Cloud Native Security:

What It Means, Why It's Hard and How to Achieve It

> The past decade has witnessed the emergence of rich new opportunities for building software and infrastructure. The advent of cloud-computing platforms in the mid-2000s created important new ways of deploying applications and storing data. More recently, as developers moved toward microservices architectures and lightweight application deployment strategies, cloud computing platforms expanded to include offerings such as hosted Docker containers and serverless functions.

While organizations at first tended to view the cloud as a complement to their existing infrastructures, cloud-based resources and services have evolved into the default means of deploying applications. Cloud adoption rates across a range of businesses and industries have reached 96 percent, and almost 90 percent of all data center workloads run in the cloud. Although on-premises resources are unlikely to disappear totally at most organizations in the near future, the cloud now forms the foundation of most IT infrastructures and strategies.

This is why the term cloud native has evolved into a common part of the IT lexicon. System architectures, developers, IT Ops professionals and everyone in between recognizes that a cloud-first strategy has become the key to unlocking new innovations and efficiencies.

New Opportunities Equal New Challenges

Yet with the advantages conferred by cloud computing come new challenges, particularly in the realm of security. When applications are deployed in the cloud rather than on-premises, new potential security issues arise. When applications are composed of a complex web of microservices, keeping microservices and the communication routes between them secure becomes much more difficult than securing a monolith. When infrastructure is built using dynamic, ephemeral containers or serverless functions, the differences between normal application operations and behavior that could signal a breach are hard to identify.

Despite these and similar cloud native security challenges, most security strategies and tools have not kept pace with the rapid changes over the past decade to the way applications are designed and deployed. Instead, they continue to rely on tools that are unable to scale as quickly as cloud workloads, are designed for environments with clear perimeters (which don't exist in the cloud), do little to help different parts of the IT organization collaborate on security, and so on.

Organizations have not, in other words, adapted their IT security strategies for the cloud native era. And even those that have updated their security practices may not have successfully implemented strategies that will allow them to continue to adapt as new types of cloud-based services appear.

This whitepaper identifies the hurdles that prevent organizations from adopting a cloud native security strategy. It then explains which tools, processes and philosophies IT teams must adopt in order to bring their security strategies up to speed with the cloud native era.

Security Before the Cloud Native Era

Planning a cloud native computing strategy starts with understanding the security strategies that were common prior to the advent of cloud native computing:

- **Perimeter-based security.** When most workloads ran on-premises, it was possible to define clear perimeters for applications and services, then secure them using firewalls.
- **Static analysis.** Before the advent of the fast-changing, highly scalable workloads associated with the cloud, static analysis often sufficed for identifying vulnerabilities. Applications or data could be scanned for security weaknesses before they were deployed.
- **Non-scalable security strategies.** Before the cloud native era, security tools and processes were not designed with scalability in mind. This approach was acceptable because infrastructure did not grow rapidly, and application updates arrived relatively slowly.
- **Siloed teams.** Traditionally, security teams worked in isolation from developers and IT Ops engineers. As a result, security planning and tests were not well aligned with the software development lifecycle.
- **Basic compliance.** Compliance needs before the cloud native era were relatively basic. Requirements such as the need to be “private by design” did not yet exist.

Some of these security strategies still have roles to play in the cloud native era. On their own, however, these approaches to security are insufficient for keeping modern cloud-based workloads secure and compliant.

Cloud Native Security Challenges

There are several key reasons why traditional security strategies no longer suffice for meeting cloud native security challenges. They reflect the new technologies and trends that define cloud native computing.

Cloud infrastructure

At the most basic level, the nature of cloud infrastructure itself creates several inherent security challenges that traditional tools and processes cannot accommodate.

One is that organizations with a cloud-first strategy do not own or directly control most of their infrastructure. Their ability to modify hardware and software environments for security reasons is therefore limited. In addition, they depend on third parties to ensure the physical security of their infrastructure.

Similarly, access control models in the cloud are more challenging. While most cloud-computing platforms provide tools for configuring access control, the tools are usually platform-specific and limited in functionality. And when access control for a cloud-based workload is not properly configured, it is easy for users to overlook, because cloud hosting platforms do not monitor for or enforce access control best practices.

Finally, the rise of hybrid cloud and multi-cloud architectures has increased even further the amount of complexity required to secure cloud workloads. When organizations are using multiple clouds at once, they have to contend with multiple access control and management tools, while also monitoring for security weaknesses and intrusions on workloads that are distributed across a heterogeneous environment.

Containers

The explosive popularity of containers since the debut of Docker in 2013 has driven a host of new security challenges.

Container environments are highly dynamic. Because containers spin up and down constantly, there is often no consistent baseline that organizations can use to determine what constitutes a normal operating state. Containers also provide a lower level of isolation between different applications as compared to virtual machines, which increases the risk that a security issue with one container could lead to a large-scale intrusion.

When it comes to networking, containers pose special challenges, too. Containers rely heavily on the network for communication. Network endpoints that are not properly secured, or that are unnecessarily exposed to external network traffic, can create significant security risks.

The fact that the container ecosystem has spawned multiple management tools also makes security particularly difficult in containerized environments. In addition to community-developed tools like Kubernetes and Docker Swarm, many cloud providers also offer their own container orchestration solutions. Identifying and adhering to best practices for secure container orchestration is difficult when there are so many tools to master.

Serverless Functions

Cloud-based serverless computing platforms, which began to achieve widespread adoption with the introduction of AWS Lambda in 2014, have also spawned special security challenges.

Cloud-based serverless computing in its modern incarnation remains a new technology, and best practices from a security standpoint are still evolving. For this reason, it can be difficult for experienced DevOps teams to know where to start when developing a serverless security strategy.

