Your Hybrid Infrastructure Is Under Attack

What you need to do to secure your distributed, interconnected hybrid cloud environment

The New Security Math for Hybrid Infrastructure

Cloud usage in general is on the rise, and so is hybrid cloud. A recent survey found that 94 percent of U.S. enterprise infrastructure decision-makers are using the cloud, with the majority being hybrid or multicloud.[1] One key reason for the popularity of hybrid models is flexibility, which allows IT teams to:

- Keep data in the particular environment (public or private cloud) best suited for that information.
- Easily move applications and data within the hybrid architecture as needs change.
- Scale in either direction with no capital investment or compromised ROI due to early decommissioning.
- Develop new cloud native development workflows and application architectures with agility.

However, the very nature of hybrid infrastructures presents network security challenges due to the exponential growth in complexity.

In the past, the number of interconnections and the complexity of the infrastructure essentially grew linearly as you added servers, applications, storage, and other resources incrementally (see figure 1).

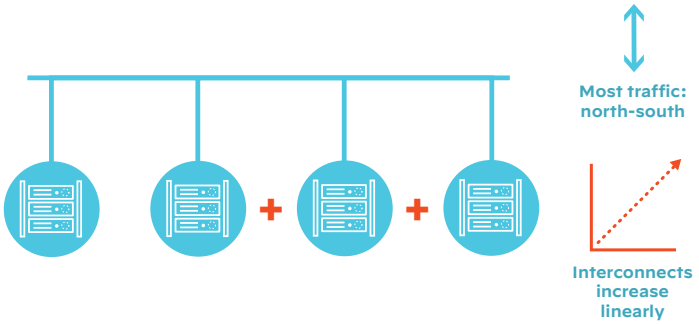

Figure 1: Complexity growth in traditional data centers

However, hybrid cloud architectures require an unprecedented level of interconnectivity — everything connects to everything. As a result, complexity grows exponentially (see figure 2).

Attack dynamics are now dramatically different as well. Massive floods of relatively simple malware attacks have given way to highly targeted, extremely sophisticated advanced threats. At the same time, increased complexity expands the attack surface exponentially by adding more entry points and paths that traverse the network.

Security platforms must adapt to this complex and dangerous new landscape — as this white paper will show. First, we examine the nature of the challenges to answer the question: Why is hybrid infrastructure security so hard? Then, the focus shifts to the solution. What are the key characteristics of a security platform designed for hybrid architectures? Finally, we test our security platform against real-world threats such as ransomware, cryptojacking, and container worms.

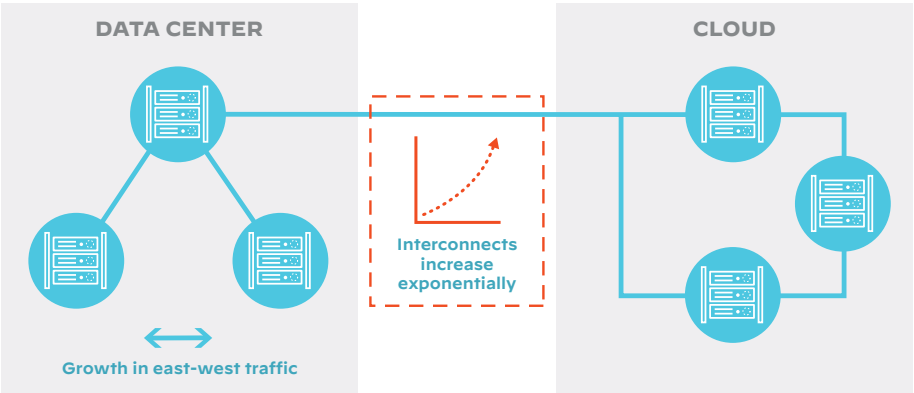

Figure 2: Complexity growth in hybrid environments

[1] "The State Of Cloud In North America, 2022: Modernization And Cloud Native Will Be The New Normal," Forrester, June 14, 2022.

Understand the Anatomy of a Modern Cyberattack

"Know your enemy." Sun Tzu's advice from the fifth century BCE in The Art of War applies equally well to today's cyberattackers. While threats vary significantly in their composition, deployment tactics, and goals, virtually all cyberattacks employ a four-stage process of surveillance, intrusion, escalation, and exploitation (see figure 3).

