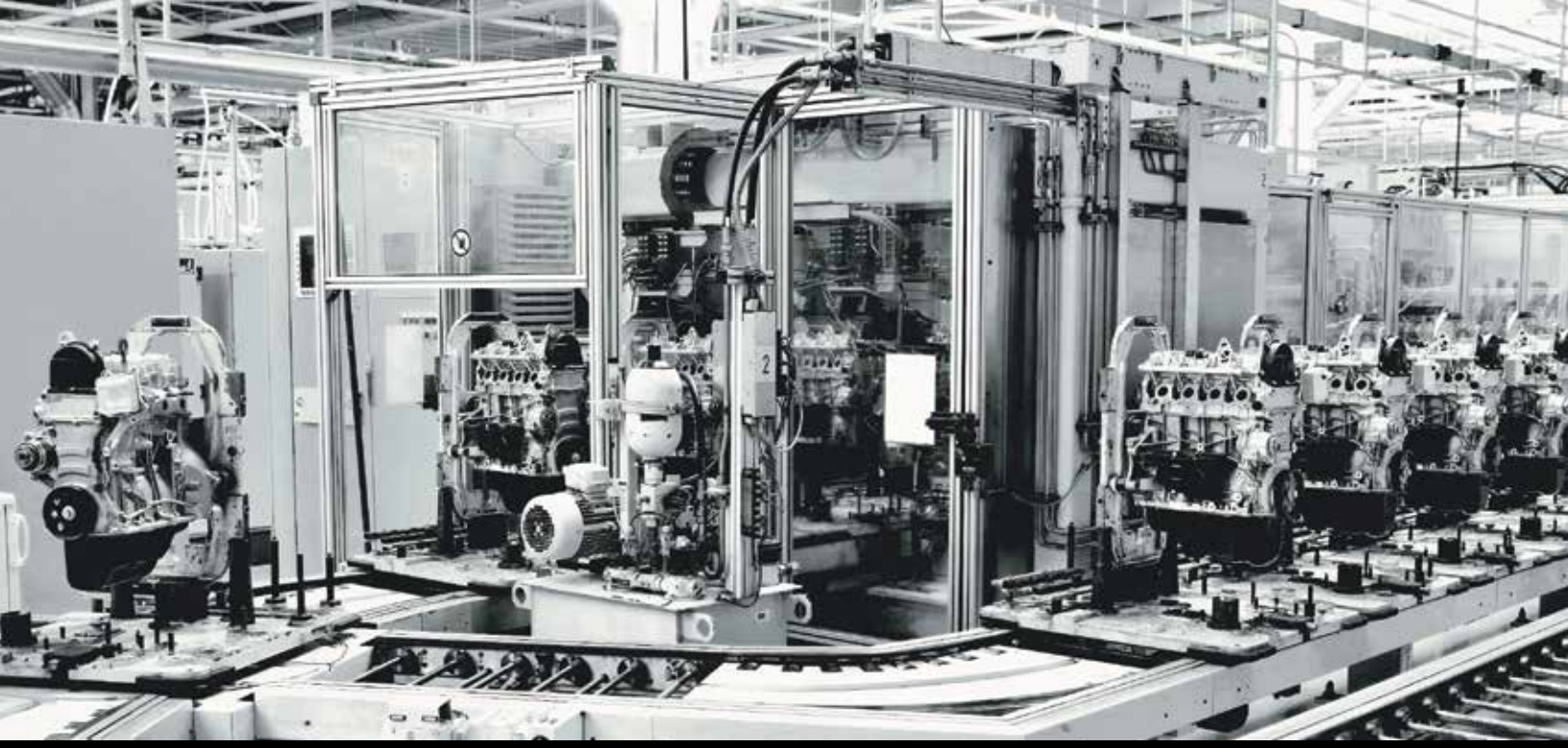


5 Areas to Secure Containers in the Cloud

White Paper | Data Sheet

www.stonedoorgroup.com | +1 800-906-0102 | letsdothis@stonedoorgroup.com

STONE DOOR GROUP

STONE DOOR GROUP

5 Areas to Secure Containers in the Cloud

Darren Hoch, Senior Partner

Mike McDonough, Hybrid Cloud Architect

Published July 2019

ABSTRACT

The implementation of container technology[1] is creating a seismic shift in enterprise architecture, unlike anything the industry has seen in the last 20 years. CIOs are faced with a bewildering array of new technologies and architectures available to digitally transform[2] their enterprises. But with these new technologies also comes new risks and challenges. The modern CIO must maintain development velocity without exposing their organization to security risks and vulnerabilities.

