Emerging risks in the public cloud platforms

How can organizations protect themselves?

Karthikeyan Vaidyalingam

- Head of Cloud Security at MetLife
- CISSP, CCSP, CCSK
- Bachelor’s degree in Electronics and Communication Engineering

- Over 18 years of experience leading global Information and Cyber security teams in various organizations.
- Rolled out multiple security initiatives for Fortune 50 and 100 companies, including Cloud Security, Identity, Access Governance, Privileged Access Management, etc.
- Bachelor's degree in Electronics and Communication Engineering from Anna University in India.
- Class of ‘24 Executive MBA from the University of North Carolina at Chapel Hill.
- Member of the advisory board for several security companies focusing on Managed Detection and Response and Cloud security.

Agenda

- Shared responsibility model and why it matters
- Emerging Risks in public cloud platforms
  - State of Cloud Security in 2023
  - State of the container security in 2023
  - The advent and the rise of SaaS attacks.
  - Software supply chain attacks observed in the last year
- Why containerized platforms in the cloud are hard to protect
- Best practices to protect containerized platforms in the public cloud.
- Best practices to secure public cloud platforms.
- Q&A and Discussion

Shared Responsibility Model and why that matters when talking about Public Cloud

Responsibility	On Premise	Infrastructure as a Service (Virtual Machines)	Containers as a Service (ECS, ACI, GCS)	Platform as a Service (Storage account, Key Vault)	Functions as a Service (Python Function, Lambda)	Software as a Service (Salesforce, O365)
Data (SSN, CCN, PHI, PII)	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Identity Management (User , Function)	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Access Management (Read Only, Admin)	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Functional Logic	Tenant	Tenant	Tenant	Tenant	Tenant	Cloud Service Provider
Runtime	Tenant	Tenant	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Middleware	Tenant	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Operating System	Tenant	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Virtualization	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Load Balancing	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Networking	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Hardware	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Physical Security	Tenant	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider

Cloud security is a key concern for Organizations migrating to public cloud platforms

46%

Object misconfiguration due to human error

27%

Over provisioned access resulting in compromise

21%

Insecure data transit resulting in data loss/leakage

23%

Unmitigated vulnerabilities in compute

47%

Lack of skilled resources to manage cloud security

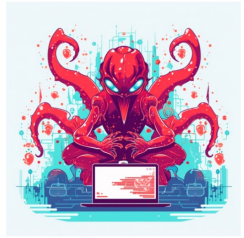
27%

Too many APIs to protect

Attacks on SaaS platforms are getting sophisticated too!

SECURITY ADVISORIES | 5 MINUTES

SaaS Ransomware Observed in the Wild for Sharepoint in Microsoft 365



Background

SECURITY GUIDANCE | 6 MINUTES

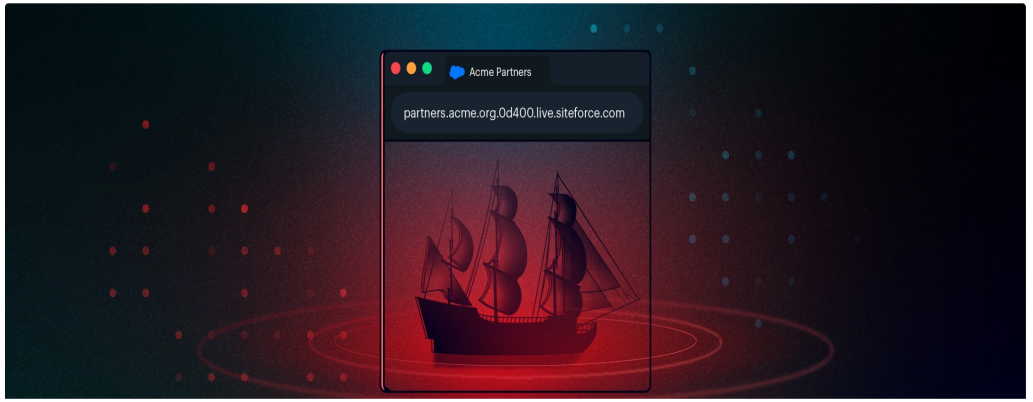
Pure Storage on Launching a Corporate SaaS Security Program

VARONIS Platform Integrations Why Varonis? Company Partners Resources Contact us

Ghost Sites: Stealing Data From Deactivated Salesforce Communities

Varonis Threat Labs discovered that improperly deactivated Salesforce "ghost sites" remain accessible and vulnerable to risk.

Nitay Bachrach | 2 min read | Last updated May 31, 2023



https://www.darkreading.com/cloud/researchers-report-first-instance-of-automated-saas-ransomware-extortion

https://www.varonis.com/blog/salesforce-ghost-sites

Container security is a key concern for Cloud native applications

53%

Detected a misconfiguration in Kubernetes in last 12 months

57%

Worry the most about securing workloads at runtime

51%

Require developers to use validated images

78%

Have a DevSecOps initiative in either beginning or advanced stages

43%

Consider "DevOps" as the role most responsible for Kubernetes security

55%

Delayed or slowed down application deployment due to security concern

https://www.redhat.com/rhdc/managed-files/cl-state-of-kubernetes-security-report-2022-ebook-f31209-202205-en.pdf

Software supply chain attacks are on the rise compounding the damage to cloud-native platforms

Malicious Software Supply Chain Attacks Increase Another 633% YoY

- Typosquatting
- Cousin brandjacking
- Dependency Confusion
- Malicious code injections

