accelerated strategies

KUBERNETES (K8s) DATA PROTECTION REPORT

COMMISSIONED BY Zettaset

CONTENTS

EXECUTIVE SUMMARY

BUSINESSES ARE FACED with many challenges as they strive to ensure their information technology infrastructure is up to the task. The fast pace requires rapid development and the fielding of new applications. The fast deployment of applications was true before the worldwide health pandemic of 2020 and remain an issue in the aftermath. Enterprises will continue to deal with work from home, remote customers, and partners. To make this work, enterprises have ramped up their development and the use of cloud technology. The linchpin of this development is containerization. The extensive deployment of containerized applications require organizations to orchestrate their use with Kubernetes.

Over the last five years, companies have been eager to incorporate containers and microservices to promote enterprise IT innovation and boost digital transformation. These enterprises must weigh the benefits against the security risks that could result from deployment. Understanding how organizations are using these technologies and how they are doing so securely is why Accelerated Strategies Group conducted this research survey.

In the third quarter of 2020, we surveyed more than 200 professionals and executives to understand how companies are handling the security of Kubernetes deployments. This research can give entities valuable insight into the issues people have noticed as they have moved forward with Kubernetes deployments.

Before looking at security, we need to understand how organizations deploy, use and manage containers and Kubernetes. This survey demonstrates that companies are fully embracing the technology by moving multiple applications to the cloud using containers and they are utilizing Kubernetes for orchestration. It was interesting to discover that 39% of the survey respondents have multiple production applications deployed on Kubernetes. Another 24.6% have limited or internally facing deployments. Many others are moving towards fielding production applications using these technologies.

While applications are packaged in Kubernetes managed containers, the integration of containerized databases is lagging. Only 30% of the applications deployed to Kubernetes have a database that is also containerized. Many (28.6%) are leveraging a software service to handle database operations and others (27.6%) still have the database on a virtual machine.

It was not a surprise that cloud service providers have considerable influence in this sector. A third of the organizations rely on the Kubernetes capability provided by the cloud service provider. Cloud vendors also have considerable influence with containerized databases, with one out of five users choosing to have the cloud vendor manage this operation. The influence of cloud service providers is most significant when it comes to small businesses (less

than 1000 employees). Fully two thirds (66.1%) of small businesses utilize either the cloud providers Kubernetes offering or their database.

Organizations are moving forward with Kubernetes, but the survey uncovered that the current state of security of Kubernetes is immature. Enterprises adopting it in production environments are struggling with all the complexities associated with securing their deployments. Emerging technologies offer attackers new attack vectors, but with Kubernetes deployments there are multiple vulnerable attack surfaces. Nearly half (43.2%) of those polled selected all the available threat vectors when asked that question. Container vulnerabilities was the most significant single concern for 20.3%. The other individual concerns all registered less than ten percent (10%).

One of the perceived problems with Kubernetes security is the majority of organizations believe there must be more education on the best practices. Having people understand the optimum methods to close vulnerabilities is by far the best way for the community to foster additional protection. This need to better understand the underlying technologies is born out by the interactions between the DevOps developers and InfoSec teams. Nearly half of the organizations bring together DevOps and Infosec to secure the environments and applications, but in nearly half of those interactions, the skills gap hinders the contributions from the InfoSec team.

Data security is one of the most important requirements for organizations, and the development of new solutions does not change that. Many organizations are relying on conventional security tools for data protection

There is a common misconception around encryption within container and Kubernetes environments. Respondents feel as though they are sufficient enough to secure data, but in reality, the results are telling us otherwise.

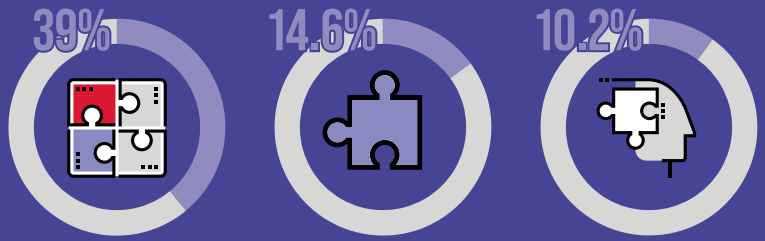
within their Kubernetes clusters. It is an open question as to how well traditional data protection mechanisms work with containers and Kubernetes. While a little over half of the people believe standard data encryption is working well, almost as many do not support that those tools are well suited for encrypting Kubernetes clusters. Digging down into the data, it is clear that many who are using traditional solutions still feel they do not have proper integration, are not mature enough, and negatively impact performance.

