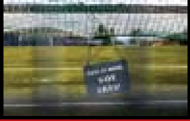
5 Best Time & Productivity Tracking Tools

Surge In Social Gaming During The Lockdown



₹125

VOL. 33 | ISSUE 6 | JUNE 2020

www.pcquest.com

PCQUEST

UNDERSTAND • CHOOSE • IMPLEMENT IT

On-Demand Mobile Apps Are Mushrooming In 2020

MOBILE WILL RULE THE POST-COVID ERA

The smartphone will unleash digital transformation

Special Subscription offer on page 58

76 pages including cover

JUNE 2020

WORK FROM HOME

COVID-19

COVID-19

DEVELOPERS

DEVELOPERS

GAMING

SECURITY

DEVOPS

TECH MIRROR

GADGETS CORNER

REVIEW

TECH NEWS

SUBSCRIBE NOW!

Turn to page 58

HOW TO SECURE CLOUD NATIVE APPLICATIONS?

Hackers are smarter, discovering new zero-day vulnerabilities and developing sophisticated way of attacking cloud applications, so that leaves your production environment vulnerable to attacks

Bhuvan Bhatt

Cloud Native is a buzzword used to describe the new generation of cloud applications; ones made to run in the cloud in a scalable, automated fashion. Public cloud is forecast to be US$~350 Billion by the year 2022 and when the market grows, challenges grow with it as well. Security is one of the biggest challenges in this rapidly growing market. These days, Security is a very important aspect for any organisation, and it may cause damage. It's not just loss of business continuity and revenues, but also the loss of reputation in the market, making customers will think twice before buying again from you. Having 7 years of experience in the security domain and seeing the security products from the eyes of Developer, QA, Product Manager and R&D head, I have seen the "shifting left" of security into the development process in many organisations. It starts when developer writes the code and continues through deployment to the application running in production.

Fast moving industry with cloud technologies

The industry is very agile and dynamic, and things move faster than ever, with container and cloud updates. Upgrades happen in environments within minutes.With this, fast-paced security becomes the biggest challenge. To help with security we need an end-to-end security solution from dev to prod and provide security right from the development process and bridge the gap between developer, DevOps and the security team. Cloud made a lot of things easier and faster for organizations, and adoption is happening at a fast pace, which is why we must be quick with security as well. When you have a registry with 100,000 container images that are used in your production environments, then it is very important that you ensure that those images don't have container vulnerabilities, malware or other security issues, and do so in a way that doesn't slow down development.

Key security challenges

When enterprises want to reap the benefits of cloud technologies, at the same time they need to make sure of securing their environments against any security issues, data breaches or data loss. While moving to the cloud places some of the security burden on the cloud providers (especially around infrastructure and networking), customers who remain responsible for the security of their own applications, user authentication, and compliance. Data loss is another challenge which may happen through accidental deletion or malicious tampering like DDoS, which could be disastrous for any enterprise business. With these kinds of challenges what are the actions enterprises can take? Your cloud must have right Identity management and access control, encryption, auditing, secured API, authentication and authorization. But you must ensure the security of your code, monitor your applications for indicators of attack, and ensure that your cloud services are properly configured against your security and compliance needs.

Security should be considered during the architecture & design phase of development, so that possible threat scenarios are considered upfront. Mitigating controls & compliance should be in place

BHUVAN BHATT, R&D Head, Aqua India

Preventive measures: Shift left with security

Historically, security was enforced outside the application development phase. This changed with DevSecOps, an approach that makes it easier and more effective to find security issues earlier in the game, when development happens. It means that security should be considered during the architecture and design phase of development, so that possible threat scenarios are considered upfront. Mitigating controls and compliance requirements should be in place to counter threats before they actually occur. Today enterprises use their CI/CD pipelines to find security issues, bad configuration, malware and many more issues, preventing deployment of applications with security issues, rather than deploying them only to discover the security flaws when the application is already exposed. Having a DevSecOps practice or

