Brought to you by:

WIZ

AWS Security Foundations

for dummies®
A Wiley Brand

Explore cloud security best practices

Secure AWS resources, identities and access

Respond to AWS security incidents

Wiz Special Edition

Ed Tittel

Hello readers!

Before you wave your wand and go to the next page, here's what you need to know about us at Wiz.

Founded in 2020, Wiz is the fastest growing software company in the world.* Our mission is to make cloud environments secure for companies, no matter what cloud provider they use and no matter how big or small they are. Use Wiz to provide your security and development teams with full-stack visibility and exact accuracy to fix critical risks in your cloud.

Yours,
Assaf Rappaport
CEO of Wiz

*Frost & Sullivan: 2023 Entrepreneurial Company of the Year Recognition

AWS Security Foundations

Wiz Special Edition

by Ed Tittel

for dummies®
A Wiley Brand

AWS Security Foundations For Dummies®, Wiz Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-20674-2 (pbk); ISBN 978-1-394-20675-9 (ebk)

Publisher’s Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Jen Bingham

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Acct. Mgr: Cynthia Tweed

Content Specialist: Pradesh Kumar

Introduction

These days, security professionals have an urgent need to address potential threats and ensure safe, secure cloud deployments. This comes with ever-increasing use of API calls for top cloud platforms such as Amazon Web Services (AWS).

At the same time, many companies use more than one cloud platform. This requires them to increase the skills and knowledge in their security teams to cover all the bases (including the sometimes tricky interfaces used to tie multiple clouds together, and to the data center).

Data leaks and the risks of data exposure are especially worrisome. In other words, cloud security is more than just a nice-to-have kind of thing. It's absolutely essential, and can save your business from losses or reputational damage, not to mention possible fines and penalties from compliance failures. In this book, find out how to steer clear of trouble, and make the most of AWS resources, tools, and security coverage.

About This Book

The pages that follow discuss how using a modern cloud environment like AWS services can be kept safe and secure according to the following approaches or techniques:

- **AWS security foundations:** Explains how responsibility is divided between the provider and the customer and what kinds of actions customers can take to cover their side of the ledger.
- **Securing AWS infrastrure:** Employing zero trust to protect your environment at every layer, including hosts, applications, and the network.
- **Protecting identity and permissions:** Using best practices, tools, and approaches to identify users, and make sure they can access the right stuff for the right reasons at the right time.

- **Monitoring, protecting, and responding to activity:** Working in the cloud means expecting and dealing with danger or attack, while remaining calm and collected. You'll learn about detection and response, data protection, and incident handling. This book tells you what to do, and provides examples of how to do it.

Icons Used in This Book

Throughout this book, you'll find the following icons that highlight tips, important items to remember, and more:

TIP

This icon guides you to faster ways to perform essential tasks, such as better ways to put a cloud data lake to work.

REMEMBER

Here you'll find ideas worth remembering as you immerse yourself in the exciting world of data lake concepts.

WARNING

Steers you clear of a potential gotcha, or pitfall, that might otherwise invite unwanted outcomes or consequences.

TECHNICAL STUFF

This marks out information with technical content.

Beyond the Book

AWS maintains a collection of guidance to help architects build and run secure, high-performance, resilient, and efficient cloud-based instrastructures for their applications and workloads. This huge body of content includes key aspects, called "pillars." Together, that collection is called AWS Well-Architected and the Six Pillars. One of those pillars is security, and runs well over 100 pages. Find it at `https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html`. The parent document, with links to all of the pillars resides at: `https://aws.amazon.com/architecture/well-architected/`. This is great stuff, so knock yourself out!

IN THIS CHAPTER

- » **Examining security in the cloud**
- » **Listing key AWS areas**
- » **Looking at security foundations**

Chapter 1

Introduction to AWS and Cloud Security

AWS is short for Amazon Web Services. Though Amazon's roots are in the book business, it's now best known for its vibrant, global online marketplace and for the underlying web and cloud infrastructures it makes available on demand to organizations and users anywhere and everywhere.

Indeed, it's no lie to say that information technology and processing are heading for the cloud, if they're not there already. In fact, AWS supports over 1 million active users, of which 10 percent are enterprise class, and the rest small to medium-sized businesses. That includes most of the Fortune 500 and over 90 percent of the Fortune 100.

Pondering Cloud Security

According to the Cloud Security Alliance, AWS holds over 41 percent of the cloud computing market (more than Microsoft Azure, Google Cloud, and IBM combined). For those who work in modern IT, working with cloud platforms, tools, and technologies is inevitable. So is working with AWS (or rather APN, the AWS Partner Network).

Cloud security is a term that encompasses the policies, procedures, technologies, and tools needed to handle business security threats as organizations move into the cloud — both internal and external. Because one can deploy oodles and scads of cloud-based systems with the push of a button, a solid security posture is crucial. New technologies like the cloud need new security solutions to protect digital assets, while making them available to consumers, users, and customers.

REMEMBER

Protecting the data and applications that run in the cloud is key as organizations move into and depend on the cloud to connect them to employees, partners, customers, and supply chains. In today's world, insecure cloud configurations can invite breach and possibly theft or loss of data. More reasons why protecting what's in the cloud is central to maintaining proper security posture and due diligence.

Six Key Areas of AWS

When working with AWS in particular, and the cloud in general, a set of key elements serves to help users understand how best to protect their cloud-based workloads and applications. These six pillars for security — with brief explanations — include the followings:

- **Security foundations:** How to make best use of cloud technologies to protect data, systems, and assets safely and security. It includes a set of design principles to implement strong identity management, enable traceability, apply security at ever layer, automate best practices, and more.
- **Infrastructure protection:** Embraces methods of security control — such as defense-in-depth — to implement best practices and comply with organizational policies, laws, and regulations. Such methods are essential for successful, always-on cloud operations.
- **Identity and access management (IAM):** The methods and tools whereby you identify users and applications, and grant them permissions to access cloud-based resources. IAM

helps ensure that the right people can access the right resources under the right conditions. AWS offers a wide range of options through which to manage machine and human identities and their associated permissions.

- **Detection:** Simply put, detection means noticing what's happening, especially if it involves unexpected or unwanted configurations, or unexpected (even suspicious) behavior. Configuration checks should occur during development and test, prior to deployment, and then constantly in production environments for real use. Unexpected behavior may be detected through monitoring tools or by analyzing frequency and type of events (such as API calls, file encryption, unusual data deliveries, and more).
- **Data protection:** Before creating or running any workload, basic data security practices should be in use. Data classification is a good example: It provides ways to categorize data by its level of sensitivity. Likewise, data encryption renders it unreadable to unauthorized access. Such practices prevent mishandling of data, and comply with regulatory requirements.
- **Incident response:** A set of procedures and practices for responding to (and handling, or mitigating) potential impacts of security incidents. This is an arena where practice makes perfect and ensures that security teams can operate as needed during an actual incident. The key steps are to identify and isolate the incident, contain its impact, collect forensics to understand what happened, and to restore operations to a known, good, working state. This means putting tools and access in place in advance, and practicing response through game days, penetration testing, and adjusting to reflect lessons learned.

Security Practice Foundations

With the building blocks of a workable and effective security practice in place, you can gain the control and confidence needed to run your business within the flexible and secure confines of a cloud platform like AWS. AWS customers can take advantage of data centers and a network purpose-built to protect data, identities, applications, and devices. Thus, AWS improves an organization's capability to meet essential security requirements, including data protection, data locality, and data confidentiality.

Better yet, AWS supports easy automation of manual security tasks. That frees your security team to focus on scaling up, and providing new services or solutions for your customers. In 2014, the US Government inked an agreement with AWS through the National Security Agency and the CIA for $600M worth of top-secret classified on-demand computing and analytic services. If it's secure enough for the Feds, it's probably secure enough for your company.

AWS provides extensive guidance on how to implement, control, and use its 175 available services safely and securely. For more information, visit any or all of these links:

- **AWS Well Architected:** Learn, measure, and build using architectural best practices: Security Pillar `https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html`
- **AWS Cloud Security:** Infrastructure and services to elevate your security in the cloud `https://aws.amazon.com/security`
- **Security, Identity and Compliance on AWS:** `https://aws.amazon.com/products/security`

TIP

AWS (and the cloud) can be as secure as you need it to be given the right approach to security. This can be attained by following the foundational principles and establishing the right practices to maintain and monitor security.

