CONTAINER SECURITY REFERENCE ARCHITECTURE

MELBOURNE MEETUP
OPENSHIFT

29-05-2019

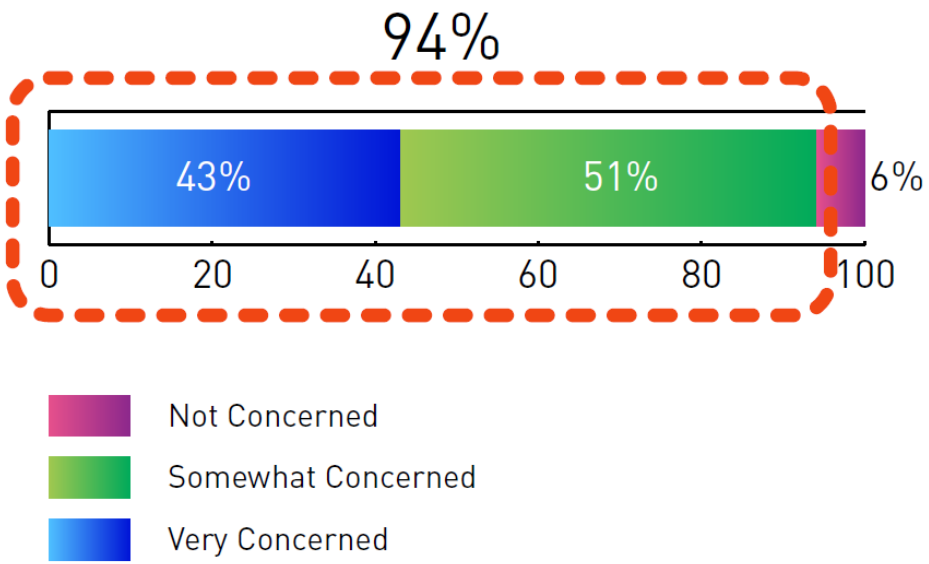
Andreas.Kafka@accenture.com
04 1894 4306

accenturesecurity

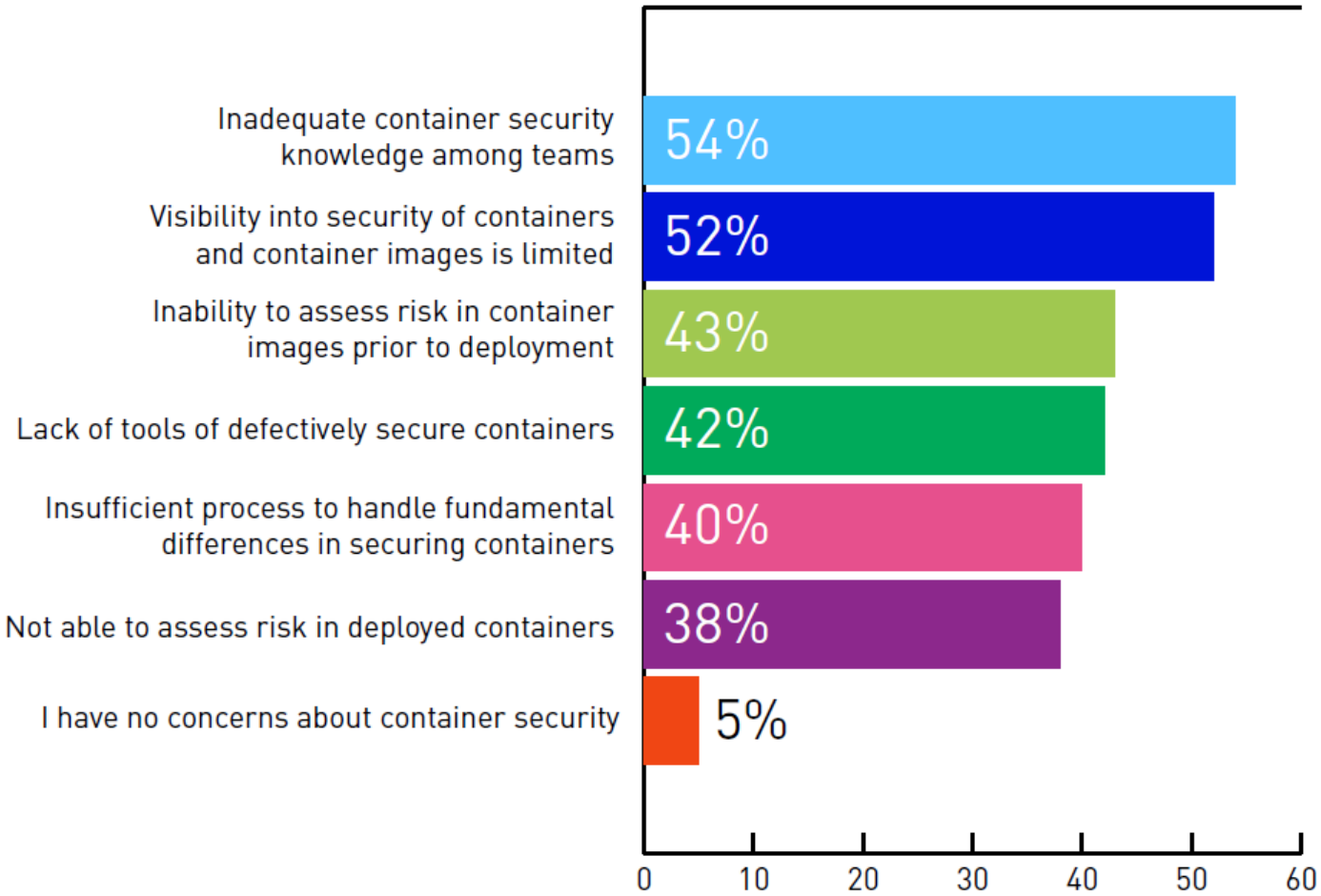
WHY IS CONTAINER SECURITY IMPORTANT?