Overall, this research validates that many enterprises have embraced containers and they are using Kubernetes to orchestrate those containers. They are attempting to secure the environment using available tools. Accelerated Strategies Group's assessment is these solutions are stop gaps, and in the long run, organizations will look to solutions designed to operate in a Kubernetes environment.

APPLICATIONS FIRST

Organizations are moving multiple applications to the cloud using containers. They also are using Kubernetes to orchestrate multiple applications. 39% of the survey respondents have multiple applications deployed on Kubernetes. Another 24.6% have limited or internally facing deployments.

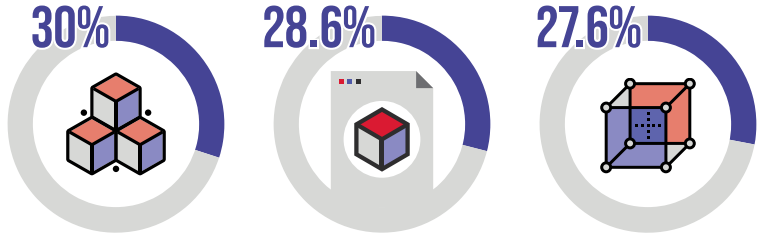
Production Applications deployed on Kubernetes:

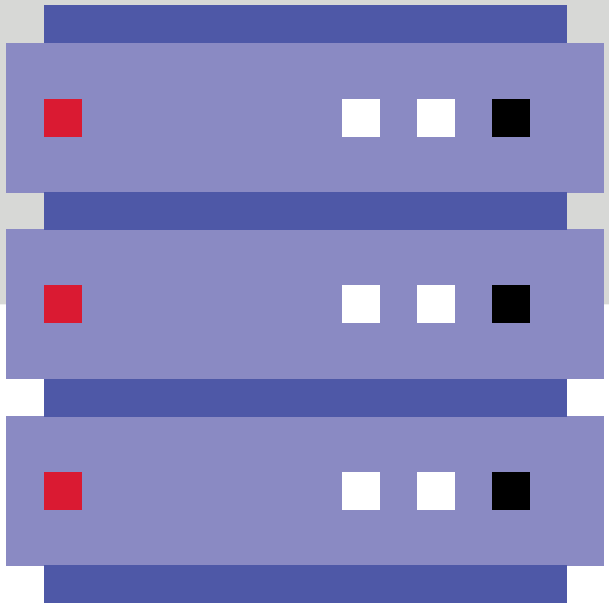


DATABASES FOLLOW

While applications are being packaged in containers and being fully deployed on Kubernetes, the use of containerized databases is lagging. Only 30% of the applications deployed to Kubernetes have a database that is also containerized. Many (28.6%) are leveraging a software service to handle database operations and others (27.6%) still have the database on a virtual machine.

Database also Containerized?:





CLOUD PROVIDERS CONSIDERABLE INFLUENCE

37.2%

are using a Kubernetes offering managed by a cloud provider
(i.e. AWS, Google, Azure, IBM)

66.1%

of small businesses use either a cloud providers Kubernetes offering or containerized database

Kubernetes is available as open source software, from software vendors (including Red Hat, VMware, SuSE), and as an offering from cloud service providers. The flavor of Kubernetes used by survey respondents is split nearly evenly between those three categories. Kubernetes offered by cloud service providers is used 37.2% of the time. Vendor product versions follow with 34% and open source Kubernetes is used in 28.7% of deployments.

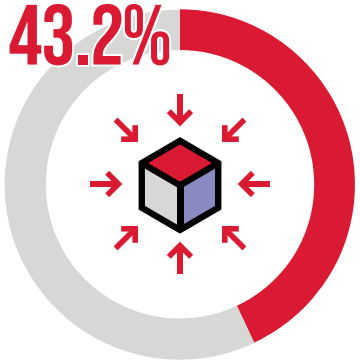
Regarding containerized databases, the cloud vendor also has considerable influence with one out of five users choosing to have the cloud vendor manage this operation. The influence of cloud service providers is greatest when it comes to small businesses (less than 1000 employees). Fully two thirds (66.1%) of small businesses utilize either the cloud providers Kubernetes offering or their database.