IN THIS CHAPTER

- **» Sharing security in AWS**
- **» Governing risk**
- **» Configuring AWS**

Chapter 2 AWS Security Foundations

Cloud security describes various policies, procedures, technologies, and tools used to anticipate and address security threats in an organization. These may be internal (employees, contractors, consultants, and so forth, perhaps with an axe to grind) or external (third-parties in search of illicit information, profit, or advantage). Either way, organizations must prepare for and deal with security threats and exposures, as a matter of good practice and governance, as well as comply with regulations surrounding sensitive, proprietary, and personal data.

This is as true in the cloud as it is on an organization's premises. It might be tempting to surrender security oversight to service providers or other third parties, especially in the cloud. You're paying them for access and resources, so shouldn't security coverage come as part of the deal? Not completely! Security comes down to data protection, ownership, and control: You don't want to surrender any of those.

AWS Security Is a Shared Responsibility

Surprisingly, security in the cloud is easier because your cloud service provider handles the physical security for the data center (and what is shared in a shared responsibility model). Indeed, you are still on the hook for the security of your data, which applications, and uses. That's why it's so important to have a security foundation in place. You can take advantage of physical security and overall access controls baked in by the cloud service provider, but you must still take responsibility for data security, accounts and privileges, monitoring access and use, and ensuring compliance with security policies, governance, and compliance requirements.

TIP

Find the details on who's got what at `https://aws.amazon.com/compliance/shared-responsibility-model/`.

Covering your end

Indeed, it's important to understand the responsibilities that you, the customer, retain while operating in the cloud. In general, a cloud provider (AWS, in this discussion) is responsible for securing the underlying cloud infrastructure. The customer retains responsibility for securing whatever workloads they deploy within that environment. That also means protecting data and applications running inside those workloads, and all that goes with it. Figure 2-1 shows a diagram of what's involved for customers and AWS.

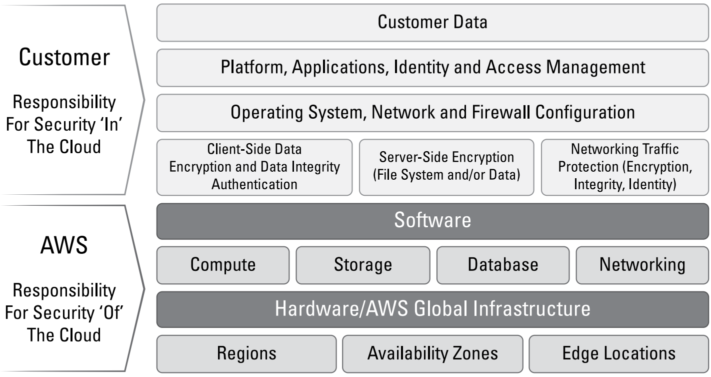

Customer
Responsibility For Security 'In' The Cloud
Customer Data
Platform, Applications, Identity and Access Management
Operating System, Network and Firewall Configuration
Client-Side Data Encryption and Data Integrity Authentication
Server-Side Encryption (File System and/or Data)
Networking Traffic Protection (Encryption, Integrity, Identity)
AWS
Responsibility For Security 'Of' The Cloud
Software
Compute
Storage
Database
Networking
Hardware/AWS Global Infrastructure
Regions
Availability Zones
Edge Locations

FIGURE 2-1: Responsibility for cloud workloads (customer up, AWS down).

As shown in Figure 2-1, AWS covers protection for the infrastructure that run services provided in the AWS cloud. That includes the hardware, software, networking, and capabilities that run AWS Cloud Services.

Consider service choices

Customer responsibilities vary depending on the AWS Cloud Services they run. This determines the configuration work they must perform as part of their security responsibilities.

For example, the Amazon Elastic Compute Cloud (EC2) works like an infrastructure-as-a-service (IaaS). This requires customers to handle all necessary security configuration and management tasks just as they would on any infrastructure they might operate. As shown in the upper portion of Figure 2-1, this means managing the following (from the bottom up):

- Data protection including client-side data encryption, data integrity controls (IAM), server-side encryption (for instance file-based systems and data), and managing traffic within the virtual network on which the infrastructure runs
- The guest operating system (including security patches and updates), whatever applications or utilities they run inside those instances, and configuration of an AWS-provided firewall (known as a security group) for each such instance
- The platform and applications running on the guest OS instances, including IAM to control login, access, permissions, and so forth
- The data that's ingested, manipulated, used, and stored inside those guest OSes, including data protection, access controls, monitoring and tracking, and more

REMEMBER

Some compliance regimes or organizational policies may require tracking, auditing, and reporting on access to sensitive information (PII, health records, and so on).

On the other side of the cloud connection, AWS covers the underlying cloud infrastructure, including computer, storage, database, and networking capabilities. Beneath those abstract services, AWS also manages — and provides security for — the underlying regions, availability zones, and edge locations where AWS services work and run.

Manage Risk via Governance

As a matter of best practice, organizations should separate AWS accounts for different workloads, so they can control who has access (and monitor what accounts are doing). This also means establishing a strong boundary between production and test environments, with each one distinct and apart from the other. The same approach is good for workloads that process data with differing levels of sensitivity. That is, you don't want to mix accounts that handle sensitive data with those for more routine and mundane tasks.

TIP

At the same time, when accounts are set up, preventative policies help keep things properly scoped and controlled. You can limit accounts to specific services, regions, and service action. For example, a user account can access specific services as defined by an administrator, such as launching EC2 instances. That user would be denied access to other services not specifically allowed, such as reading data from a particular database.

Centralized AWS Configuration

AWS organizations provide a single, consistent way to configure AWS services that apply to all accounts. For example, you can configure centralized logging to use AWS CloudTrail for all your member accounts. This supports a single data repository that you can use to monitor (and document) account actions to detect unwanted or unexpected behaviors, and to provide forensic data during or after a security incident.

Indeed, it makes sense to automatically provision new AWS accounts around your security requirements. This means you can use a tool like AWS CloudFormation StackSets to manage the infrastructure — that is, CloudFormation stacks — that baselines new accounts. This provides important visibility into and control over who can see beyond the publicly exposed user interfaces into your AWS cloud services and presence. It's essential to proper security posture and practice.

For more information on the topics covered in this chapter please consult the following online assets:

- **AWS Service Control Policies (SCPs):** `https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html`
- **AWS account management and separation:** `https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/aws-account-management-and-separation.html`
- **AWS Organizations, accounts, and guardrails:** `https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/organizations.html`

IN THIS CHAPTER

- » Keeping your network safe
- » Making protection automatic
- » Looking at AWS resources

Chapter 3
Secure Your AWS Infrastucture

Zero trust is a key concept in modern cybersecurity approaches. It’s a logical extension of the notion of trust no one. Essentially, zero trust requires any and all users to first authenticate, then obtain authorization, and finally obtain continuous validation for security purposes before they are granted (or keep) access to applications and data.

Importantly, zero trust means there’s no traditional network edge so there’s no boundary inside which everything is okay and outside which everything is *verboten.* Instead, zero trust recognizes that networks might be local, in the cloud, or a combination of the two — usually described as *hybrid* — with resources anywhere and everywhere, and users able to obtain access from any location.

Zero trust is the right approach to take toward today’s networks, on-premises, in the cloud, or wherever they might be situated. It presumes nothing, checks everything, and keeps checking for validity as long as connections remain active. It’s the only way to be sure that access and permissions apply at the current moment in time.

Protect Your Networks

Infrastructure protection is necessary to follow best security practices, as well as to meet an organization's obligations in terms of policy, governance, and compliance. Following such protection practices is essential for successful, ongoing cloud operations, just as it is for other aspects of proper security.

For example, it's advisable to separate the virtual networks to run classes of workloads on separate and distinct subnetworks (aka *subnets*). This prevents users in any given workload class from exposure (and attempting access) to the applications and services exposed in other workload classes. The AWS Network Firewall protects traffic between different subnets, even in the same Virtual Private Cloud (VPC). A VPC supports setting up a separate subnet for each availability zone in a Region, with distinct Elastic Cloud Computing (EC2) instances in every subnet, and an Internet gateway for general access.