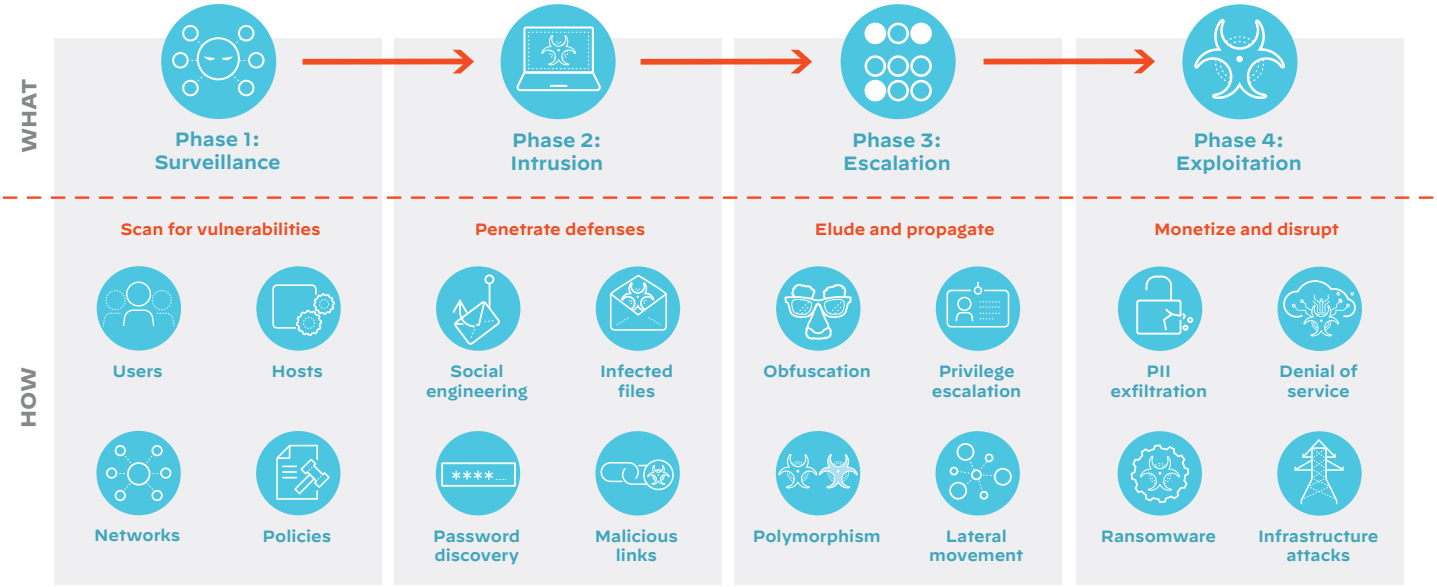

Figure 3: Anatomy of a modern cyberattack

Surveillance Sets Up the Attack

Like any good commando, the cyberattacker starts by surveilling the enemy's defenses. The goal is to know the network better than the network managers and find vulnerabilities of which the target is unaware. During this phase, the attacker gathers as much information as possible about the network, host, people, and policies.

The focus of the specific information required depends on the intended attack vector. For example, a spear phishing attack against a top executive can be made more convincing if the attacker possesses human intelligence such as home addresses, cell phone numbers, patterns of behavior, and even dark and embarrassing secrets.

When the chosen point of attack is aimed at one or more hosts, hackers seek to learn about the computer architecture (e.g., x86 or ARM), operating system, and user and group names. Network information such as IP addresses, open ports and domain names can be valuable tools for attackers as they propagate their threats. Finally, knowledge of security policies, for example, password requirements and change frequency, can be an invaluable aid in finding ways into the corporate network.

Intrusion Gets the Ball Rolling

Armed with information about the target, the cyberattacker then tries to exploit those vulnerabilities and thereby gain a foothold in the environment. The number and sophistication of potential avenues of attack is staggering. Research conducted by Unit 42, the global threat intelligence team at Palo Alto Networks and a recognized authority on cyberthreats, found that 77% of intrusions are caused by three initial access vectors: phishing, exploitation of known software vulnerabilities, and brute-force credential attacks focused primarily on remote desktop protocol (RDP).[2]

Another popular gambit is embedding malicious links in a web site, either a fake one or a legitimate site that is not secure. A recent trend impacting intrusions is the rise in human errors as a cause of breaches. In fact, 82% of breaches involve the human element: stolen credentials, phishing, or simple errors.[3]

Then there is the exploitation of unpatched servers, which remains one of the most common ways attackers gain entry into a network—and it's often overlooked. There are often times when a patch legitimately cannot yet be applied. Downtime constraints and other dependencies that prevent the patch from being deployed can provide attractive targets for attackers.

Escalation Is Designed to Overwhelm

Your organization should do everything possible to avoid breaches. However, breaches are an unfortunate fact of life today. The most prudent approach is to assume your defenses will be breached and develop a plan for identifying and mitigating attacks within the network.

In the escalation phase, the attacker's objective is to elude defenses and propagate throughout the network. One way to avoid detection is obfuscation, which involves changing the overall signature and fingerprint of malicious code to circumvent signature-based antivirus defenses. (As an interesting side note, obfuscation techniques are also used in cybersecurity defenses as a method to make users invisible, locations untraceable, and data unusable to potential threat actors.)

To spread beyond the point of entry, cyberattacks often rely on lateral movement within the network. Lateral movement starts with compromised user account credentials, which allow the threat to access other nodes and thereby move undetected through the network. Another propagation technique is privilege escalation, which exploits a design flaw or configuration oversight in an operating system or software application to gain elevated access to resources normally protected from an application or user.

Exploitation Is the End Game

Cybercrime is a business, and like any business, hackers have business objectives, either financial or disruptive. The fastest-growing form of financial attack is ransomware in which attackers encrypt valuable information and then demand money to perform the decryption — which may or may not happen after the payoff. A popular exfiltration technique is to smuggle data out through encrypted network flows, such as DNS, to avoid being detected.

Disruptive cyberattacks are a second kind of business objective. These threats aim to disrupt company operations or critical infrastructure such as power distribution for political or ideological reasons as well as financial gain through extortion. The most familiar such attack is distributed denial of service (DDoS), which floods a website with bogus requests, eating up virtually all of the available access time.

[2] "Incident Response Report 2022," Unit 42, 2022.

[3] "Verizon 2022 Data Breach Investigations Report," Verizon, 2022

Challenges of Hybrid Security

The days of securing the network at the perimeter are over. In a distributed, interconnected hybrid cloud environment, even the concept of a perimeter becomes problematic (see figure 4). For example, when you use Infrastructure as a Service (IaaS), part of the network edge is embedded in the service provider's environment and thus opaque to your security staff.

The very nature of hybrid infrastructures presents security challenges. For one thing, relatively poor visibility into virtualized infrastructure and public clouds means that security architects cannot get the information they need to fully evaluate the risk of cyberattacks. In addition, the dynamic nature of hybrid architectures poses challenges for policy consistency and compliance. The proliferation of cloud native technologies (containers, orchestration, and microservices) introduces new potential attack vectors and further complicates the security challenges.

The net result is that now threats can come from anywhere—inside or outside the organization. Nothing can be automatically trusted, everything must be secured, whether part of the perimeter or not. In a word, hybrid security must be ubiquitous.

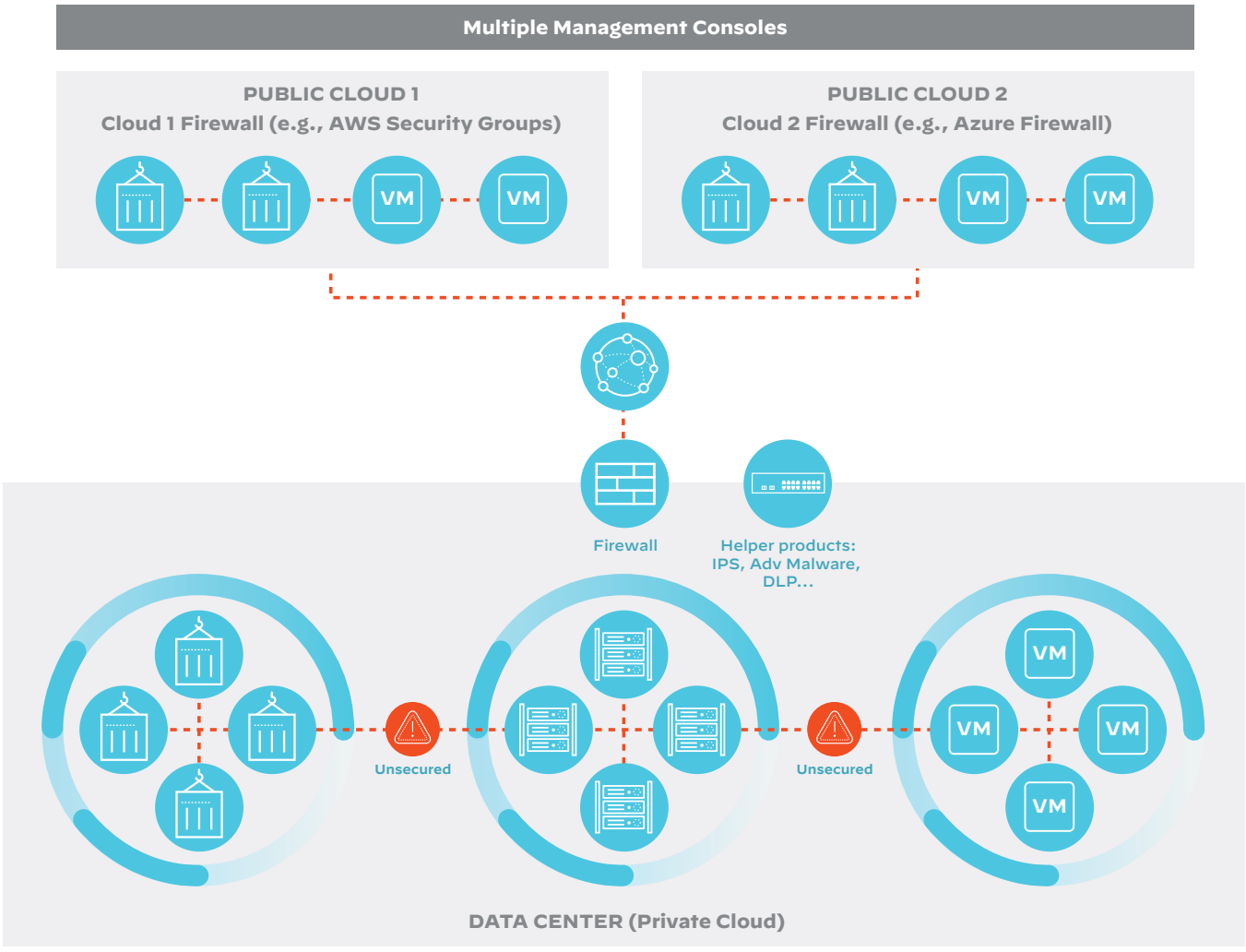

Figure 4: Highly interconnected, geographically distributed hybrid infrastructure

Cloud + On-Premises = Visibility Challenges

Every major cloud provider offers tools that provide limited visibility into their environments. However, these tools often fail to provide the level of granular visibility security managers need to make informed decisions about costs, performance, and security. Typical challenges include:

- Uncertainty about how apps map to ports
- Inability to monitor data in motion, for example, as it moves through a virtual switch
- Misconfigurations that expose data storage resources to the internet
- Lack of advanced threat prevention capabilities, such as malware analysis, URL filtering, and DNS security

The problem is compounded for businesses that use more than one cloud provider—a normal business practice today—because each provider's tools are specific to their environment. In addition, legacy tools designed for the data center in which everything was on-premises often do not have the technical flexibility to be adapted to a multi-cloud hybrid world.

Using multiple tools inevitably creates blind spots, which hamper the ability of the IT organization to effectively manage the hybrid infrastructure. Significant problems can be hiding in those blind spots, including shadow (unapproved) IT, underused resources, poor application performance, and non-compliance with industry regulations.

Attack Surface + Virulent Threats = Protection Challenges

The attack surface itself has greatly expanded with the adoption of virtualization, containerization, and cloud. This trend by itself would be cause for concern; however, the sophistication of the threats also puts additional pressure on security experts. To make matters worse, attackers are using automation and artificial intelligence to penetrate even the strongest perimeter defenses.

Complexity + Dynamic Architectures = Resource Challenges

Hybrid environments are dynamic by their nature, allowing organizations to easily add computing resources, move data based on security and compliance requirements, and control spending across clouds (see figure 5).

Yet managing these dynamic architectures can be challenging because they change faster than humans can respond in a timely way, which often make it difficult for security teams to innovate so the organization remains competitive. Relying on manual security procedures can result in inconsistent policies that compromise security and compliance and create bottlenecks.

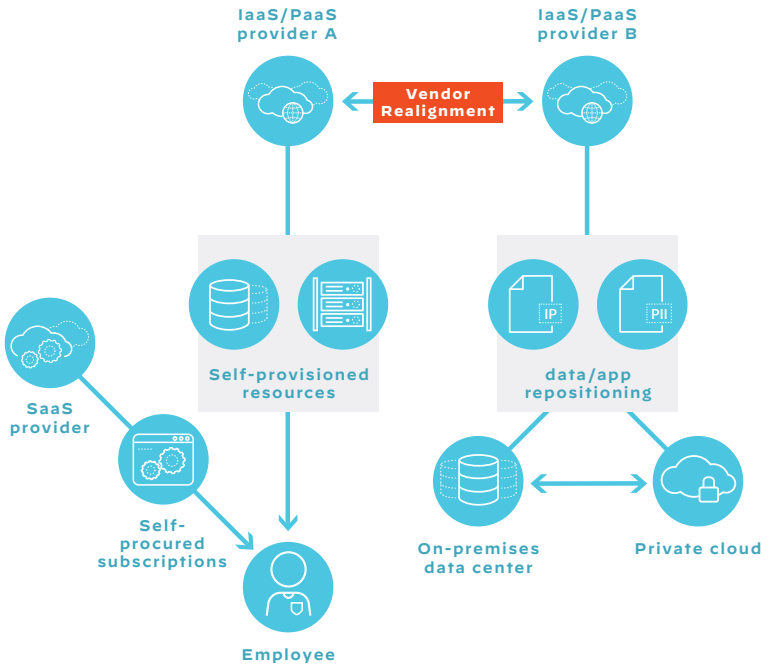

Figure 5: Typical factors driving infrastructure dynamics

Multiple Consoles + Resource Constraints = Management Challenges

Only a small percentage of hybrid environments are the result of greenfield projects. Most hybrid environments are built by stitching together resources located on-prem in virtualized and containerized environments and public cloud infrastructures. These distributed and interconnected environments make it hard for network security teams to gain consistent visibility and control. In an effort to get a clear picture of the infrastructure, security managers must bounce between multiple consoles, diverting valuable time from critical day-to-day operations and troubleshooting.

Key Requirements for Securing Hybrid Infrastructures

Each of the challenges discussed above establishes a matching requirement for a comprehensive hybrid cloud solution.

See Clearly: Consistent Visibility and Enforcement

The hybrid environment may be cobbled together but effective hybrid security cannot be — a holistic approach is required. The need is for pervasive visibility and consistent policy enforcement across the complete hybrid infrastructure. In particular, security managers need visibility to make decisions about whether to allow a request based on application content, not just the destination port.

Additionally, the solution must uniformly enforce security policies to protect applications everywhere they are hosted and be deployable in virtualized, containerized environments — both on-premises and public clouds.

Work Smarter: Intelligent Threat Protection

While signature-based security remains an important threat-prevention technique, it is no longer enough. Many of today's sophisticated exploits can easily elude these security measures. The need is for intelligent threat protection that can address myriad attack vectors and adapt to evolving threats quickly and effectively. Ideally, these protections incorporate machine learning to better identify both known and unknown threats.

Be Dynamic: Automation and Scalability

To keep up with the dynamic nature of modern environments, the entire solution must be conducive to automation. As new workloads are spun up, they should be automatically protected with the appropriate security policies. When developers build and deploy new applications and infrastructure, security measures should automatically be provisioned as part of this process. Finally, when traffic spikes the solution should automatically scale quickly to avoid service outages.

As the threat landscape continues to intensify in volume and sophistication, security teams cannot afford to spend time racking and stacking physical boxes. Instead, that time must shift to ensuring automation scripts are tuned to perfection as a way to better leverage scarce security resources.

Come Together: Centralized Management

To reduce operational complexity, security management must be centralized. Centralized management simplifies day-to-day operations and troubleshooting, and reduces the risk of gaps in security policies by eliminating the need to manage different policy sets for different parts of the environment.

How We Secure Hybrid Infrastructure

The Palo Alto Networks security platform approach consists of three components, each of which is described below: NGFW form factors, cloud-delivered security services (CDSS), and centralized management (see figure 6).

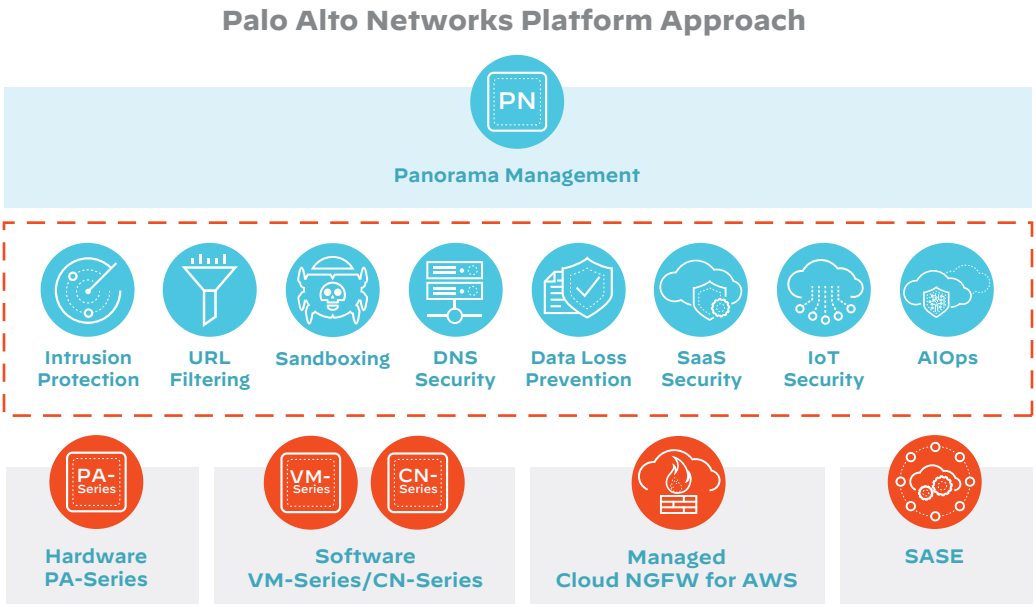

Figure 6: The Palo Alto Networks security platform

NGFW Form Factors

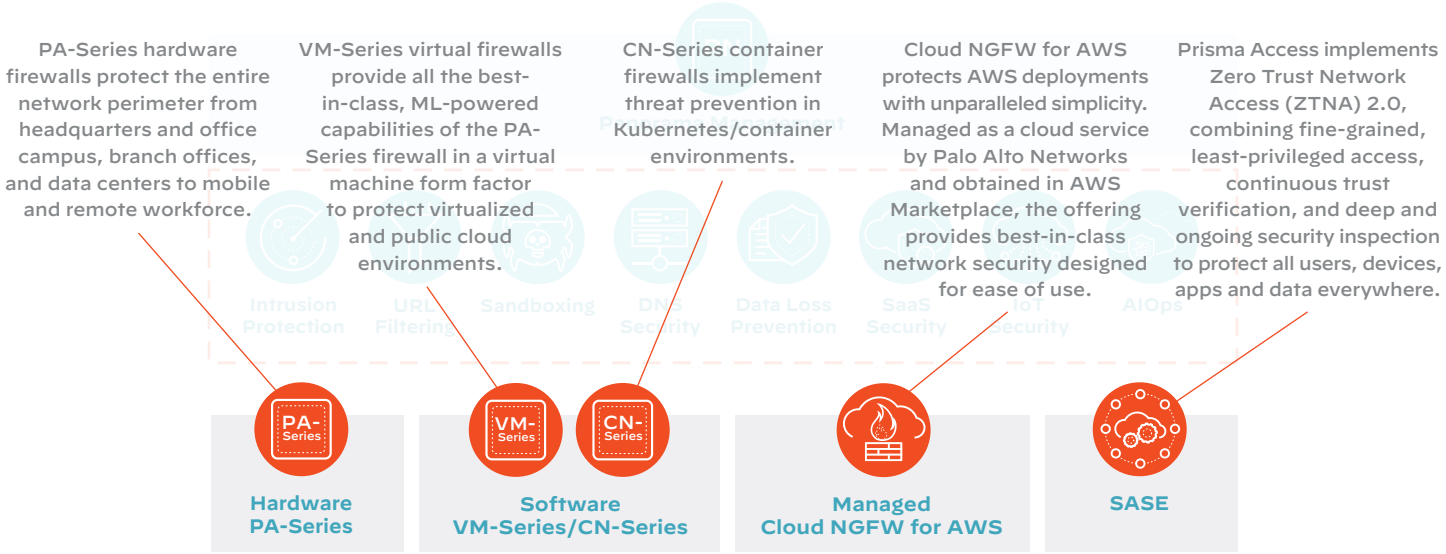

Figure 7: Components of the Palo Alto Networks security platform

Cloud-Delivered Security Services

Our cloud-delivered security services combine globally crowd-sourced intelligence and leading threat research from Unit 42 with machine learning to deliver inline protection from all known and unknown threats across myriad threat vectors. Each service can be enabled on top of hardware, software, and cloud form factors, ensuring protection during every stage of cloud transformation without needing to deploy additional agents, appliances, or sensors into the environment.

The Palo Alto Networks approach is designed for speed, a vital requirement for effective threat prevention. Threats detected in one service are analyzed, unpacked, and shared with others, then distributed globally to every customer within seconds, providing protection for every stage of the attack lifecycle. Security teams can now proactively reduce risk by automatically eliminating gaps across their entire estate, stop threats faster than the rate of infection, and take advantage of unprecedented ROI.

Management Must Span the Hybrid Infrastructure

As discussed earlier, hybrid environments can be extremely challenging to manage because of their inherent complexity and the proliferation of disparate monitoring tools. Palo Alto Networks Panorama™ offers easy-to-implement and centralized management features to gain insight into network-wide traffic, logs, and threats. With Panorama, IT teams can reduce complexity by simplifying configuration, deployment, and management of the firewall platform.

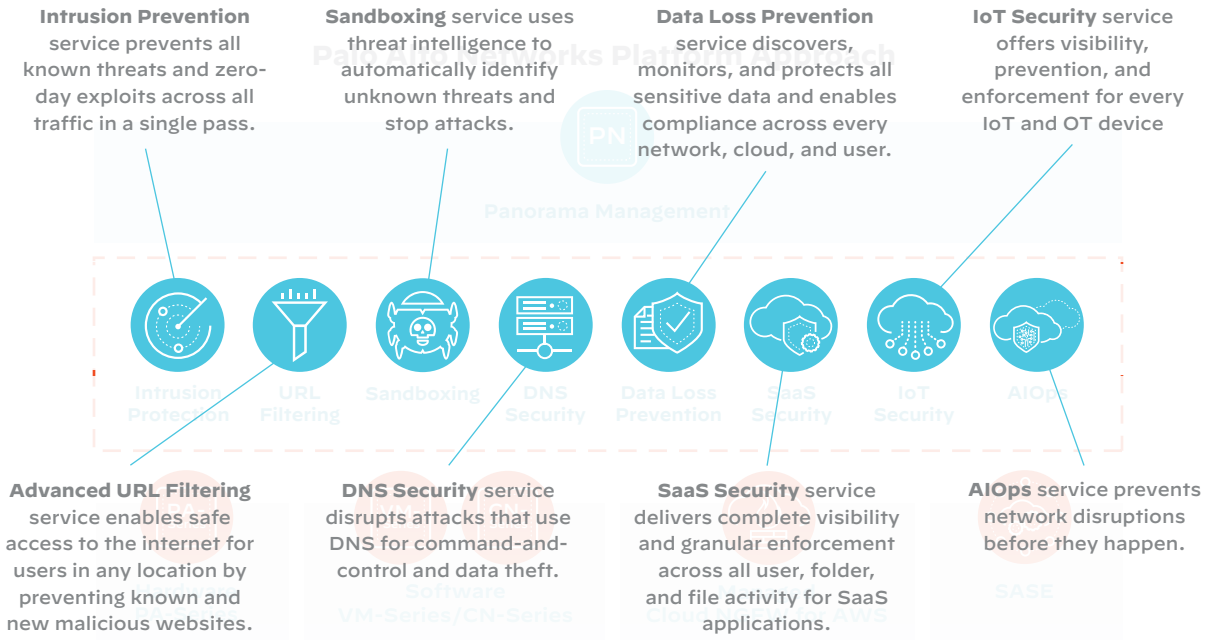

Figure 8: Cloud-Delivered Security Services (CDSS) in the Palo Alto Networks security platform

Hybrid Security Use Cases

To show how Palo Alto Networks secures hybrid infrastructures against real-world attacks, this section looks at three common categories of threats: ransomware, cryptojacking, and cryptoworms.

Ransomware: Pay Up or Lose Your Data

Without question, ransomware is becoming more of a headache for organizations by the day. The top means of initial access are software vulnerabilities (48%), brute-force credential attacks (20%), and phishing (12%). Ransom demands are skyrocketing, reaching $30 million in one recent case. One such attack is called Xbash, ransomware that can self-propagate quickly through the environment via Windows or Linux servers.[5]

To gain entry to the network, the Xbash attack scans for open ports and services with known vulnerabilities. When attackers find an unpatched service, they typically use a brute force attack to gain access to the server. From that beachhead, attackers use port scans to map the environment and identify potential targets within the network and also establish a connection to their Command and Control server via HTTP protocols.

With these connections in place, the attacker is ready to strike. The specific type of attack depends on the operating system of the targeted server. For Linux servers, the attacker deletes the existing databases, downloads and installs CoinMiner, a software cryptocurrency mining tool, on the compromised system and begins mining cryptocurrency. Windows servers require a different approach: the attacker downloads a malicious script, which installs ransomware.

Palo Alto Networks countermeasures: Palo Alto Networks offers a specific and effective defense for each phase of this attack. Those actions prevent port scans and thwart brute force attacks, shut down command and control communication, and prevent the execution of the CoinMiner software (see figure 9).

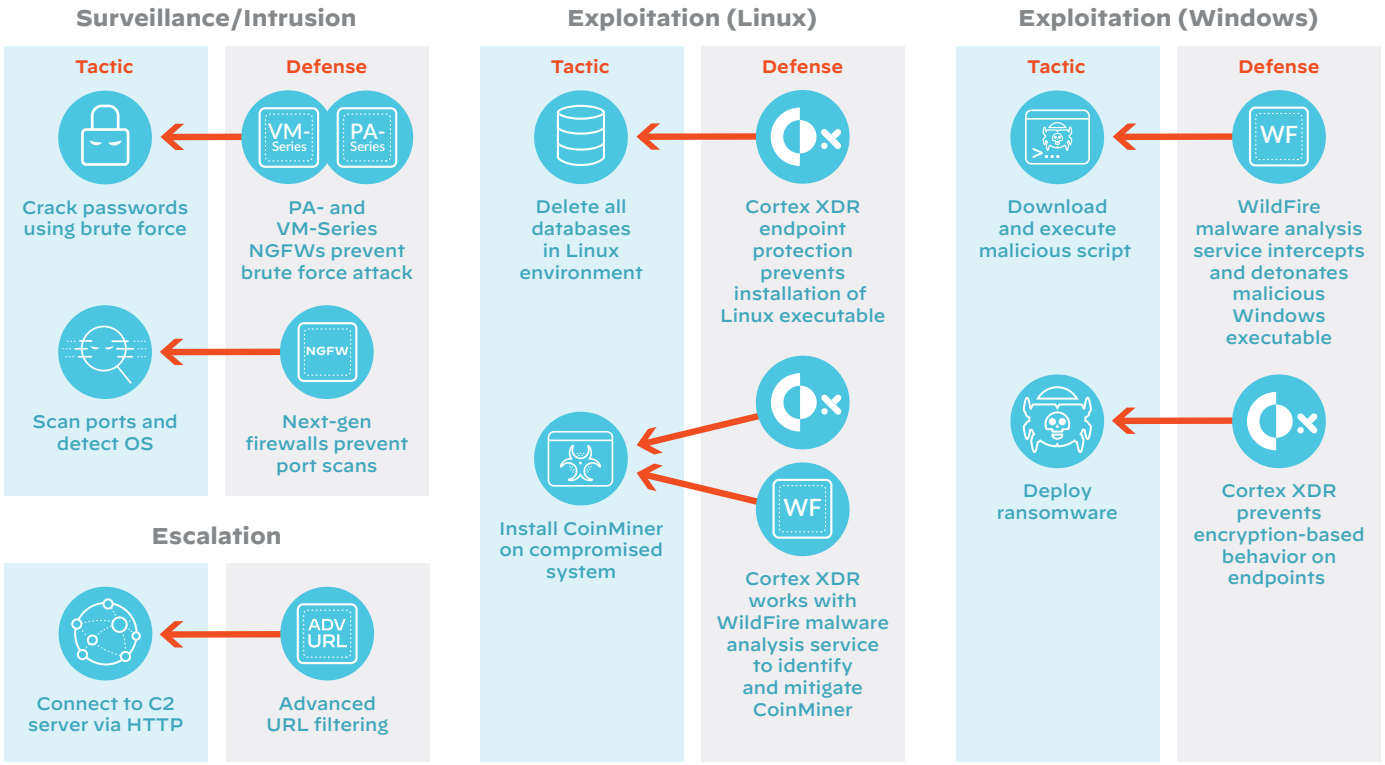

Figure 9: Ransomware tactics and Palo Alto Networks countermeasures

[5] "Incident Response Report 2022," Unit 42, July 2022.

Cryptojacking in the Public Cloud: Leaving the Keys in the Car

A second typical use case is cryptojacking, a technique for stealing computing resources to mine BitCoin and other digital currencies. Cryptojacking starts with an intrusion that allows malware to enter the network and take over a vulnerable server, essentially turning it into a command and control server under the control of the hacker. This technique underscores the importance of keeping patches up to date. An unpatched server is like leaving your car keys in the ignition — it makes the task of stealing your assets an order of magnitude easier.

To illustrate the problem, take a recent attack by the Rocke Group, a Chinese threat actor specializing in ransomware and cryptojacking within cloud environments. As first reported by Unit 42,[6] in 2019 Rocke developed a new coin-mining malware that gains access to Linux servers via unpatched vulnerabilities. Once inside the server, the attacker uploads a piece of code that creates a backdoor, which allows the malware to connect to a command and control (C2) server.

At this point, the server is open for business — the wrong kind of business. Attackers can execute shell commands with administrator rights to buy time by uninstalling endpoint security protections. Then the malware installs and executes CoinMiner. Once this action takes place, a significant percentage of the server's computing power is redirected to the coin-mining activities for minutes or hours until someone notices the drop in server performance.

Palo Alto Networks countermeasures: Defensive tactics start with Prisma® Cloud, which continuously monitors cloud workloads for vulnerabilities and prevents the installation of CoinMiner as well as the uninstallation of other security protections. Additional security solutions stop threats at the network level and prevent the attacker from communicating with its command and control server (see figure 10).

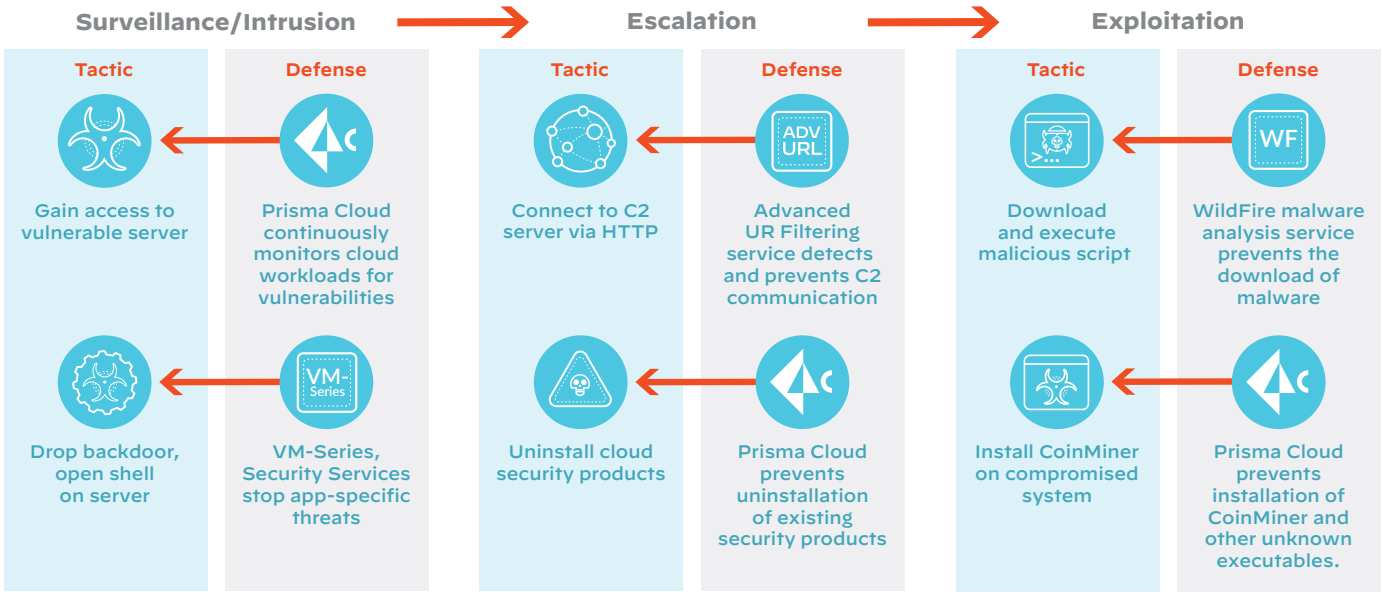

Figure 10: Cryptojacking tactics and Palo Alto Networks countermeasures

[6] Larry Loeb, "Unit 42 Finds the First Cryptojacking Docker Container," Dark Reading, October 17, 2019.

Cryptoworms: Opening Pandora's Container

With the dramatic rate of adoption of containerized workloads, it was only a matter of time until cyberattackers went containerized as well. Containers are a good hiding places for malware, because traditional endpoint protection software cannot inspect data and workloads inside containers.

The first such attack in the industry, discovered by Unit 42, is the Graboid cryptoworm, a virulent worm that exploits unprotected containers for cyptojacking and is capable of self-propagation. To gain an initial foothold, Graboid first locates an unsecured Docker host — the same theme as the last cryptojacking scenario. Graboid then uses that host to run a Docker image that can communicate with other Docker hosts — in effect, spreading tentacles throughout the containerized environment. The attack itself is a sequence of executable scripts that install cryptoworms and orchestrate cryptojacking activities to minimize the likelihood of discovery.

Palo Alto Networks countermeasures: Containerized attacks require container-aware tools, and Palo Alto Networks has them. First, Prisma Cloud identifies containers open to the internet and ensures that only secure container images are deployed. During the escalation phase of the Graboid attack, CN-Series NGFWs — themselves deployed inside containers — prevent lateral movement and thus minimize the extent of the breach. Finally, Prisma Cloud prevents the installation of the cryptojacking payloads (see figure 11).

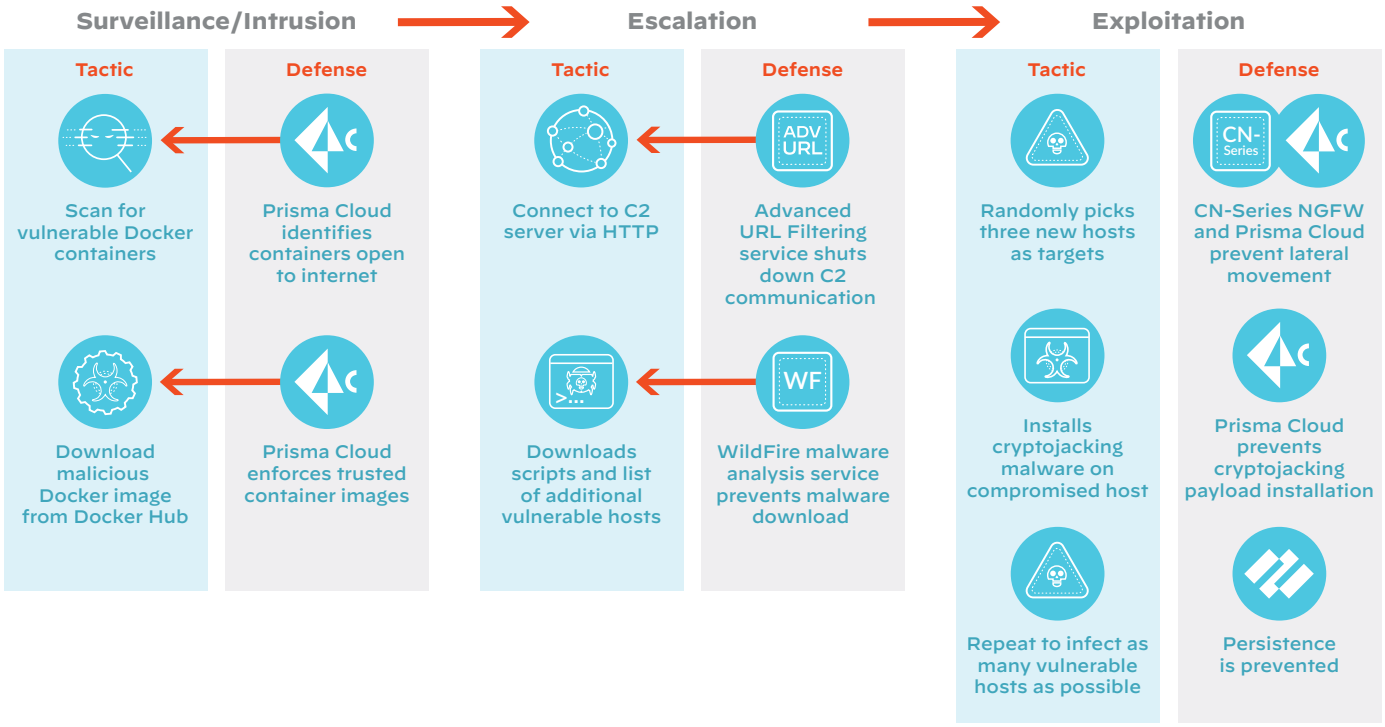

Figure 11: Cryptoworm tactics and Palo Alto Networks countermeasures

Looking Ahead With Confidence

Beyond the specific measures described in this white paper, Palo Alto Networks also brings a philosophy of adapting its security solutions to your infrastructure — not the other way around. As you can see from the use cases, our solutions are as granular as the attack vectors. Palo Alto Networks offers a purpose-built countermeasure for each attack tactic, for example, we counter containerized threats with CN-series containerized NGFWs.

What that means to you is confidence. Now you can build hybrid infrastructure to meet your specific needs, modify it as necessary, knowing that Palo Alto Networks can secure it — without compromise. As attackers continue to develop new and more virulent exploits, even taking advantage of sophisticated technologies such as automation and AI, you can trust Palo Alto Networks to develop effective countermeasures quickly. After all, our Unit 42 Threat Research group has an excellent track record for discovering new threats, case in point being the Graboid Worm discussed earlier.

In sum, the hybrid cloud architecture affords significant benefits such as cost savings and organizational agility, but also introduces new and unfamiliar security challenges. Now you can face forward to meet the challenges of a dynamic and dangerous environment without fear — Palo Alto Networks has your back. Find out how to move forward with a personalized demo tailored to your needs.

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