Security Challenges in the Cloud

SOLVING FOR VISIBILITY AND PROTECTION ACROSS ARCHITECTURES

PRISMA
BY PALO ALTO NETWORKS

MediaOps

With the rise of cloud native applications, IT organizations in the never-ending pursuit of increased agility have now started to embrace new platforms at faster rates than ever before. There are now no less than three distinct layers of cloud native abstractions that are simultaneously being employed to run varying classes of cloud native application workloads that, unfortunately, are largely managed and secured in isolation from one another.

The first and most commonly used form of cloud computing essentially involved shifting virtual machines that were once deployed exclusively in on-premises IT environments to shared public infrastructure such as Amazon Web Services (AWS) or Microsoft Azure. A second phase of cloud native computing is now being defined by the rise of containers, which provide developers with a smaller, highly portable unit of computing that can be deployed on-premises or on a public cloud.

Containers are also the most ephemeral unit of computing ever invented. Many containers only run for a few minutes before being replaced. As many cybersecurity professionals have already discovered, securing containers present new, unique challenges.

At the same time, a third phase of cloud native computing based on serverless computing frameworks is starting to emerge. Serverless computing frameworks promise to make it simpler for developers to dynamically invoke additional IT infrastructure resources for a short amount of time whenever required.

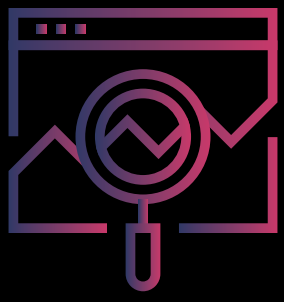
None of these three cloud native computing abstractions are meant to supplant the other. Instead, organizations will collaboratively employ all three to run multiple classes of application workloads. These capabilities will provide IT organizations with more options than ever to manage IT in an agile fashion. However, all that increased flexibility comes with a price. Managing and securing all the different layers of abstraction on which application code now runs has never been more challenging.

A RAPIDLY CHANGING IT LANDSCAPE

A little more than 10 years ago cloud service providers discovered they could leverage traditional virtual machines to transform the IT landscape. Instead of relying on commercial instances of virtual machines, cloud service providers built their own virtual machines to make compute resources available on an hourly basis. While that capability certainly made it simpler for developers to programmatically spin up compute resources at will, organizations needed to adjust to a new shared-responsibility model for cybersecurity. The cloud service provider is responsible for securing its IT infrastructure, while the security of the applications deployed on those platforms needs to be secured by the internal IT team. Ten years later and most organizations are still struggling with how best to master cloud security issues as they are known today.

The additional challenge organizations now face is that two more classes of cloud-native computing platforms are now gaining traction. The first is based on containers such as Docker, which packages application code and all its associated dependencies in a way that makes it simpler to move code from one platform to another. As an alternative approach to achieving virtualization, the cybersecurity issue containerized applications create is that legacy cybersecurity tools developed for virtual machine environments lacked visibility into the containers. Without new tools, it becomes impossible for cybersecurity teams to determine if any vulnerabilities had been packaged within a container that might, for example, include a module based on outdated software that had not been recently patched.

To solve that problem a new generation of cloud security tools were developed by pioneers such as Twistlock, which is now part of the Palo Alto Networks family. At the core of the Twistlock portfolio is a suite of security technologies that includes:



CONTAINER MONITORING

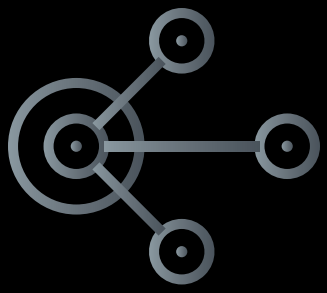
Core to any ability to apply and maintain container security, container monitoring tools are needed to track what are among the most ephemeral atomic units of computing ever devised.

CONTAINER SCANNING

Containers need to be continuously scanned for vulnerabilities both before being deployed in a production environment and after they have been replaced.

