Trends in Hybrid Cloud Security: Minding the Gap

ESG Research

450 IT/information security professionals worldwide were surveyed on their challenges, readiness and plans regarding hybrid clouds and container security

Summary

The findings in this report are based on the results of a survey by ESG highlighting challenges organizations have today in securing their hybrid cloud and container environments and their short-term security-related plans up to 2020. This survey zeros in on the disparity between the current and near-future containerized application deployment plans to the level of threats organizations are already facing and the lack of sufficient security controls and skills to deal with these challenges.

Top Challenges

Based on 450 IT/information security peers' responses from around the globe, cross different industries, adoption levels, and company sizes, the survey results highlight the growing needs for container-native security controls cross environments (e.g. on-premise, hybrid and cloud).

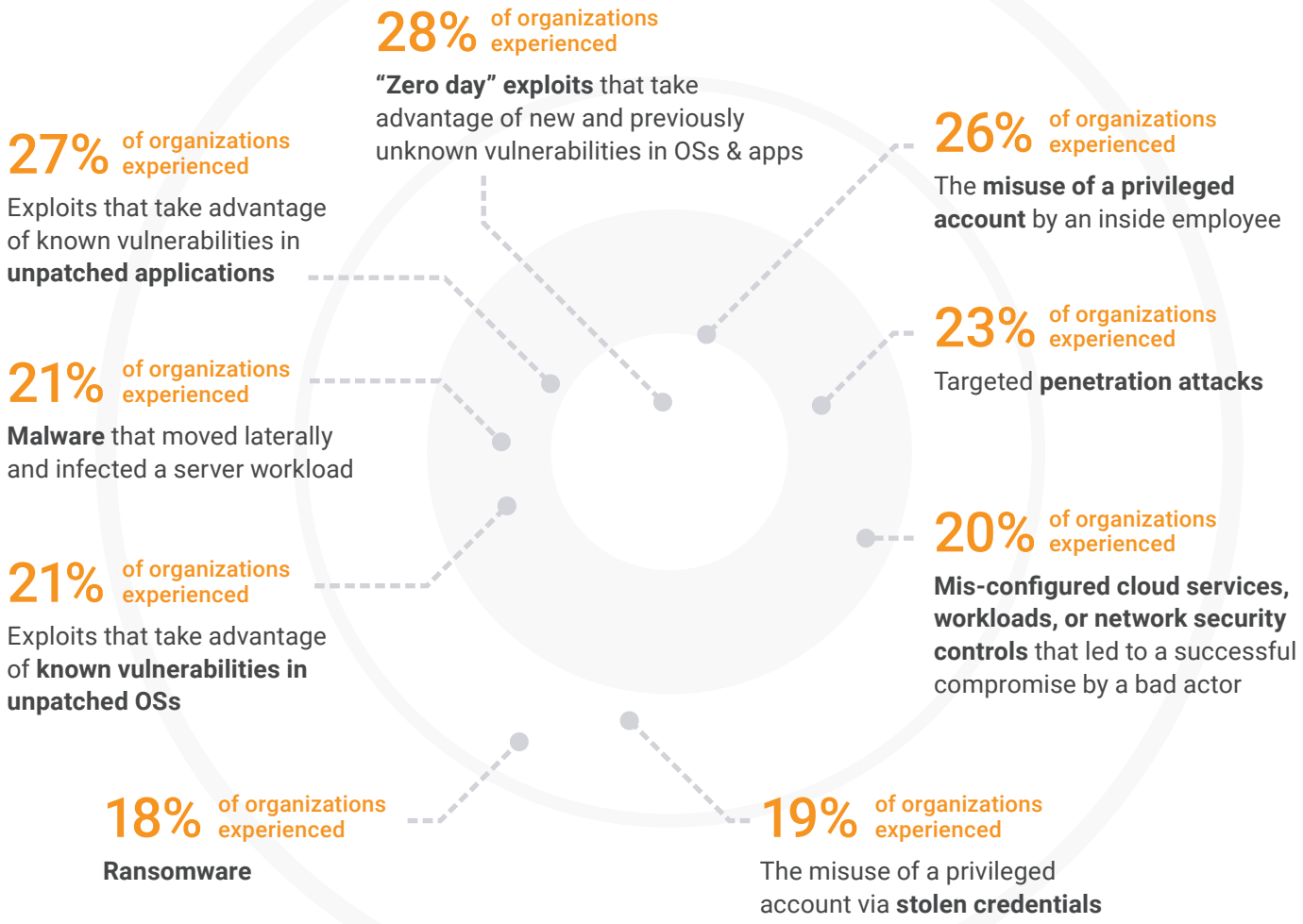
As many organizations are currently testing DevOps environments in their labs, 56% of organizations already have few to extensive numbers of containerized applications in production, whereas most of the new apps are already being containerized and gradually being deployed to public clouds. Container adoption is accelerating and by 2020, 80% of organizations will use containers in their production environments.