INTRODUCTION

The last disruption and displacement of this magnitude happened around 2000, when enterprises moved away from physical hardware to virtualization as a means to deploy applications. This shift inevitably matured into Infrastructure as a Service (IaaS) as the prevailing methodology to build data centers and the first generation of cloud technologies.

Over the last 10 years, as IaaS matured, CIOs and enterprise architects were able to create their reference architectures, best practices, and most importantly their security and compliance blueprints.

CIOs are now entering a new 6-to-10 year phase where containers are redefining the understanding of IaaS and moving us towards Platform as a Service[3] (PaaS) as the preferred method to deploy applications.

According to research firm Gartner[4], currently, over 360 vendors across 21 market segments are delivering more than 550 PaaS offerings. The latest Gartner forecast estimates that the total PaaS market revenue will reach $20 billion in 2019, and exceed $34 billion in 2022.

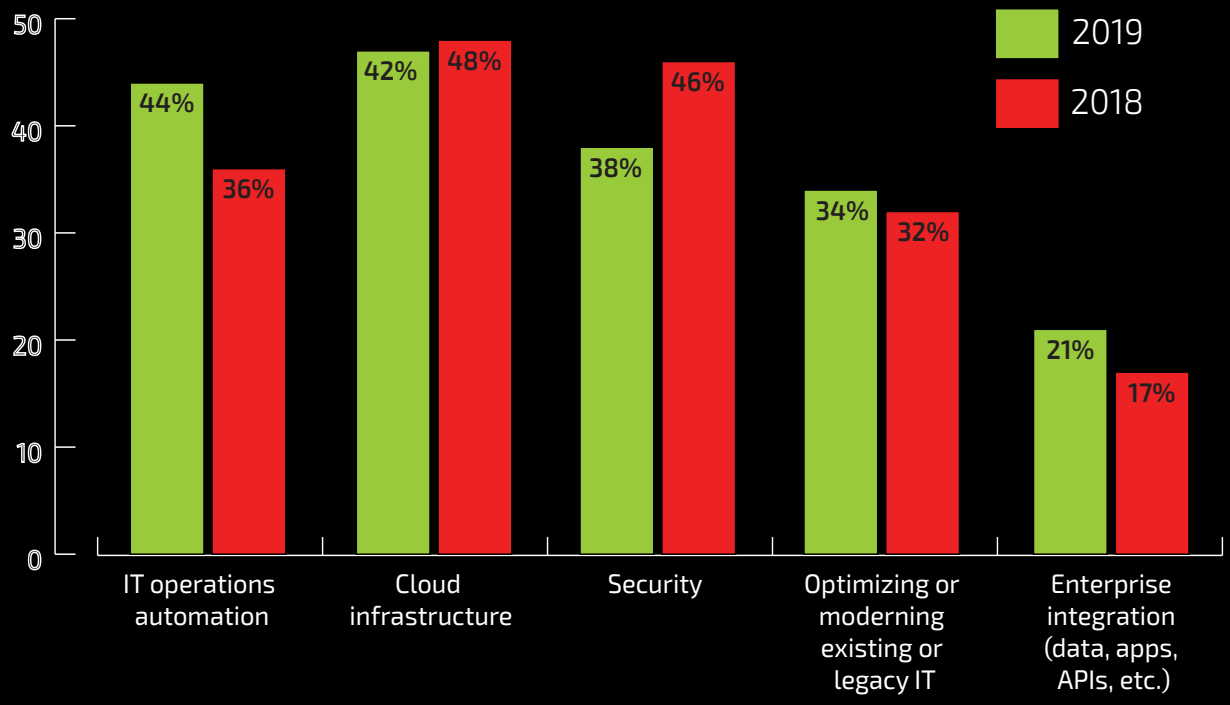
In this shift to cloud[5], database and application platform services represent the largest market segments, with blockchain[6], digital experience, serverless[6] and artificial intelligence/machine learning (AI/ML)[7] platform services as the newest.

