FOGHORN WHITEPAPER SERIES

A Resource Guide For Navigating The Cloud

DevSecOps Enablement On AWS

Best Practices and Advantages of AWS Tools In Building a Compliant Cloud

aws partner network

Premier

Consulting Partner

DevOps Competency

Security Competency

Solution Provider

foghornconsulting.com

In this whitepaper you will find out:

> The benefits of a DevSecOps approach

> Security roles and responsibilities on AWS

> How layered security enhances peace of mind

> How containers are changing incident response

> Microservice Security Checklist

> 12 Security Best Practices on AWS

Best Practices and Advantages of AWS Tools In Building a Compliant Cloud

INTRODUCTION

Whether in transit or at rest, data is the lifeblood of enterprise. From passwords to credit cards, from health records to personal information, from business secrets to intellectual property, armies of black hatted hackers from around the world are lurking around the digital perimeter poking, prodding, cajoling, and always inventing new ways to steal data. With nefarious intentions the damage they can inflict can bring a company to their knees. Revenue loss, fines, business reputation crisis, career ruin are the potential fallout.

Hackers need to be correct or lucky just once. Security professionals with workloads in the cloud need to be correct 100% of the time. Risky configurations, anomalous user activities, suspicious network traffic, and host vulnerabilities remain front of mind for CISOs. Compliance such as FINRA/SEC, GDPR, PCI, HIPAA/HITRUST and California Privacy laws further complicate the data protection landscape.

According to Forrester Research spend on public cloud security tools will rise from $5.6 billion in 2018 to an estimated $12.6 billion in 2023. The efficacy of cloud native security tools is proving to be a worthwhile investment as only 12% of breaches targeted the public cloud. Notable breaches of Marriott, British Airways and Ticketmaster in 2018 and the costs associated make detection and prevention a much wiser investment over cure.

With market leading security tools implemented with best practices and the assistance of security experts, cloud ecosystems on AWS are the industry gold standard for availability

Hackers need to be correct or lucky just once. Security professionals with workloads in the cloud need to be correct 100% of the time

and security. The bad news for hackers is; with the correct planning, architecture and use of tools, common attack vectors can be thwarted and prevented. Amazon Web Services has innovated on the leading edge in the development of secure infrastructure and Foghorn has the depth and breadth of experience to help design, build and implement tools and best practices to eliminate the damage that bad actors can do to an organization.

The threat, response and prevention landscape is changing in real time. In this whitepaper we will explore best practices for securely migrating and maintaining workloads on AWS. AWS clients with the proper guidance can achieve high levels of peace of mind, as they take advantage of the innovation leaps that AWS affords them today.

DEVELOPMENT + SECURITY + OPERATIONS

According to Gartner, DevSecOps will be practiced by more than 80 percent of development teams by 2021. The amount of DevSecOps practitioners In 2017 was around 17 percent. [2] A recent Veracode survey states that of enterprises adopting a DevSecOps approach will locate and mitigate flaws 11.5 times faster than companies without such programs.[3]

