











Deloitte.



AWS network and infrastructure security

Fundamentals for a solid foundation

Contents

	A challenge	03
	Incorporating cloud security into dynamic network and infrastructure	04
	Securing your organization's AWS network and infrastructure	06
	Maturing your organization's AWS network and infrastructure	09
	Incorporating resiliency into AWS network and infrastructure	10
	Securing Infrastructure as Code and automating security	11
	Harness the benefits of Infrastructure as Code to secure the cloud	13
	The strength of the Deloitte/AWS relationship	14

A challenge

As leaders learn how the cloud can present their organizations with growth opportunities and dramatically transform their business in terms of cost efficiency, effectiveness, and agility, they sometimes underestimate the challenges that come from small differences between traditional on-premises computing paradigms and the new considerations that are specific to the cloud.

A common misstep is to replicate the existing traditional network and infrastructure security strategies when migrating to the cloud. The organization misses an opportunity to adopt a network and infrastructure architecture that capitalizes on the benefits of cloud. An unplanned cloud infrastructure might actually produce worse performance or increase costs over an on-premises infrastructure.

In addition, organizations sometimes mistakenly believe that cloud service providers are responsible for controls that are out of the scope of the cloud provider's responsibility. This misunderstanding of the shared responsibility model can leave the organization's cloud infrastructure susceptible to threats. Organizations that haven't defined a cyber risk strategy, cloud governance model, or begun planning in earnest can easily find themselves in a situation with more complex security challenges, resulting in exposure to compliance and security incidents and eroding the business case for cloud adoption. Taking full advantage of Amazon Web Services (AWS) with a cyber risk strategy that incorporates a well-architected solution can bring significant improvement to network and infrastructure security posture and cost optimization.

A cyber risk strategy should include several components. First, identity and access management (IAM) capabilities and tools are needed to establish permission boundaries to prevent unauthorized changes. Network protection (e.g. intrusion detection, content filtering) and monitoring tools should be incorporated to help protect and record traffic patterns as well as ingress and egress points. Security monitoring solutions should be integrated to trace events and provide correlation to identify malware, privilege escalation, and other threats. In addition, organizations need experience to integrate third-party security solutions that work with

AWS and are cost effective. Finally, it is also critical for organizations to implement solutions that leverage serverless computing where possible, to take advantage of the native AWS services as well as provide automated responses and remediation of threats while keeping in mind the shared responsibility model where AWS manages the security of the cloud and organizations manage the security in the cloud.

Implementing the AWS network and infrastructure security means tying multiple pieces together like securing the communication and access to your organization's AWS network traffic, securing and monitoring the AWS services and endpoints through appropriate configuration and integration with marketplace security tools. Use a dedicated AWS account for housing security related operations as well as leverage services like AWS Security Hub to automate and centralize security checks and alerts. While dealing with multi-account AWS environments, it is also recommended to leverage certain AWS services like the AWS Organizations and AWS Control Tower which can assist in effectively consolidating and centrally managing the accounts as well as setting up landing zones following the prescriptive leading practices, respectively. New operational responsibilities, processes, and techniques are required to be introduced to manage your AWS infrastructure and capabilities previously unavailable with on-premises technology.

According to Gartner®, "The extensive security capabilities of IaaS+PaaS providers, as well as third-party vendors, enable enterprises to improve the protection of their cloud infrastructure. Properly managed, security and risk management leaders can make their IaaS+PaaS environments more secure than their data centers."¹

¹ Gartner, How to Make Integrated IaaS and PaaS More Secure Than Your Own Data Center, Esraa ElTahawy, Dale Koeppen Nov 30, 2023

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Incorporating cloud security into dynamic network and infrastructure

Cloud has dramatically changed how networks and infrastructure are provisioned, maintained, secured, and monitored. The accessibility and flexibility of cloud reduces much of the friction when deploying infrastructure, which can result in a situation where it becomes easier and appears to be more cost effective for individual business units to deploy their own infrastructure in virtual silos. This reduction in friction comes from the relative ease with which network and infrastructure components can be deployed and managed in the cloud. With the help of AWS Organizations and Control Tower, businesses can manage their governance policies, security controls and other management of multi-account environments through an automated, centralized service. This solution allows deploying new infrastructure to be both more convenient and cost-effective.