DEEP CONCERNS

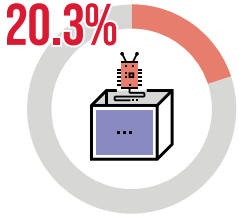
Organizations are moving forward with Kubernetes but there are considerable concerns regarding security. Kubernetes security is immature. Enterprises adopting it in production environments are struggling with complexities associated with securing their deployments. Emerging technologies offer attackers some new attack vectors but with Kubernetes deployments. The feeling is there are multiple vulnerable attack surfaces. Nearly half (43.2%) of those polled selected All-Of-The-Above when asked that question. Container Vulnerabilities was the greatest single concern for 20.3%. The other individual concerns all registered less than ten percent (10%).

ON MULTIPLE ATTACK SURFACES

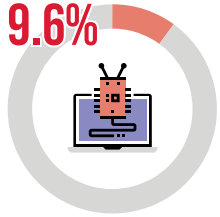
What is the most vulnerable attack surface for Kubernetes deployments?



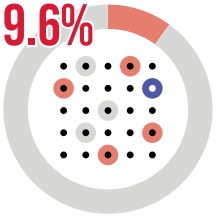
All Attack Surfaces are Vulnerable



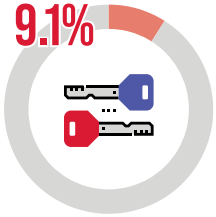
Container Vulnerabilities



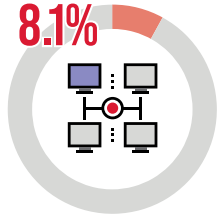
Core Platform Vulnerabilities



Platform Complexity



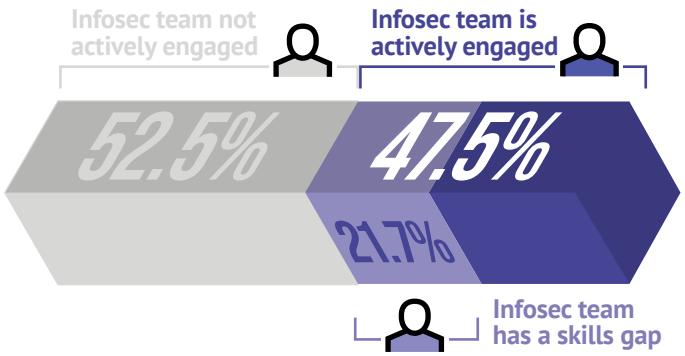
Access Control

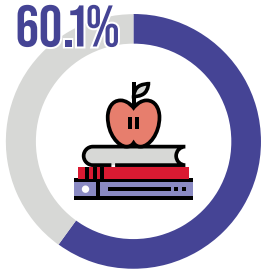


Network Management

KUBERNETES SECURITY SKILLS GAP

One of the perceived problems with Kubernetes security is the majority of organizations believe there must be more education on the best practices. Having people understand the optimum methods to close vulnerabilities is by far the best way for the community to foster additional protection. This need to better understand the underlying technologies is born out by the interactions between the DevOps developers and InfoSec teams. Nearly half of the organizations bring together DevOps and InfoSec to secure the environments and applications but in nearly half of those interactions the skills gap hinders the contributions from the InfoSec team.



