Your Containerized Applications are Still Vulnerable: Countering Containerized Threats with the CN-Series NGFW

Containerized infrastructure continues to be revolutionary in the world of computing. Containers virtualize operating systems—in contrast to virtual machines, which *only* virtualize hardware—which allows for the deployment of smaller and faster applications. This saves compute costs and reduces operational complexity. According to the Palo Alto Networks State of Cloud Native Security 2020 report, 30% of companies use containerized infrastructure for their business, and 86% expect their usage of these resources to increase or stay the same over the next two years.[1]

However, as containers become a standard part of businesses, the vulnerable attack surface area increases. One reason is that containers allow for such rapid application development and deployment that security teams can struggle to keep pace with tracking and protecting containers. This calls for healthy security practices in the new infrastructure.

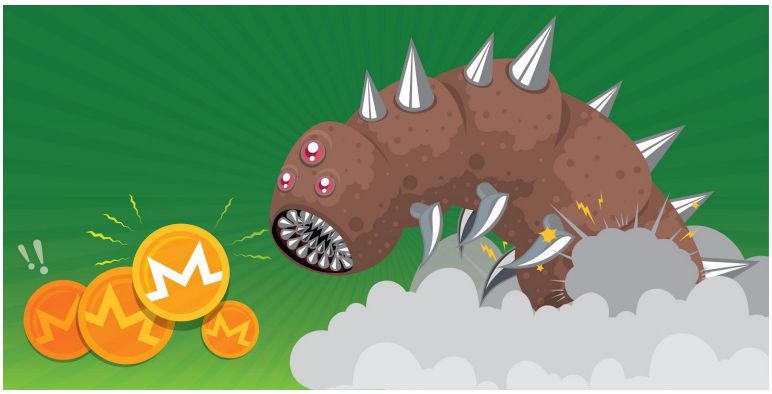
There is a common misconception that containers are inherently safe. Unfortunately, containers are susceptible to the same threats that have dogged traditional infrastructures—virtual machine, cloud, bare-metal servers—along with new threats capable of exploiting Kubernetes infrastructure, such as Kubernetes APIs, default exposed ports, and Docker Daemons.

Fortunately, there's a solution to these network security challenges. The Palo Alto Networks CN-Series containerized NGFW enables network security teams to prevent network threats and confidently migrate business-critical applications to containers without compromising network security posture.

How does a NGFW protect your containerized infrastructure from both legacy network threats and the new threats unique to your Kubernetes environments? Let's walk through a few of the most prevalent and advanced threats to explore how protection is delivered with the industry's first NGFW for Kubernetes environments.

Cryptojacking: The Biggest Threat to Containerized Infrastructure

Cryptojacking has been a particularly prominent form of containerized infrastructure attack. In these incursions, cryptojackers hijack computer resources to mine cryptocurrencies for profit at the victim's expense (Monero, in particular, is commonly mined cryptocurrency in cryptojacking attacks).[2] These attacks exploit vulnerabilities within the instances themselves—Kubernetes API and Docker Daemons—as well as application vulnerabilities such as Confluence, Redis, and Hadoop. Cryptojacking is the most popular attack method against containerized infrastructure, comprising more than 75% of attacks.[3] In 2019, cryptojacking operations were estimated to affect 23% of all cloud environments, up 8% from the previous year.[4]

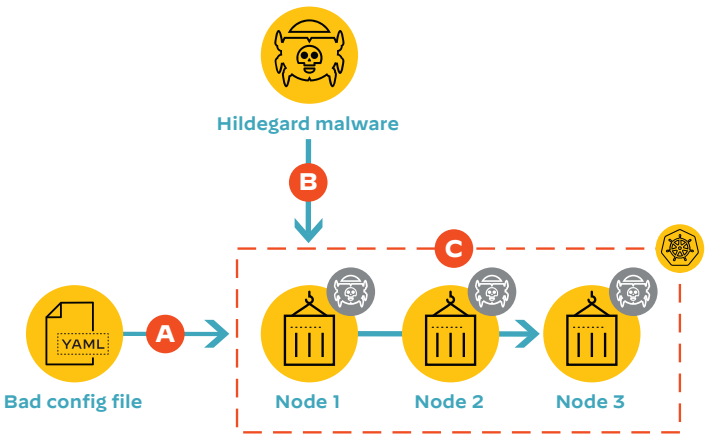


1. "The State of Cloud Native Security 2020," Palo Alto Networks, June 24, 2020
2. "Threat Brief: What's Driving the Shift to Cryptocurrency Mining Malware?" Unit 42, Palo Alto Networks, March 6, 2018
3. "Docker Honeypot Reveals Cryptojacking as Most Common Cloud Threat," Unit 42, Palo Alto Networks, March 6, 2018
4. "WatchDog: Exposing a Cryptojacking Campaign That's Operated for Two Years," Unit 42, Palo Alto Networks, February 17, 2021