Keeping up with a dynamic, ephemeral environment requires special skills, tools, and enhanced processes. For example, auto-scaling and automation using AWS CloudFormation Templates can result in the instantiation of resources such as Amazon Virtual Private Clouds (VPCs) and Elastic Load Balancers (ELBs) with auto-provisioned Amazon Elastic Compute Cloud (EC2) compute resources and Internet Protocol (IP) namespace ranges allocated automatically. Resources can also be deprovisioned automatically. While this dynamic design is a cornerstone of the agility offered by the cloud, it requires new approaches for security and compliance. An underprepared IT department will likely struggle to keep up with the compliance, security, and visibility of the environment and assets. If organizations are not adequately prepared for these challenges, they may face increased cost, overextended infrastructure, strained security staff, and lack of adequate security threat mitigation, visibility, and control. Businesses also run

the risk of employee turnover which would decrease organizational knowledge and security posture. With the right cyber risk strategy and resulting infrastructure design, organizations can understand what security capabilities they should prioritize and enhance in alignment with the overall cloud transformation for network and infrastructure security. Overcoming these challenges can result in opportunities to tailor a framework that can mitigate issues while providing ease of use and scale through automation as the path forward.

Leveraging AWS can reduce the scope of required security (e.g., data center security, hardware) for the organization, but it doesn't eliminate it. Once an organization understands what its control requirements are, it can place emphasis on using the capabilities of the cloud not only for technology deployment with DevOps, but for security (DevSecOps).

This shift creates opportunities for automation of security controls, real-time defense of the environment, greater efficiency, and agility by utilizing cloud-native services, templates, and scripts to help deploy and manage security solutions.

Deloitte's cyber risk framework for AWS provides the blueprint and accelerators for implementing enhanced cyber risk capabilities in a prioritized approach tailored for AWS and the organization's cyber risk profile. For example, important design considerations include landing zones with embedded security configurations and establishing VPCs based on data classification and shared services.

Deploying shared services for security, monitoring, and administration can improve security while taking advantage of the operational benefits of cloud.

Also, establishing standard “golden” configurations for the infrastructure services such as EC2 is a critical practice in order to realize the benefits of automation and the deployment lifecycle for Infrastructure as a Service (IaaS). With automation and a configuration-driven approach, the environment can constantly be refreshed with the latest patched golden images. The regular patching requirements of EC2 instances can be automated utilizing Patch Manager functionality within AWS Systems Manager service. Patch Manager can be used to apply patches for both operating systems and applications. Opportunities to automate many aspects of traditional security and compliance tasks should be identified during the AWS adoption journey. Once the more routine security and compliance tasks have been automated through features such as AWS CloudFormation and AWS Lambda scripts, security professionals are free to concentrate on other proactive

and strategic security activities. Lambda scripts are especially helpful with automation due to their ability to reduce friction when deploying new infrastructure and its ability to be serverless and can easily integrate with other AWS Services. Lambda functions are the primary choice to configure corrective control policies within the AWS accounts against cloud misconfigurations.

Designing security for your organization’s AWS environments requires alignment with the cloud strategy and planning that addresses which controls can be automated. In addition, planning should factor in the evolution of automation scripts and security and compliance requirements for modularity. This approach enables flexibility and allows for standardization and re-use for additional AWS environments. This automation should be implemented across the organization’s AWS accounts consistently.



Securing your organization's AWS network and infrastructure

One component of [Deloitte's Cyber framework](#) describes reference security architecture patterns to protect the AWS network and infrastructure. These patterns focus on protecting network traffic, hardening endpoints, devices, and protecting Application Programming Interfaces (APIs) and services.