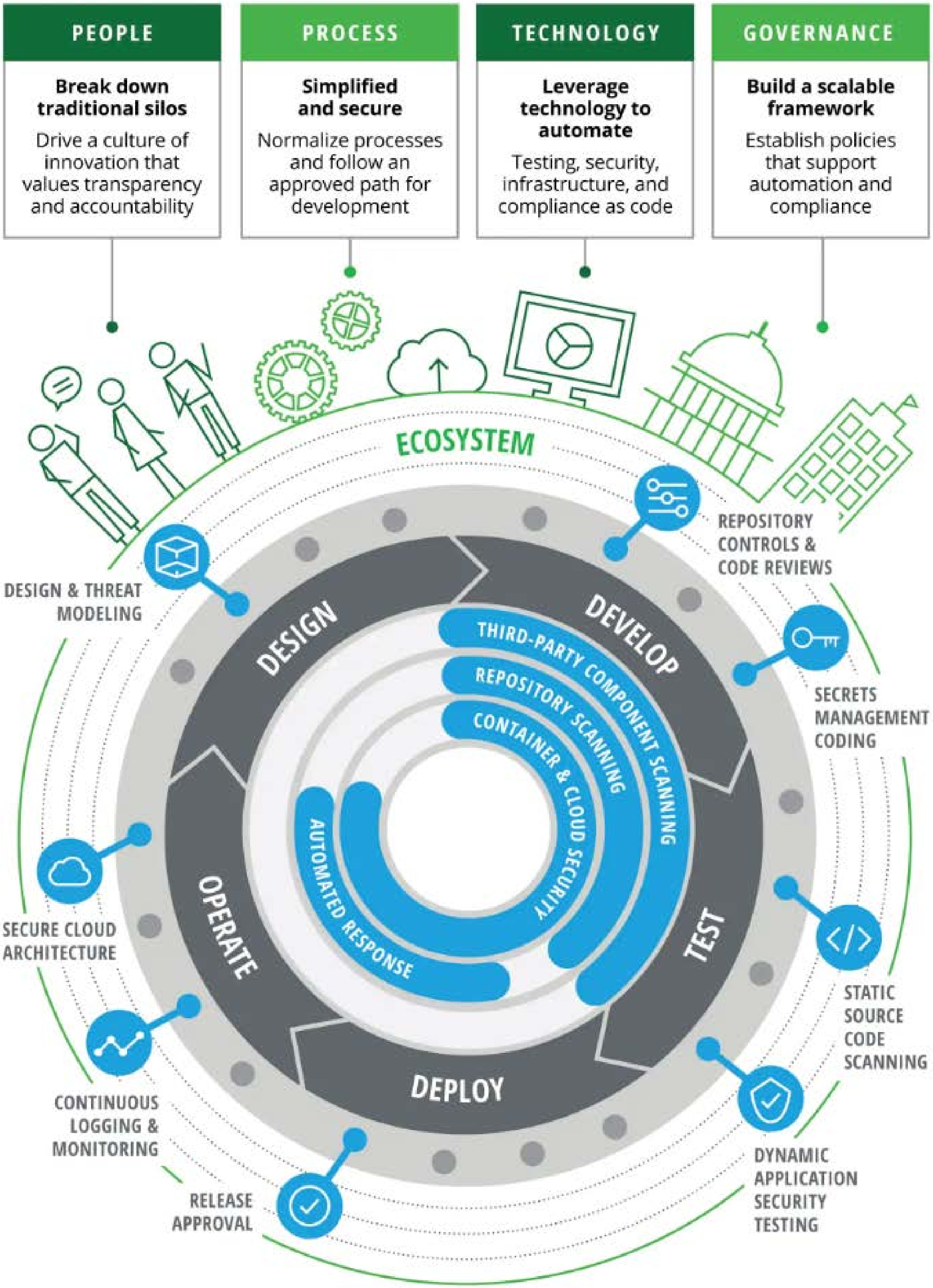
Security "Shifts Left" in DevOps

Over the past years, as development and operations teams aligned their energies, procedures and initiatives, business subscribing to agile methodologies on AWS have realized innovation leaps. Their customers have taken note. While security was always part of the conversation in the Venn diagram of DevOps, the security circle was often considered as bolted on after. As hackers become more and more sophisticated and in the interest of continuous improvement, security has now rightly taken its place in the center of a DevOps practice.

According to Gartner, DevSecOps will be practiced by more than 80 percent of development teams by 2021. The amount of DevSecOps practitioners In 2017 was around 17 percent. A recent Veracode survey states that of enterprises adopting a DevSecOps approach will locate and mitigate flaws 11.5 times faster than companies without such programs.

By bringing security and security professionals into DevOps at the design, build and test phase and not just as a final editor, a cloud's health can be brought into greater homeostasis. The industry term for moving security closer to the design and build is "shifting left."
Whether a workload is containerized or on VMs, customers should leverage an immutable build pipeline. These pipelines make it easier to architect security at build stages, emphasising early collaboration to bake security into the software. Greater efficiencies and security can be gained with this DevSecOps synergy.

What is DevSecOps? A transformational shift that incorporates secure culture, and tools into each phase of the DevOps process.


PEOPLE
Break down traditional silos
Drive a culture of innovation that values transparency and accountability
PROCESS
Simplified and secure
Normalize processes and follow an approved path for development
TECHNOLOGY
Leverage technology to automate
Testing, security, infrastructure, and compliance as code
GOVERNANCE
Build a scalable framework
Establish policies that support automation and compliance
ECOSYSTEM
DESIGN & THREAT MODELING
REPOSITORY CONTROLS & CODE REVIEWS
SECRETS MANAGEMENT CODING
STATIC SOURCE CODE SCANNING
DYNAMIC APPLICATION SECURITY TESTING
RELEASE APPROVAL
CONTINUOUS LOGGING & MONITORING
SECURE CLOUD ARCHITECTURE
DESIGN
DEVELOP
TEST
DEPLOY
OPERATE
THIRD-PARTY COMPONENT SCANNING
REPOSITORY SCANNING
CONTAINER & CLOUD SECURITY
AUTOMATED RESPONSE

Source: Deloitte analysis.

For example, the Infosec Team can provide a hardened and instrumented base image for development teams to build from. Developers can develop with the approved and hardened base image as approved for OS distribution, making security scans for image vulnerability more aerodynamic. These foundational security vetted images, whether for VMs or containers can be re-used speeding up development and making any remediation if necessary much quicker.