BACKGROUND

Both commercial vendors and open source communities are offering versions of popular projects like Docker and Kubernetes as the basis for comprehensive PaaS cloud solutions. Red Hat, IBM, AWS, Microsoft, and Google all offer full suites of container-enabled products for enterprises to develop modern digital-enabled applications.

In addition to container software, a new way to package and deploy applications has emerged, known as DevOps. Software development teams are quickly migrating away from monolithic software architectures, waterfall development models, and legacy development models. Instead they are adopting microservice-based architectures[8], agile development models and using tools like Ansible, Terraform, Jenkins and Git to build sophisticated CI/CD development pipelines.

TOP 3 FUNDING PRIORITIES FOR 2019: AUTOMATION, CLOUD, AND SECURITY



Source: RedHat Global Customer Tech Outlook 2019: Automation, Cloud & Security Leading Funding Priorities, Red Hat, Dec 2018

This new approach to software development has accelerated the velocity of application feature release to levels unimaginable 20 years ago. Developers, in some cases, are releasing features hourly instead of daily, quarterly or yearly[9]. It has fundamentally changed the way CIOs think about infrastructure[10]. An article published in *IT Business Edge* cites a recent Forrester report which states that 60% of CIOs believe DevOps have already been implemented in their organizations and are expanding.

Much ground has been covered over the last 2 years on container and orchestration technology, what it is, why it's important, and how to use it. Containers have been in existence for almost 20 years, first popularized by Sun Microsystems Solaris Zones.

What is not often discussed is a comprehensive guide to container security. The following are the critical container security areas a CIO needs to focus on when deploying container technology in the enterprise.

THE SECURITY CHALLENGE

The evolution of IaaS allowed ample time for CIOs to develop the required blueprints for reference architecture and compliance. The evolution of PaaS is happening at an exponential pace relative to IaaS. This is forcing CIOs to have to accelerate how they bring cloud technology to their customers in a way that satisfies the need for digital velocity and also meets the needs for corporate governance and regulatory compliance.

A key concern for Chief Information Security Officers is the lack of existing security blueprints for containers. According to an article published by ZDNet, 94%[11] of IT security pros worry about container security with 60% having had container security incidents in the past year.

For highly regulated industries like financial services and healthcare, there are multiple interesting greenfield applications running on containers that can't be promoted to production out of a lack of security reference architectures. This creates a frustrating backlog for CIOs as they have invested in implementing DevOps principles and training their employees on modern technologies, only to have important digital transformation initiatives stalled by regulatory compliance.

The Solution - A Comprehensive Approach

Securing containers is not as difficult as it may seem. Modern container technology has the advantage of integrating 20 years of information security experience. Contributors to upstream container projects develop new features through a security lens. Combined with DevOps, and 12 Factor App Development[12], modern microservice cloud applications are developed in a much more secure and scalable way than their monolithic predecessors.

As with all information technology security, securing containers[13] comes down to having the right set of skills to plan and configure enterprise environments.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Most modern high profile data security breaches happen due to lax identity and access management controls. Long gone are the days of simple Microsoft Active Directory and UNIX password management in typical enterprises. In addition to the provisioning of standard user and system accounts, administrators now have to provision accounts at the cloud and application level. Previously, something simple like an Apache web server would require a standard privileged account to run. Now, individual APIs within applications can have their own permission set. Modern IAM systems[14] such as AWS Identity and Access Management (IAM) and Microsoft Azure Active Directory (Azure AD) offer more granular role-based access controls (RBAC), allowing accounts to have specific permissions over a subset of calls.

While the intent of granular IAM is to ensure a very fine level of control over security, most IT organizations simply don't have the skills, training or process to effectively implement them.