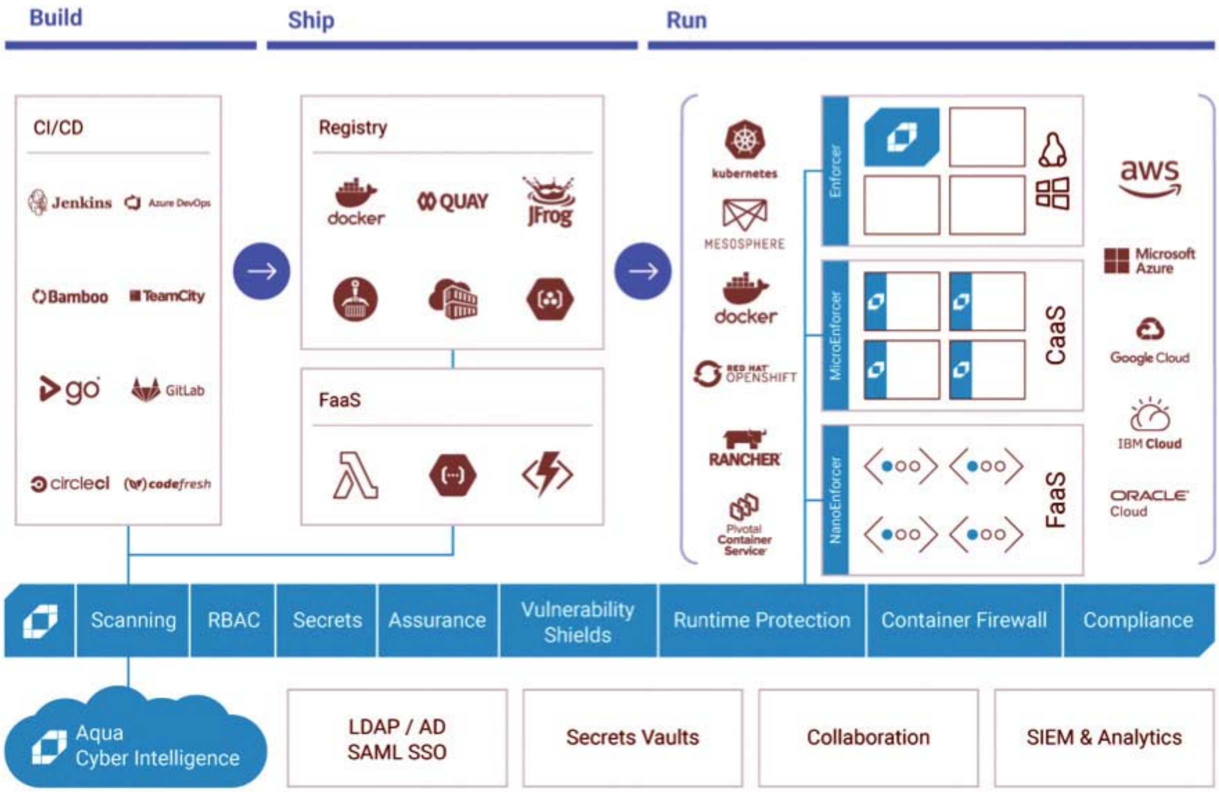


Image Source: Aqua

process in place, enterprises can reduce the impact of security flaws and reduce the attack surface from the start. It's a necessity for any enterprise when moving to cloud.

Is the shift left enough?

Now the question arises whether it is enough to only consider security during development, having taken care of all the security flaws, and considering the application to be bulletproof. The truth is that it is not enough. Hackers are smarter, discovering new zero-day vulnerabilities and developing sophisticated way of attacking cloud applications, so that leaves your production environment vulnerable to attacks.

How to secure cloud native then?

To secure your cloud environments even though we have taken care of that in our CI/CD pipeline we need to make sure of following principles.

1. **Vulnerabilities Management:** Run continuous and regular scan against vulnerabilities for your cloud environments and application.
2. **Audit and Compliance:** Run audit, monitoring and compliance scans using cloud posture management tools. Have a strong auditing capability in the system with right integrations in place to find out the as well as stop the attack if situation arises.
3. **Scanning:** Scan your clusters and cloud infrastructure against benchmarks and best practices.Follow and run benchmarks for your environment e.g. CIS Benchmarks for Docker, Kubernetes and Linux.
4. **Penetration tests:** Run Penetration tests on your clusters
5. **Right access to right resource:** Work with least privilege rules and provide only enough access which is required.
6. **Runtime protection:** Ensure that your workloads are monitored and protected against unexpected changes, anomalous behaviour, and automated threat detection and blocking.

To Summarize, securing your cloud infrastructure and applications is part of the journey to the cloud and it should be considered as part of your cloud native journey with containers and Kubernetes, serverless. Development team, DevOps teams and security teams need a unified view to bridge the gap between the teams and to handle security issues effectively and quickly.

The author is Aqua India R&D Head