With security auditing part of the build process, vulnerabilities can be caught before they become a problem, when they are cheaper and easier to fix. The purpose of this system is to not think of security as a barrier, but as a service. Trust-but-verify, security builds and policies minimize friction, fostering a culture of development creativity and security oversight.

With the promise of DevOps realized, software development is placed within a loop of continuous improvement and continuous development. In the new state of DevSecOps dev teams are having increased synergy by also adding a state of continuous security and compliance. Integrated security teams protect developers and operators, and vice versa. Everyone wins except the hackers.

With automation already at the very core of DevOps design, there is the opportunity for many organizations to bring automation to the security layer, and automate those processes from the inception of an application's design. The main benefit of a DevSecOps philosophy and approach is enhanced security and compliance, with automation delivering efficiencies and the avoidance of errors present with manual processes.

Without the DevSecOps skills in house, AWS partners with the Security Competency and DevOps Competency like Foghorn can help define processes and roles, integrate security tools, and automate processes. Their seasoned advice and invaluable opinions can reconfigure or build your DevSecOps practice on a firm foundation. As DevOps has matured, speed is still valued, but security has "shifted left", as prevention is cheaper and easier than cure.

1. https://www.darkreading.com/cloud/cloud-security-spend-set-to-reach-$126b-by-2023/d/d-id/1334473
2. https://www.itproportal.com/features/the-challenges-of-shifting-to-devsecops/
3. https://www.techrepublic.com/article/organizations-with-strong-devsecops-find-flaws-11x-faster-than-those-without/

SHARED RESPONSIBILITY MODEL

When beginning with AWS it is important to understand the roles and responsibilities of AWS and customers. AWS is a partner with customers with the shared goal of creating a secure and compliant cloud ecosystem. This shared responsibility model allows customers to focus on their data in the cloud, while AWS focuses on the infrastructure.

When implementing DevSecOps with the Shared Responsibility Model, AWS is responsible for the security of the cloud, while customers are responsible for security in the cloud. AWS would be responsible for the hypervisor and hardware, while the customer would be responsible for securing their applications and network. Security shifts left at the build phase, to minimize vulnerabilities being released to production and to maximize infrastructure and application integrity.

With the knowledge that well configured AWS design architecture is as secure as infrastructure can be and regulators have vetted this model. In many cases, like FINRA, these regulators utilize the power of AWS to run their own operations. AWS customers across verticals have built their own compliance success upon AWS's proven backbone. No longer is the cloud thought of as a vulnerable unknown in the IT space, instead it is the gold standard of best practices.

AWS and Customer's Responsibilities

Depending on the services that a customer procures from AWS impacts the amount of configurations that the customer is responsible. For Infrastructure as a Service (IaaS) products like Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and Amazon S3 customers are responsible for the necessary configuration, management, and monitoring. In some container and serverless environments customers are just responsible for the application, and the rest of the security is in the purview of AWS.

In addition to AWS Inherited Controls of physical and environmental layers, customers can also shift management of certain controls to AWS in a custom control environment. Certain configurations and requirements can create a distributed control environment that further relieves the customer of the burden of operating controls. Beyond freeing up in-house resources these relationships can aid compliance, as customers can take advantage of AWS documentation of control evaluation and verification procedures.

For example, in Patch Management, AWS would be responsible for fixing flaws with infrastructure while customers are responsible for patching their guest OS and applications. In Configuration Management, AWS maintains the integrity of the infrastructure, but does not get involved on the OS, database or application layer. AWS trains their own employees, while their customer partners are responsible for training their own staff.