The good news is that CIOs can mitigate the risks from weak IAM controls fairly quickly. The first is to implement quarterly user access reviews. For any CIO that deals with regulatory compliance, this is not a new idea and the solution is rather simple. Once a quarter, print off all accounts for a given system, for example Amazon Web Service, and conduct an account review of all accounts. The scope of the review will need to be broadened beyond user and system account review to also include application accounts. In addition to reviewing traditional account/passwords, also broaden the review to encompass the allocation of authorization keys to applications.

Another facet of IAM to consider is cost. In fact, a *RightScale 2019 State of The Cloud Report by Data Center Knowledge*[15] finds that 43% of organizations do not have automated or manual policies to use the lowest-cost cloud service. Another 38% have not developed policies to use their cloud providers' lowest-cost regions. About 29% do not have automated or manual policies to shut down workloads after hours, 27% do not have policies to eliminate inactive storage, and 20% do not have policies to right-size their instances.

The end result is that IT organizations create simplified and often too liberal sets of permissions that inadvertently expose access to sensitive data, something either outside malicious attackers or rouge employees may eventually exploit.

SECURING OUTSIDE CONTAINER CONTENT

One of the reasons why containers have been widely adopted by developers is portability[16]. The portability of containers has led to the creation and sharing of microservices. A microservice[17] consists of a stripped out application function fully capable of running on its own and in conjunction via APIs with other microservices. Containers[18] allow developers to create all kinds of microservice-based applications and then share them. Sharing software and running software content via containers has been one of the key driving forces in developer productivity and capacity to deliver more high quality features to users faster.

Public repositories like DockerHub and GitHub offer unrestricted access to microservices and other software content that allow developers to download and access quickly. As any CIO could imagine, unrestricted access to public software repositories has always been a serious issue. With the proliferation of containers, access to available, compiled software content has never been more easily available.

Trusted container registries offer CIOs the capacity to regulate the origin of container based software content. Tools like Google Trusted Registry[19], Red Hat Quay[20], and Docker Enterprise Edition[21] offer private container registries for software developers. These trusted registries offer the capacity to limit where developers find their content, digitally sign the images they use, and scan images for vulnerabilities.

BUILDING SECURE CONTAINER CONTENT

In addition to getting access to existing container content, developers will inevitably build applications around the containers they download. A container will be the deployment method of their application code. Along with a set of microservice-based containers they download, the developer's final application may consist of a combination of containers they built and containers they acquired.

A trusted container registry will scan existing containers and may also scan some of the software libraries a developer used to compile code against common vulnerability databases. However, what about the actual code the developer wrote? How does the CIO ensure that the actual application code is free from security vulnerabilities. If that code is then packaged and widely distributed across the enterprise, then the vulnerability risk becomes exponential.

One of the features of Docker[22]-based container images is that they are immutable[23]. Once a developer creates a container image, that image can't be edited. Any modification to the container image results in a new container image. Therefore, once code has been built and put into a container, it is impossible for nefarious attackers to embed or hide code in that image.

In addition to immutability, there are multiple tools like IBM AppScan and Micro Focus Fortify Static Code Analyzer that conduct code security scanning along with real-time scanning tools like Black Duck and JFrog XRay. These tools should all be integrated into a robust CI/CD pipeline as part of the development process. By integrating one or many automated vulnerability checks during the automated build of a container image, the CIO can ensure that the code developers are writing enters into production having gone through multiple security checks.

The last consideration around building secure container content[24] involves implementing controls around the content development process[25]. While microservices breaks down applications into smaller increments, it does not negate the fact that containers still need a base OS, middleware components, and development libraries. This is an area where the CIO can borrow from existing policies around virtual machine provisioning. Similar to VM governance, the CIO can split up container provisioning along familiar lines. The systems group controls the base container OS images, architects pick the supported middleware/runtimes/databases, and developers develop their code within these standards.

SECURING CONTAINER RUNTIMES

Once the CIO has secured both external and internal content, the next consideration revolves around which containers are allowed to run and when. If the developer team has adopted microservices fully and is developing with velocity, there will inevitably be an order of magnitude number of containers and versions available. Given the highly automated nature[26] of pulling applications and features through a mature CI/CD pipeline, there are multiple risks that the wrong container versions may find their way into the runtime environment. In addition, while there may be containers that have been approved and scanned for vulnerabilities, they may not be authorized to run in a production environment.