- IT Systems are **constantly exposed to security threats and risks**. It is the mission of IT Security professionals to create, maintain and monitor security processes and controls to prevent loss of data, and revenue due to security breaches and business reputation.
- All IT systems must have in place a **complete set of security controls and processes to minimize and mitigate risks**. Containers, as another component of the IT ecosystem, also have risks and threats that need to be mitigated and prevented. Even thought containers provide many security features out of the box, there are still well known container architecture specific risks that need to be mitigated and protected from.
- Serious security threats like **kernel exploits, vulnerable library exploits, cross-host containers attacks, compromised secrets, and vulnerable application exploits are threats that apply specifically to containers** and which are not necessarily or clearly addressed by the typical IT infrastructure and application controls, security processes and tools.

94% are concerned about container security



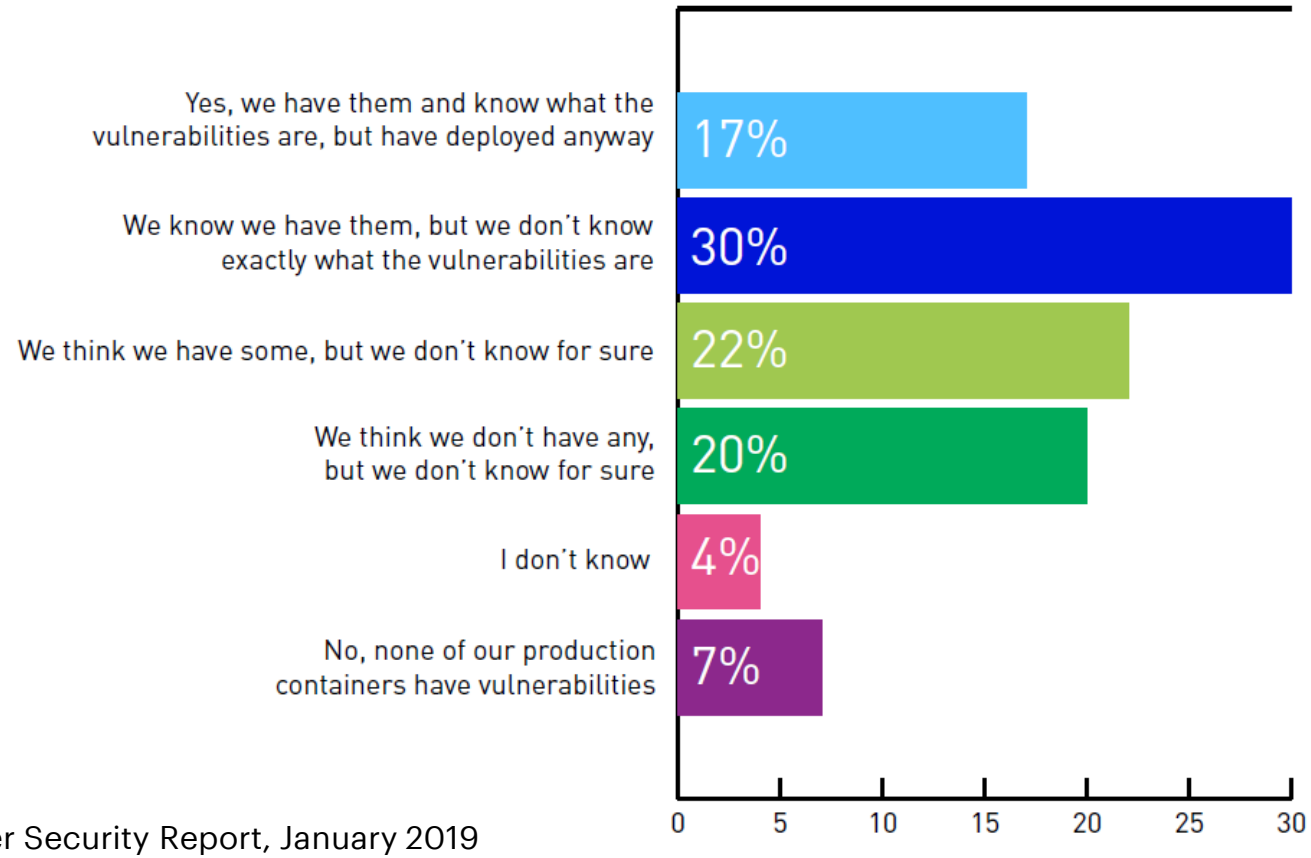
What specific security concerns do you have about containers?



Source: Tripwire State of Container Security Report, January 2019

47% have vulnerable containers in production and 46% don't know if they do

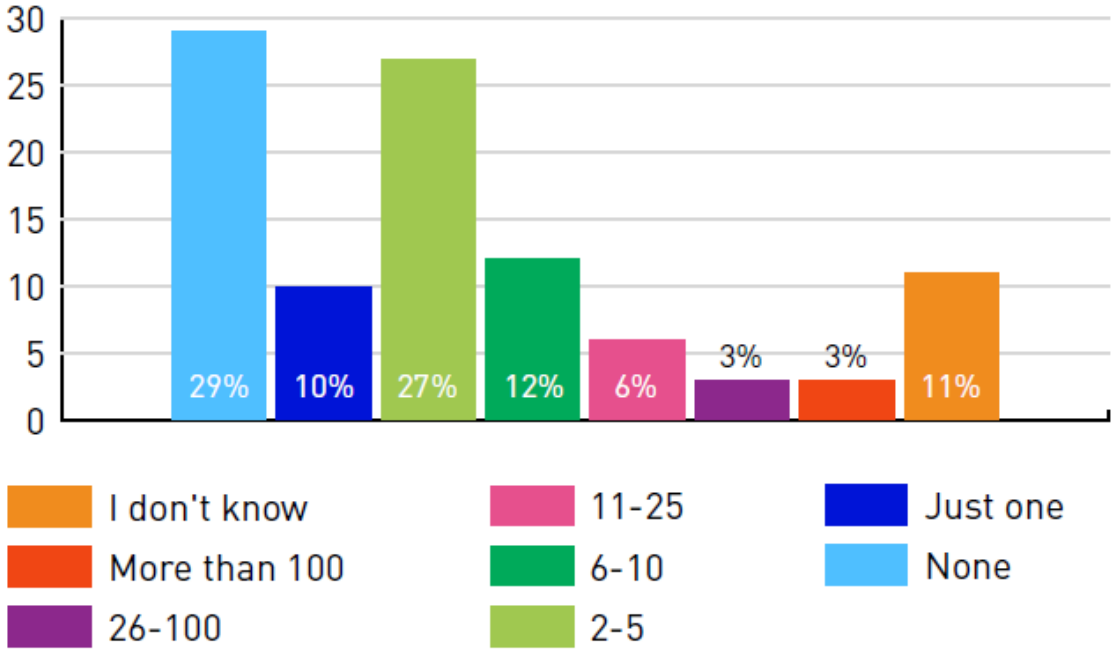
Do you currently have vulnerable containers deployed in production at this time?