AWS and Customer's Responsibilities

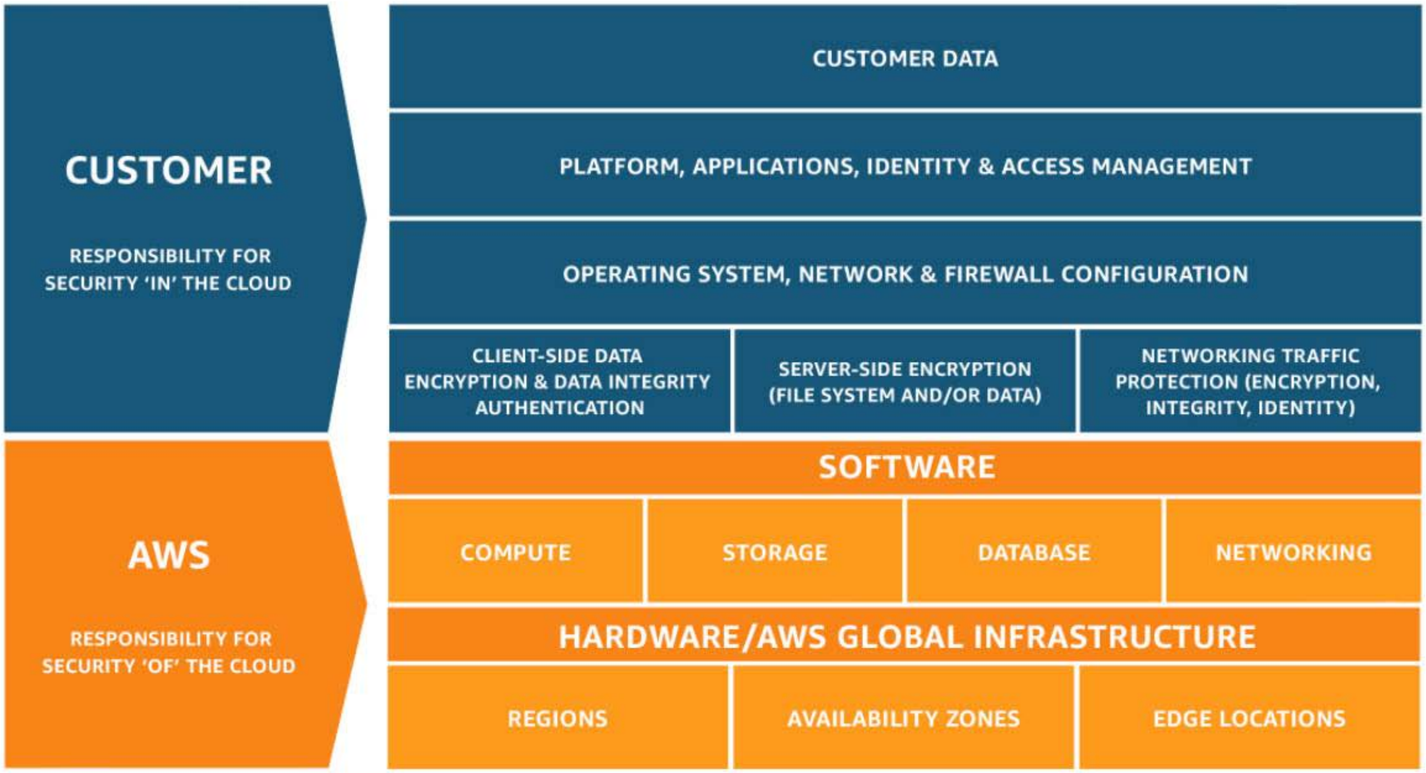

CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Image Courtesy of AWS: https://aws.amazon.com/compliance/shared-responsibility-model/

LAYERED SECURITY

Just like the protection of the Whitehouse, security is much more than a fence and strategically placed secret service agents. Security professionals understand the threat levels and realize that a 360 degree, holistic, belt and suspenders approach must be practiced.

