Hackers Are Coming For Your Cloud-Based Applications

Cloud native development and cloud ubiquity create need for a fundamentally new approach to application security

“Cloud First” Is the New Normal for Application Deployment

Cloud adoption keeps growing in virtually every industry. A recent survey found that at least 75% of respondents work for organizations that use clouds, with the most cloud-proactive industries being retail and ecommerce, finance and banking, and software.[1] Another survey found that more than 85% of organizations will embrace a cloud-first principle by 2025 and will not be able to fully execute on their digital strategies without the use of cloud-native architectures and technologies.[2]

The shift to cloud-first strategies is poised to revolutionize the way companies do business. Moving applications to the cloud reassigns infrastructure tasks from in-house IT groups to cloud service providers (CSPs). Freed from time-consuming “keep the lights on”activities, scarce and often highly compensated IT resources can be redirected to focus on innovation at the application level, driving business growth, opening new markets, and improving the customer experience.

Hybrid/multi-cloud architectures increase agility and boost competitiveness by presenting organizations with a broader range of technology options compared to standalone on-premises data centers. Rather than follow three-year technology refresh cycles common in on-premises deployment, public cloud providers have a strong incentive to provide their customers with access to the most advanced computing, storage, and networking technology soon after these offerings are introduced. As a result, IT planners can respond rapidly to marketing opportunities and gain advantage over competitors that don’t have the same cloud-driven flexibility.

In the cloud, geography is no longer a barrier to service delivery. All major CSPs provide local access virtually everywhere in the world. This means organizations can move service delivery closer to their own customers, boosting responsiveness and service availability—while also more easily meeting data residency requirements and local regulatory compliance.

The Disappearing Perimeter Creates Security Challenges

The concept of a traditional security perimeter separating the inside and outside of the network has been challenged for some time. Today’s modern architectures make it even harder to define a perimeter. In hybrid/multi-cloud environments, much of your architecture consists of clouds run by your service providers, requiring constant movement of information across the internet. In addition, external integrations with third parties in your supply chain can compromise security – it really is true that a chain is only as strong as its weakest link. The eroding perimeter has led to the development of Zero Trust, a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

Cloud Opportunity Lies in a More Virulent Threat Landscape

Legitimate businesses are not the only ones excited by the opportunities of the cloud revolution – cyberattackers are taking note as well. In fact, 40% of businesses have already suffered at least one cloud-based data breach, a remarkable percentage given the short duration of the cloud era.[3] The victims of these successful attacks are not just cloud novices, but rather established enterprises with considerable investment and expertise in network security. Here are four kinds of attacks that threaten cloud deployments.

[1] Mike Loukides, “The Cloud in 2021—Adoption Continues,” O’Reilly research report, 2021.

[2] “Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences,” Gartner press release, November 2021.

[3] Maria Henriquez, “40% of organizations have suffered a cloud-based data breach,” Security Magazine, October 29, 2021.

Command and Control Attacks Let Hackers Take Over

Data is the currency of the dark web, the part of the internet that is not visible to search engines and requires the use of an anonymizing browser called Tor to be accessed. Stolen information can be easily monetized on web sites that contain lists of stolen personal data such as credit card numbers, social security numbers, and bank account usernames. Attackers only need a foothold within the network—as simple as getting one user to click on a link in a phishing email—to launch malware that gives command and control (commonly called C2) to the external attacker. C2 attacks rely on the ability to move laterally within the network to locate and exfiltrate valuable information.

Ransomware Takes Organizations Hostage

Another way hackers monetize a network breach is to encrypt the information and demand payment of a ransom to provide the decryption key. Malicious actors continue to adjust their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay, and publicly naming and shaming victims as secondary forms of extortion. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics such as deleting system backups to make restoration and recovery more difficult or infeasible for impacted organizations (see figure 1).[4]

Supply chain attacks

Supply chains often are easier to access than other potential network entry points. A successful supply chain breach can affect other organizations in the same supply chain, increasing the attacker's potential profits.

Double-extortion ransomware

In a double-extortion ransomware attack, the hacker not only encrypts the targeted information but also exfiltrates those files. If the ransom is not paid (and sometimes even if it is), the hacker can sell the stolen information on the dark web or publish it online.

Ransomware as a service

Ransomware as a Service (RaaS) is a variation of the SaaS business model, complete with 24/7 support and user forums. Hackers can buy an RaaS kit for as little as $40 to initiate ransomware attacks with relatively little technical knowledge.

Figure 1: Recent trends in ransomware attacks

Distributed Denial of Service (DDOS) Attacks Disrupt Users

Cyberattacks can also be used by bad actors or state actors to disrupt the operation of legitimate websites. The basic technique is to flood the website with spurious HTML requests, overwhelming the web servers and creating bottlenecks for legitimate users. DDOS attacks are frequently used by state actors to disable service delivery, degrading the user experience for citizens and creating dissatisfaction with government agencies. Unscrupulous enterprises can use DDOS attacks to disable a competitor's business-critical applications and thereby affect employee productivity.

Cryptojacking Siphons Resources

The bitcoin gold rush fueled a new kind of cyberattack known as cryptojacking, in which attackers gain unauthorized control of computing resources, which are then used to mine bitcoins and verify blockchain transactions. Like malware, cryptojacking attacks start with an intrusion, then move laterally to locate available computing resources such as graphic processing units (GPUs).