Source: Tripwire State of Container Security Report, January 2019

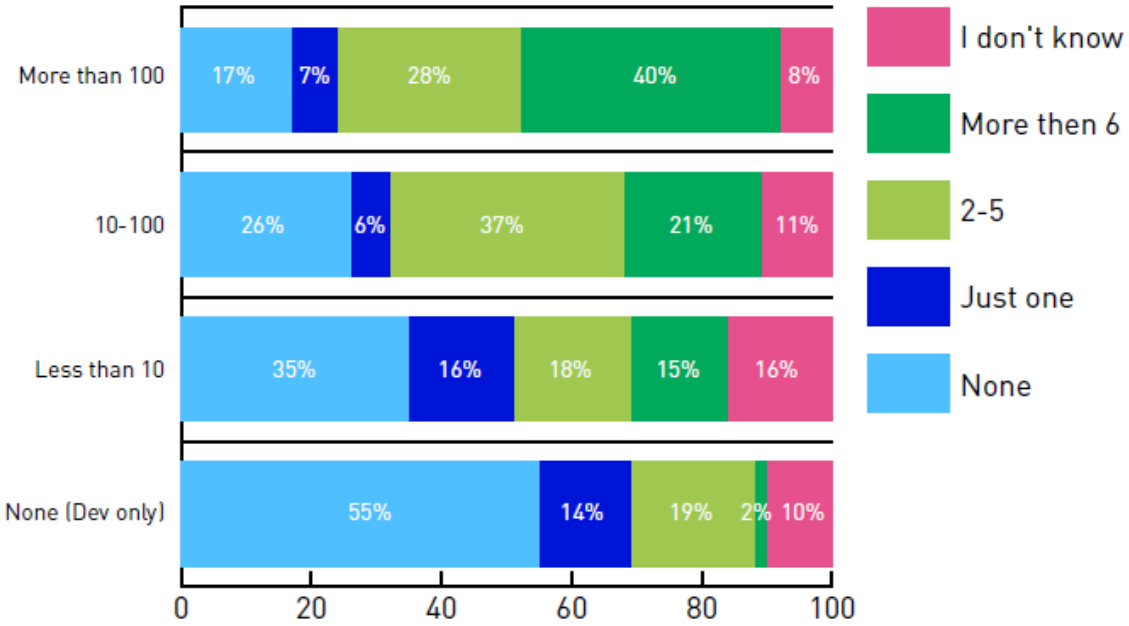
60% have had container security incidents in the past year

Approximately how many security incidents have occurred in your container infrastructure in the past 12 months?