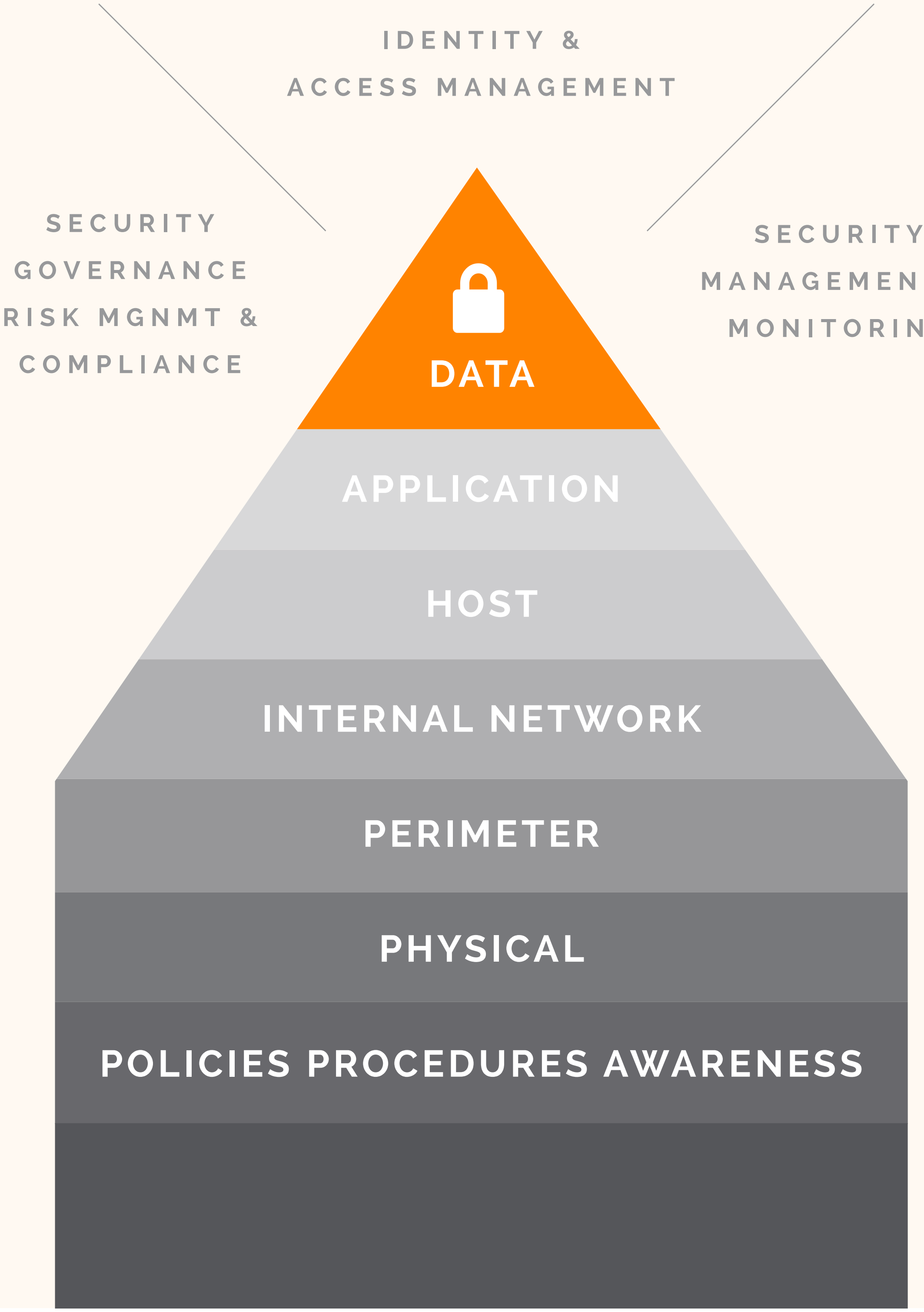
AWS's best-in-breed, fault tolerant, high availability, global infrastructure has the physical security covered. Costs and energy associated with building and managing physical infrastructure from man traps to video surveillance are a thing of the past. In Uptime Institute parlance, AWS's global, distributed Data Centers are built to a minimum of Tier III standards.

Cloud consumers can now focus on rubber meets the road details such as data categorization, data segmentation, server access control, resource-based access control and access control lists, user IAM, data-at-rest encryption, data-in-transit encryption, encryption key management, logging and anomaly detection, and role-based access control.

Included for free, Identity and Access Management (IAM) on AWS is elegant, powerful and user friendly tool, out of the box. Based on policies, users, groups and permissions, IAM on AWS assigns access to specific permissions for all AWS services. Only team members with the right credentials can access certain VMs, compute, storage, database and application services. Granular access control enable pinpoint access, including the enforcement of MFA compliance for IAM users. Using AWS CloudTrail audits and logs of all IAM management is documented to aid in regulatory audit and compliance.

Encryption and key creation, distribution, and management can be arduous, but with AWS Key Management Service (KMS) AWS has strengthened and automated the process by default. Amazon S3 uses server-side 256-bit Advanced Encryption Standard (AED-256). Data can be encrypted with a unique key. An additional safeguard encrypts the key itself with a master that rotates regularly. Using best practices, data on AWS servers is useless to attackers and therefore another level of deterrent. Responsible for the provisioning of cloud hardware, software and platforms, Application Programming Interfaces (APIs) act as the connective tissue of a modern microservices architecture. The average organization manages over 300 APIs, many of which are external and available to customers and partners. As transformative as APIs have been they are also a potential vulnerability. According to Mark O'Neill of Gartner, "By 2022, API abuses will be the most frequent attack vector resulting in data breaches for enterprise web applications."

DEFENSE IN DEPTH : LAYERS



IDENTITY & ACCESS MANAGEMENT

SECURITY GOVERNANCE RISK MGNMT & COMPLIANCE

SECURITY MANAGEMENT & MONITORING

DATA

APPLICATION

HOST

INTERNAL NETWORK

PERIMETER

PHYSICAL

POLICIES PROCEDURES AWARENESS

APIs are everywhere, and as they grow so do the number of API based breaches. From harvesting massive amounts of personally identifiable information (PII) to an API calls that quickly morph into DDoS attacks, an API strategy and defense is essential for security teams.

For the protection from and mitigation of DDos attacks, AWS provides AWS Shield for no extra charge. For business more likely the target of DDoS attacks AWS Shield Advanced provides vigilance for layer 3, layer 4, and layer 7 attacks and 24/7 support.

