.html
AWS Security Incident Response Guide:
https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html

Have a question?
Contact us for general support services.

© 2023, Amazon web Services, or its affiliates. All rights reserved.