TIP

A VPC works like a traditional network that you might operate in a data center. Once a VPC is created, it can support multiple subnets (a range of IP addresses within the VPC, each with associated AWS resources). Figure 3-1 shows a typical VPC.

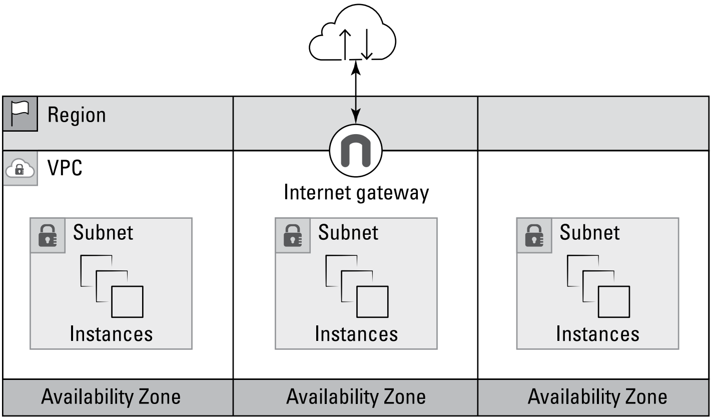


FIGURE 3-1: An example AWS VPC, with a subnet for each availability zone in a region (EC2 instances for each subnet, and an Internet gateway for all).

TIP

If your cloud environments use numerous VPCs (more than dozens) you'll want to put an AWS Transit Gateway in place. It can route all traffic to and from virtual networks for thousands of VPCs, with a single interface through which to manage and monitor all connections. For more info see `https://aws.amazon.com/transit-gateway`.

Automate Protection at Every Layer

Protection works best when software handles the front line of defenses via automation. Automation brings many advantages, once it's thoroughly tested and vetted, including the following:

- **Automation responds to events at machine speeds.** Response time is in milliseconds, not seconds or minutes as would be more typical for human responses, best case.
- **Automation doesn't make mistakes.** Humans driving interfaces or poking keyboards can (and often do) make mistakes.
- **Automation works all the time, around the clock, 24/7/365.** We don't want humans to do that!

What does this mean in practice? AWS CloudFormation can automatically deploy a set of Web Application Firewall (WAF) rules that can fend off common web-based attacks. Admins can select from preconfigured features that define such rules in a web access control list (ACL). The rest is . . . well . . . automatic.

TIP

AWS partners also offer a wide range of industry-leading products to extend and improve on controls for existing AWS environments. Such products complement and extend AWS services to boost security posture and provide a better experience across cloud and on-premises environments. For more information, please visit `https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_network_protection_auto_protect.html`.

Set up host layer protection

In AWS a *security group* controls traffic allowed to enter and leave associated resources. Thus, if you associate a security group with an EC2 instance, it will control inbound and outbound traffic for that instance. Security groups may be associated with resources only in the VPC for which they're created. Security groups can be set up for load balancers, web, and database servers.

Each VPC comes with a default security group, but you can create additional such groups for any VPC (no added charges). Web servers can have public subnets (to support Internet access), while database servers can have private subnets (so only authorized applications or users can access them, and only database requests from the web server could be allowed).

Set up application protection

As described in a previous section, the AWS WAF can cover fundamental security protections and customize them to cover specific applications. This helps organizations visualize actions so they can establish a dynamic and proactive security posture.

TECHNICAL STUFF

AWS preconfigured rules, aka *Managed Rules,* provide protection against common attacks. These rules are curated from multiple sources of security intelligence within AWS. Marketplace Rules (available from third parties) provide an additional layer of protection. Security savvy admins can even create their own custom rules for additional protection and coverage.

AWS WAF integrates with AWS Shield Advanced (no extra charge). It offers easy setup, low overhead for ongoing operation, minimal latency impact, and fully customizable security. It even uses advanced automation to analyze web logs and identify malicious activity and it updates security rules on its own.

Achieve network protection

Within AWS, network protection also comes from Security Groups, the WAF, and various Shield elements. These work together to define what and how servers may be reached, especially in transitioning from public to private subnets, and in filtering and managing incoming IP addresses to protect such servers. Basic IP address management harvests security intelligence from known black lists and information about bad actors gleaned from the vast global pool of AWS users (including rejected ones).

TIP

AWS Shield also detects and handles challenging Distributed Denial of Service (DDoS) events, and can customize application protection against such risks through integrations with AWS Shield Response Team (SRT) Protocols or AWS WAF rules. For more information visit `https://aws.amazon.com/shield`.

In addition, AWS provides the Network Access Analyzer tool as part of its environment support. This tool identifies unintended network access to AWS resources. It also allows admins to specify network access requirements to identify unwanted or potentially insecure network paths. Thus, the Network access analyzer helps to understand, verify, and improve network security posture. It can also demonstrate compliance, by showing that your AWS network meets related access and control requirements. The Network Analyzer's coverage includes the following:

- **Network segmentation:** Verifies proper isolation for production, development and other sensitive VPCs.
- **Internet accessibility:** Identifies AWS resources accessible from Internet gateways; verifies these are limited only to resources that require such access.
- **Trusted network paths:** Verifies that proper network controls (network firewalls, NAT gateways, and more) cover all network paths between resources and gateways.
- **Trusted network access:** Verify resources permit access only from trusted IP address ranges over specific ports and protocols, or specific resource IDs, types, and tags. Everything else is blocked!

Protecting compute resources

In addition to establishing network layer protection, it is also recommended to use a vulnerability management tool to discover and scan workloads for software vulnerabilities. Vulnerability scanning should be done across all compute including EC2, AWS Lambda functions, and containers, and be automated to ensure all your workloads are protected, all the time.

In general, the guiding principle to protect software and data running within various AWS environments (IaaS, EC2 instances, containers, virtual servers, and more) is to reduce the exposed attack surface as much as possible. In addition to detecting and handling vulnerabilities, it's also good practice to harden Amazon Machine Images (aka AMIs) for further protection. AWS offers a guide to what's involved entitled "Best practices for building AMIs" (search on that title for easy access).

This guide describes how to reduce AMI attack surfaces in detail, including a list of policy and region constraints, AMI image sources, patch and update strategies, virtualization settings, and more. Other related best practices also include developing a repeatable process for building, updating, and republishing AMIs. This also permits building an automated process for handling canonical AMIs (also called "golden AMIs" indicating they're ready to use) over their lifecycles (creation, update, republishing).

TECHNICAL STUFF

In addition, the guide recommends using consistent user names, and configuring a running instance from a final AMI to create the desired end-user experience. It also advises testing all installation methods, performance, and features *before* submitting any AMI to the AWS Marketplace. Default access ports for Linux and Windows are covered, too (SSH port 22 for Linux, RDP port 3389 for Windows, plus WinRM port 5985 open to 10.0.0.0/16).

Another important technique for securing AWS computer resources is to automate compute configuration management as much as possible. To that end, Amazon recommends AWS OpsWorks, a configuration management service that runs on managed instances of Chef and Puppet. These are two widely used automation platforms that support use of code to automate server configuration and deployment across EC2 instances and on-premises compute infrastructures.

A variety of AWS OpsWorks offerings — visit `https://aws.amazon.com/opsworks` for more info — covers configuration management, compliance and security, as well as continuous deployment within a fully managed set of automation tools. Your existing automation choices — that is, Chef, Puppet, or the AWS OpWorks Stack environment — will guide your OpsWorks platform choice.

REMEMBER

Best practices for AWS automation are many and varied. At a minimum, the fundamental principal involved is easily described as "automate everything." Such automation must include use of patch management and deployment tools for AMIs of all kinds, especially EC2 instances, containers, OS images, and so forth. See the "Best Practices and recommendation" section of "AWS Prescriptive Guidance" for more information (search on that latter title for quick access to this helpful document).