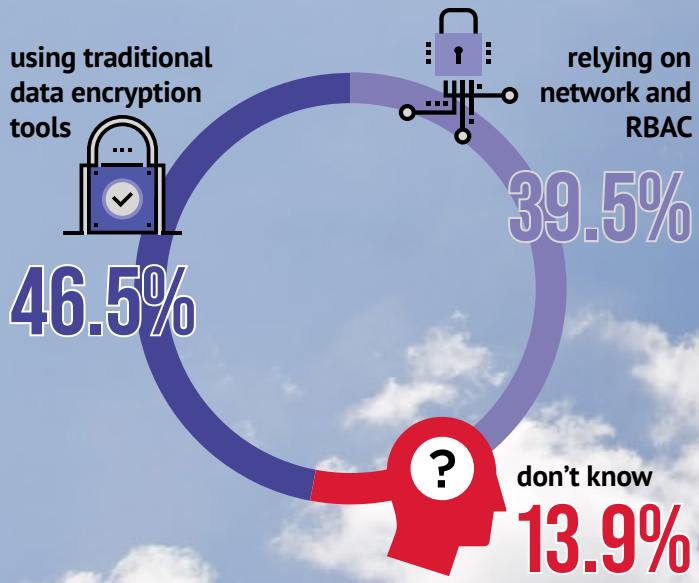


more education on best practices for security in production

ORGANIZATIONS RELY ON TRADITIONAL DATA SECURITY

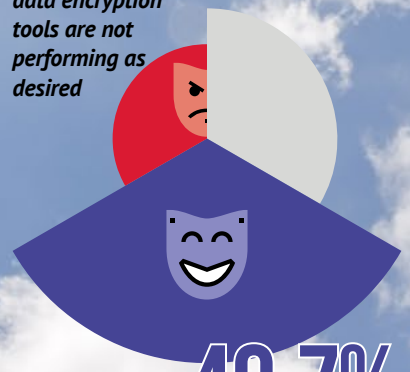
Data security is one of the most important requirements for organizations and the development of new solutions does not change that. Many organizations have moved to adopt traditional security tools to protect data in their Kubernetes clusters. Most of the organizations feel that they have been effective in making that transition. One in five admit that traditional data encryption is not performing as desired.

Organizations who have persistent data stored in Kubernetes clusters are protecting their data by:



21%

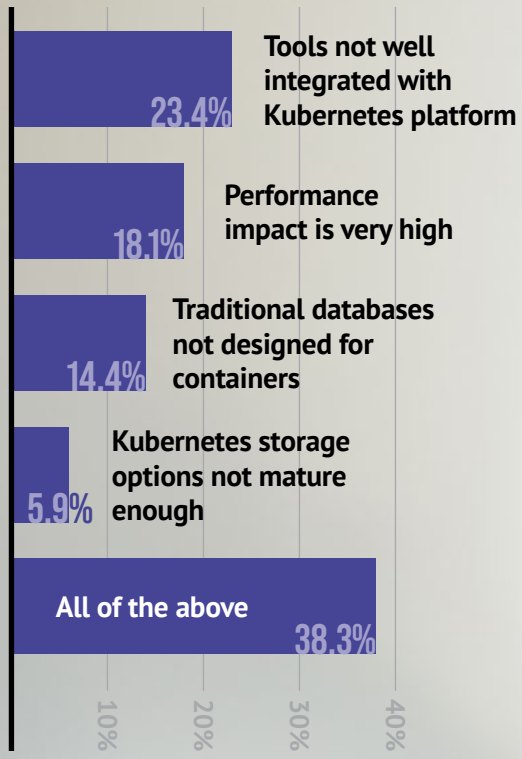
say traditional data encryption tools are not performing as desired



49.7%

feel they are very effective or somewhat effective in adopting data encryption tools to their Kubernetes clusters

Most significant challenge to encrypting data stored in Kubernetes clusters:



KUBERNETES DATA SECURITY CAN BE IMPROVED

It is an open question as to how well traditional data protection mechanisms work with containers and Kubernetes. While a little over a half of the people believe traditional data encryption is working well almost as many do not support that those tools are well suited for encrypting Kubernetes clusters. Digging down into the data it is clear that many who are using traditional solutions still feel they do not have proper integration, are not mature enough, and negatively impact performance.

Are traditional data encryption tools well suited for encrypting data stored in Kubernetes clusters?

THE ACCELERATED STRATEGIES GROUP VIEW

THERE IS NO QUESTION organizations have embraced cloud technologies, containerized applications and Kubernetes orchestration. The overarching objective for this research was to determine whether security and data protection capabilities were up to the task. A quick perusal of the survey data would suggest that security does not appear as a considerable barrier. Most of the companies surveyed are using traditional security they deploy or that is offered by cloud service providers. Additionally nearly fifty percent of the survey respondents said these standard security measures, especially encryption was very or somewhat effective when used with Kubernetes.