As part of the framework, Deloitte has developed assets specifically aligned to AWS cloud environments that focus on protecting ingress and egress points, segmenting internal traffic, managing AWS IAM to provide access to resources using a least privileged approach, gaining visibility to data assets, monitoring events, and remediating vulnerabilities.

Architecting and securing AWS network and infrastructure services begin with a focus on data classification that the cloud environment will process, transfer, and store. Multiple standard architectures should be created for environments with different classifications by applying a tailored set of controls and configurations in alignment with the data classification and related regulatory requirements. There are two important design aspects relating to data classification and the network and infrastructure design for AWS environments. First, the classification informs design decisions for addressing specific security requirements such as segmenting the environment into manageable VPCs and subnets to provide segmentation for access, administration, and automation of the security configurations. Second, different data requirements should factor into balancing risk and cost management across different environments and rationalizing costs of regulated and non-regulated workloads. For example, a reduced number of controls are required for a development environment with non-critical data vs. a production environment with confidential data that typically would require additional protection such as compliance with Payment Card Industry (PCI) security standards. To track data classification

within resources, organizations can use Amazon Macie, a machine learning application that scans an organizations Simple Storage Service (S3) bucket storage for personally identifiable information (PII) and other forms of sensitive data. Macie can perform an inventory of the resources, classification of the data stored within, and analyze access control and privacy settings for each. Findings discovered by Macie can be delivered to AWS Security Hub and centralized with other alerts from the environment.

Deloitte's approach to manage cyber risks associated with network and infrastructure for AWS also enables and supports other cyber domains. Just as a configuration management database (CMDB) supports threat and vulnerability management, predictable network security design aids with managing access controls and security monitoring in a standard manner. Automation is also easier to re-use across environments with standardized network and infrastructure security designs.

Network security

When addressing security while architecting on AWS, it's important to establish effective ways for devices to securely communicate. You can apply secure communications by controlling traffic at each network layer, automating network protections, and implementing inspection and detection.

Proper network management begins with one simple concept: routing. The way traffic is routed through the network has a significant impact on ease of security for internal teams and the external customer experience. AWS Transit gateway helps enterprises achieve greater customization in their network routing configurations and determines secure data transfer at scale. Transit Gateway acts as a central hub for traffic between VPCs and on-premises networks. By routing traffic through one central location, you can collect detailed flow logs on each packet that traverses the network. This data can be forwarded to various AWS services

like Amazon S3, CloudWatch, or Amazon Kinesis Data Firehose where it can be deeply analyzed to produce comprehensive analysis on the security of your network. Furthermore, Transit Gateway enables greater network segmentation which enhances traffic flow management, fortifies security, and helps increase the resilience of your network architecture. It is these capabilities that make Transit Gateway an essential piece of scaling and securing your networking footprint in the cloud.

When looking deeper at the central hub architecture of Transit Gateway, one should consider what tools go into securing each spoke around the hub. Using Network Access Control Lists (NACLs), Security Groups, and subnets, traffic can be restricted to only authorized connections and services by using a zero-trust model. These control features provide micro-segmentation of the internal cloud networks and layers of security to create a defense-in-depth approach. NACLs protect the perimeter of subnets by defining stringent rules for permitting and rejecting traffic. Security Groups can protect network interfaces in your environment with narrow configurations for IP and port ranges on which the interface is allowed to communicate. Finally, subnets segment networks based on different characteristics and sensitivity levels treating each subnet as its own siloed network. Organizations can follow swim-lane isolation for securing sensitive data in AWS data stores through a combination of applying appropriate IAM controls and network flow controls. The network flow controls include a NACL on the subnets of your data store layer or allow access to your data store only from the appropriate endpoint and deny traffic from other origins.