Recommended AWS Resources

For more information about the many and varied topics covered in this chapter, please follow the links or search for titles already mentioned earlier in this chaper. Or, you can consult any or all of the following references online:

- **What is Amazon VPC?:** `https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html`
- **AWS Infrastructure Protection:** `https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/infrastructure-protection.html`
- **AWS WAF, Shield, Firewall Manager:** `https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html`
- **Best practices for building AMIs:** `https://docs.aws.amazon.com/marketplace/latest/userguide/best-practices-for-building-your-amis.html`
- **AWS Patch management:** `https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html`

IN THIS CHAPTER

- » **Establishing and verifying identities**
- » **Managing and monitoring permissions**
- » **Crafting organizational guardrails to steer clear of trouble**

Chapter 4 Securing Identities and Permissions

In the world of cybersecurity, matters of identity and access management (aka *permissions*) is usually abbreviated as IAM. IAM is a whole subdiscipline that embraces multiple technologies and business processes. The guiding principle for IAM is "get things right" — that is, make sure the right accounts (people, processes, or machines) access the right assets for the right reasons at the right time. Not incidentally, IAM also seeks to deny unauthorized access and thereby defeat attempts to breach security and steal information.

Implementing IAM usually occurs within a framework that establishes business processes and policies and then uses technologies to impose and enforce them. Common systems associated with IAM include single sign-on (SSO) systems, two-factor or multifactor authentication (2FA and MFA), and privileged access management (PAM). Such technologies provide ways to store identity and profile data securely, along with governance functions that make sure only necessary and relevant data is disclosed or shared.

IAM automates processes involved in assigning and tracking user identities and privileges, along with granular access control and auditing of access on-premises and in the cloud.

AWS and IAM

If you want to use AWS services, your users and applications must be granted explicit access to resources in one or more AWS accounts. Given typical situations with hundreds or thousands of AWS workloads running, organizations need serious and robust identity management and permissions in place.

REMEMBER

That's how you "get things right" in the IAM arena. This means the right parties (people, processes, and machines) can get into the right assets (the resources they're allowed to see and use) for the right reasons (items for which they have a legitimate need) at the right time (while systems and services are available to authorized users).

AWS offers a wide range of capabilities to manage human and machine identities, and associated permission. Best practices for IAM on AWS fall into the broad buckets of identity management and information management. Those provide the focus for the following sections.

Manage Identities in AWS

Two kinds of identities need to be managed to successfully operate secure AWS workloads. These are:

- **Human identities:** These include the people who need access to AWS environments and applications (resources). They're usually categorized by job or user role. Thus, they include admins, developers, operators, and ordinary users of applications and services involving AWS resources. This means internal users (employees, contractors, and so forth), partners, or authorized external users who might interact with AWS resources using a web browser, some client application, a mobile app, or command-line tools from a login prompt.
- **Machine identities:** These include processes such as workload applications, operations tools, or software components. They also require an identity to interact with AWS services (for example, to read or write data). Such

identities typically include EC2 instances or AWS Lambda functions. AWS also permits machine identities for external processes that need access, along with machines outside AWS that need AWS access.

Best Identity Practices

Under the AWS umbrella, a number of practices come highly enough recommended that they should be implemented as a matter of proper policy and procedure. These include the following:

- **Enforce strong passwords:** Set complex password requirements. For example, a randomly generated string of minimum length 20 characters, composed of a mix of upper and lower case letters, plus numbers and special characters (@#$%. . .) prevents easy guessing and dictionary attacks.
- **Require strong sign-ins:** Requiring MFA (2FA, at a minimum, perhaps more for admin and developer accounts) means that even if a password is known, the lack of other authenticating factors prevents successful sign-in.
- **Regular credential rotation:** For password-only systems especially, but in general, security experts recommend changing passwords at least every 90 days (if not more frequently). Mandatory use of password management tools nowadays makes this burden much less onerous. Specify password storage and management requirements for users, and cover passwords in awareness training. Auditing credential use, especially for high-level accounts, is also a good idea.
- **Use temporary credentials:** Especially important for AWS API and command-line requests, temporary credentials expire quickly and can't be reused when stale. It's especially important to warn operators and developers against embedding passwords in automation and applications. By default, AWS uses temporary credentials when applications or services federate to AWS or when IAM roles are assumed.
- **Use a centralized identity provider:** Strong, well-managed identity providers — such as AWS Identity and Access Management — make it easier to manage access across

multiple locations and services. This supports creating, managing, and revoking access from a single point of control. A default identity store, to manage users and groups, lets you configure an identity provider one time, then grant access to existing and new accounts managed within the organization.

- **Leverage user groups and attributes:** With users in large numbers, it's much easier to organize them into groups to manage them at scale. Users with common security requirements belong in the same group, which makes those requirements easier to manage and update for access control.

  Use groups and attributes to control access, not individual user accounts. This approach sustains central access management by using group memberships or attributes, not individual policies as users' access needs change. AWS IAM Identity Center provides extensive user group and attribute set-up and management capabilities.

WARNING

In this same vein, be careful in using AWS root user accounts (these are always the point of departure for any AWS resource). Employ this account only for initial user set up (and other tasks that require root user access). Be sure to delegate routine admin and operator activities to designated groups for those roles. It's vital to turn on MFA for this account, because it holds the "keys to the kingdom." Then, secure the root user following the AWS best practice guide at `https://docs.aws.amazon.com/wellarchitected/latest/framework/sec_securely_operate_aws_account.html`.

In general, incorporating an identity management facility into the technology that supports IAM is the foundation on which identity management rests. Such a platform usually guides how the identity management process works and helps organizations ensure they follow best practices and principles.

Manage Permissions in AWS

Permissions are used to check and enforce what actions are allowed for human and machine identities known to AWS and its workloads. In other words, permissions establish who can access which objects and under what conditions. By anchoring permissions to specific human and machine identities (most often, through membership in security groups) permissions control access to specific actions on specific resources.

TIP

In addition, it's important to specify conditions that must hold for access to be allowed. Thus, you might permit developers to create new Lambda functions, but only in some particular region. Using policy types lets AWS use identity-based policies that attach to users, groups, and roles. Each such identity can do certain things (permissions). Identity-based policies may be AWS-managed or customer-managed. Customer-based policies provide more granular control over permissions that do AWS-managed ones.

REMEMBER

The guiding principle for permissions is called "the principle of least privilege." It's often abbreviated as PLP. PLP translates into: Grant only as much permission as needed, and no more. The overriding goal is to avoid granting more permission than is needed, and frequent (automated) reviews are recommended to avoid *permission creep* over time. Indeed, this is another good reason for using roles or groups to manage permissions, because it's much, much less work to do it that way than by individual user account.

Continuous evaluation of the use of permission means organizations must set policies to monitor and manage access. This is especially important for identities allowed public access, or cross-account access (from one AWS account to another). Likewise, it's essential to identify AWS resources shared with external identities (those outside the scope of an organization's IAM). These can pose grave security threats and must be watched carefully and closely for signs of untoward behavior or unauthorized access and use.

Establish Organizational Guardrails

AWS Organizations helps provide centralized control, governance, and management for multiple AWS accounts. These come in the form of service control policies (SCPs) to set up the controls that all IAM principals (users and roles) must obey. In short, SCPs help organizations set up permission guardrails using the highly granular controls that the AWS IAM policy language enables. The idea is to help you set up and fine-tune policies that meet the strict and precise requirements of governance rules for your organization.

TECHNICAL STUFF

SCPs provide central access controls for all IAM entities in AWS accounts. Use them to enforce permissions everyone in the organization should follow. With SCPs, developers can be granted freedom to manage their own permissions because their accounts operate within the boundaries defined for them.

SCPs permit definition of specific policy elements across accounts. These may be used, for example, to deny access across accounts in an entire organization or within an organizational unit (OU). SCPs might serve to restrict access to particular AWS regions. Or they could prevent IAM principals (those who run the IAM system) from deleting common resources. SCP also permits defined exceptions to governance controls, and can restrict high-level service actions for everybody except a specific administrator role.

To implement permission guardrails using SCPs, use the new policy editor within the AWS Organizations console. That editor helps you to create SCPs, and guides you to create actions (AWS actions to which an SCP applies), resources (AWS resources to which an SCP applies), and conditions (sets conditions when the policy statement for an SCP applies). For more information on SCPs and permission guardrails, please search for "AWS set permission guardrails across accounts."