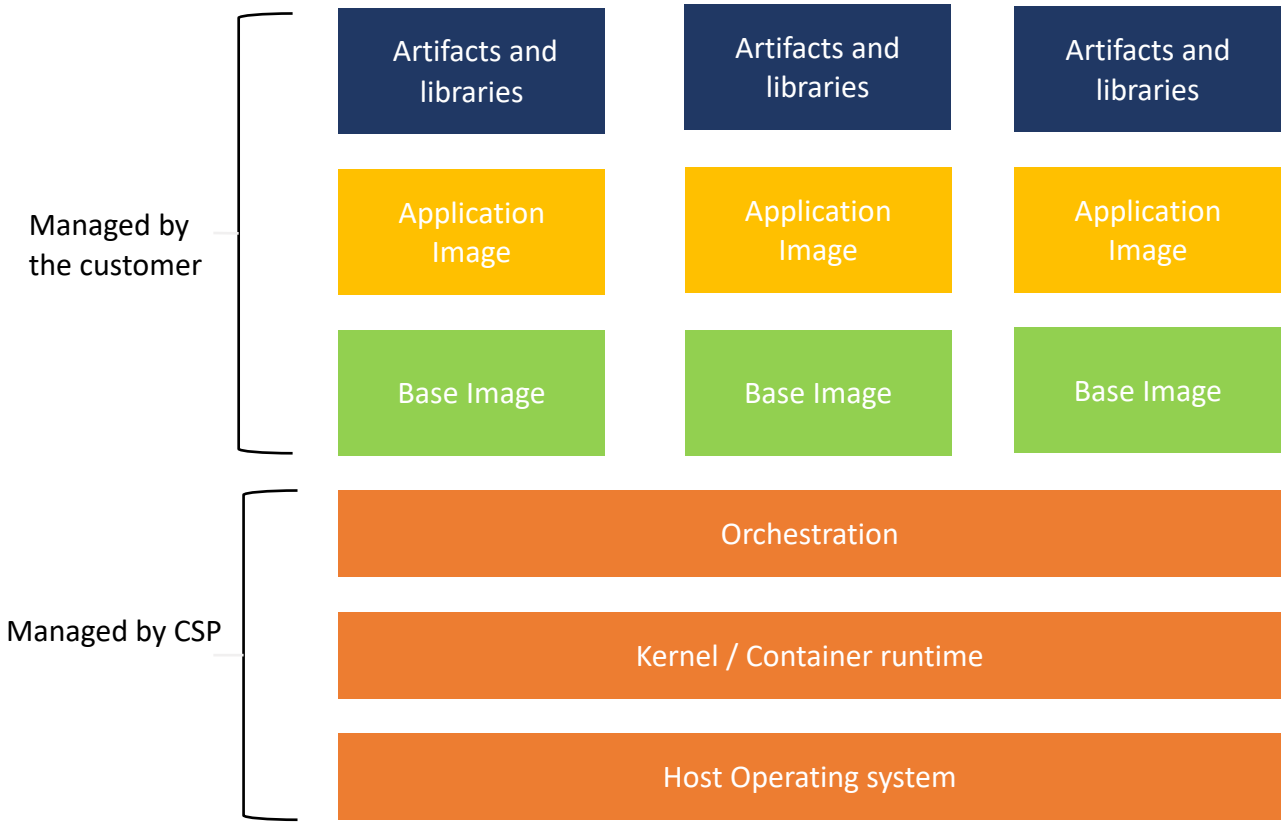
FIG 1.7. HIGHEST PROFILE VULNERABILITIES AND ATTACKS, 2021–22

https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security

Vulnerability management in containerized platforms involves remediation at multiple layers

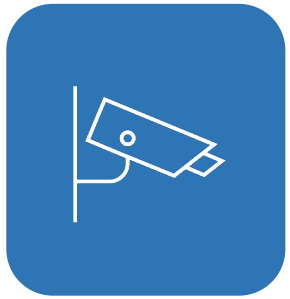
What should we do differently:

- Scan container platforms during runtime and registries during the build phase.
- Define a clear Image management and attestation strategy for Infrastructure and Application development teams to follow.
- Construct effective Software Bill Of Materials (SBOM) at the build cycle to establish visibility into an application.



Key pillars for Container security to protect the entire stack and the lifecycle

Real time threat detection



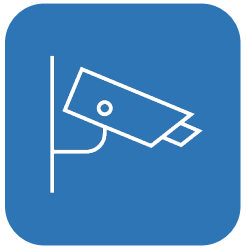
Continuous visibility for compliance

Advanced traceability through logging at multiple levels

Build and runtime integration

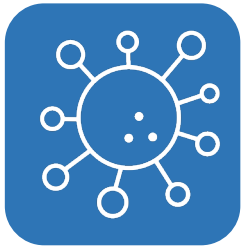
Continuous audit and compliance

Best practices to secure public cloud platforms

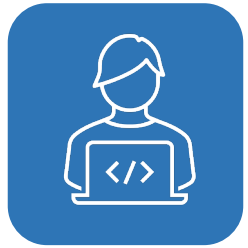


Maintain security posture

Secure privileged access

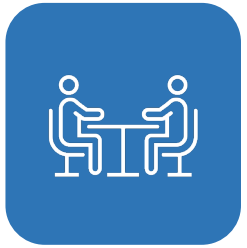


Real-time threat detection



Enforce shift left controls

Secure cloud workloads



Cloud service lifecycle management

Secure data hosted in the cloud

Monitor SaaS applications

Questions?