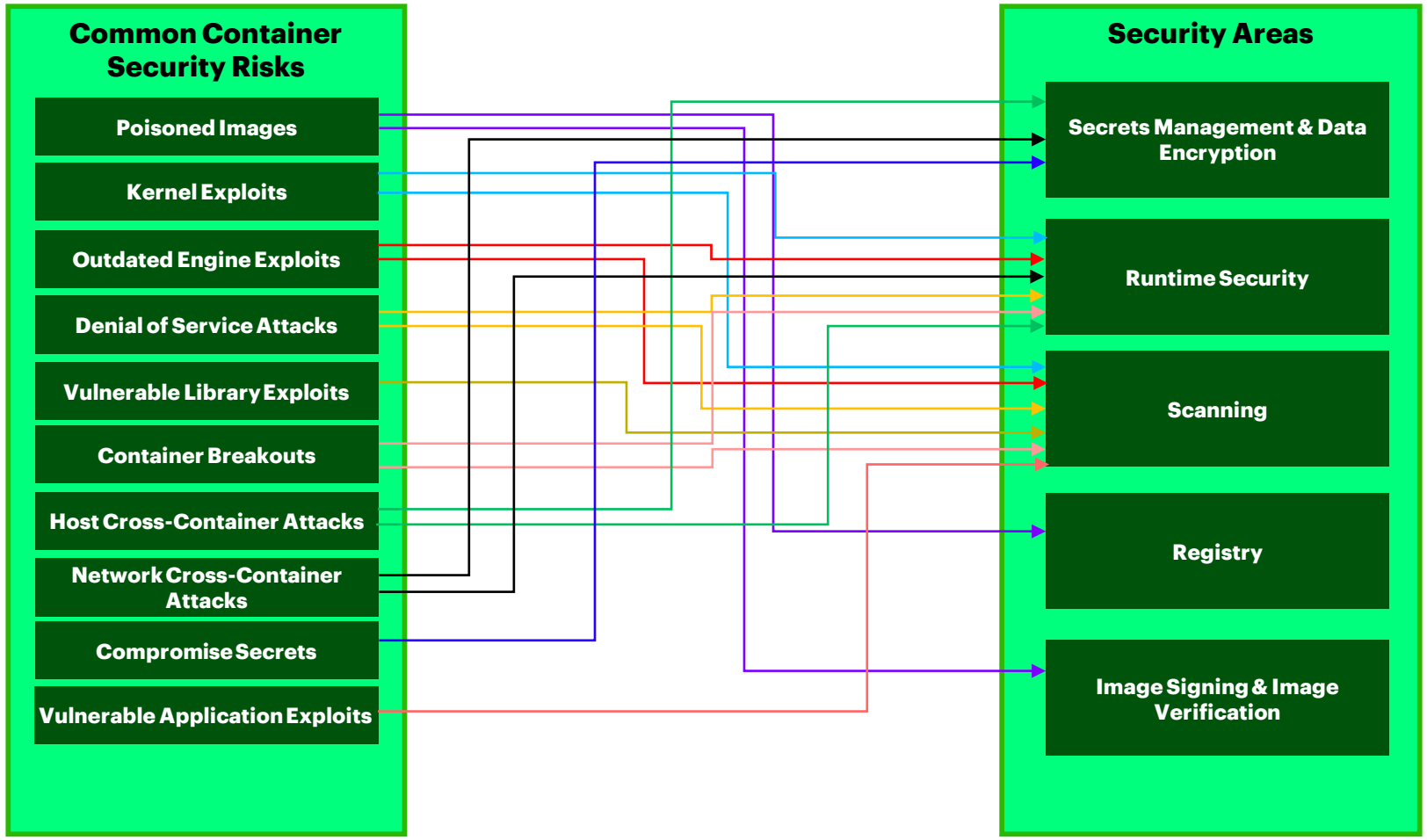
The more containers deployed, the more likely there had been a container security incident.

Approximately how many security incidents have occurred in your container infrastructure in the past 12 months? (By # of containers in production)



Source: Tripwire State of Container Security Report, January 2019

CONTAINER SECURITY THREATS AND RISK



Containers provide security through isolation from the host operating system. However, containers in a production environment are still exposed to known security threats and risks that must be eliminated or mitigated.

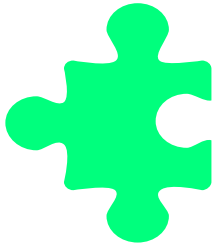
In this diagram, we use the most common container security risks to facilitate the identification of the right set of security tools and platform technologies to protect the containers.

The security areas, in the right column, provide the high level categorization of the security features required in container security tools.


CONTAINER
SECURITY
REFERENCE
ARCHITECTURE

INTRODUCTION

The Container Security Reference Architecture provides a set of capabilities, components and product mappings to guide architecture teams to better identify the required security capabilities in a CaaS implementation, or to strengthen the security capabilities in an existing one.