More AWS Resources

To dig more deeply into IAM in the context of AWS and hybrid cloud, please follow the links and searches already mentioned earlier in this chapter. If you're left wanting more, check these other resources out, too:

- **IAM Best Practices:** `https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html`
- **Get started with AWS Secrets Manager (includes AWS credentials):** `https://docs.aws.amazon.com/secretsmanager/latest/userguide/getting-started.html`
- **Using AWS Identity and Access Management Analyzer:** `https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html`

IN THIS CHAPTER

- » **Logging services and applications**
- » **Implementing and automating security response**
- » **Dealing with danger, delicately and definitely**

Chapter 5 Dealing with Danger

As the now-obligatory "scary statistics" section in any current cybersecurity report can attest, there's plenty of reason for concern — if not outright alarm — with the state of things. Take the Wiz blog "State of the Cloud 2023" as an example to assess how things look from that lofty perch at the moment.

As that report states, "cloud adoption has continued to grow with more organizations increasing their footprint in the cloud." Cloud API calls in corporate code are up, too: 15 percent for AWS, 20 percent for Azure, and 45 percent (!) for the Google Cloud Platform (GCP). This serves to "broaden attack surfaces and create more challenges for cloud defenders." Given that nearly 3/5s of companies use more than one cloud platform, there are concerns related to more expansive skills and knowledge, not to mention cross-platform interfaces.

At the same time, "well-known prevalent risks such as data exposure" also loom large. Nearly one-half (47 percent) of companies have one or more databases or storage buckets exposed to the Internet. Attackers, the report says, "can discover and access an exposed bucket . . . in less than 13 hours." Zowie! Scary indeed. For more information, please visit `https://www.wiz.io/blog/the-top-cloud-security-threats-to-be-aware-of-in-2023`.

Configure Logging for Services and Applications

The key to dealing with danger is to keep an eye on what's happening in the world around you. For AWS environments, that means enabling and configuring service and application logging. Such logs can be collected and aggregated across all AWS Organization elements.

Indeed, Amazon CloudWatch lets organizations observe and monitor resources and applications on AWS, both on-premises and even in other clouds (including AWS, of course). CloudWatch offers compelling features, including facilities to:

- Collect, view, and analyze resource and application data with powerful visualization tools
- Improve operational performance with alarms and automated actions that trigger on specific thresholds or events
- Integrate with over 70 AWS services for simple monitoring and scalability
- Troubleshoot operational issues using actionable insights that come from logs and metrics in CloudWatch dashboards

TECHNICAL STUFF

AWS Config is another Amazon tool that lets you assess, audit, and evaluate configurations for AWS resources. It continuously oversees and records configuration changes to simplify change management. At the same time, it audits and evaluates resource configurations against your policies. Config also helps simplify operational troubleshooting by correlating configuration changes to account events. This is vital to security and helps fend off reconnaissance and stymie attacks. Config can also compare current configurations to pre-defined "ideal" configurations to let you know when changes might degrade performance or security.

AWS GuardDuty is another security monitoring tool of potential interest (as with most Amazon tools, third-party options and integrations are also available through the Amazon Partner Network, or APN). Such tools work with threat intelligence and detection to catch ominous developments quickly and apply automated remediation or workarounds, where available.

Overall, AWS makes it easy to aggregate and centralize security information from a range of security tools and platforms. The idea is to create a comprehensive view of the state of security, and to provide visualizations and dashboards to make it easy to assess and respond to security situations in real time (or as close as technology and automation can get). The Amazon Security Hub tool centralizes security alarms and alerts, and provides a consistent and coherent view of security, including means to:

- Detect deviations from security best practices with a single mouse click
- Automatically aggregate security findings in a standardized data format (ASFF, or AWS Security Finding Format) from AWS and partner services
- Accelerate MTR (mean time to resolution) for security issues using automation for response and remediation actions

If you need a fully contextual platform that ingests risks from AWS and automatically correlates them with other risk factors, consider using a Cloud Native Application Protection Platform (CNAPP). Such a platform also helpd with security for multi-cloud computing environments (increasingly common in today's organizations and enterprises).

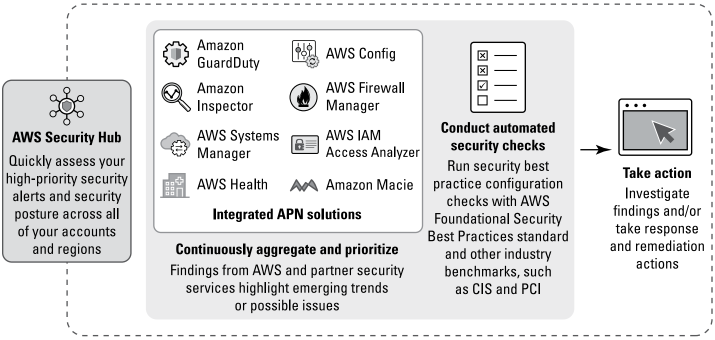
REMEMBER

AWS seeks to provide visibility and transparency for security data and status information of all kinds via its various tools and platforms. This supports a holistic and consistent view of security state and events, on-premises and in the cloud.

Implement, Automate Security Actions

AWS Security Hub includes all-important automated remediation for security events that require a response (for which remediation in known and available). Figure 5-1 shows the overall AWS toolset that provides this capability.

AWS Security Hub works with inputs from Amazon GuardDuty, AWS Config, Amazon Inspector, AWS Firewall Manager, AWS Systems Manager, AWS IAM Analyzer, AWS Health, Amazon Macie, and all integrated APN solutions. It continuously aggregates and prioritizes such findings, to highlight emerging trends or potential issues.



AWS Security Hub
Quickly assess your high-priority security alerts and security posture across all of your accounts and regions
Amazon GuardDuty
AWS Config
Amazon Inspector
AWS Firewall Manager
AWS Systems Manager
AWS IAM Access Analyzer
AWS Health
Amazon Macie
Integrated APN solutions
Continuously aggregate and prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues
Conduct automated security checks
Run security best practice configuration checks with AWS Foundational Security Best Practices standard and other industry benchmarks, such as CIS and PCI
Take action
Investigate findings and/or take response and remediation actions

FIGURE 5-1: AWS Security Hub consolidates and coordinates inputs across a range of security tools, does automated checks, and responds or remediates when it can.

In addition, Security Hub also runs automated security checks, including best practice configuration checks from the AWS Foundational Security Best Practices standard, and according to industry benchmarks including CIS (the Center for Internet Security's Critical Security Controls) and PCI (the Payment Card Industry Data Security Standard), among others.

CROSSING THE EventBridge

Amazon EventBridge is another tool that supports automation for AWS services. It allows such services to respond automatically to events that include application availability issues and resource changes. Simple rules identify events of interest, and matching automated actions to take in response. Such actions include:

- Invoking AWS Lambda functions
- Invoking Amazon EC2 run command
- Relaying events to Amazon Kinesis Data Streams
- Activating an AWS Step Functions state machine
- Notifying Amazon SNS topics or SQS Queues
- Sending a finding to some third-party ticketing, chat, SIEM or incident response and management tool

EventBridge rules may be configured to response to each such event. For more info, please visit `https://docs.aws.amazon.com/eventbridge/latest/userguide/what-is-amazon-eventbridge.html`.

Thus, Security Hub provides alerts against threats and misconfigurations. It can also run automated response and mitigation routines as and when they're available, to handle known (or suspected) attacks or suspicious actions. Taking action on security findings includes identifying and setting status for associated workflows, and sending inputs to already-defined custom actions.

Implementing Actionable Security

Because new services can fire up in the cloud at the click of a mouse, they can sometimes surprise operations staff. Lacking notification, intervention or response can't be timely. Indeed, the volume and speed of cloud deployments make manual intervention iffy in enterprise environments. That explains why automation is key to keeping up with current events (and avoiding possibly late reactions to them).

Tooling automation provides the answer to this otherwise vexing situation. It lifts the burden of common processes from human resources and frees them to focus on higher-value tasks. Properly implemented, automation provides actionable security information for the response team when an alarm or alert happens, to put them to work ASAP. This means packaging up all the necessary data — including logs, traces, analysis, threat, and remediation data (where applicable), regions and organizations involved, and so forth — so security teams have everything they need to understand and move forward right away.

TIP

Once a security response gets underway, security teams must also investigate so they can document and understand what happened (and explain how to avoid or mitigate recurrences). This is well-served using playbook processes (scripted sequences of actions, documentation, analysis, and so forth) to make sure everything is understood and all forensics data gathering takes place (required when compliance or policy issues arise, but a best practice in general).