If all this configuration complexity is beginning to sound like a headache, there are a plethora of AWS-managed services that will make managing your network security much easier. One such example is the Amazon VPC Lattice service. VPC Lattice is a solution to connect, secure, and monitor application layer communications at the VPC and account level of your AWS infrastructure. In the form of “service networks”, Lattice creates logical boundaries that are used to control inter-application connectivity within a VPC. Traffic can be routed based on defined request characteristics and weighted routing depending on the deployment strategy. Fine grained authentication can be configured through Lattice's integration with IAM. Teams can simplify their application deployment with this managed networking

service by simply deploying into the desired service network and letting Lattice manage the day-to-day operations. In addition to security configurations within Lattice, managed firewalls will help secure the perimeter of your network and monitor traffic going in and out. As organizations scale, they can easily reach hundreds of AWS Network Firewalls, Web Application Firewalls (WAF) and thousands of AWS Security Groups deployed across the environment. It is critical to plan for this scale early on. AWS Firewall Manager provides the capability to manage your AWS firewall administration and maintenance centrally across your environment. This means your WAF, Shield, Security Group, Network Firewall and Domain Name Service (DNS) firewall maintenance lives in one place and adapts to new accounts or resources created in your environment.

Infrastructure security

Each AWS service provides a specific set of functions and therefore has a specific set of risks to address that may require tailored security controls applied with the installation of the service. For example, as of April 2023, S3 buckets are encrypted and private by default. Even with such secure default configurations, features like access logging should be enabled in order to confirm access requests are accounted for and a proper documentation trail can be followed if investigation is required.

Each specific AWS service has a variety of security configurations that may be mistakenly overlooked or misconfigured by technical teams. By templating infrastructure deployments using infrastructure as code (IaC), such as Terraform or the AWS Cloud Development Kit (CDK), teams can enforce compliance at scale and increase their deployment velocity. Terraform can be used to declare a variety of infrastructure resources across multiple cloud providers. The AWS CDK provides a CloudFormation wrapper in the form of libraries of code in a variety of well-known programming languages for constructing complex infrastructure configurations that can be secured and deployed at scale.

AWS partner organizations like Deloitte can provide the security infrastructure for your environment and manage the security operations so that your team can focus on what matters most: your business. There should be additional focus for securing organizations' Amazon EC2 configurations in your cloud environment. Enterprise-

level “golden” Amazon Machine Images (AMIs) should be created and made available which can be leveraged to deploy secure instances by AWS DevOps teams. The goal should be to continuously improve the security through hardening, vulnerability scanning, and patching of the “golden” AMI. The utilization of a “golden” AMI can facilitate deployment speed in a secure manner and reduce operational overhead. For example, the Center for Internet Security (CIS) defines security benchmarks and controls for hardening your EC2 instances. These benchmarks are configured on AMIs that are sold as pre-hardened images for deployment into your environment via the AWS marketplace. This minimizes overhead and provides a simplified path to an operational “golden” AMI. If cost or greater configurability is a concern, the CIS pre-hardened images are also available as build kits to provide the baseline security configurations but with greater customization to better fit the clients’ needs. Each of these preconfigured solutions and more can be found through the AWS marketplace.

After defining requirements for the golden AMIs and writing the IaC code needed to deploy them, the next step is to utilize an orchestration tool to help deploy your code. Services such as AWS Code Build, AWS CodeDeploy, and AWS CodePipeline can facilitate a seamless Continuous Integration/Continuous

Deployment (CI/CD) flow and allow your IaC to scale with your business needs. To extend the necessary governance with the growing infrastructure footprint, AWS Control Tower orchestrates the necessary guardrails to help secure your environment. Leveraging these tools in tandem will create a secure and scalable solution for deploying your AWS infrastructure.

If a less customized solution for server configuration and management is required, a service like EC2 image builder can provide a simplified server build process, managed by AWS. Image builder will help you automate the creation, management, security, and deployment of your server images. You can automate through image builder by configuring pipelines for deployment and patching. You can also utilize stand-alone commands to create one-off, customized images for specific use cases that may arise.