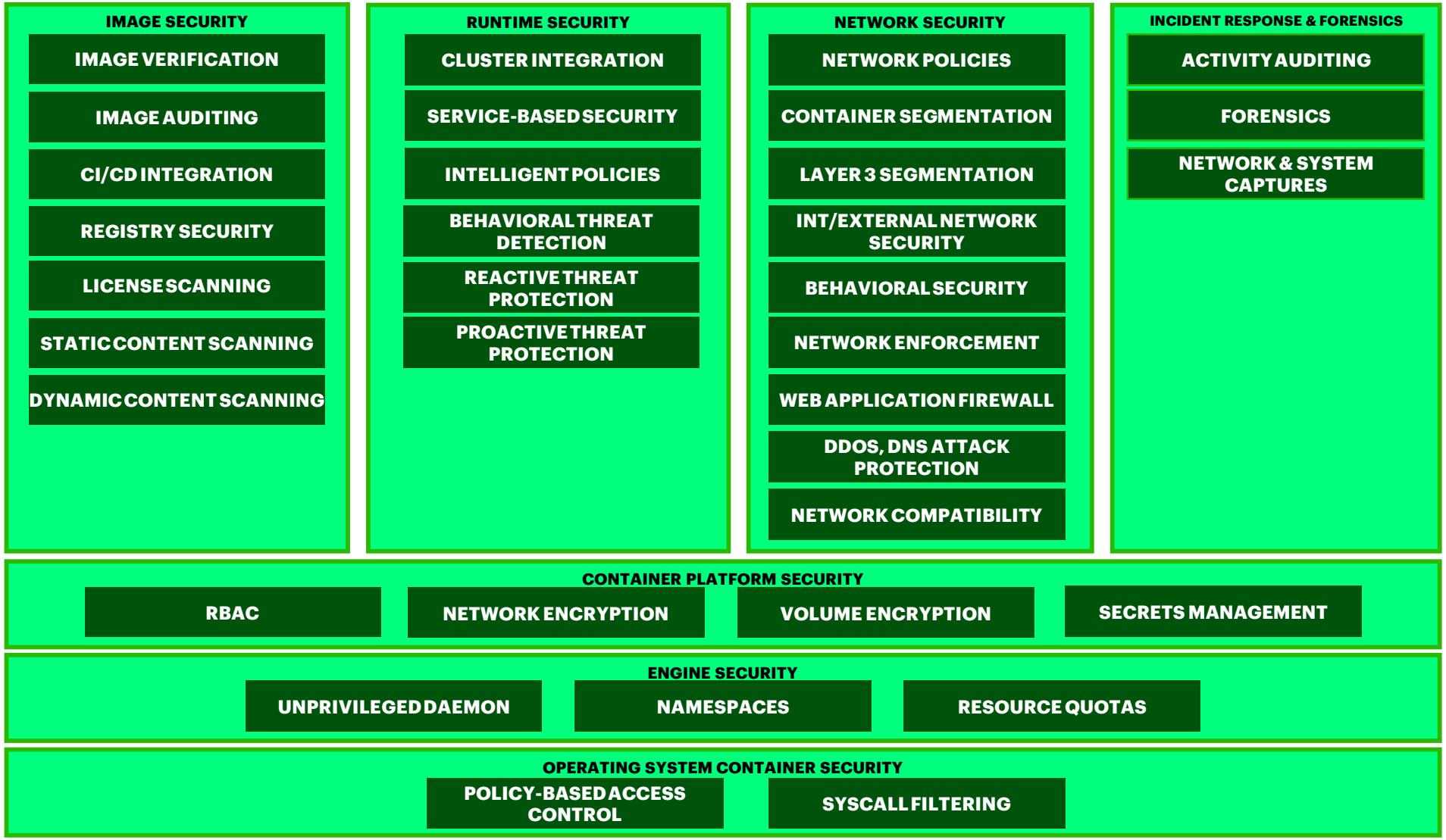
Container Security does not replace existing Security Architectures, but it is complementary and enhances them whenever containers are involved, e.g. Cloud Architecture, Infrastructure Architecture.

A LAYERED APPROACH TO CONTAINER SECURITY

Container security best practices recommend implementing security following a “layer” approach. This approach is designed to address the security threats of the entire infrastructure running diverse and complex application stacks. Also known as “**security in depth**”, it calls for the integration and combination of multiple security tools and technologies to ensure the infrastructure and applications running as containers are secured.