The protection of APIs does not differ from the security posture with other infrastructure. Web Application Firewalls (WAF) can filter most bad traffic, but for more granular control AWS's comprehensive platform, Amazon API Gateway makes it easy to define, secure, deploy, share, and operate API's at scale.

This holistic API tool accepts and processes up to hundreds of thousands of concurrent API calls. With best practices realized this automated tool becomes event driven. High risk actions are automatically evaluated against policies to determine whether to log, alert, or remediate.

The developer portal makes it easy for API publishers to connect to API subscribers, to monitor, manage, and updating ease. With the correct configurations, API layer vulnerability is ameliorated, as API calls such as traffic management, authorization and access control, monitoring, and API version management are automatically and seamlessly delivered.

Security first organizations operating in the cloud are placing the correct emphasis on administrator management and security processes. Security awareness training empowers everyone in an organization to take ownership of employing best practices. With the right visibility and control, logging and reporting, context, system and developer awareness, security concerns morph into peace of mind, but never complacency.

CONTAINER SECURITY

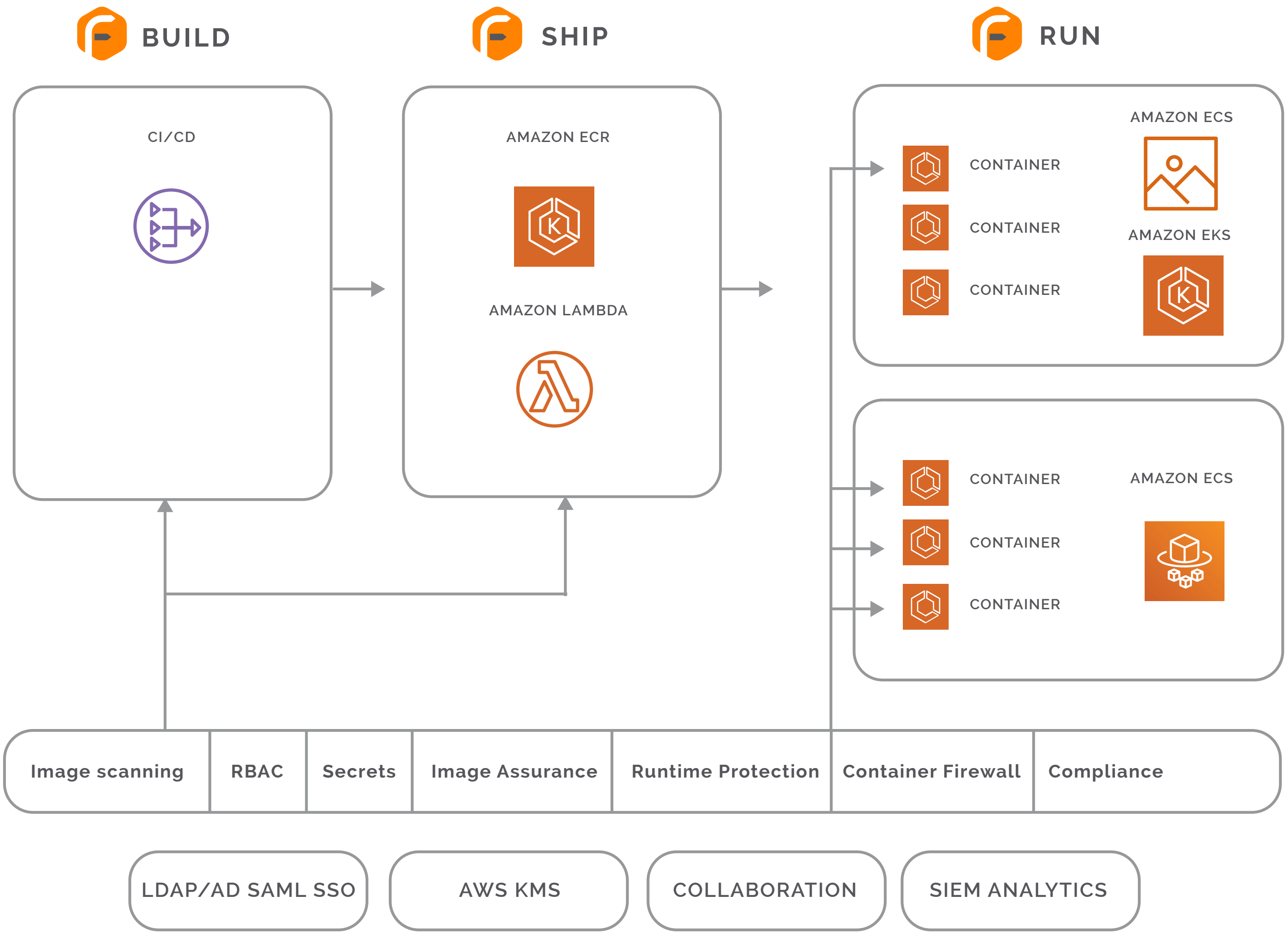
Polyglot, lightweight, immutable, disposable containers are an attractive option for developers working on scalable, cloud native applications. With application libraries and binaries built into the microservice's image along with a virtualized OS, containers start up much quicker than a traditional VM based application. In a CI/CD practice their flexibility and isolation enhance agility.