AWS Security Hub provides the functionality necessary to support automation, security response and post-mortem data analysis, documentation, and audit trails. Use it (or an equivalent third-party solution) to help your organization survive and thrive in the face of outrageous fortune.

More AWS Resources

Please consult the various links mentioned earlier in the chapter to learn more about tools and technologies covered therein. For more AWS security insight on detection and response, please visit any or all of these items as well:

- **AWS Security Detection:** `https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/detection.html`
- **Amazon CloudWatch User Guide:** `https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html`
- **AWS Configuration Management:** `https://www.wiz.io/academy/why-configuration-management-is-essential-to-cloud-security`
- **Why Automation is Essential for Cloud Security:** `https://www.wiz.io/academy/why-automation-is-essential-for-cloud-security`

IN THIS CHAPTER

- Classifying data, especially sensitive stuff
- Securing data in motion and at rest
- Encrypting everything, all the time
- Enforcing access controls

Chapter 6
Protect Your Data

Think about what delivers value to information technology. Sure, lots of hardware is involved. And software plays an important role in getting things done (especially custom- or purpose-built code that implements intellectual property). But the real crown jewels in any organization reside in its data. Data's what describes your customers or clients, tracks their history and interactions, and captures their interests and trends. Data's also what drives supply chains, financial activities for both sales and purchasing, and a whole lot more. It's where your business lives, and how it breathes and grows.

In a nutshell, protecting data is all about protecting key assets that represent your organization's lifeblood. One of the biggest security threats to an organization comes from what's called a *data breach.* Essentially, this means someone unwanted and unauthorized has busted through security and obtained access to your organization's data via its systems. Mayhem often follows a breach. It can include damaged reputations and brands, costs for clean-up and making users whole, and possibly even fines, penalties, and occasionally, jail time for employees responsible. Not good!

A brief summary of scary statistics for data breaches in 2023 goes as follows. Average cost: $4.35 million. Major root cause for breaches: phishing (22 percent of cases). Seventy-nine percent of critical infrastructure organizations (such as cloud providers) did not adhere to zero trust approaches to security. Cloud-based breaches account for 45 percent of the total, with 30 precent of all large breaches in hospitals. For a plethora of more info, visit https://www.getastra.com/blog/security-audit/data-breach-statistics/.

The bottom line is that protecting data is at least arguably the most important priority for delivering proper security. If it's not number one, it's definitely somewhere very near the top of the list of things that proper security must include.

Classify Your Data

All data is not the same. Some data is more important than other data. By way of example, consider the difference between data that describes personally identifiable information (PII) about an employee or customer versus an audit trail of the former's recent workflows or the latter's recent orders. Not only does PII warrant more attention and protection than the other stuff, but plenty of regulations and compliance schemes insist that it be carefully protected, audited, and tracked — and reported if breached.

REMEMBER

Data classification provides a set of rules by which to categorize data. Such rules cover varying levels of sensitivity, based on an assessment of the risks, financial losses, or other consequences incurred in the event of a breach or unauthorized disclosure. Data classification is important because it supports security and business objectives to prevent mishandling or unwanted access, and to comply with regulatory obligations or organizational policy.

One definition of data classification reads: "a way to categorize organizational data based on criticality and sensitivity . . . to help you determine appropriate protection and retention controls" (search "AWS data classification" for the source). In practice, this breaks down into a series of tasks to put a classification scheme in place and keep it going:

- **Identify all data within each workload:** Determine the type and classification for each data item, associated business processes, where it's stored, and who owns it. Legal and compliance requirements and enforced controls should appear, too. Identification is a first vital step toward classification and protection. At this stage, you can move toward automating the data-discovery process, and make use of tools to recognize and call out sensitive data (PII, account or credit card information, health data, intellectual property, and so forth). On the tools side, take a look at "AWS Glue DataBrew" a visual data preparation tool (search for that string to learn more).

- **Define data protection controls:** These are based on classification levels. A whole laundry list of approaches helps this process — namely, resource tags, separate AWS accounts per sensitivity, IAM policies, SCPs, and more. Given a classification scheme, you can discover security controls within AWS services to apply relevant security and protection controls. For each such service, turn to its security section in the AWS Documentation for details (see `https://docs.aws.amazon.com/` to get started).

  REMEMBER

  Controlling access to AWS resources works well using tags (including IAM resources). Tags can be attached to a resource itself, or passed in a service request that accepts tag data. Tags can be a big help in controlling access to AWS resources. For more information, visit `https://docs.aws.amazon.com/IAM/latest/UserGuide/access_tags.html`.
- **Automate identification and classification:** Once defined, the best way to use technology for consistent, reliable data handling is by automating these activities. Amazon Macie (see next section heading) can provide such capabilities, using machine learning to automatically discover, classify and protect sensitive data.
- **Define data lifecycle management:** A data lifecycle strategy derives from its sensitivity, legal, and policy requirements. This includes data retention periods, the data destruction process, data access management, data transformation, and data sharing considerations. Data classification methods balance usability against access (as is the general case for information security). Multiple levels of access must be secure, but still usable, to work well. Finally, users should come from trusted network paths and require access to decryption keys.

DOING DATA DISCOVERY

If you view data as an organizational asset, it doesn't really belong to individuals or departments anymore. Analyzing all the data provides profound insights into the types and kinds of data the organization uses, and what its value, risks, and handling requirements should be. That's what data discovery is all about. It generally follows these five distinct steps:

- Define the business value
- Identify user personas
- Identify data sources
- Define storage, catalog, and data access needs
- Define data processing requirements

To read about this process in more detail, and learn about tools and techniques to implement and automate it, please visit `https://docs.aws.amazon.com/wellarchitected/latest/analytics-lens/characteristics.html`.

Working with Macie or . . .

Amazon Macie is an AWS add-on that provides sensitive data discovery at scale. It provides cost-efficient visibility into sensitive data stored in Amazon S3 cloud object storage (used in many AWS applications or services). Macie offers S3 storage bucket inventory assessments on security and access controls. Macie uses machine learning and pattern matching to discover and help protect sensitive data (see Figure 6-1).

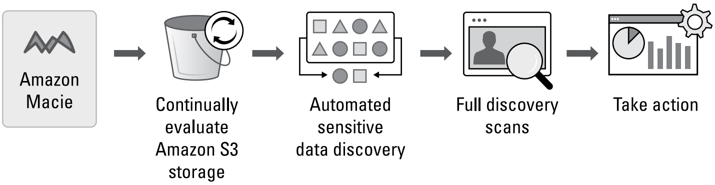

Amazon Macie
Continually evaluate Amazon S3 storage
Automated sensitive data discovery
Full discovery scans
Take action

FIGURE 6-1: How Macie handles data discovery and protection.

From left to right, you can track what's involved in setting up and using Macie to deal with sensitive data. Once enabled, Macie goes to work. It automatically generates and maintains S3 bucket inventory, with insights into bucket-level security and access controls. It builds and maintains an interactive map of sensitive S3 data. You can order targeted data discovery jobs based on the map at any time. Macie can generate findings and pass them to Amazon EventBridge or AWS Security Hub for automated remediation and workflow integration (where available).

Data in Motion and at Rest

Encryption is the best technique to make data opaque to those who lack the keys necessary to unlock its contents. And indeed, best practices dictate that data transmitted from one point to another should be encrypted inside a wrapper. Then, if any of the constituent packets are intercepted, they remain opaque. Likewise, data stored in the form of files, objects, blobs, or whatever, should also be encrypted. If located and viewed or copied they likewise remain opaque.

Powerful encryption technologies rest on a foundation of secure cryptography, key, and certificate management schemes. Standards organizations OWASP offer a stellar Key Management Cheat Sheet (search on that title) to describe in detail how such technology works. Similarly, IETF standards such as those for IKE (Internet Key Exchange) and ISO/IETF X.509 Public Key Infrastructure (PKI) and certificate handling define equivalent open, public frameworks for cryptography, certificates, and keys.

It suffices here that key and certificate management address the ins and out of issuing keys for cryptography (generating, issuing, distributing, and decommissioning) and powerful tokens called certificates used to establish identity. Such proof enables authorized users to obtain and use keys for encryption (when writing data at rest, or transmitting data in motion) and then decrypting such data (when reading data at rest, or receiving incoming data in motion). Encryption algorithms vary depending on the use case, but are the same overall.