However, many organizations already experience a diverse range of attacks on their cloud environments, as well as fall short when it comes to adequate security controls and workforce skills.

56%
of organizations already have few to extensive numbers of containerized applications in production

80%
of organizations will use containers in their production environments by 2020

Exploits and credentials misuse are the top attacks organizations are experiencing [1]



But that is not all...

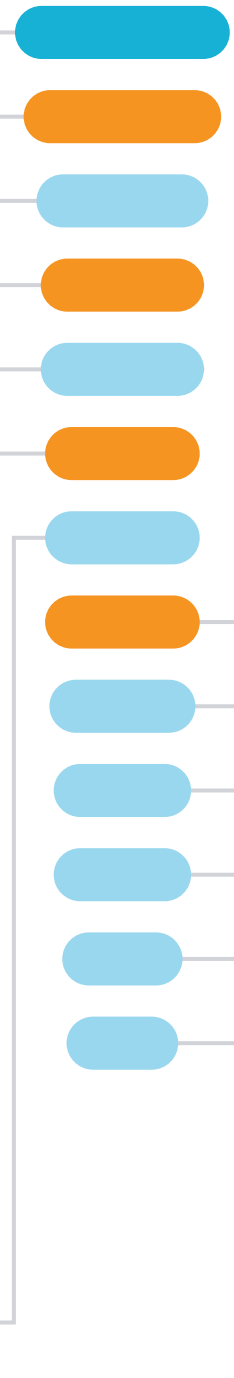
While cyber-attacks are a reality in organizations' cloud environments, the survey also shows other security challenges organizations are facing today. This include inadequate security solutions - legacy security controls that lack the visibility and maturity to protect this new and dynamic environment, whereby disparate security solutions are implemented and used by different teams in different environments. Therefore, it becomes even more challenging to enforce a unified and consistent security policy.

What is particularly worrying is the fact that organizations are still lacking the workforce skills needed to implement security controls in DevOps and cloud environments.

[1] N=450, multiple responses accepted

Consistency, shadow IT and keeping up with the ever-changing, hybrid cloud environment are the top challenges [2]

A silo approach to security | Skills & collaboration | Inadequate security controls



25%

Maintaining strong and **consistent security** across our own data center and multiple public cloud environments

23%

Employees signing up for cloud applications without the approval and governance of our IT departments (i.e. shadow IT)

20%

Keeping up with the rapid pace of change via DevOps automation makes it challenging to maintain security controls

19%

Our DevOps and application owners do not want to involve our security team in their cloud initiatives due to the **fear that security requirements will slow them down**

19%

Meeting prescribed best practices for the configuration of cloud-resident workloads and the use of cloud APIs

18%

Satisfying our security team that our public cloud infrastructure is secure

18%

The inability for existing network security controls to provide **visibility into cloud**

18%

Lack of skills needed to align strong security with our hybrid cloud strategy

17%

Some of our business units are doing app **development and deployment on public cloud infrastructure outside** of the purview of corporate IT

16%

My organization's **existing security tools do not support cloud native** conventions, such as on-demand instances, APIs for provisioning servers, and tag-based naming

16%

Aligning regulatory compliance requirements with my organization's cloud strategy

14%

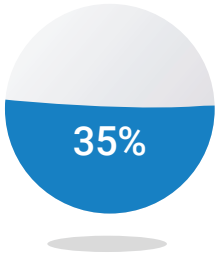
Lack of visibility into the network related activity of our cloud-based workloads

13%

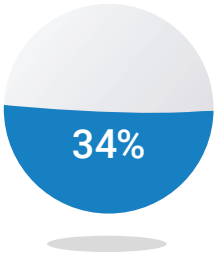
Inability to automate the application of security controls due to the lack of integration with DevOps tools

[2] N=450, three responses accepted

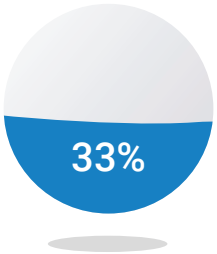
When it comes to container security, organizations' top concerns are [3]
the lack of adequate and disparate security tools, vulnerabilities in images, and the need for granular access-control between containers



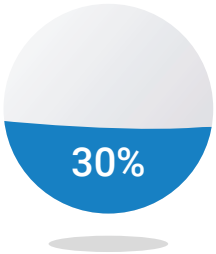
Our current server workload security solution does not support or offer the same functionality for containers, requiring that we use a separate container security solution adding cost and complexity



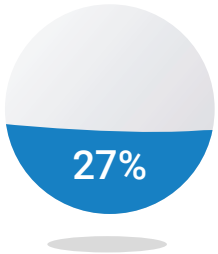
We need to verify that i**mages stored in a container registry meet our security and compliance requirements** to be trusted for production