Cryptojacking Exploit Is No Match for CN-Series

In January 2021, the Palo Alto Networks Unit 42 research team detected a malware cryptojacking campaign targeting Kubernetes.[5] By gaining access through a misconfigured kubelet node agent, the malware known as Hildegard spread to as many containers as possible (Figure 1a) before launching cryptojacking operations to mine Monero (XMR) (Figure 1b). The campaign eventually reached 25 KH/s hashing power by leaching compute resources to make money from unsuspecting corporate victims.

This attack was preventable. By deploying the CN-Series in both north-south and east-west configurations, the company could have either defeated the attack altogether or prevented lateral spread of the malware (figure 2).

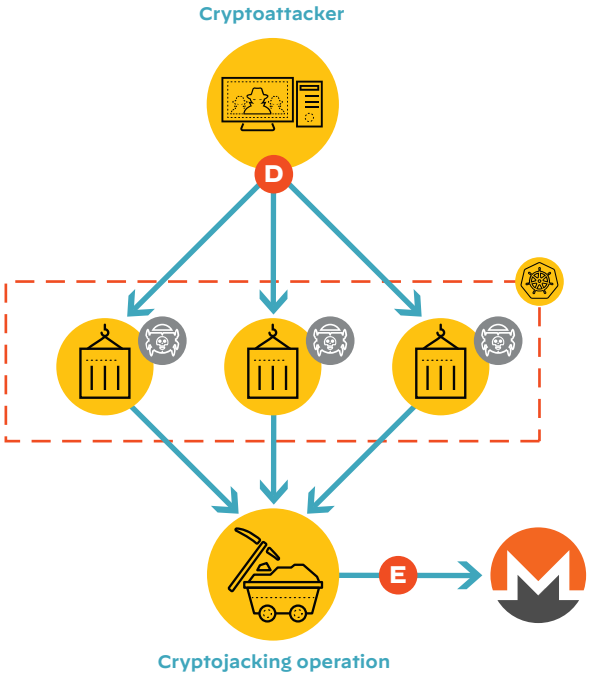


A Malformed YAML configuration file leads to a misconfigured container.

B Hildegard enters the cluster through the vulnerable container and delivers malware payload.

C Malware spreads laterally (east-west) to infect other containers in the cluster.

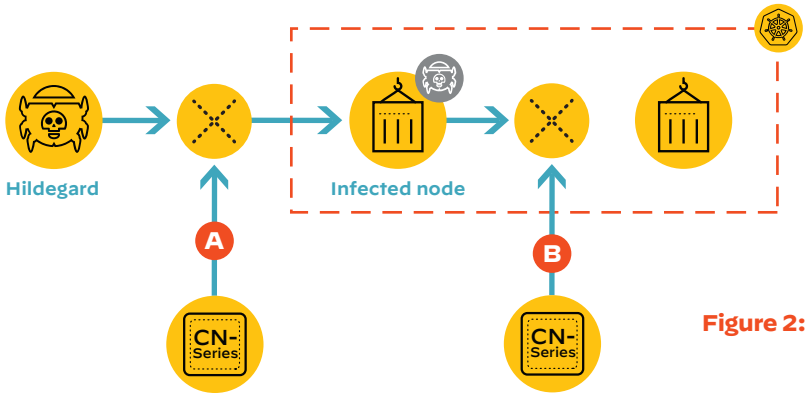
Figure 1a: Exploiting the vulnerability



D Hacker establishes command and-control communications with the containers to launch north-south attack.

E Containers are cryptojacked to mine cryptocurrency such as Monero.

Figure 1b: Launching the cryptojacking attack



A CN-Series blocks most malware from entering the cluster (north-south protection).

B If malware does get into the cluster, CN-series blocks lateral spread (east-west protection), rendering the cryptojacking attack harmless.

Figure 2: Defending against Hildegard and other malware

5. "Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes," Unit 42, Palo Alto Networks, February 3, 2021

Additionally, in 2019, Unit 42 detected a cryptojacking worm called Graboid.[6] Infecting more than 2,000 unsecured Docker hosts, the campaign gained access to hosts through unsecured Docker daemons. Afterwards, the worm would connect to a command-and-control (C2) domain to install malicious Docker images to mine Monero currency, all while periodically querying the network for more vulnerable hosts.