In addition, the architecture of serverless computing can make it inherently difficult to strike the right balance between security and functionality. The chief attraction of serverless architectures is that they minimize the amount of management required on the part of organizations to deploy code in the cloud. This is efficient and convenient from an IT Ops perspective, but from a security perspective it means less user control and more dependency on cloud providers to keep workloads secure. To deploy serverless functions effectively and securely, organizations need to develop security strategies that keep their serverless workloads secure without undercutting the agility of serverless environments.

Software-Defined Everything

As more and more workloads have moved to the cloud, organizations have also transitioned in many cases toward software-defined infrastructure. Storage systems, networking and other infrastructure components are often abstracted away from the underlying infrastructure. This strategy increases agility and scalability by decoupling software systems from physical hardware.

At the same time, however, software-defined everything also makes security difficult. In addition to increasing management complexity by adding additional layers to an organization's infrastructure, software-defined systems don't map consistently to physical systems, which can make it difficult to track and isolate security problems. At the same time, the introduction of more software to an environment (which is what happens when a DevOps team uses software-defined storage, networking or other tools) means that potential attack vectors become larger, too.

Constant Change

Perhaps the greatest security challenge of all in the cloud native era results from the fact that cloud infrastructure and services are always evolving.

At the outset of the cloud native era, cloud services were limited primarily to basic cloud-based storage and virtual servers. Those offerings have evolved over recent years to become much more sophisticated. Users can now take advantage of multiple tiers and types of cloud storage, as well as many dozens of different virtual machine instances. In addition, cloud services have expanded to include solutions such as hosted Docker container environments, serverless computing, cloud-based big data tools, monitoring services, and more. All of these additional services have added to the list of security challenges that organizations must master in order to secure cloud workloads.

That list will keep growing as the cloud continues to evolve. While no one knows what the cloud will involve in five or 10 or 20 years, it's a safe bet that cloud services will be even more sophisticated and diverse than they are today. DevOps teams will need to adapt their security tools and strategies on a continuous basis as the cloud technologies of the future debut.

Achieving Effective Cloud Native Security

While traditional security tools and processes are insufficient for meeting the security needs of the cloud native era, it is possible to adapt security strategies for today's cloud workloads—as well as to achieve the adaptability that is necessary to keep workloads secure as the cloud continues to evolve.

Doing so requires adopting a security strategy that is itself cloud native. In practice, this involves the following.

Thinking Beyond the Perimeter

Perimeter-based security strategies and tools have a role to play in the cloud. Static firewall rules and networking monitoring tools can help to secure network endpoints and block malicious traffic.

On their own, however, such tools, which are designed for a perimeter-based security strategy, are not enough for the cloud. Organizations must also think beyond the perimeter. Runtime security tools that monitor applications themselves—rather than the network traffic they send and receive—are also a key resource for cloud native security. So are dynamic firewalls that can adapt automatically to keep networks secure even as environments change.

Securing All the Clouds

Cloud native security strategies should not be designed for any one cloud in particular. In order to support agility and accommodate multi-cloud computing architectures, modern security tools and processes must enable organizations to move workloads between different clouds, or to run multiple clouds at once, without having to update security strategies each time they introduce a new cloud platform or service.

While platform-specific security tools, such as AWS IAM, can be useful in some circumstances, DevOps teams should strive at a higher level for a security strategy that is cloud-agnostic and works with whichever set of cloud services and tools the organization chooses to adopt.

Integrating Security with CI/CD

Isolating security processes from the rest of the software development lifecycle is not possible for organizations seeking to maintain today's rapid pace of software delivery. Instead, DevOps teams must embrace the DevSecOps concept, which encourages security engineers to work in close collaboration with developers and IT Ops staff. With this approach, security problems can be identified and addressed quickly, without slowing down the delivery of the rest of the application.

In addition, DevSecOps optimizes the process for fixing vulnerabilities that are discovered once code is in production, at which time a fast remediation is particularly critical for keeping users and data secure.

A security strategy founded upon DevSecOps principles is the only way to maintain a fast, efficient software delivery process without compromising security.

Supporting Multiple Deployment Models

In the cloud native era, applications can be deployed in a number of ways. Some still run on-premises. Some run in cloud-based virtual machines. Some are deployed using containers, serverless functions or other next-generation technologies.

An effective cloud native security strategy must be able to support all of these deployment models, as well as those that might appear in the future. Rather than developing security processes and tools that cater to a specific type of deployment solution, DevOps teams should strive for security practices that can accommodate any type of workload or architecture.

Conclusion

Just as the cloud has revolutionized the way data and applications are deployed over the past decade, it has also fundamentally changed IT security needs. The security tools and processes that once sufficed simply cannot be adapted to secure cloud-based workloads effectively. Although legacy security processes might still play some role in securing modern workloads, organizations that are fully committed to the security and compliance needs posed by the cloud today must fully overhaul their security strategies for the cloud native era.

Twistlock, a next-generation security platform designed specifically for the cloud, is one key resource for implementing a cloud native security strategy. Visit Twistlock.com to get more details on Twistlock's unique abilities for securing containers, serverless functions, and more.

Ready for a deeper conversation?
Sign up for a trial and custom evaluation.

Twistlock

Twistlock is the leading provider of container and cloud native cybersecurity solutions for the modern enterprise. From precise, actionable vulnerability management to automatically deployed runtime protection and firewalls, Twistlock protects applications across the development lifecycle and into production. Purpose built for containers, serverless, and other leading technologies — Twistlock gives developers the speed they want, and CISOs the control they need.

Follow Twistlock

Twitter

Facebook

LinkedIn