In this security approach, security risks are identified and mitigated by integrating security tools at each layer of the container architecture levels.

A COMPREHENSIVE CONTAINER SECURITY REFERENCE ARCHITECTURE

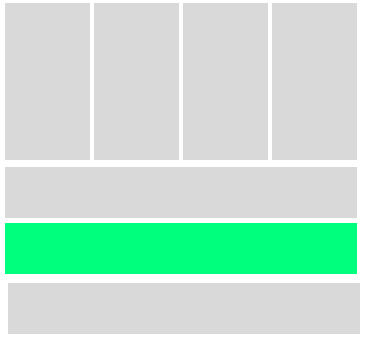


OPERATING SYSTEM SECURITY

- Operating System Security capabilities are provided by the underlying OS alongside the basic building blocks for running containers
- OS container security capabilities are OS-dependent, and may vary between platforms e.g. Linux and Windows
- In Linux, OS container security capabilities include policy-based access control (AppArmor, SELinux), namespaces, quotas and system call filtering

ENGINE SECURITY

The container engine is the part of the client server architecture that establishes communication with the kernel and makes systems calls to create, operate and manage containers.



- Engine security consists of enabling and ensuring the daemon is only accessed by trusted client connections
- Verify that a Docker daemon, for example, has been configured to use certificate-based client–server authentication to ensure the daemon has the right access to images in a registry
- Ensure the daemon socket is protected
- Configure secure computing mode policies to keep system calls in a container secure

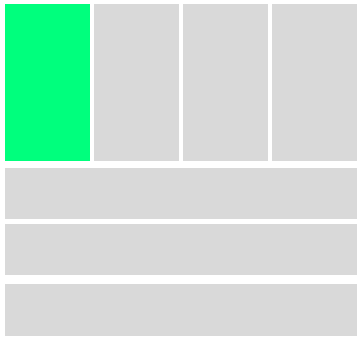
CONTAINER PLATFORM SECURITY

Container platforms security is the configuration, installation and enforcement of controls designed to protect the collection of services and programs that provide support for the container architecture across a fleet of container hosts managed by a top-level scheduler/controller.

- These capabilities include features and components that are typically available out of the box in CaaS platforms.
- Example platforms include OpenShift, OpenStack.

IMAGE SECURITY

Across the application lifecycle, developers, QA and IT will download many images for different needs. It's important to monitor these images, and perform checks before they are installed:



- Ensure the integrity and the authenticity of images used to run containers
- Verify the source of images
- Scan the contents of images at rest and at run-time, create a Bill of Materials and identify existing vulnerabilities
- Implement role-base access control (RBAC) to stored images and repositories

RUNTIME SECURITY

Provides real-time visibility into container activity, when the container is running

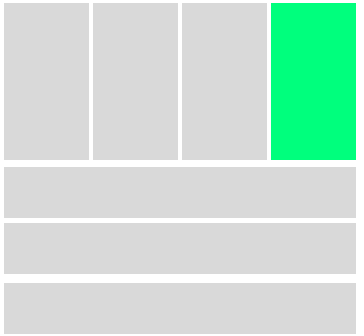
- Restricted access to host from the containers
- Detect and prevent configuration errors, security exploits and attacks
- Container deployments can suffer from most of the same threats common to virtualized or single-OS server environments

NETWORK SECURITY

Protection of traffic flowing through overlay networks using encryption and authentication of information

- Implementation of user-defined and bridge to protect and isolate containers from the host and each other
- Network isolation and segmentation at the container level