While often flying under the radar in many CISO's minds, cryptojacking is surprisingly common. In the European Union Agency for Cybersecurity's (ENISA) annual report, cryptojacking was the third most prevalent cybersecurity threat in 2021. In the same year, Google's Cybersecurity Action Team found that 86% of compromised cloud platforms resulted from cryptojacking.

[4] "Ransomware FAQs," Cybersecurity and Infrastructure Security Agency (CISA), accessed November 17, 2022.

Cloud and Network Teams See the Same World Through Different Lenses

Shifting to cloud-first strategies has profound implications for security, starting with application development. Security is not always top of mind for cloud developers. Their mandate is to develop and release—as quickly as possible—applications that deliver business value. Yet it can be difficult to deliver value when applications are susceptible to attack. A recent survey found that only 14% of cloud developers listed application security as a top priority, while two–thirds routinely left known vulnerabilities and exploits in their code.[5]

To remedy these vulnerabilities, the network security group must have a seat at the table. However, organizational barriers and attitudes can get in the way. Network security often arrives late in the development lifecycle, limiting the range of available options. Furthermore, when the network security team recommends a security solution such as a next-generation firewall (NGFW), they bear the burden of proof to show that their recommendations will not slow the business down or delay time to value. At the same time, the development group can be tempted into thinking the native security provided by cloud service providers is "good enough," so why bother adding more? This situation is particularly frustrating because the network security group is responsible for preventing breaches, compliance failures, and other security issues but does not have the authority—and sometimes knowledge—to implement necessary security changes to the cloud (or CI/CD) application development process. In addition, many of today's cloud developers lack the deep knowledge of modern sophisticated cyberattacks and their ability to morph and thereby evade traditional security measures.

Cloud-Native Techniques Transform Application Development

Another trend that influences hybrid/multi-cloud security is the profound shift in the way that applications are developed, secured, and delivered. In the traditional on-premises data center environment, developers write the code for applications, IT teams build and maintain the underlying infrastructure that runs those applications, and then security teams apply the necessary security. In this siloed model, software engineers work within the constraints of infrastructure and operating systems. Security managers have the final word on what can and cannot be done in the application development process—they are the arbiters of application security.

That model has been turned on its head with the advent of cloud-native development, a method of building applications that take full advantage of the unique characteristics of cloud platforms. Compared to traditional development methodologies, cloud-native development empowers software engineers to create highly scalable applications with unprecedented flexibility and resiliency that run on any cloud, public, private, or hybrid. Cloud-native technologies have transformed every aspect of application development, including the hosting platform, the code architecture, and the/integration/delivery methodology (see figure 2).

[5] "Where does secure code sit on the list of development team priorities?," Secure Code Warrior, November 7, 2022.