All modern hybrid and public cloud tools offer container runtime authorization tools. These tools are designed specifically to ensure that only the authorized container images are allowed to make it to both runtime and production environments. Red Hat OpenShift[27] (using a derivative of Kubernetes) offers their Image Policy and Admission Plugin and Security Context Constraints (SCC) while native Kubernetes offers their Admission Controllers[28] interface. These tools ensure that only the authorized containers are allowed to execute within the runtime environment.

SECURING THE ORCHESTRATION ENVIRONMENT

The final step the CIO must take in securing containers is the orchestration environment[29]. Securing this environment ensures that the actual code in the applications runs at the right level of privilege. It is possible at this point in the security chain to make it this far with securing content only to have the actual applications run with either elevated permissions or too liberal of permissions. This creates a security condition that has been around for the last 40 years, allowing a nefarious attacker to compromise a system and gain escalated privileges to internal resources.

More than likely, developers are using either native Kubernetes or a derivative of it from one of the major providers, like Azure Kubernetes Service or Google Kubernetes Service. Kubernetes has offered very robust Role Based Access (RBAC) controls since version 1.8, released in 2017. These controls are different than the previous

IAM controls we discussed. Kubernetes executes Pods. A pod is nothing more than one or many containers in a specific configuration. Kubernetes RBAC[30] enables administrators to set permissions at the pod level, locking down what the actual resources (network, disk, etc) the pod does or does not have access to. In addition to RBAC on the pods, there are additional authentication tools like LDAP, OAuth and X.509 certificates that can be integrated into the Kubernetes execution environment, adding another level of control on which accounts, either system or user, can actually execute pods. These two main sets of features allow the CIO to control both who can execute pods and what access those pods have to resources.

SECURING EVERYTHING ELSE

The CIO may wonder how container security[31] fits into an already existing corporate security infrastructure consisting of intrusion detection and prevention, vulnerability scanning, host intrusion, and SIEM. The answer is quite simple, container security is layered on top of these existing services. Traditional corporate information security really doesn't change much, either in the cloud or on premises when it comes to integrating container security. Container security becomes a subset of information security[32], adding to an existing defense in depth strategy.

> CONTAINER NETWORK

The Kubernetes container orchestration platform relies on a software defined network (SDN) for container to container network traffic. Microservices-based applications significantly increase East-West network traffic, which is carried across this SDN. When combined with the ephemeral nature of containers, managing and monitoring container-to-container network traffic can be a challenge.

Container network specific tools and design patterns are evolving. The Kubernetes SDN utilizes a plugin architecture, allowing different SDN technologies to be implemented easily. The default, bundled SDN plugins cover a number of typical deployment scenarios. Additional SDN capabilities are available via 3rd party SDN plugins, including commercial and open source options.

Inspection of container-to-container network traffic can be performed today using specialized products from companies like NeuVector[33]. Nuage Networks[34] and Tigera[35] offer SDN plugins which add features such as policy based networking, real-time SDN visibility, and security monitoring to container networking.

Enterprises running VMWare NSX-T in their environment can use the Kubernetes NSX-T SDN plugin[36] to enable Kubernetes to leverage NSX-T for the container network, enabling containers to work with existing virtual machine centric network security processes.

> IDS/IPS

The existing edge intrusion detection (IDS) and prevention systems (IPS) stay in place. More than likely, the datacenter systems are all utilizing an SDN and on a converged backplane. In this case, container applications can be treated much like non-containerized applications from a high-level network security perspective.

Traditional IDS/IPS tools may not be able to effectively monitor network traffic between containers as it travels across the container SDN. However, existing IDS/IPS tools can be used to monitor North-South network traffic as it enters/leaves the Kubernetes cluster.

> NETWORK VULNERABILITY SCANNING

Applications running on containers represent as any other port bound service on a network. For example, an inbound Nginx server hosting a web API still runs on port 80 or port 443 like any other application.

> HOST VULNERABILITY SCANNING

Containers run as a standard Linux/Windows based process on the host system. All host intrusion processes in place run as expected. Layering on the container image scanning techniques described in this paper complete the host based intrusion detection process.