CONTAINER FIREWALL

A container firewall inspects and protects all traffic into and out of containers as well as the traffic moving to and from external networks and legacy applications.



CONTAINER POLICY ENGINE

Cybersecurity teams need to define policies that essentially whitelist who and what can access any given microservice.

Like any other form of software, containers naturally need a place to run. Most containers today are deployed on a cluster such as Kubernetes that needs to be secured like any other host. Kubernetes clusters can be deployed on hosts located either on-premises or on a public cloud. It's more than likely most cybersecurity teams will soon find themselves being asked to secure multiple distributions of Kubernetes running on different platforms as organizations embrace hybrid cloud computing. For example, it will not be uncommon for a containerized application running on a local server to query a database running, for example, on an instance of a Kubernetes cluster deployed on a public cloud that in turn is accessing backend databases such as RDS and storage services such as S3 on the AWS public cloud. Cybersecurity teams will be expected to secure the entire application environments as well as all the network connections in between.

The most common place containers are deployed today is on top of virtual machines. Most IT organizations today make extensive use of virtual machines to provide isolation between workloads. That level of isolation prevents a compromised workload from taking over an entire server. However, cybersecurity professionals should note that containers are also starting to be deployed more frequently on bare-metal servers running on-premises or in the cloud,

especially as platforms such as Kubernetes continue to mature. The primary drivers of any decision to deploy containers on bare-metal servers come down to wanting to avoid any form of a "virtual machine tax" that might adversely impact application performance or increase the total cost of ownership for a containerized application, or the need to run a containerized workload on a graphical processor unit (GPU) or field-programmable gate array (FPGA) that doesn't support virtual machines.

Cybersecurity tools that can monitor, manage and remediate issues regardless of where containers are deployed will be essential.

THE RISE OF SERVERLESS

As big an advance as containers represent in the world of enterprise IT, the IT landscape is also now shifting to also make room for serverless computing frameworks. Built using containers, a serverless computing framework makes it simpler to dynamically invoke external compute resources using an event-driven architecture. Whenever additional compute resources are required to, for example, run an analytics module, the application invokes an application programming interface to create a function—an even smaller unit of computing than a container—that then runs that workload on a serverless computing framework. The serverless computing framework may be deployed on a public cloud in the form of, for example, AWS Lambda, or in an on-premises environment using any number of open source instances of a serverless computing framework such as OpenWhisk.

To secure those serverless computing environments, Palo Alto Networks acquired PureSec, a provider of a serverless application firewall that dynamically spins up anytime a function is invoked. Behavioral analytics enabled by machine learning algorithms are applied to ensure each function only launches the specific task allowed.

The PureSec approach to securing serverless computing frameworks is extensible across AWS Lambda, Microsoft Azure Functions, Google Cloud Functions, and IBM Cloud Functions, which means cybersecurity teams won't have to master different cybersecurity frameworks for each serverless computing framework their organization decides to adopt.

CLOUD-NATIVE SECURITY AND THE RISE

With three major forms of cloud-native computing abstractions to contend with, cybersecurity isn't going to get simpler any time soon. Cybercriminals have already shown themselves to be adept at compromising cloud-native computing environments. For example, cybercriminals are increasingly scanning for unprotected Docker APIs that would allow them to hijack compute resources to mine cryptocurrencies, a process known as cryptojacking.

While most organizations are going to approach any new platform with a certain amount of natural trepidation, one of the best things about the rise of cloud native computing is it presents organizations with a unique opportunity to embrace best DevSecOps processes. The rise of the DevSecOps movement is largely being driven by the need to find a way to better secure what is becoming a complex, highly distributed IT environment. Given the already chronic shortage of cybersecurity professionals, there's no way cybersecurity teams on their own will be able to secure both emerging platforms such as Kubernetes and existing legacy IT environments.