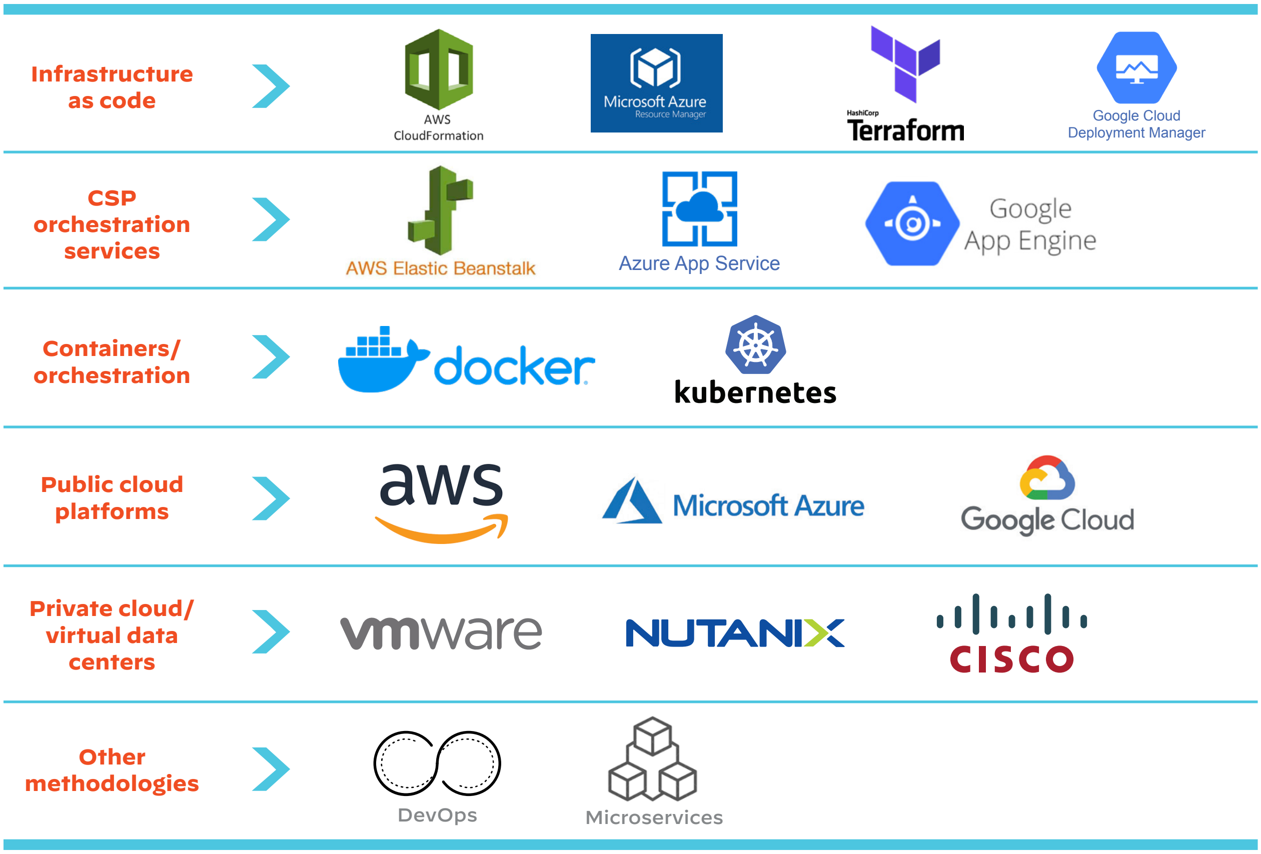

Figure 2: Typical components used in cloud-native application development

One particularly disruptive change in development methodologies is the use of vendor-specific orchestration services such as AWS Elastic Beanstalk, Azure App Service, and Google App Engine. With these tools, the developer simply uploads the application code and the orchestration service automatically handles the deployment, from capacity provisioning, load balancing, and auto scaling to application health monitoring. While this level of automation greatly simplifies life for the developer, it also compounds the problems of network security in hybrid/multi-cloud architectures. As the speed of development continues to accelerate, IT security teams struggle to keep up with the dynamic nature of workloads running on virtual machines and within containers.

US SIGNAL

CASE STUDY
US Signal Cuts Firewall Provisioning Time By 97%
Read the case study here.

Architectures Move From Centralization to Hyperconnectivity

Why are cloud architectures so vulnerable to these kinds of attacks? One reason is the evolution of the infrastructure itself, from centralized data centers to dispersed, hyperconnected hybrid/multi-cloud environments, which makes it difficult to design an effective security strategy.

In the centralized model, a gateway firewall located at the data center edge secures north-south traffic for both local applications and software-as-a-service (SaaS) applications. Additional physical firewalls can be employed to enhance security for individual subnets and prevent east-west threat propagation. Network security teams have complete visibility into the network architecture and can ensure that firewall policies are consistent and effective using centralized tools.

However, this architecture is somewhat inefficient for remote workers and branch offices because SaaS traffic has to pass through the data center—a practice called hairpinning—thus introducing significant application latency and degrading performance. In response, many organizations have installed firewalls at remote locations, smaller physical appliances similar to the data center firewalls. Despite the use of remote firewalls, the attack surface is still relatively small and easily defined (see figure 3).

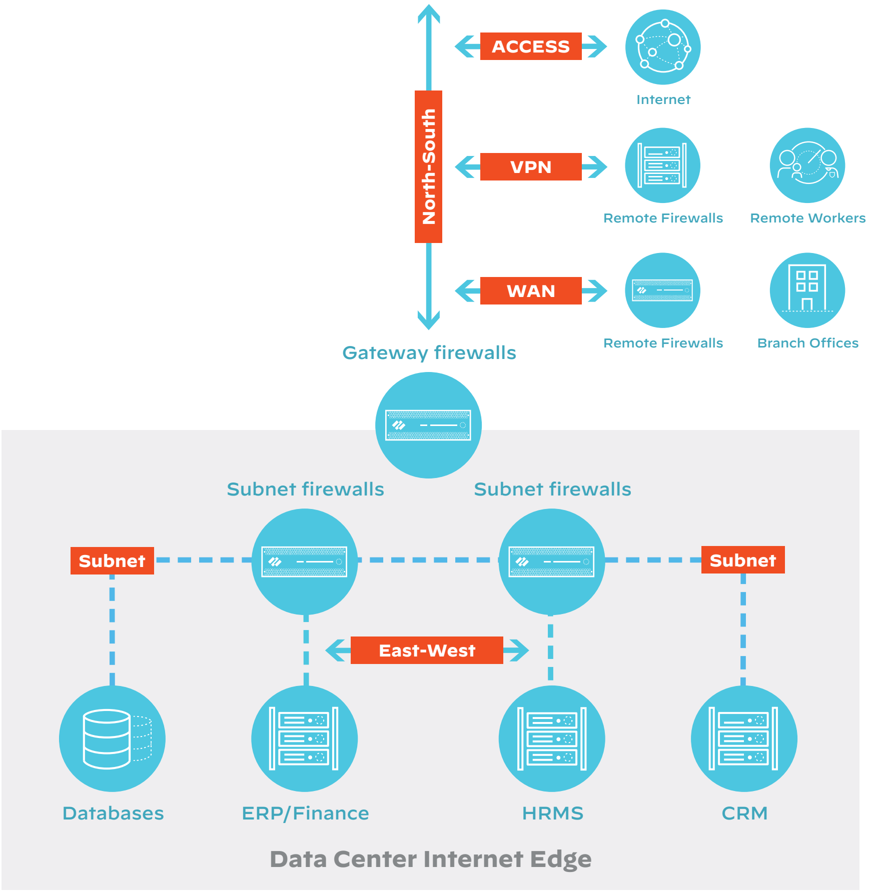

Figure 3: Firewall security in traditional data center architecture

The adoption of hybrid/multi-cloud architectures essentially explodes this model of security. For one thing, data centers are evolving into private clouds in which local applications are hosted on virtual machines, not directly on the physical servers. Other applications run in public clouds in virtualized environments, often using containers and Kubernetes orchestration. In this model, interconnections dominate the architecture, making the attack surface larger and more difficult to define (see figure 4).