CN-Series users are also protected against cryptojackers. The Threat Prevention service prevents the movement of malware components, while the DNS Security service prevents connection to known command-and-control (C2) domains.

Legacy Threats: The Oldies Just Won't Fade Away

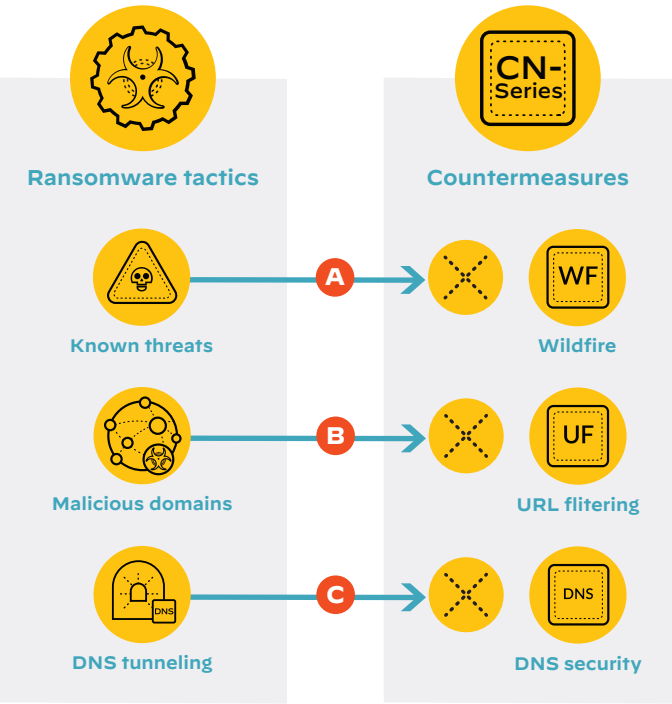
Legacy threats continue to affect business businesses using container infrastructure. For example, the Federal Bureau of Investigation's most recent Internet Crime Report stated that Americans suffered over $6.9 billion of losses in 2021, an increase of 7% from the previous year.[7] Unfortunately, the trend indicates that losses will only continue to grow. Understanding some of the top threats helps illustrate the need for CN-Series firewalls.

Ransomware

At the top of the list is ransomware, a ubiquitous form of malware that attacks all forms of infrastructure, whether physical,virtual, or container. Criminals use ransomware to shut down operations or hold valuable files, data, or information hostage until a ransom is provided. Even if ransom is paid, there is no guarantee the attacks will cease once money is paid. Oftentimes, leaked data is sent to the dark web, where other attackers can double-dip into the data to extort enterprises. In 2020, the average ransomware payment increased by 171% from the previous year to $312,493.[8]

Recently, the Ragnar Lockar ransomware campaign made headlines when it leaked screenshots showing 700 GB of confidential data stolen from one company.[9] The attackers threatened to leak the information if ransom was not paid. The campaign infiltrated networks using vulnerabilities, phishing, and BEC attacks, before spreading to as many endpoints as possible and encrypting the files, folders and extensions with the ".ragnar_*" extension.

The CN-Series identifies and blocks tactics used by ransomware attackers, including phishing emails and DNS tunneling (Figure 3).



A Wildfire uses threat intelligence from hundreds of sites to block known ransomware exploits.

B URL Filtering stops containerized workloads from accessing malicious domains.

C DNS Security blocks outside attackers from using DNS tunneling to communicate with malware.

Figure 3: Defeating ransomware attacks

6. "Graboid: First-Ever Cryptojacking Worm Found in Images on Docker Hub," Unit 42, Palo Alto Networks, October 16, 2019
7. "Internet Crime Report 2021," Federal Bureau of Investigation, March 23, 2021
8. "Highlights from the 2021 Unit 42 Ransomware Threat Report," Unit 42, Palo Alto Networks, March 17, 2021
9. "Ragnar locker malware: what it is, how it works and how to prevent it," Infosec Resources, June 25, 2020

Software Vulnerability Exploits

Most businesses have a plethora of internet-facing servers, websites or compute assets, such as IoT devices, storage, and smart devices. With software vulnerability exploits, attackers look for vulnerabilities and unintended bugs left in software—deployed in any infrastructure, including Kubernetes—to abuse for personal benefit, such as deploying malware, stealing data, and discovering the security and asset infrastructure. Vulnerability exploits often target some of the most popularly consumed software. For example, The FBI Internet Crime Complaint Center (IC3) reported that Microsoft Exchange, Office, and Sharepoint; Atlassian Confluence; and the F5 Big-IP Load Balancer were the targets of the top routinely exploited vulnerabilities.[10]