Organizations can leverage the Amazon Security Lake service from AWS that centralizes security data from AWS environments, SaaS providers, on premises, and cloud sources into a purpose-built data lake stored in your account. With Security Lake they can get a more complete understanding of their security data across your entire organization.



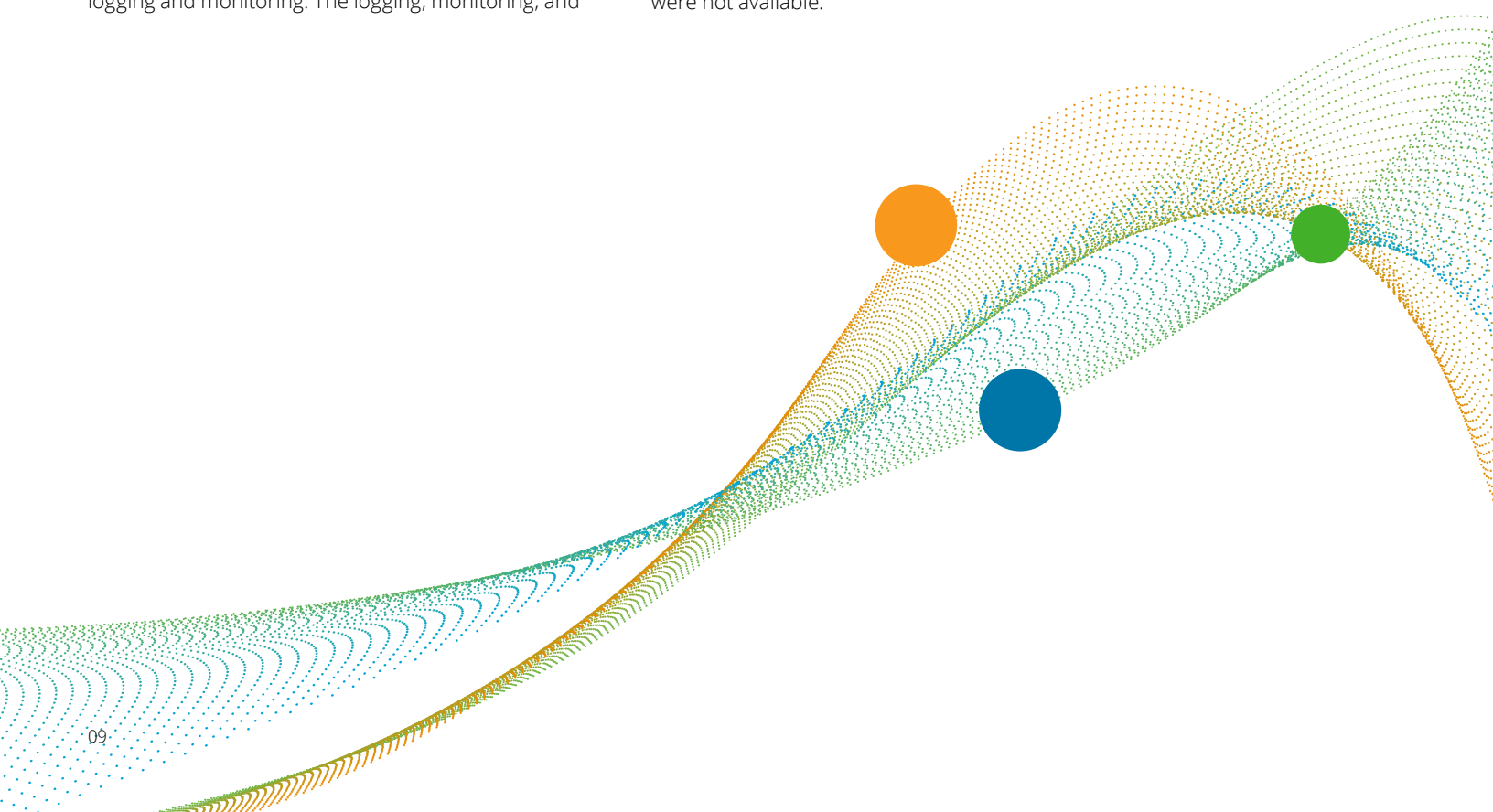
Maturing your organization's AWS network and infrastructure