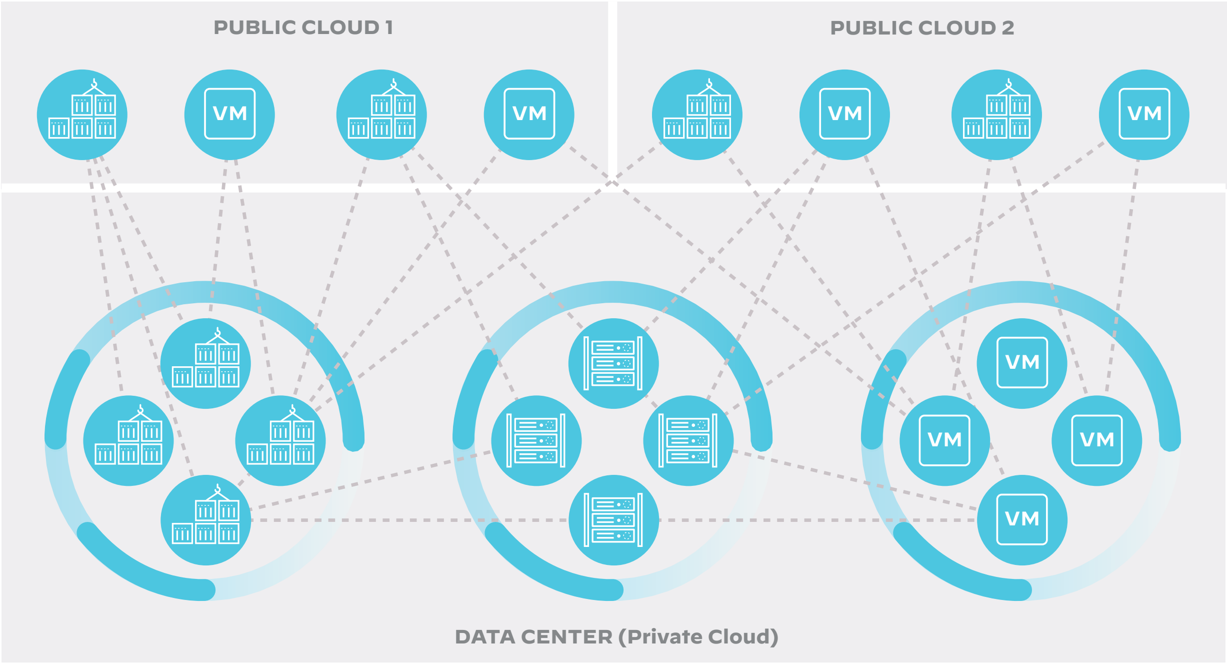

Figure 4: Hyperconnected enterprise infrastructure

CSPs and Customers Share Security Responsibilities

Visibility and control are quite different in public clouds. Unlike on-premises deployments, public clouds rely on a shared responsibility model in which the CSP secures the infrastructure, such as servers, storage, and network components. Customers, however, must secure the applications and data they place in the cloud, yet parts of the CSP's infrastructure are invisible to the customer. The challenge of this division of responsibility is to avoid security gaps where the customer and the CSP meet—gaps that attackers are only too ready to exploit, such as marginally effective security solutions (see figure 5). For example, the CSP provides the networking functionality, but the customer must manage the configuration of security-related networking components.

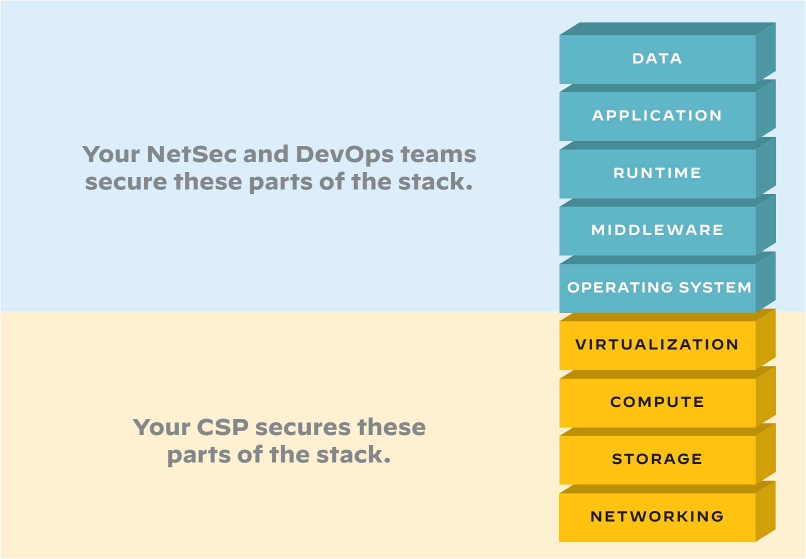
Your NetSec and DevOps teams secure these parts of the stack.
DATA
APPLICATION
RUNTIME
MIDDLEWARE
OPERATING SYSTEM
Your CSP secures these parts of the stack.
VIRTUALIZATION
COMPUTE
STORAGE
NETWORKING

Figure 5: Shared security responsibility

In hybrid/multi-cloud architectures, the big picture is even harder to see because each cloud is architected and managed differently, which creates blind spots between multiple CSPs. For example, security logs reside in multiple locations in multiple formats, making it difficult to consolidate and analyze threat information in real time. To complicate matters further, companies frequently lack the right security oversight tools. Less than one-third (32%) of organizations[6] are using security tools specifically designed for hybrid/multi-cloud infrastructures, so security managers must shift between multiple monitoring tools in their attempt to piece together a complete understanding of their environments. All of this sets up organizations for human error and delayed responses to security threats.