DevSecOps addresses that issues by defining a set of best practices for shifting more of the responsibility for ensuring security controls are implemented within applications on to the shoulders of developers. Cybersecurity teams will still need to define those controls and validate that they have been implemented. The opportunity now is to foster collaboration between cybersecurity teams and application developers to collaboratively define those DevSecOps processes within the context of a continuous integration/ continuous deployment (CI/CD) environment. Each test of an application has to verify the appropriate

OF DEVSECOPS

cybersecurity controls have been implemented. Each new vulnerability discovered needs to be addressed as part of ongoing updates being made to the application. The challenge is to achieve that goal in a way that doesn't place dramatically slow the rate at which modern applications can be developed.

Achieving that goal will require organizations to be able to first proactively collect data across the entire IT environment and then use that data to inform automation frameworks infused with machine learning algorithms to prescriptively activate the controls anytime an anomaly is detected and verified. The goal now is nothing less than leveraging best DevSecOps process to implement a Zero-Trust framework for ensuring cybersecurity across heterogeneous IT environments in a way that can still be centrally managed.

To get started down that DevSecOps path, organizations need to be able to regularly monitor:

CONTAINER IMAGES: The container images that developers often download from a central hub can be infected with malware. There needs to be a mechanism for certifying that container images have not been compromised before a developer unwittingly downloads them.

VULNERABILITIES: Just because the container is secure it's doesn't necessarily follow that everything in that container can be trusted. Developers regularly make use of a variety of libraries within an application, but they don't always check to make sure whether new vulnerabilities within those libraries have been discovered.

CONFIGURATIONS: Like any piece of software, a container can be subject to being misconfigured in a way that leaves a door open for cybercriminals to exploit. This can be especially problematic when the host or run-time environment a container is running on has been misconfigured.

Each of these issues of course, always been a long-standing concern for cybersecurity professionals. The difference now is rather than tackling each of these tasks in isolation, they become elements of a continuous DevSecOps process that results in a much more secure IT environment.

THE CASE FOR UNIFICATION

The need for a cybersecurity framework that can be applied to virtual machines, containers, and associated serverless computing frameworks becomes more obvious with each passing day. Organizations of all sizes will be running a mix of legacy and emerging cloud-native applications well into the end of the next decade. The need for a cybersecurity platform through which IT organizations can build, deploy and automatically maintain cybersecurity policies across all these environments via common console is becoming crucial.

As the attack surfaces continue to expand along with the volume of application code deployed on those platforms, the only way cybersecurity teams and their application developer colleagues will be able to achieve that DevSecOps goal is to rely more on automation. It is simply not going to be possible for any human to keep pace with the rate of change occurring across cloud-native computing environments without relying on automated cybersecurity frameworks.

Palo Alto Networks has already invested millions of dollars developing a Prisma framework to automate the management of cybersecurity within legacy monolithic application environments. Following the acquisitions of Twistlock and PureSec, the Prisma platform is being extended to add support for cloud native computing applications based on containers and serverless computing frameworks. Prisma will be the most comprehensive cybersecurity lifecycle management platform ever built to specifically enable organizations to embrace best DevSecOps processes. Now more than ever, cybersecurity is everyone's responsibility.

CONCLUSION

As is always the case with IT, tools are only one part of the cybersecurity equation. The rise of cloud-native computing platforms will require fundamental changes to cybersecurity processes that will impact every member of an IT team. Platforms ranging from traditional virtual machines to emerging serverless computing frameworks will soon be routinely employed.

Rather than trying to forestall the transition to cloud-native computing platforms, cybersecurity professionals should embrace them. Like most things that might initially be intimidating, confidence always comes when IT professionals face new situations and use cases. It's only then that IT professionals tend to acquire and master the skills required to truly succeed.

Interested in learning how your organization's infrastructure can be more secure than ever before? Visit *www.paloaltonetworks.com/cloud-security.*


PRISMA™
BY PALO ALTO NETWORKS