AWS supports these best practices in its services and related toolsets. It describes "protecting data at rest" in its Security Pillar documentation. This includes how to implement secure key management, enforce encryption at rest, automate data at rest protection, enforce access control, and more. For data in transit a similar wealth of topics exists — namely implement secure key and certificate management, enforce encryption in transit, automate detection of unintended data access, and authenticate network communications.

Behind the scenes, the AWS Key Management Service and the AWS Certificate Manager provide supporting infrastructure for organizations that need them. As always, AWS Services also readily integrate with APN equivalents to accommodate existing investments. AWS service users should also follow best practices that include using and configuring secure protocols (for example. TLS, IPSec, and so forth), and using a Virtual Private Network (VPN) to secure external connections.

TIP

In the general areas of data protection, encryption, and certificates, the AWS Secrets Manager is a helpful tool, as it supports secure encryption and audit of API keys, database credentials, tokens, and so forth. It works with AWS IAM and resource-based policies, and provides automatic generation and rotation of secrets to meet security and compliance needs. Finally, Secrets Manager can replicate secrets under its purview for disaster recovery and multi-region applications.

Enforce Access Controls

Permissions are the gatekeeper for evaluating access requests, then granting or denying them. Permissions are absolutely essential to establish conservative access controls that deny by default and allow only by verified exception. This is the famous "principle of least privilege" that is a hallmark of modern, zero-trust security approaches. No user should be allowed access to anything without establishing and proving identity to begin with. If connections persist over time, such users must continuously revalidate to obtain additional access. And because access controls are best driven by data classification, a user's role, group memberships, SPCs, and other rules and filters will apply to each and every access request. That's the best way to put AWS services to work.

IN THIS CHAPTER

- Understanding incident response
- Preparing the response team
- Gathering forensic evidence
- Practicing via simulation is key

Chapter 7
Respond to (and Mitigate) Incidents

In security-speak, *incident* is a polite euphemism for an attack, attempted or successful. Incidents sometimes happen — and when they do, organizations must be ready to deal with them. That drives incident response.

A formal definition of i*ncident response* is*:* a planned, organized, and strategic method to detect and manage cyberattacks. Incident response seeks to limit risks and costs — and minimize recovery time. Generally, incident response has a well-defined set of associated security policies and procedures to identify, contain, and mitigate cyberattacks.

One more thing: When an incident occurs, that's no time to improvise. Incident response personnel should know what tools to use, what kind of information to report, who to report it to, and more. Indeed, detecting an incident usually leads to declaring that an incident is underway. At that point, a well-defined (and frequently rehearsed) response plan should kick in. Incident response isn't usually as noisy or dramatic, but it works best when it's a familiar, well-practiced drill.

Prepare the Response Team

It’s essential to have both incident response teams and incident response plans in place before an incident occurs. Indeed, there’s a whole laundry list of stuff involved in doing incident response right. Let’s march through, and look it over:

- **Identify key people, roles, and responsibilities:** This starts with a group of key players (such as stakeholders, legal staff, and management) to set goals for incident response. They’ll turn those goals over to IT to take things further. IT managers will identify members of the response teams, tell them what roles they need to play, and assign responsibilities for actions and reporting.
- **Develop incident response plans:** Declaring an incident invokes an incident response plan. Such plans must include response objectives, related mechanisms and tools, communication directives (who gets called in, and who gets notified), and recovery methods. All should be clearly and explicitly defined and documented. Be prepared to adjust them based on use and experience.
- **Create playbooks or runbooks to drive responses:** In football, a playbook tells players what to do when a play is called. In IT, a playbook tells players (those who fill specific roles) what to do when some event — including a security incident — occurs. Runbooks are like playbooks, except they’re built around digital workflows and incorporate automation to the max. Using such tools helps security teams tackle tasks in the right order and ensure nothing gets overlooked.

  REMEMBER

  Obviously, the security team first needs to put detection mechanisms in place, and use them constantly, so when an incident is detected it can be declared.
- **Categorize incidents by severity and impact:** As incidents occur, it’s vital to prioritize them based on their effects. Think about how severe a threat the incident poses, and how much impact it could have, worst case. Focus on high-priority, high-impact stuff first and foremost. You can use threat feeds and intelligence services, CVE (common vulnerabilities and exposures) data, and similar information from the AWS community for ranking and prioritization.

TIP

AWS Incident Detection and Response offers round-the-clock proactive monitoring and incident management. It helps lower failure risks and accelerate recovery. It also offers access to AWS experts for detection, response, and recovery assists. For more info, visit `https://aws.amazon.com/premiumsupport/aws-incident-detection-response/`.

- **Standardize security controls:** Working with AWS Security Hub and related tools, organizations can define standard security controls for their resources. This makes things look and work the same everywhere. Your incident response team can concentrate on detection and correction rather than figuring out how things work in some particular region or organization.
- **Use automation everywhere:** Incident response benefits from lightning-fast reactions to signs of impending or actual cyberattack. Automation vastly outpaces human reaction time, so using it whenever and wherever possible is not just a good idea, it's also the fastest and best way to respond. When incidents occur (real or simulated) one thing to look for after the event is more ways to add or improve automation in the response.
- **Implement mechanisms to capture lessons learned:** As incidents occur, it's important to capture and document information along the way. This should include workflows, communications, logs, traffic snapshots, plus notes and observations from the response team. After the fact, it's important to get together to understand and document lesson learned.

The best way to respond to an incident is to follow the plan, then make sure the plan makes sense and works well. The AWS Well-Architected Framework has a whole section on incident response; find it by searching for "AWS incident response." Also, check out the "AWS Security Incident Response Guide."

Ready Forensics Capture. . .

Computer forensics is another cybersecurity subdiscipline. It concentrates on finding, capturing, and preserving evidence of attack, unwanted or unauthorized access or use, and other cyber-crimes. Indeed, this subdiscipline aims to meet legal standards for the collection, preservation, and presentation of evidence in court (or to meet compliance requirements) to show exactly what happened, when, to what.

As it happens, AWS offers a suite of capabilities to support forensic analysis of actions and activities in AWS resources. Such tools serve forensic analysts and security professionals to help investigate data breaches, cyberattacks, and other incidents in the cloud. Figure 7-1 shows how various AWS tools work together to gather forensics data.

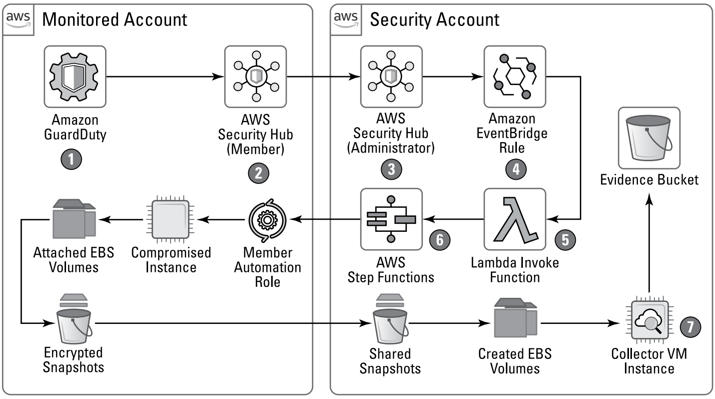


FIGURE 7-1: GuardDuty, Security Hub, and other tools and facilities work together to create a defensible chain of evidence from AWS services data.

TIP

AWS has a platform to automate incident response and forensics in AWS, Azure, and Google Cloud Platform. There's also a free playbook that describes how to respond to security incidents in the cloud. Search for the title "PB: Ultimate Guide to Incident Response in AWS." Also, a December 2022 blog post at Medium.com offers a great overview and lots of links to AWS forensics topics and open source tools. Find it at `https://medium.com/@cloud_tips/aws-forensics-tools-e87de0be16f2`.

A response plan should define what evidence to collect, and what tools to use. If you identify and prepare suitable forensics investigation support in advance, your team will have access to special accounts, plus tools and automation, and consult external specialists if and when they're needed. Consider you may have to collect data from live systems, because volatile memory or active network connections disappear as a system is powered off or rebooted.