The Cloud Complicates Compliance

The shared responsibility model is just one aspect of hybrid/multi-cloud architectures that can make it difficult to achieve compliance. The service provider implements some of your required controls and therefore must provide evidence that you can incorporate into your audits. Fortunately, you can often "inherit" controls from the service provider, which actually streamlines compliance as long as the documentation is in place. The items the CSP does not oversee, such as applications, are your responsibility for auditability.

Another compliance challenge can be found in the way hybrid/multi-cloud architectures often span multiple geographies and jurisdictions. This can bring into play requirements for data locality and data protection regulations such as the European Union's General Data Protection Regulation (GDPR), as well as regulations specific to individual states in the United States.

[6] "State of the Cloud Report," Flexera, 2022.

Zero Trust Holds the Key to Cloud Security

Zero Trust is the conceptual shift that makes it possible to secure today's complex hybrid/multi-cloud architectures. What is Zero Trust? For network security professionals, Zero Trust represents a shift in the way they must now think of security. The traditional security model essentially divides the world into untrusted and trusted regions using a perimeter firewall. The main goal is to keep the bad actors out of the network and only allow the trustworthy users inside the network (see figure 6).

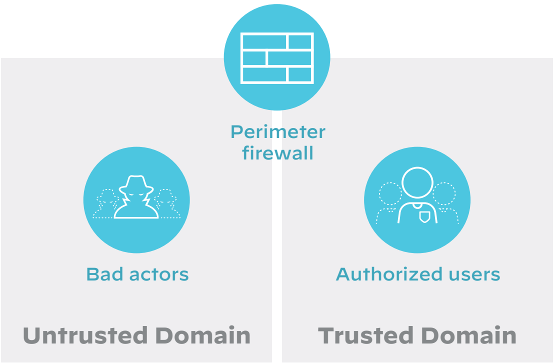

Figure 6: The traditional approach to network security

Zero Trust moves beyond this worldview by assuming that bad actors can be anywhere. Every person requesting network access is considered an unknown, and the security practice calls for a range of verified traffic identification to determine whether to grant access or not. Trust is not assumed but rather earned—literally every time a user, application, or device to access a network service (see figure 7).

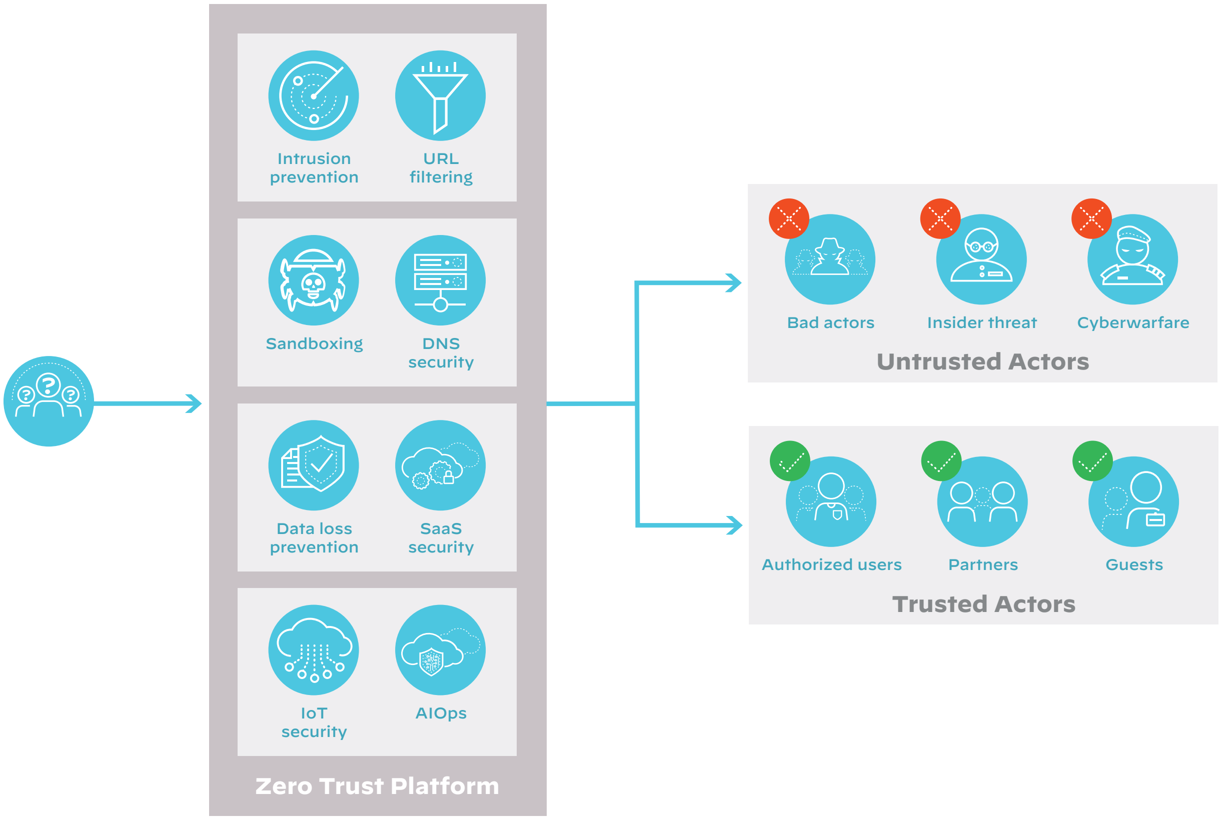

Figure 7: The Zero Trust approach to security

A more formal definition of Zero Trust is:

> *Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates these three core principles: 1) All entities are untrusted by default; 2) least privilege access is enforced; and 3) comprehensive security monitoring is implemented.*[7]

BARRETT
STEEL LIMITED

CASE STUDY
UK Steel Firm Supports 800% Increase In Remote Workers with Zero Trust
Read the case study here.