CONCLUSION

Securing container infrastructure in the enterprise is not difficult. Even though industry blueprints and best practices have not fully emerged, CIOs can still implement a robust container security strategy. Container infrastructure for the cloud was built from the ground up with security in mind. All enterprise cloud providers[37] offer robust security tools to secure containers on their platforms. Third-party software vendors provide additional components to complete a comprehensive container security strategy.

As with everything in enterprise IT, securing containers will take a comprehensive and intentional approach by the CIO, including discovery, planning, investing in the right skills for an effective implementation, and putting the proper measures and policies in place to satisfy all regulatory requirements. When done correctly, the CIO can maintain the development velocity that containers, DevOps, and CI/CD bring to the digital enterprise, without further exposing their organization to security risks and vulnerabilities.

ABOUT THE AUTHORS

Darren Hoch | Senior Partner, Stone Door Group

Mr. Hoch is a founding partner of Stone Door Group and manages the Cloud and DevOps consulting practice. He has been helping enterprise customers for over 20 years solve very large IT problems. Over the last 3 years, he has led multiple Fortune 500 customers through their DevOps journey and transformation to the digital enterprise.

Mike McDonough | Hybrid Cloud Architect, Stone Door Group

Mr. McDonough consults with enterprise IT organizations on advanced infrastructure and information security topics with a focus on cloud technology and emerging technology. He has helped businesses across a wide range of industries, including alternative energy, finance, retail, and travel, successfully implement Red Hat's OpenShift container application platform.

ABOUT STONE DOOR GROUP

SDG is a certified solutions integrator that bridges the implementation gap between the world's leading technology providers and enterprises needing to transform their applications, infrastructure, and people to DevOps best practices. Stone Door provides a fully-integrated managed service, including consulting, license reselling, cloud hosting, and training. Online at www.stonedoorgroup.com.