Creating more mature capabilities includes extending security monitoring to a virtualized cloud infrastructure, managing ephemeral assets, and integrating threat intelligence. It also requires AWS-aware alerts leveraging a variety of services such as AWS CloudTrail, CloudWatch, Lambda, Amazon GuardDuty, and a security information and event management (SIEM) tool.

Existing enterprise vulnerability management capabilities should be enhanced and integrated with AWS Systems Manager to augment vulnerability scans of configurations at the application, Operating System (OS), and AWS service layers. For example, vulnerabilities related to containers and other application code should have vulnerability scanning and penetration testing as part of the deployment cycle to identify issues before they are deployed to production. Patching, hardening, and endpoint protection should be integrated with the AWS service environment as well. The assets deployed to AWS should be tracked as part of the environment's lifecycle. AWS Config and Lambda functions can tag and record assets, creating an inventory or feeding an existing CMDB.

Another important aspect for enabling visibility into assets and the AWS environment is to implement logging and monitoring. The logging, monitoring, and

alerting services for capturing VPC flow logs, activity, and event logs via CloudWatch and CloudTrail should be integrated with the security monitoring program to provide visibility into inter-network and intra-network communications, providing an opportunity for detection or post-mortem investigation of misconfigured or unauthorized traffic. Organizations should implement these logging and monitoring tools for the resources across the organization. These logging tools can be ingested into a central repository such as AWS Security Hub or a third-party tool such as SIEM. This will provide organizations with insight into the security and performance of the resources that are being run within the organization and promote resource management at scale. Additional AWS services such as GuardDuty with its ability to identify anomalous behavior and leverage external threat intelligence sources should be integrated for additional visibility, alerting, and analytics. Furthermore, AWS Security Hub may be enabled as a central mechanism to aggregate security alerts from multiple AWS services, accounts, resources, and third-party solutions. These capabilities can be standardized and applied for each cloud deployment and integrated as part of a shared services module. The dynamic nature of infrastructure in AWS provides opportunities for cost effective fault tolerant designs in ways that previously were not available.



Incorporating resiliency into AWS network and infrastructure

As cloud computing becomes a more integral part of core business operations, it's imperative to take advantage of the dynamic nature of the cloud and reduce downtime due to disruptions from minutes to seconds. Virtual infrastructure and services in AWS provide opportunities for cost effective and fault tolerant designs in new ways. Resiliency includes elastic designs for "always on" solutions, new models for contingency planning, recovery, and availability. AWS provides accessible features such as highly scalable, on-demand APIs that enable companies to create highly available and scalable serverless architectures. Incorporating a network and infrastructure design that leverages multiple availability zones and cross-region failover can provide efficient and rapid recovery and response from the AWS architecture, thereby reducing impacts from unplanned incidents.

In addition, virtual infrastructure can be deployed with automatic and redundant backups with low latency and optimized costs through elasticity and efficient data storage to mitigate disruptions. For example, an organization could use techniques such as cross-region replication of virtual instances and data archiving services like Amazon S3 Glacier to enhance

recovery from a disaster recovery scenario. When implementing resources organizations should utilize Cloud Formation templates or Infrastructure as Code scripts to deploy their resources with these redundant backups in mind. This will allow organizations to increase their efficiency and remain scalable through disaster recovery scenarios.

Implement proactive measures for incident response, such as the use of security "trip wires" to accelerate incident identification, and automate orchestration of pre-tested self-healing infrastructure solutions. Create scripts for incident management to rapidly and consistently collect and analyze evidence, utilizing tools such as CloudWatch and Lambda to quickly achieve containment and eradication.