The Reality of Software Patching

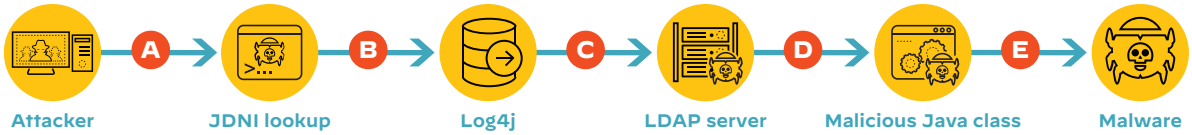
While patching applications is an important aspect of a security team's duties, patching all software vulnerabilities is not realistic. Vulnerabilities can take years to discover, and then more time is needed to develop a patch. Yet even more time is needed for security teams to ultimately roll out the application in affected infrastructure. Additionally, 65% of security teams already struggle to prioritize their list of known vulnerabilities.[11] As such, organizations are recommended to take the defense-in-depth approach of having a deploy-time solution to manage Common Vulnerabilities and Exposures (CVEs), as well as a containerized NGFW for safeguarding against malware and C2 activities used after an attacker penetrates the infrastructure.

New Threats See Rapid Evolution

Countermeasures for Log4j Attacks

One of the biggest cybersecurity scares was revealed December 10, 2021, a date that will go down in the annals of cybercrime as a watershed moment. This moment in time saw the appearance of the Log4j vulnerability. Log4j lets attackers log code to execute Java Naming and Directory Interface (JNDI) commands to connect to malicious external domains, effectively creating a brutal and global C2 scenario. Affecting up to 3 billion devices, the Log4j vulnerability threatened any application built upon Java or any application using third-party libraries with Java dependencies, even if they are deployed on Kubernetes.[12]

Attacks that exploit the log4j vulnerability have a particular pattern of steps, all of which must take place if the attack is to be successful (figure 4) The CN-Series offers a series of countermeasures to interrupt the step-by-step attack and prevent malware from entering the network (figure 5).



A Attacker inserts JDNI lookup string in a header field that is likely to be logged.

B The string is passed to log4j to be logged.

C Log4j executes the JDNI lookup string, querying the compromised LDAP server that is part of the attack.

D The LDAP server returns a location to a malicious Java class.

E The Java virtual machine executes the malicious Java class, launching the attack.

Figure 4: How attackers exploit the log4j vulnerability

10. Joint Cybersecurity Advisory, Federal Bureau of Investigation, Australian Cyber Security Centre, United Kingdom's National Cyber Security Centre, July 28, 2021
11. "Costs and Consequences of Gaps in Vulnerability Response," Ponemon Institute, 2020
12. "Log4j vulnerability cleanup expected to take months or years," SC Magazine, December 13, 2021