REFERENCES

1. *5 Business Cases For Containers*, Information Week, January 19, 2017; https://www.informationweek.com/cloud/5-business-cases-for-containers/a/d-id/1327931
2. *5 Infrastructure Trends To Watch Out For In 2019*, Forbes.com, December 20, 2018; https://www.forbes.com/sites/janakirammsv/2018/12/20/5-modern-infrastructure-trends-to-watch-out-for-in-2019/#67ea488817db
3. *Gartner Says Nearly 50 Percent of PaaS Offerings Are Now Cloud-Only*, Gartner.com, February 27, 2019; https://www.gartner.com/en/newsroom/press-releases/2019-02-27-gartner-says-nearly-50-percent-of-paas-offerings-are-
4. *Cloud Shifts Impact All IT Markets*, Gartner.com, January 29, 2019; https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets/
5. *Gartner Identifies The Top 10 Strategic Technology Trends For 2019*, Gartner.com, October 15, 2018; https://www.gartner.com/en/newsroom/press-releases/2018-10-15-gartner-identifies-the-top-10-strategic-technology-trends-for-2019
6. *Gartner Identifies The Top 10 Trends Impacting Infrastructure*, Gartner.com, December 4, 2018; https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras
7. *Gartner Identifies Five Emerging Technology Trends That Will Blur The Lines Between Human and Machines*, Gartner.com, August 20, 2018; https://www.gartner.com/en/newsroom/press-releases/2018-08-20-gartner-identifies-five-emerging-technology-trends-that-will-blur-the-lines-between-human-and-machine
8. *Top 3 Considerations When Refactoring Monolithic Applications To Microservices*, Stone Door Group, May 24, 2019; http://www.stonedoorgroup.com/blogs/2019/5/24/top-3-considerations-when-refactoring-monolithic-applications-to-microservices
9. *How DevOps Tools Accelerate Software Delivery*, infoworld.com, August 24, 2017; https://www.infoworld.com/article/3219305/how-devops-tools-accelerate-software-delivery.html
10. *How DevOps Affects The CIO*, IT Business Edge, February 7, 2018; https://www.itbusinessedge.com/blogs/infrastructure/how-devops-affects-the-cio.html
11. *Survey Reveals Growing Concern About Container Technology Security*, Zdnet.com, January 4, 2019; https://www.zdnet.com/article/time-to-tighten-up-container-security/
12. *The 12 Factor App*, 12factor.net, https://12factor.net/
13. *Why Securing Containers And Microservices Is A Challenge*, csoonline.com, May 3, 2018; https://www.csoonline.com/article/3268922/why-securing-containers-and-microservices-is-a-challenge.html
14. *Identity And Access Management*, Search Security, Techtarget.com, https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system
15. *Survey: Most Companies Are Failing At Cloud Cost Management*, Data Center Knowledge, February 28, 2019; https://www.datacenterknowledge.com/cloud/survey-most-companies-are-failing-cloud-cost-management
16. *What Does Container Portability Really Mean?* Infoworld.com, September 11, 2017; https://www.infoworld.com/article/3223073/what-does-container-portability-really-mean.html
17. *What Are Microservices?* Opensource.com, https://opensource.com/resources/what-are-microservices
18. *What Are Containers And Why Do You Need Them?* IBM, January 31, 2019; https://developer.ibm.com/blogs/what-are-containers-and-why-do-you-need-them/
19. *Container Registry*, cloud.google.com, https://cloud.google.com/container-registry/
20. *Red Hat Quay*, Red Hat OpenShift, https://www.openshift.com/products/quay
21. *Using Your Own Private Registry With Docker Enterprise Edition*, January 10, 2018; https://blog.docker.com/2018/01/dtr/
22. *What Is Docker? Docker Containers Explained*, Infoworld.com, April 19, 2019; https://www.infoworld.com/article/3204171/what-is-docker-docker-containers-explained.html
23. *The Forrester Wave Enterprise Container Software Suites Q4, 2018*, Docker.com, https://www.docker.com/resources/report/the-forrester-wave-enterprise-container-platform-software-suites-2018
24. *7 Best Practices Securing Enterprise Container Environments*, Techbeacon.com, https://techbeacon.com/enterprise-it/7-best-practices-securing-enterprise-container-environments
25. *Ten Layers of Container Security*, Red Hat, https://www.redhat.com/en/resources/container-security-openshift-cloud-devops-whitepaper
26. *What is CI/CD? Continuous Integration And Continuous Delivery Explained*, Infoworld.com, May, 10, 2018; https://www.infoworld.com/article/3271126/what-is-cicd-continuous-integration-and-continuous-delivery-explained.html
27. *OpenShift Container Platform 3.9, Red Hat OpenShift*, https://docs.openshift.com/container-platform/3.9/admin_guide/image_policy.html
28. *Using Admission Controllers, Kubernetes Reference*, https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/
29. *Automation Orchestration And Response Evolution Incident Management*, Enterprise CIO, June 20, 2018; https://www.enterprise-cio.com/news/2018/jun/20/automation-orchestration-and-response-evolution-incident-management/
30. *Using RBAC Authorization, Kubernetes* Reference, https://kubernetes.io/docs/reference/access-authn-authz/rbac/
31. *What Is Container Security?* Red Hat, https://www.redhat.com/en/topics/security/container-security
32. *6 Best Practices For Creating A Container Platform Strategy*, Gartner.com, April 23, 2019; https://www.gartner.com/smarterwithgartner/6-best-practices-for-creating-a-container-platform-strategy/
33. NeuVector, https://www.neuvector.com
34. Nuage Networks, https://www.nuagenetworks.net
35. Tigera, https://www.tigera.io
36. *Cluster Networking*, Kubernetes Concepts, https://kubernetes.io/docs/concepts/cluster-administration/networking/
37. *Cloud Providers Step Up Security Tools. Are They Up To The Job?* Techbeacon.com, March 28, 2019; https://techbeacon.com/enterprise-it/cloud-providers-step-security-tools-are-they-job

DATA SHEET

Container Security Optimization Accelerator℠

Increase application delivery. Securely.

STONE DOOR GROUP

ENGAGEMENT OVERVIEW

The purpose of this engagement is to perform an audit, gap analysis, and remediation of your current container implementation. Stone Door Group conducts a discovery of your cloud, DevOps, and container strategy, along with required regulatory controls. Our consultant then performs a gap analysis on the current container, orchestration, automation, and CI/CD configurations. You will be provided a gap analysis report (GAR) and container security blueprint (CSB) that identifies the gaps in container security and the required remediations. Finally, the consultant will work with your designated teams to implement the controls defined in the CSB and train teams on container security best practices.