INCIDENT RESPONSE & FORENSICS

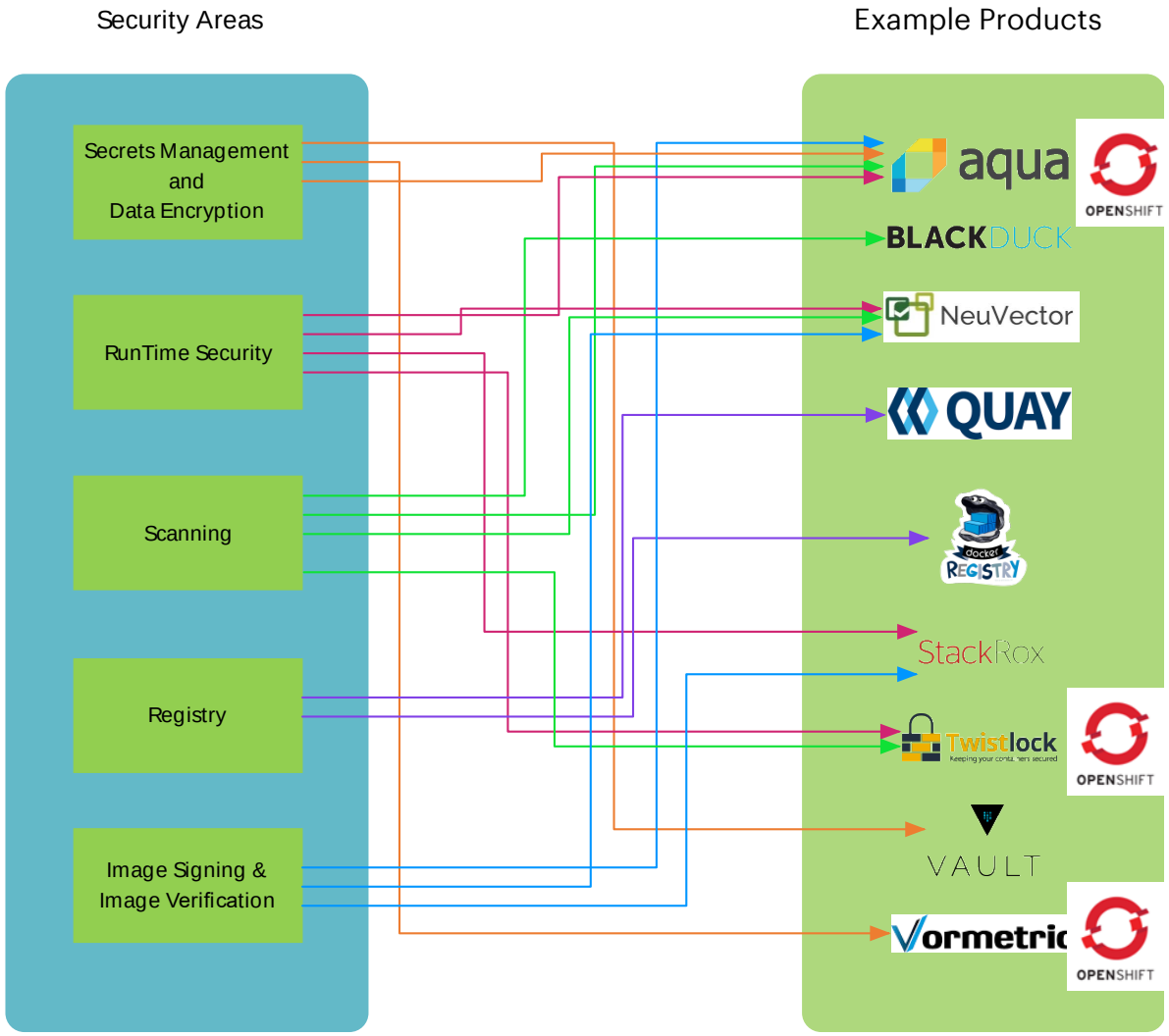


Processes and components to stop, remediate and manage the actions after a security incident or event has been identified

- IT security professionals use forensic procedures and tools to determine the source, extend and cause of the security event
- Monitoring, logging, auditing and alerting tools/systems are part of the tools used to respond and analyze security breaches and events

SECURITY ECOSYSTEM

CONTAINER SECURITY THREATS AND RISK MITIGATION TOOL MAP



The “Security Areas” section provide the high level categorization of the security features required for container security tools.

The ”Example Products” includes the container security tool in the current ecosystem. The security areas arrows provide the map for the tools that provide each set of controls features.

The list of example products lists the products which should be identified by your architects. The map diagram helps create a security tool stack that could address all levels of the “Security Areas” categories.