Virtual infrastructure and services in AWS provide opportunities for cost effective and fault tolerant designs in ways that never existed before.



Securing Infrastructure as Code and automating security

AWS provides the ability to implement network, infrastructure, and services as part of the total technology solution. Cloud introduces core virtual infrastructure services as additional configuration and coding components rather than physically separated assets in a data center.

Implementing the design of AWS infrastructure services can be accomplished with reusable AWS CloudFormation Templates and configuration modules of the base network architecture and infrastructure service configurations. Composite architectures can be achieved through the combination of containers, scripting, templates, and dynamic inputs. Infrastructure can be rapidly deployed, scaled, and destroyed through automation and configuration. This is known as "Infrastructure as Code".

Because the AWS environment can be expressed through code and configuration, the code should follow secure development practices in addition to having security controls embedded as part of the automated code and standard configuration templates.

Secure development practices: Secure development practices are a critical control for mitigating cloud security risks related to the Software Development Life Cycle (SDLC) and DevOps processes for "Infrastructure as Code", given there is more code developed related to automation for cloud. The automation code and configuration applies network and infrastructure changes which introduces new risks within the SDLC. A higher priority should be placed upon confirming that the security controls for the SDLC and CI/CD processes are in place. For example, it is important to implement access controls for the code repository and tracking privileged users for critical automation code and configuration templates, as well as conducting application security testing and hardening of the development software and tools used. The automation should stop code migration should these controls not be satisfied.

Automated code analysis plays a key role in improving code quality and compliance. Organizations can leverage Amazon CodeGuru Reviewer service which provides automated recommendations that can assist developers in identifying defects and deviation from coding leading practices. For instance, CodeGuru Security automatically flags potential security vulnerabilities such as SQL injection, hardcoded AWS credentials and cross-site

request forgery, to name a few. After becoming aware of these findings, developers can take decisive action to remediate their code.

Developers can use Amazon Q Developer to improve the quality and security of the code. Q Developer provides automated code analysis and recommendations and offers a low-friction environment that enables them to gain insights on the CodeGuru recommendations and to find creative ways to remediate issues in their code.

Organization Security team can leverage Amazon Bedrock service for accelerated security investigations by using automatically generated SQL queries and can focus on the natural language processing capability of AWS Service to answer questions like "Which AWS Account has the most AWS Security Hub findings", "Irregular network activity from AWS Resources", "Which AWS Identity and access management principals invoked highly suspicious activities". With the identification of possible vulnerabilities or misconfigurations, further time to detect and pinpoint specific resources to assess overall impact can be minimized.

Automating security: The standard scripts that the DevOps teams use to deploy and manage AWS services and the virtual infrastructure should also apply security controls with each component introduced to the AWS environment by a deployment script. Efforts can be made to include security and logging controls directly into the deployment elements. This proactive approach provides improved value and agility instead of trying to secure and monitor the infrastructure reactively, after deployment to production.

A variety of compliance and monitoring controls as well as repetitive security tasks, such as scanning, creating backups and generating alerts, can be automated. For example, the automated detection and remediation of misconfigured resources as well as generating alerts for unauthorized access attempts can be implemented. Deloitte's collaboration with AWS includes ConvergeSECURITY, a suite of managed end-to-end enterprise cloud security and compliance services that focuses on four areas of cloud security: manage, detect, respond, and recover. Managed Extended Detection & Response (MXDR) by Deloitte provides a dedicated three-tiered threat detection and response team that supports planning, deployment, operations, and incident containment and response.

Additionally, features such as AWS Config and AWS CloudFormation related to configuration combined with the automation with Lambda and CloudWatch can help manage standard configuration settings. To illustrate this point, AWS Config can record instances where an Amazon S3 bucket is created, updated, or deleted, allowing for visibility on how those events occurred. AWS Config and CloudFormation Configurations can also be integrated within AWS Security Hub. Security Hub can alert and preform change-checks and provide alerts if misconfigurations or compliance issues are detected. Lambda can also be used to initiate active alerting for where compliance issues are detected.