KEY BENEFITS

- ✓ Identify previously unknown container security vulnerabilities due to lack of container controls
- ✓ Understand the key areas of container security
- ✓ Develop an integrated defense strategy for containers
- ✓ Integrate container security policies into existing infrastructure security policies
- ✓ Enable IT and developer teams to design applications and infrastructure with container security in mind

The following section describes the specific phases of the Cloud Container Security Optimization Assessment. Each phase builds on the previous phase, increasing the capability of the overall solution.

Phase 1 > Discovery

The goal of the discovery phase is to evaluate the existing customer cloud infrastructure for the purpose of creating a cost analysis report.

TASKS

- ▫ Review Regulatory and Compliance Requirements
- ▫ Review Container and DevOps strategies
- ▫ Review cloud IAM users and roles
  - Determine system vs user accounts
  - Identify job roles needing cloud resources
  - Determine if IAM permissions match job role requirements
- ▫ Review Application Workloads
  - Number of and purpose for applications
  - Required data access
  - Application requirements for Dev, QA, and Prod environments
- ▫ Review Application Lifecycle
  - Acquiring existing container content from public sources
  - Secure registries for content storage and trustof public image content

WHAT FEATURES ARE INCLUDED?

Review current container strategy and regulatory requirements	Review container infrastructure configuration settings in key areas	Identify, prioritize, and assess risk of gaps in container configuration	Deliver gap analysis report (GAR) and container security blueprint (CSB) to key stakeholders	Guide IT teams through required configuration changes to implement CSB	Provide extensive security training

Container Security Optimization Accelerator℠

STONE DOOR GROUP

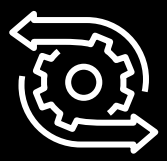
- Vulnerability scanning of content sources
- Practices for creating net new container content
- Runtime authorization of container content
- Access controls to data sources by users and container images

OUTPUTS

- Container Gap Analysis Report (CGAR): a 10 – 15 report that describes the current state of cloud consumption
- Review CGAR report with key executive stakeholders

Phase 2 > Analysis

The goal of the analysis phase is to synthesize the CGAR report into a Container Security Blueprint (CSB):



TASKS

- Synthesize data into an executable Container Security Blueprint (CSB)
- Generate container security blueprint for customer to implement:
  - Configuration of Identity and Access Management
  - Configuration Trusted Registries for container images
  - Implementation of container vulnerability scanning
  - Best practices for developing new container content
  - Configuration of secure container and orchestration runtime environments
  - Implementation of least privilege access to data from container based applications

OUTPUTS

- Container Security Blueprint: a 10 – 15 page report that describes the prescriptive actions required on the cloud platform to meet the Cost Reduction Goal.
- Container Security Blueprint Executive Deck: a 5 – 7 slide deck providing the executive highlights of the Cost Reduction Plan

Phase 3 > Review

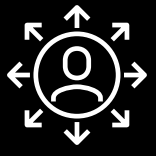
The goal of the Review Phase is to review the Container Security Blueprint (CSB) with key executive stakeholders and discuss possible implementation of recommendations within the CSB to achieve the required corporate and regulatory compliance.

TASKS

- Conduct executive stakeholder review of Container Security Blueprint
- Review implementation options for the Container Security Blueprint
- Answer questions and ideate with executive stakeholders on future container implementation goals and how they interface with the Container Security Blueprint

OUTPUTS

- Meeting notes detailing executive stakeholder next steps



OUTCOMES

- ✓ Bring container infrastructure into corporate and regulatory compliance
- ✓ Accelerate application and feature delivery through a secure container infrastructure
- ✓ Obtain full container and infrastructure security accountability

QUESTIONS?

Give us all call at 1-800-906-0102 or email us at letsdothis@stonedoorgroup.com.

STONE DOOR GROUP

www.stonedoorgroup.com

Ansible CI/CD Helm

Python microservices

DevOps Kubernetes

Git Containers

Linux Docker

Jenkins