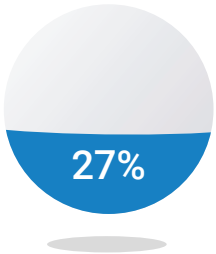
There is a **lack of mature cyber-security solutions for containers**



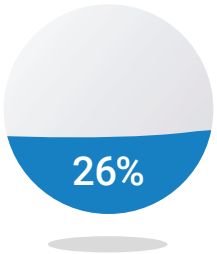
The potential for container sprawl creates **loose access controls between containers** that could leave our production environment(s) vulnerable



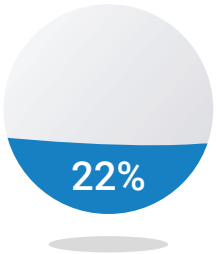
Portability makes **containers more susceptible to "in motion" compromises**



The host-level equivalent of a hypervisor is a standard operating system which we feel **is more susceptible to compromise**



An infected container can **cross-contaminate other containers**



The general best practice of **not running security agents within containers makes them less secure**

[3] N=427, three responses accepted

What do Organizations Intend to Do?

Organizations' security focus areas include trusted images, vulnerability detection, access privileges, network segmentation and runtime visibility

- Build cloud security strategy cross environments (public and private) by taking a workload centric approach to segment access and traffic between dev/test/production, as well as between regulated vs. not regulated sensitive environments
- Integrate security best practices with CI/CD tools
- Increase visibility into IaaS/PaaS-hosted workload by detecting vulnerabilities and non-compliant workload configuration, maintaining an audit trail, as well as alerting on detected anomalous activity
- Employ security controls both in the pre- and the production environment, such as vulnerability and configuration errors detection before deployment, activity monitoring, and workload access controls
- Deploy unified controls for all workload types and environments (e.g. on-premise and cloud)
- Centralize and unify firewall management and access controls across hybrid clouds

> *"As container adoption is accelerating, the need for container-native security controls cross any environment (multi-cloud, on-premise) is increasing."*
>
> Doug Cahill, Senior Analyst, Cybersecurity at Enterprise Strategy Group

The most important capabilities to protect production of containerized applications which organizations consider [4]

31%
Of organizations consider **software vulnerability scanning and remediation**

31%
Attack protection via the **detection and prevention of the lateral movement**

30%
Software **vulnerability detection**

30%
Access controls for **inter-container communication**

30%
Container **monitoring and anomaly detection**

29%
Container **registry monitoring** and protection

26%
Secure secrets management for containers

21%
Container hardening

21%
Container **relationship mapping**

[4] N=427, three responses accepted

A Proven Framework to Implement Key Controls Around Containers

To help organizations secure their container environment and demonstrate compliance, we created a recommended action plan designed to provide a clear perspective on how to implement effective security controls in an automated way, without impeding development efforts.

1 Discover all images, running containers and map out network traffic

Increase visibility into container environment by discovering and maintaining up-to-date inventory of containerized applications, image repositories, and hosts across the cloud environment. Map container network traffic across application services, regardless of actual network infrastructure used, and including networking within and across hosts.

2 Perform ongoing image risk assessment and host hardening

It is recommended to continuously scan images for known vulnerabilities and misconfiguration. For increased effectiveness and preventive measures, images should be scanned immediately after build, to enable developers to remediate images early in the pipeline. This is enabled via integration with CD tools such as Jenkins. In addition, continuously scan images pulled from outside the pipeline, in case they will be used as a base image.

Further, the host itself should also be analyzed for vulnerabilities, patched and hardened. This can be done against CIS benchmarks, to ensure container engine compliance and access rights to OS and host resources are enforced.

3 Automate image usage policy

To ensure only trusted images are running in the environment based on security mandates, it is highly recommended to set image assurance policies. An image assurance policy enables you to define the makeup of acceptable vulnerability levels to allow/disallow an image from running (e.g. blocking images with high severity of vulnerability from running).

4 Establish fine-grained user access control and secrets management policies

Set and enforce user access policies to resources (e.g. images, containers, volumes, and network devices) and continuously monitor and block unauthorized access attempts.

Further, as a security best practice, embedded secrets should be removed from code and configuration files, rotated and securely delivered into containers in runtime, with no container downtime, based on an organization's security policy.

5 Apply runtime protection for enhanced visibility and control

Your insights into images in the pre-production environment can be utilized later in runtime to prevent changes to image executables (e.g. image drift) once a container is instantiated. In addition, you would establish runtime container behavior profile and set network communication rules to enforce container isolation. By applying these runtime controls you can rapidly detect and respond to unauthorized container activity.

For more information on the Aqua Container Security Platform, or to schedule a product demo

Contact us