The Right Form Factors for the Job Move Beyond Physical Firewalls

Faced with virtualized, decentralized environments, a new approach to security is needed, one that is quite different from the data center world. In a traditional data center, the network nodes are physical locations that you can see and touch. Adding a physical firewall requires tangible activities, such as rearranging cables and then setting key configuration parameters with a command line interface.

In all clouds, network nodes are virtual entities embedded within the CSP's infrastructure or your own virtualized environment. In addition, the use of containers creates another layer of abstraction, complicating firewall deployment even further. Physical firewalls cannot be deployed close enough to these workloads, and consequently cannot provide effective security capable of preventing threats from moving laterally between virtual or container workloads.

The answer for cloud environments is software firewalls, an emerging security technology that promises to revolutionize cloud security in the same way that the physical firewall revolutionized network security. Software firewalls embody the same next-generation firewall (NGFW) technology as physical firewalls in form factors that match the needs of hybrid/multi-cloud environments and modern cloud applications. Virtual firewalls can be associated with virtual machines and thereby secure virtualized workloads in a way that physical firewalls cannot. To secure Kubernetes-managed container workloads, a special kind of software firewall designed for containerized environments is required. Newer additions of software firewalls for workloads in the public cloud include fully managed firewall-as-a-service that provide all the security depth as a NGFW with the ease of cloud-native deployment (see figure 8).

[7] David Holmes and Jesse Burn, "The Definition Of Modern Zero Trust," Forrester blog, Jan 2022.

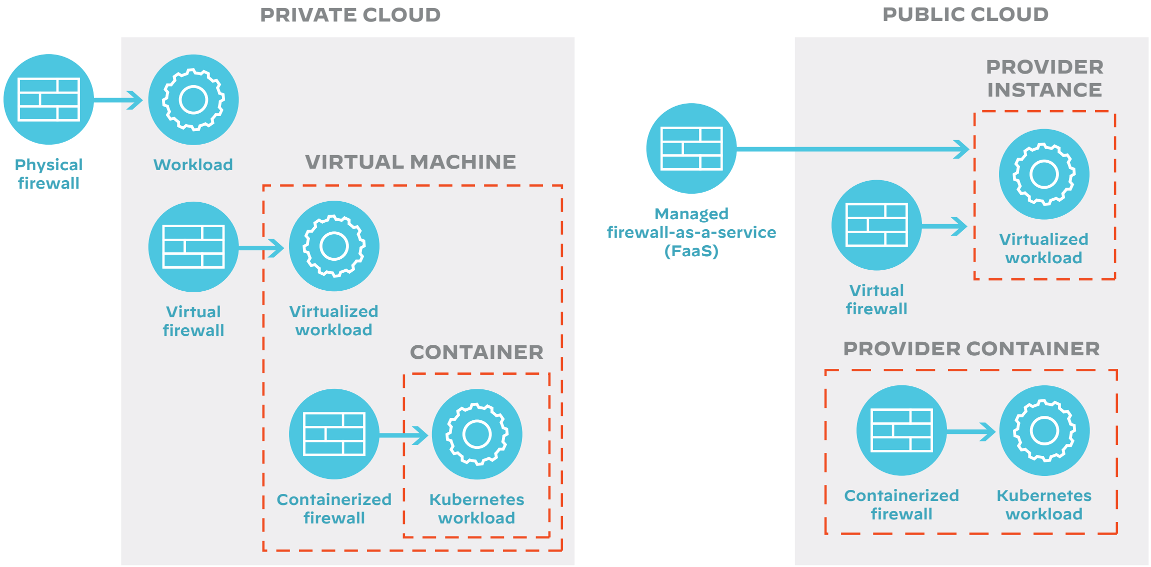

Figure 8: Software firewalls in hybrid/multi-cloud security

CASE STUDY
DISH Secures 5G Network with NGFWs from Palo Alto Networks
Read the press release here.

Software Firewalls Meets a Range of Cloud Needs

To secure today's complex hybrid/multi-cloud architectures, cloud architects and network security managers need an integrated solution that can secure any network based on any combination of public clouds, private clouds, virtualized data centers, and remote locations. As an integral part of Palo Alto Networks Network Security Platform there is just such a solution: Palo Alto Networks Software Firewalls.

Palo Alto Networks software firewalls are built from the ground up to support Zero Trust. They combine artificial intelligence, machine learning, and software automation with threat research from the Palo Alto Networks Unit 42 team to protect applications from cyberattacks with agile, best-in-class network security for all clouds—public, private and hybrid. The platform features deep integration with clouds and virtualization technologies, automated DevOps deployment and scaling, and centralized management for all private, public, and hybrid/multi-clouds (see figure 9).