Moving to smaller microservices within containerized applications compared to monolithic applications enable even more fine grained IAM. If a vulnerability is exploited, it is isolated to the image and just the limited capabilities of that function. The corrupted image is immediately replaced with a clean image, and the attacker is stymied, as the application regains full functionality quickly.

Compared to VM's, distributed containers (and the microservice within), can make network security more complex. With increased API calls from random ports across many servers, traditional layer 3 security devices and techniques are often inadequate for the job.

Application service mesh technologies like AWS app mesh and Istio for Kubernetes can efficiently manage transparent authorization and encryption, and agent based intrusion detection systems can bring monitoring and alerting to ephemeral networks.

As DevOps matures, images running on containers have also matured, ensuring security and compliance. With the depth and breadth of options available within the AWS ecosystems to build, ship and run containers let's dive deeper into the exciting tools available on AWS.



Amazon Elastic Container Registry (ECR) is a Docker container registry designed to store, encrypt, and manage container images enabling quick start up time and global availability. IAM resource based policies ensure compliance. Images are transferred via HTTPS, and are encrypted at rest. ECR is backed by S3 with tight integration into ECS.

Amazon Elastic Container Service (ECS) is the AWS native container orchestration solution to run containerized applications or build microservices. There is no need to install and operate your own container orchestration software.

.**Amazon Elastic Container Service for Kubernetes (EKS)** taps into the power of open sourced container orchestration tool Kubernetes. EKS integrates your Kubernetes control panel into the AWS ecosystem, enabling scalable containerized applications with speed, agility and security at their core.

Amazon Fargate scales and manages the servers required to run your containers. Scale your clusters, or optimize cluster packing with automated infrastructure provisioning enabling developers to focus even more keenly on microservice design and security. For containers AWS Fargate is a strong solution, while serverless solution **Amazon Lambda** excels for serverless execution for simple functions and the compute layer.

Amazon CodeDeploy is an excellent tool to launch a new version of your containerized application. With this blue/ green deployments, a new version can be put into a production test alongside the older version. Once the tests come back positive traffic can be rerouted to new version. If there is an issue your can quickly rollback to previous version.

.

BUILDING SECURE AMIs CHECKLIST

- □ Establish a deployment pipeline.
- □ Create library of reusable, modular images repurposed for different AMIs.
- □ Implement tagging and versioning practice.
- □ Use the same OS as host.
- □ Give AMIs bootstrapping capabilities.
- □ Keep AMIs small.
- □ Use private registry.
- □ Don't embed passwords, private keys or sensitive information in AMIs.
- □ Always test for vulnerabilities with automated security checks.

12 AWS CLOUD SECURITY BEST PRACTICES

With CI/CD, and ephemeral workloads that come along with cloud architectures, the constant code changes dictate more reactive security postures and protocols. With over a decade of development under their belt, AWS's world-class engineers have built tools to deliver an incredibly strong state of security. A state of constant compliance and monitoring is always scanning the ecosystem. By automatically comparing current state to desired state, teams can rest easy knowing that resources are appropriately tagged, secured, and patched. Having the tools and desire is one thing, but having the best practices and know how, is where the security/ compliance rubber meets the road.

1.Enable Cloud Trail and Cloud Watch

By creating and maintaining an auditable log of AWS Management Console actions and API Calls, customers and their security auditors have greater visibility into user and resource activity. Enable Cloud Trail for all regions and ensure that access to log files are restricted based on bucket policies or fine grained IAM policies. Cloud Watch is an ideal tool for monitoring and alerting.

2. Secure Root Account

Disable root API access and server keys. This simple step is sometimes overlooked leaving the Root account open. Foghorn recommends that root user access keys should be deleted, and be replaced by AWS IAM user credentials and keys. Cloud Watch Events can be configured to alert on failed logins.

3. Establish IAM Password Policy and Roles

To minimize surface area for attack; security policies and administrators should be established and individual users assigned specific credentials, tasks and access built upon granular Least Privilege methodologies. Many regulatory bodies require strong passwords. Establishing IAM User Groups makes assigning bulk permissions seamless. As users leave the group or organization it is easy to reassign groups or remove access. Policy generator and simulators are invaluable for creating roles for EC2.