Once the infrastructure has been designed, for example, using AWS CloudFormation templates, Security Groups can be standardized and configured for automated deployment. Scripts can include standard information or allow for input to dynamically assign values for constantly changing elements, such as IP addressing. Therefore, the same automation that deploys the resources can deploy the security controls to the environment.

Embedded security: AWS deployments can be combined and architected with containerization to enable cloud infrastructure for applications with modules that have security already built in for re-use. For example, automated security scanning can be added to the CI/CD process and toolset that builds the container. Implemented in the appropriate manner, these standard containers can enable rapid deployment of infrastructure to support a diverse range of applications and business services with embedded security. This approach allows modules to be combined into portable templates and containers with security built in.

Prioritize security code enhancements to the DevOps workflow to account for securing code repositories and integrations with AWS and third-party tools to automate control checks within the pipeline before code is deployed to production.

Harness the benefits of Infrastructure as Code to secure the cloud

- ✓ Provide a highly available infrastructure by taking advantage of the multi-region, multi-availability zone nature of AWS.
- ✓ Improve security by automatically deploying, configuring, and monitoring standardized environments.
- ✓ Reduce latency, connectivity issues, and optimize costs by fully utilizing automatic elasticity of the cloud by dynamically expanding and contracting with demand, not based on guesses or unreliable predictions.
- ✓ Promote business value and market agility by reducing time and investment with the ability to rapidly prototype, fail fast, and accelerate value through more deployments of product iterations.
- ✓ Protect against evolving cyber threats and leverage features such as access controls and direct visibility to network and infrastructure services.
- ✓ Benefit from AWS native services and features such as VPCs, Security Groups, AWS Shield, and AWS Web Application Firewall.



The strength of the Deloitte/ AWS relationship



Premier
Consulting Partner

Security Competency

Government Competency

Financial Services Competency

Public Sector Partner

MSP Partner

Our relationship brings together Deloitte's extensive industry experience in cyber and enterprise risk management **with the security-enabled cloud infrastructure of AWS.** In 2006, AWS began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. Today AWS provides a highly **reliable, secure, scalable, low-cost** infrastructure that powers hundreds of thousands of businesses in 190 countries around the world, with over a million active customers spread across many industries and geographies.

Deloitte can help organizations adopt AWS securely and establish a security-first cloud strategy. Deloitte is a leading information technology and advisory company. Deloitte is an **APN Premier Consulting Partner** and an **AWS Security Competency Partner (Launch Partner)** and was one of the first eight organizations globally to achieve the **Security Competency** as a launch partner. Deloitte's vast experience in Cyber Risk, combined with its extensive experience with AWS and Cloud technologies, enable us to provide **end-to-end** security solutions.

Authors

Henry Li

Managing Director, Cyber Risk Services
AWS Security Leader
Deloitte & Touche LLP
henli@deloitte.com

Arya Ray

Specialist Master, Cyber Risk Services
Cloud Security Architect
Deloitte & Touche Assurance & Enterprise Risk Services India Private Limited
aryaray@deloitte.com

Amazon Web Services

Cristian Critelli

EMEA Lead Networking and Resilience Specialist
PSA
criscrit@amazon.com

Keith Hodo

Partner Solution Architect
hodok@amazon.com

Contributors

Jonette Jones

Senior Consultant, Cyber Risk Services
Deloitte & Touche LLP
jonejones@deloitte.com

Garuav Thapliyal

Lead Solution Advisor, Cyber Risk Services
Deloitte & Touche Assurance & Enterprise Risk Services India Private Limited
gthapliyal@deloitte.com

Seth Markarian

Analyst, Cyber Risk Services
Deloitte & Touche LLP
semarkarian@deloitte.com



This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

All product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2024 Deloitte Development LLC. All rights reserved.