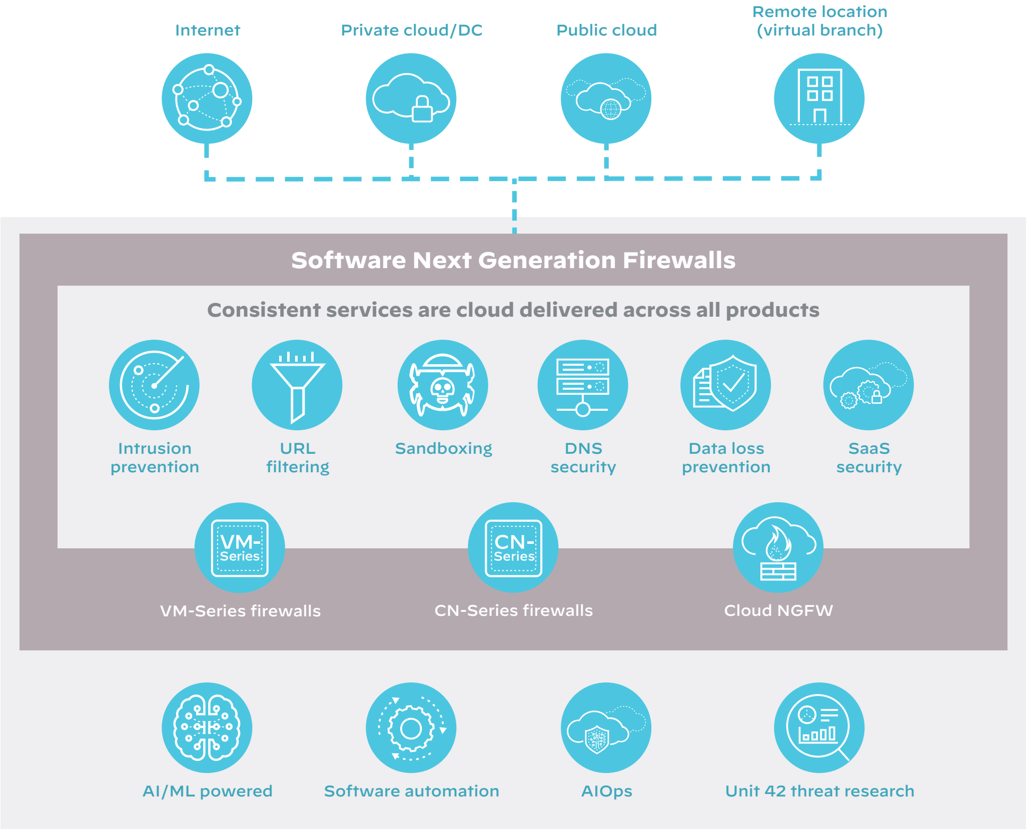

Figure 9: The Network Security Platform from Palo Alto Networks

Palo Alto Networks software firewalls come in three proven NGFW cloud form factors (see figure 10), each of which is described in more detail below.

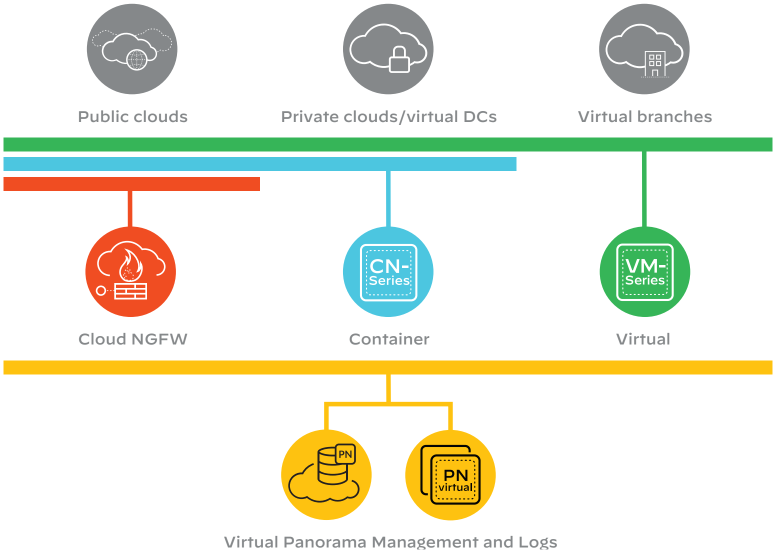

Figure 10: Software firewalls in the Network Security Platform from Palo Alto Networks

VM-Series Virtual Next-Generation Firewall

The software firewall workhorse is the VM-Series virtual firewall, which secures workloads anywhere in the hybrid/multi-cloud environment, including public and private clouds, virtualized data centers, and software-defined branch environments. The VM-Series virtual firewall features automated deployment, built-in scalability, and deep integrations with all major clouds hypervisors, and software-defined networks, protecting your applications wherever they reside. The VM-Series virtual firewall can be flexibly procured using Software NGFW Credits or directly from CSP marketplaces with pay-as-you-go usage.

Research Shows 115% ROI with VM-Series Virtual Firewalls

Palo Alto Networks VM-Series virtual firewalls pay for themselves. According to a Forrester Consulting study, these virtualized NGFWs can provide a significant 115% return on investment (ROI) over three years with a six-month payback period. Read the full study here.

115%

ROI
6-month playback

30%

Reduction
in time achieving a proper security posture

CN-Series Container Firewall

Container workloads are difficult to secure with traditional firewalls because they are embedded in the Kubernetes environment. The Palo Alto Networks CN-Series container firewalls go where the need is. Deployed on Kubernetes clusters, the CN-Series container firewall protects against known and unknown threats seeking to move laterally between container workloads and other applications in the cloud environment. The CN-Series container firewall scales dynamically to extend protection as your infrastructure grows without compromising DevOps speed or agility. Like the VM-Series virtual firewall, the CN-Series container firewall can be procured using Software NGFW Credits and from integrated CSP marketplaces.