A deeper study of the results presents a rather different story. Encryption of production data was a focus area of the research and while people are utilizing encryption and being positive about its use there are issues. The survey results tell us significant challenges exist with the encryption of data stored in Kubernetes clusters. The reality would appear to be that traditional encryption tools are not sufficient to secure Kubernetes clusters with efficiency and performance.

The Accelerated Strategies Group revealed that while many people pronounce they are satisfied with their existing security capabilities they also provided insights on weaknesses associated with container and Kubernetes security capabilities. It was most telling that nearly half of the people surveyed believe that multiple attack vectors are equally vulnerable for Kubernetes deployments. An environment with a high level of vulnerabilities across multiple surfaces is not one where standard security solutions can excel.

In addition to technology issues there are considerable problems related to people and processes. Security technology needs to be supported by competent personnel and policy. The survey results point out that although companies have engaged the InfoSec team to support the DevOps developers there are considerable skills gaps that need to be closed before security professionals can be fully engaged. The data also affirms that security best practices relative to Kubernetes security are not well known. Although not explicitly stated in this research, Accelerated Strategies Group analysts' contend that appropriate security processes associated with containerized data and Kubernetes are immature. More effort is needed in this area.

Overall the results of this research substantiates that many enterprises have embraced containers and are using Kubernetes to orchestrate those containers. They are attempting to secure the environment using available tools. Accelerated Strategies Group's assessment is these solutions are stop gaps. In the long run organizations will look to solutions that are designed to operate in a Kubernetes environment.

SURVEY DEMOGRAPHICS

Accelerated Strategies Group conducted research into the data protection capabilities surrounding Kubernetes deployments. The survey was conducted during Q3 of 2020. We gathered a total of 209 responses from people familiar with their organization's Kubernetes efforts for this survey.

Survey responses came from a global cross-section of 28 countries and regions including **North America (46%), EMEA (23.8%), India (21.8%),** and **Asia (7.7%)**

Respondents hold a variety of roles and come from a broad spread of organizational sizes:

57% of respondents came from small organizations (<1,000 employees)

18.7% of respondents represent large organizations (>5,000 employees)

57.6% self-identified as managers or leadership (Director up to CEO)

ABOUT THE AUTHOR

CHARLES J. KOLODGY is a security strategist, visionary, forecaster, historian, and advisor who has been involved in the cyber security field for over 30 years. His views and understanding of information and computer security were shaped during his years at the National Security Agency. During that time he held a variety of analyst and managerial positions within both the information assurance and operations directorates. Following NSA is was a a research vice president covering security markets for IDC and then a senior security strategist for IBM Security.

Over the years he has identified market trends and authored numerous documents to explain market realities and has been a speaker at many security conferences and events, including the RSA Conference, CIO Conference, CEIG, and IANS. He has been widely quoted in the press.

He is best known for naming and defining the Unified Threat Management (UTM) market which continues to be one of the strongest cyber security markets with vendor revenue of $3 billion per year. He has been a leading analyst on software security, encryption, and the human element.

Charles holds a B.A. in Political Science from the University of Massachusetts at Lowell and an M.A. in National Security Studies from Georgetown University.

Speak with the Author: ***Charles Kolodgy*** at ***charles@accelst.com***

ABOUT THIS REPORT

This report is based on an inclusive survey conducted by Accelerated Strategies Group to assess the current state of security associated with Kubernetes deployments. This worldwide survey of developers, managers, and executives provided specific insights on the security deployments and concerns people have regarding their production deployments of containers associated with Kubernetes. This brief summarizes and provides analysis of the findings. ***Zettaset*** commissioned the research.

ABOUT ACCELERATED STRATEGIES GROUP

ACCELERATED STRATEGIES GROUP is out to democratize access to industry expertise and knowledge. Our expert analysts leverage their experience-based knowledge to deliver insightful, intelligent and actionable information about digital transformation, DevOps, cloud-native and cybersecurity to IT and product organizations. Like open source software, we widely share our work products for free because we believe **Knowledge Wants To Be Free.**

Contact Accelerated Strategies Group at ***info@accelst.com*** and get more great research, reports, commentary, videos and more at ***https://accelst.com***.