4. Utilize AWS AssumeRole

For cross development teams and 3rd party access to resources outside of the long term access, temporary credentials can be given. IAM users can be granted access from 15 minutes to 12 hours (15 to 60 minutes by default) and gain access by multi-factor authentication access key ID, a secret access key and security token.

5. Enable Multi Factor Authentication (MFA)

[4] Using social engineering hackers have been known to break into a username/ password security system. According to Panda Security, 52% or users, reuse passwords for multiple accounts. Using MFA with tokens has proven to be an effective deterrent. MFA is free for AWS customers, and effective.

6. Rotate Keys Regularly

Changing the locks on the doors every 90 days is strong security practice to prevent costly unwanted access. From APIs to encryption keys, AWS key rotation can be automated and be built to not disrupt your AWS environment. With current key active, a second key is created and supplied to automated process where it is tested, and if passed, the older key is deactivated.

7. Employ Virtual Firewalls

With pattern matching, anomalous activity monitoring, and geolocation blocking AWS WAF is a potent tool to deflect unwanted requests.

8. Mitigate DDoS Attacks

As a belt and suspenders approach to DDoS attacks, and especially for mission critical applications, elastic AWS environments are unsatisfying target for bad actor using DDoS techniques. With AWS Shield, Distributed Denial of Service (DDoS) attacks can be mitigated in subseconds compared to minutes without Shield. Greater fault tolerance can be achieved as spikes in traffic are automatically rerouted to multiple Amazon EC2 instances.

9. Secure S3 Buckets

Secure by default, user error and lack of knowledge can make S3 buckets vulnerable. Misconfigured and readable S3 buckets can expose data to bad actors. Taking the necessary precautions, like assigning bucket policies based on the sensitivity of the data is standard operating procedure. For a large organization, constantly monitoring S3 buckets is a necessity. For certain workloads and accounts, automatic remediation is a good practice.

10. Review Permissions

Employees switch jobs and roles often. For large organizations, Single Sign On integration allows standard employee offboarding procedures to streamline this process. Regular access reviews ensure that users still require the same level of access as previously granted. To test and review IAM policies and permissions in real world scenarios, AWS's IAM Policy Simulator is an excellent tool. A consistent analysis of permissions strengthens access and security of AWS resources, such as Amazon S3 buckets, Amazon SQS queues, Amazon SNS topics, or Amazon S3 Glacier vaults.

11. Disable Regions Not is Use

To prevent servers from being spun up in regions outside of relevance, compliance and to control spend diable regions outside of purview.

12. Encrypt Everything

EC2, Glacier, at rest and in transit. Ensure all data is encrypted, always. AWS is secure by default. With custom configurations, AWS native and 3rd party tools AWS can support and scale your business unleashing team potential, innovation velocity and end user satisfaction. This Swiss Army Knife of tools and configurations can be daunting. AWS Security and DevOps experts like Foghorn offer valuable experience and opinion to help deliver exceptionally secure and compliant AWS environments that support business goals.

[4] https://www.pandasecurity.com/mediacenter/security/password-reuse/

FOGHORN DELIVERS BUSINESS TRANSFORMATIONS ON AWS

Whether you are new to AWS or have an existing AWS environment you are looking to optimize, Foghorn can help. For over 10 years we have delivered outstanding results for clients on AWS. From DevOps in the Cloud to Security in theCloud, Foghorn has the talent, experience and credentials to deliver a velocity of innovation designed to increase performance while optimizing costs

aws partner network

Premier
Consulting Partner

DevOps Competency
Security Competency
Solution Provider

AWS SECURITY COMPETENCY

Foghorn knows cloud security and DevSecOps in the cloud. In 2017 AWS launched a security competency to highlight their partners who satisfy and exceed AWS Cloud security best practices. The framework for this certification covers incident response, logging and monitoring, security, access management and data protection. Foghorn delivers DevSecOps results for customers from HIPPA/HITECH to PCI.

SECURE A CLOUD COMPLIANCE REVIEW WITH FOGHORN

SCHEDULE A CALL

Foghorn Consulting was founded in 2008 with a mission to ensure that cloud computing initiatives deliver maximum value for its customers. Based in the Silicon Valley, Foghorn provides domain expertise in strategy, planning, execution and managed cloud services to high-growth and enterprise companies seeking a cloud partner. Our team of DevOps engineers, SRE's and certified cloud architects bring over 20 years of domain expertise to ensure your cloud initiatives are a success.

FOGHORN

330 Townsend St, Suite 202
San Francisco, CA 94107
foghornconsulting.com
info@foghornconsulting.com
650-963-0980