A response team often combines tools — such as AWS Systems Manager, Amazon EventBridge, and AWS Lambda (among others, see Figure 7-1) — to grab forensics inside an OS and VPC traffic mirroring for packet captures and other nonpersistent stuff. Other typical activities include log analysis and disk image analysis, run inside a special security account with access to forensics workstations and tools.

An Ounce of Pre-provisioning

Incident response and forensics teams need special access to AWS services, and their activities must be audited to make sure the "watchers get watched." Indeed, AWS warns against "reliance on long-lived credentials . . . in favor of temporary" ones. For management tasks — including response team roles — AWS recommends implementing identity federation and temporary escalation for admin access. This means a response team member requests elevation to higher role, and that goes to someone with approval authority. Once approved, the requester gets and uses a set of temporary credentials to tackle incident response. After those temporary credentials expire, a new request must start this cycle over again.

If federated identities aren't available (perhaps because of issues with the identity provider, DDoS attack, or other causes), AWS recommends setting up emergency "break glass" credentials so investigation and remediation proceeds in timely fashion. Use a specific user, group, or role with permission to handle response tasks and access related AWS services. But the idea is to use them only in an emergency.

This is where pre-provisioning comes in. Those accounts must be set up in advance and surrounded with tight controls and monitoring. PLP dictates that responders should be granted the fewest and most restrictive permissions that let them perform required tasks. Such access should come from playbooks created as part of the incident response plan.

TIP

See the AWS Security Pillar section entitled "Pre-provision access" for lots of additional considerations in setting up incident response and forensics accounts, including contingencies, account types and conditions, and more.

Simulation Is Key to Success

For incident handling, practice is just as important as planning, preconfiguring and predeploying tools for incident responders. That's because experience leads to familiarity and understanding so that responders can concentrate on doing the job when an incident occurs (rather than remembering what that job is, where to go, what to do, who to call, and so forth). Practice is as good for incident responders as it is for first responders of other kinds. Indeed, police and firefighters practice all the time, as a key element of their jobs.

Game days, also called tabletop exercises or simulations, are internal events to let teams practice against staged incidents while working through plans, playbooks and so on. This forces responders to use tools and techniques they'd encounter in a real incident. Game days seek to prepare responders and to develop and improve their response capabilities.

Game days have great value because they:

- Validate team readiness and increase comfort levels in stressful, unusual situations
- Develop confidence and experience learning from interactions and training staff
- Follow compliance and contractual obligations to learn from results
- Generate records for accreditation and certification
- Improve tools, automation, play- and runbooks, and so on

TIP

There's a lot to be gained from practice sessions. Be sure to capture lessons learned once a session is ended to help drive continuous improvement and capability. And look for added ways to use (and improve) on automation to help speed more accurate and useful responses.

Further AWS Reading

Consult search strings and links from this chapter for access to more detailed information on incident response in the cloud. See also the NIST SP 800-61 Computer Security Incident Handling Guide. Download it from `https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final`.

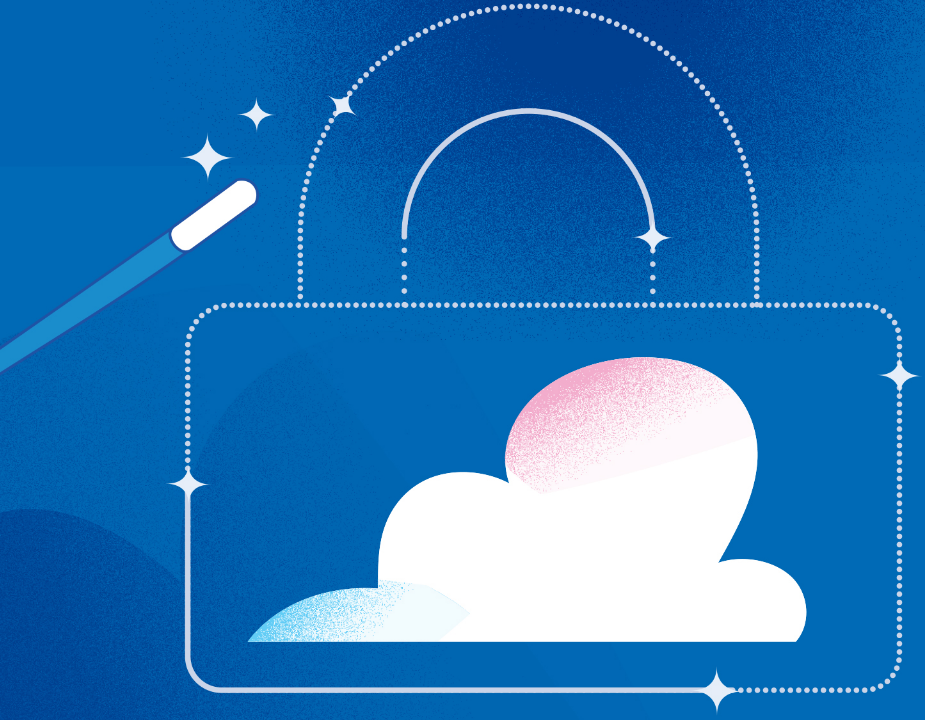
Chapter 8
Ten Tips to Securing a Multi-Cloud Network

Organizations with a multi-cloud environment, often need one tool to automate security across all clouds. In such situations, a cloud native application protection platform, or CNAPP, tool helps them secure the multi-cloud environment. Here are the top ten key capabilities a CNAPP solution should have to protect your multi-cloud environment:

- **Gain consistent visibility across multiple clouds:** CNAPP confers visibility into cloud, OS, and application layers across all cloud service providers.
- **One overarching policy regime:** CNAPP lets you use one policy regime across all clouds, to establish governance across them all. This enables you to stay compliant across your entire multi-cloud environment.
- **Normalization:** Normalize technologies and risk definitions across clouds using CNAPP (such as identity and access management resources) to make them all consistent, coherent, and intelligible.

- **Deep risk assessment:** CNAPP means you need only one tool to cover risk assessment across all vulnerabilities, network exposures, secrets, malware, identities, and sensitive data everywhere. Thus, all risks get correlated to identify toxic combinations in a complex environment where such risks are otherwise hard to identify — and hard to address.
- **Fully contextualized risks:** CNAPP provides a graph-based context surround to identify and categorize risks. This provides an end-to-end view and improved understanding of risk across the whole enterprise.
- **Prioritization of risks:** CNAPP offers a prioritized queue of risks so security and incident teams can focus on the most important ones, and tackle them in proper order.
- **Project segmentation and RBAC support:** CNAPP provides developers with ownership and visibility into the security of their resources, through role-based access control (RBAC) and project segmentation.
- **Identify risks early in the development cycle:** Integrate security checks into the development pipeline by scanning IaC templates to identify misconfigurations before they get into production. CNAPP automates such checks into development environments as built-in parts of that workflow.
- **Automatic remediation:** CNAPP supports automatic remediation where possible. This saves time in responding to issues. It also sends alerts to the right people by integrating whatever tool(s) you use into your existing ticketing system.
- **One tool to support your cloud journey:** A fully integrated CNAPP solution allows organizations to start with one specific security tool such as vulnerability management. Later, they can add more security capabilities as they grow. This might include Kubernetes security posture management to give them one solution for their entire cloud needs. It can also include a broad range of security intelligence, monitoring, and graphic capabilities. Cross-site security checks also become relatively simple and straightforward.

Secure Everything You Build & Run in the Cloud



They say a demo is worth a thousand words:
Watch Wiz in action
at *wiz.io/demo*

WIZ

Everything you need to know to protect your data in the cloud

Data, applications, and services — all moving to the cloud. This means you have to take a new approach to protecting your business and customers against cyberattacks. One that keeps up with the speed of the cloud. Learn the most important principles for effective AWS security in this user-friendly book.

Inside…

- Explain the basics of AWS and cloud security
- Secure AWS identities and permissions
- Monitor your AWS security posture
- Protect AWS data in transit and at rest
- Respond to (and fix) security incidents
- Extend security into multi-cloud uses

WIZ

Ed Tittel is a long-time computer industry writer, and the author of dozens of *Dummies* books, as well as numerous cybersecurity titles on malware, networking and CISSP. To learn more visit edtittel.com.

ISBN: 978-1-394-20674-2
Not For Resale

9 781394 206742

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT