aws | Deloitte.

AWS network and infrastructure security

Fundamentals for a solid foundation

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 designs during a "lift and shift" to the cloud. The organization misses an opportunity to adopt a network and infrastructure architecture for the cloud that enhances 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, etc.) and monitoring tools should be incorporated to protect and record traffic patterns as well as all 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 expertise to integrate third-party security solutions that work with AWS and are optimized for cost. Finally, it is critical for organizations to implement solutions that leverage serverless computing where possible to take advantage of native AWS services as well as provide automated responses and remediation of threats.

Implementing AWS network and infrastructure security means securing the communication and access to your organization's AWS network traffic, as well as securing and monitoring the AWS services and endpoints through appropriate configuration and integration with marketplace security tools. New operational responsibilities, processes, and techniques are required to be introduced to manage your AWS infrastructure and capabilities previously unavailable with on-premises technology.

"Although CSPs have proven extremely reliable, security failures in the public cloud are relatively common. Virtually all cloud security failures are the result of actions taken by the tenants of those cloud services. Gartner's advice is to stop obsessing about the security of the cloud, and start obsessing about how to use clouds securely. Reliance on several IaaS providers and hundreds, even thousands, of SaaS providers, represents a complex set of control challenges."[1]

1 Gartner, Security of the Cloud Primer for 2019, Feb 7, 2019

aws | Deloitte.

Incorporating cloud security into dynamic network and infrastructure

Cloud has dramatically changed how networks and infrastructure as a whole 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. The reduction in friction comes from the relative ease with which network and infrastructure components can be deployed and managed in the cloud.

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 VPCs (Virtual Private Cloud) and ELBs (Elastic Load Balancer) with auto-provisioned Amazon Elastic Compute Cloud (Amazon EC2) compute resources and 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. 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 has an understanding of 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).

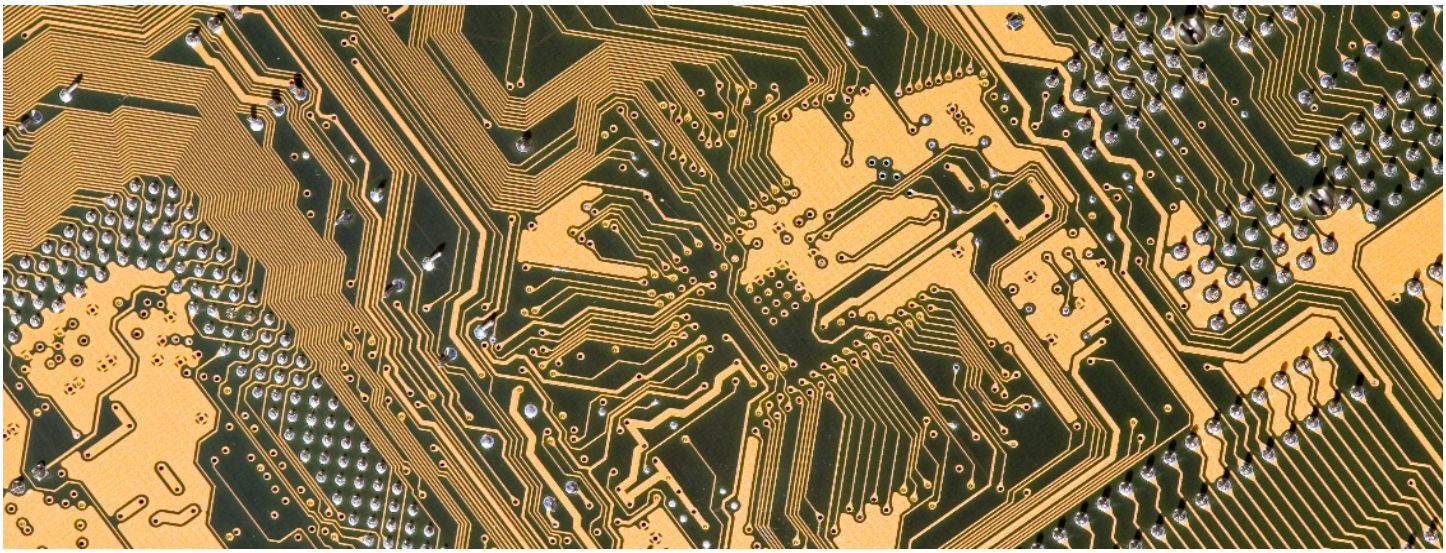
This shift creates opportunities for automation of security controls, real-time defense of the environment, greater efficiency, and agility by utilizing cloud native services, templates, and scripts to deploy and manage security solutions.

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 IaaS. With automation and a configuration-driven approach, the environment can constantly be refreshed with the latest patched golden image vs. patching in place. 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.

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 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 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 begins with a focus on the data classification for the data 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.

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 design.

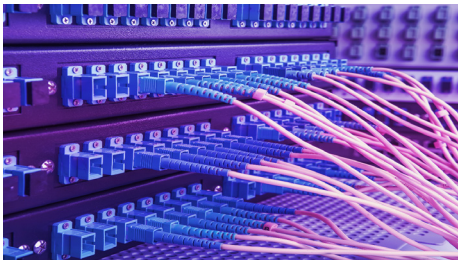
Network Security

Several AWS services can be configured for securing network communications between the enterprise, AWS VPCs, and applications deployed to AWS accounts. For example, AWS Direct Connect can be used to create a secure private network connection, which can lead to reduced costs for heavy-bandwidth workloads as well as a more consistent network experience. By transferring data directly, companies can reduce their bandwidth commitment to their Internet service provider, as well as transfer data at a reduced rate when moving large amounts of data. AWS Direct Connect also can provide a resilient connection to AWS, by connecting through two different locations and mitigating the risk of a single point of failure. This is one example that illustrates some of the value and case for leveraging additional network protection services for AWS such as AWS Shield, AWS WAF (Web Application Firewall), and AWS PrivateLink to help organizations manage security related to the virtual network. These AWS network protection services and features can be enabled and configured versus having to procure and install appliances and servers. Configuring and protecting network traffic within the AWS cloud is another important consideration. Through the use of 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 can provide micro-segmentation of the internal cloud networks and provide layers of security to create a defense-in-depth approach. NACLs can protect the perimeter of VPCs and segment networks with different characteristics and different sensitivity levels across different VPCs. Security Groups can be applied for further granularity by segmenting VPCs into smaller sub-groups for additional layers of protection.

Infrastructure Security

Each AWS service provides a specific set of functions and therefore has a unique set of risks to address that may require tailored security controls applied with the installation of the service. For example, Amazon API Gateway should implement Client-Side SSL Certificates for authentication by the backend to verify application program interface (API) requests while Amazon Cognito should implement 'Invite Only' as a security option to restrict which users can sign up for an account. Each unique AWS service has a variety of security configurations that may be mistakenly overlooked or misconfigured by technical teams. Each AWS service should have the standard security configurations applied as embedded configurations with the deployment script. AWS development teams should incorporate the security controls as part of the deployment script implementation and configuration templates. These security settings should be verified and monitored for compliance on a real-time basis with security monitoring as well. Therefore, the security monitoring use cases should be updated to include monitoring for deviations from the security standard for deployed services.

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, using the cloud's dynamic nature and services like AWS CodeDeploy, the use of blue-green deployments can be simplified, thus reducing the risk of down time as a by-product of upgrading software. Blue-green deployments is one method to automatically provision new instances of your application while at the same time controlling the routing of load balancer network traffic dynamically to the newly deployed application instances.



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, Amazon CloudWatch, Lambda, Amazon GuardDuty and a security information and event management tool (SIEM).

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. 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 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 never existed before.

Incorporating resiliency into AWS network and infrastructure

As cloud computing becomes a more integral part of core business operations, the imperative is 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 way that never existed before. Resiliency includes elastic designs for "always on" solutions, new models for contingency planning, recovery, and availability. AWS provides accessible features such as scalable, on-demand APIs that enable companies to create highly available, 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 Simple Storage Service Glacier to enhance recovery from a disaster recovery scenario.

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

aws | Deloitte.

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 has now introduced 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 and destroyed through automation and configuration. This is "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 the network and infrastructure changes which introduces new risks within the SDLC. A higher priority should be placed upon verifying that the security controls for the SDLC and Continuous Integration and Continuous Delivery (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.

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 audit controls directly into the deployment elements. This proactive approach provides better value and agility instead of trying to secure and audit the infrastructure reactively, after deployment to production.

A variety of compliance and audit controls as well as repetitive security tasks, like scanning, creating backups and generating alerts, can all be automated. For example, the automated detection and remediation of misconfigured resources as well as generating alerts for unauthorized access attempts can be implemented. 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 and provide active alerts if modifications or misconfiguration is detected. To illustrate this point, AWS Config can record instances where an Amazon Simple Storage Service (Amazon S3) bucket is created, updated or deleted, allowing for visibility on how those events occurred and Lambda can initiate active alerting for where compliance issues are detected.

Once the infrastructure has been designed, for example, using AWS Cloud Formation templates, Security Groups can be standardized and can be 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.

aws | Deloitte.

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

aws | Deloitte.

The strength of the Deloitte /AWS relationship

Partner network

Premier Consulting Partner

Security Competency

GovernmentCompetency

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

Aaron Brown
Partner, Cyber Risk Services
AWS Alliance Leader Deloitte & Touche LLP
aaronbrown@deloitte.com

Mark Campbell
Senior Manager, Cyber Risk Services
Cloud Security Architect & AWS Alliance Manager
Deloitte & Touche LLP
markcampbell@deloitte.com

Ravi Dhaval
Manager, Cyber Risk Services
Cloud & IoT Security Architect
Deloitte & Touche LLP
rdhaval@deloitte.com

Luis Pastor
Senior Consultant, Cyber Risk Services
Cloud Security Architect
Deloitte & Touche LLP
lpastor@deloitte.com

Amazon Web Services

Piyum Zonooz
Global Partner Solution Architect
pzonooz@amazon.com

Contributors

Ashwin Satyanarayan
Consultant, Cyber Risk Services
Deloitte & Touche LLP

LeeAnn Gerosolina
Consultant, Cyber Risk Services
Deloitte & Touche LLP