Cloud NGFW Managed Firewall Service

The newest member of the Palo Alto Networks of software firewalls is the Cloud NGFW Managed Firewall Service. Cloud NGFW provides a flexible option for deploying application-level (Layer 7) security as a managed service. This versatile NGFW offers cloud-native ease of deployment with the security of a modern NGFW. It integrates with a CSP's native user experience and can be deployed in just a few clicks. Cloud NGFW is available on the AWS marketplace and as a white-labeled service offered by Google Cloud Platform (Google Cloud IDS) and Oracle Cloud Infrastructure (OCI Network Firewall).

Panorama Network Security Management

Panorama network security management streamlines firewall management with easy-to-implement, consolidated policy creation and centralized management features. Now you can easily set up and control firewalls centrally with industry-leading functionality and an efficient rule base, and gain insight into network-wide traffic and threats. These policies provide consistent security across all clouds with no gaps in environments or applications—policies follow applications, while centralized log collection provides easy reviews, audits, and security history.

Stop Even The Most Sophisticated Threats In Real Time

Palo Alto Networks NGFWs provide the Zero Trust baseline capabilities to fully identify applications traffic using built-in identification features such as App-ID, User-ID, Device-ID, and Content-ID. Zero Trust enforcement can be delivered for inbound, outbound, lateral (East-West), and segmented/micro-segmented traffic.

Prevent Known/Unknown Threats: Cloud Delivered Security Services (CDSS), including advanced threat prevention, advanced sandboxing, advanced URL filtering, DNS security, data loss prevention, and IoT security, offer agile protection for business-critical applications and databases while meeting compliance requirements.

Industry's First ML-Powered NGFW: ML-Powered NGFWs identify variants of known attacks as well as unknown cyberthreats using ML models, defending against up to 95% of unknown inline threats.

Least Privilege Access and Continuous Trust Verification: Palo Alto Networks' components App-ID, User-ID, and Device-ID massively reduce risk of attack, decrypt SSL/TLS traffic, and prevent malware from entering the cloud in disguise.

Protect All Clouds with Agility—Private, Public, Hybrid

With Palo Alto Networks software firewalls, your staff now has the ability to truly protect any network, all clouds, and any virtualized environment with deep integrations that accelerate deployments and shorten the time for consistent hybrid/multi-cloud security posture. Now you can have the security foundation to protect any application and workload running anywhere your business needs across the enterprise. Palo Alto Networks software firewalls include deep integrations with all major CSPs, Kubernetes containers, and SDN networks and hypervisors (see table 1).

Table 1: The Network Security Platform Support for Vendor Offerings

Category	Premium
Cloud Service Providers	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud, Alibaba Cloud, IBM Cloud
Containers	VMware Tanzu, Rancher, Amazon EKS, Azure Kubernetes Services (AKS), Google Kubernetes Engine, OpenShift
SD Networks and Hypervisors	Nutanix Flow, VMware NSX, Cisco ACI, Openstack, VMware ESXi, Linux KVM, Microsoft Hyper-V, Nutanix AHV

Get Automated Best-In-Class Security With Agility

Palo Alto Networks software firewalls automate key processes such as deployment, scaling, and policy changes, so your staff does not have to spend hours and hours doing routine manual operations. Now your DevOps team can securely accelerate cloud migrations with familiar cloud automation and orchestration tools, including AWS CloudFormation, Azure ARM Templates, Terraform, Ansible, Kubernetes, and Helm Charts. Core network security platform features automate policy changes with Dynamic Address Groups (DAG) and Application Tagging that enable policy migration and policy enforcement as cloud applications dynamically scale up and down within your cloud environments.

Why Palo Alto Networks?

The world of network security has changed for good, and, ready or not, your security strategy has to change, too. Who can you turn to help you navigate this new and challenging landscape?

Palo Alto Networks has been helping security professionals like you meet these challenges for nearly two decades, through a succession of technology innovations and marketplace excellence. Our execution and vision is recognized by analysts. The publication of the 2022 Gartner® Magic Quadrant™ for Network Firewalls marks 11 straight years that Palo Alto Networks has been recognized as a leader in the industry (read the press release here).[8] Forrester has also acknowledged our market leadership in its most recent Forrester Firewall Wave™: Enterprise Firewalls Q4 2022 report, calling Palo Alto Networks "a leader with strong current offerings, strategy, and market presence" (read the blog post here).[9]

Take the Next Step Toward Securing Your Future

Securing hybrid/multi-cloud architectures poses challenges that traditional security solutions are not designed to overcome. Specifically, the physical firewall—a critical security tool for many network applications—is not the optimum choice when it comes to modern hybrid/multi-cloud infrastructures and cloud-native development methods. Palo Alto Networks software firewalls go where the workloads are—on virtual machines, containers, and service provider instances in the cloud.

As the key component of the Network Security Platform, software firewalls from Palo Alto Networks secure your enterprise cloud and virtual infrastructure with always-on validation and security that works the way your developers work and anywhere your applications and critical business data resides. In short, Palo Alto Networks empowers your security and cloud teams to do what other solutions cannot do—protect any cloud with agility. To learn more, get a personalized demo and discover how to secure cloud-base infrastructure.

[8] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[9] The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com