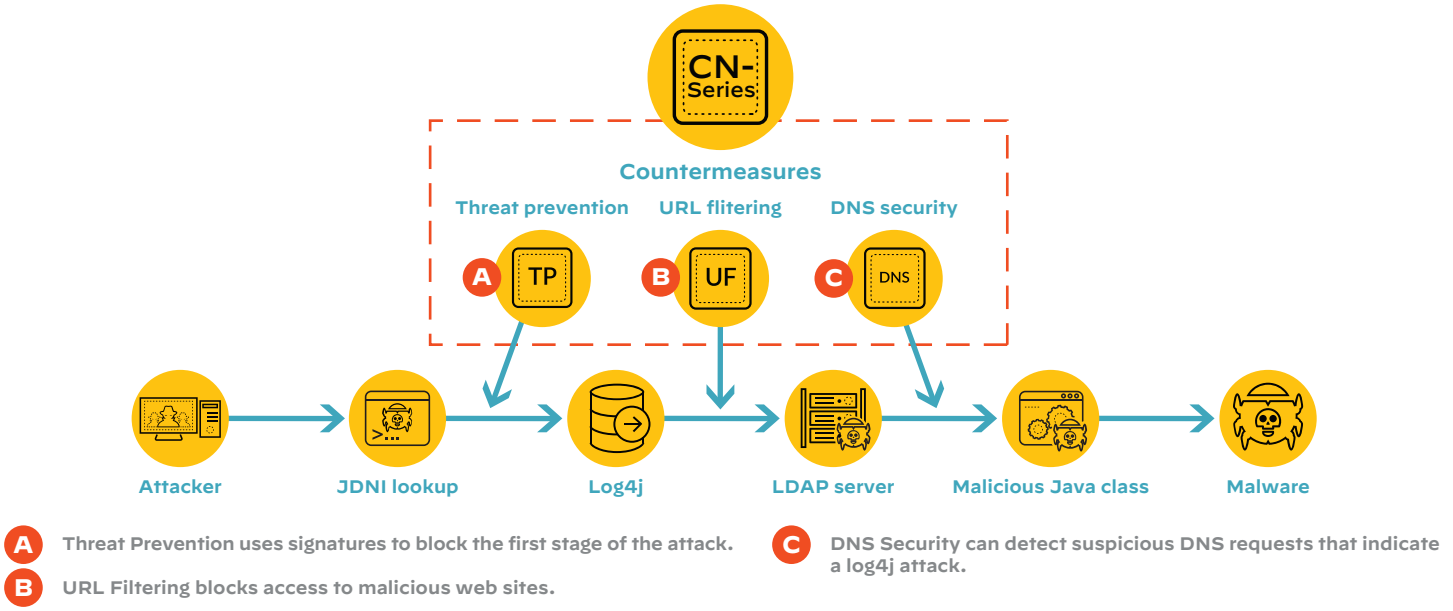


Figure 5: How the CN-Series defends against log4j attacks

Software vulnerabilities are the entry point through which attackers commit their exploits. For example, on March 2, 2021, four critical zero-day vulnerabilities were introduced to multiple versions of Microsoft Exchange Server. HAFNIUM, a state-sponsored cybercrime group operating out of China, heavily exploited the vulnerability, exfiltrating confidential data from victim infrastructure to sharing sites like MEGA. The effects of the vulnerability were widespread—initial estimates projected that tens of thousands of organizations were infiltrated and compromised by the vulnerability exploit.[13]

Another recent famous supply chain attack—the SolarWinds attack—revealed on December 13, 2020—originated in a software vulnerability within SolarWinds Orion, an IT performance and monitoring software. In this instance, attackers were able to download malware onto organizations' SolarWinds systems as fake software updates, allowing the attackers to spy on infrastructure and exfiltrate data. The attack had a huge pool of potential victims, because SolarWinds Orion was used by 425 of the US Fortune 500 companies, along with the US Government and Military.[14]

It's important to note that SolarWinds servers are used to monitor IT infrastructure, including containers. By compromising a SolarWinds server, attackers now have access to a victim's infrastructure—including their Kubernetes infrastructure—since they have network reconnaissance from SolarWinds.

Deploying the Threat Prevention service with CN-Series provides protection against vulnerability exploits such as Log4j and SolarWinds. Threat Prevention and WildFire prevent malware and spyware from entering and propagating within the network. Advanced URL Filtering blocks access to malware domains, while DNS Security prevents C2 connections to malware domains. This is important, because the number of threats simply continues to grow, as evidenced in IC3's list of top exploited vulnerabilities.[15]

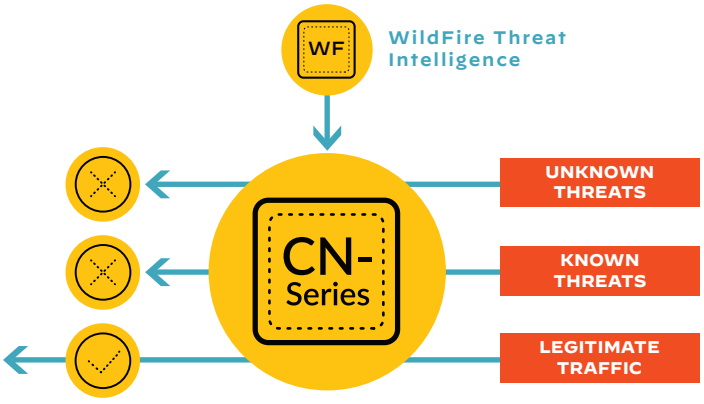


Figure 6: Wildfire can help prevent malware and spyware from entering and propagating with a Kubernetes cluster network.

13. "Microsoft Exchange Server Attack Timeline," Unit 42, Palo Alto Networks, March 11, 2021
14. "DHS, DOJ And DOD Are All Customers Of SolarWinds Orion, The Source Of The Huge US Government Hack," Forbes Magazine, December 14, 2020
15. Joint Cybersecurity Advisory, Federal Bureau of Investigation, Australian Cyber Security Centre, United Kingdom's National Cyber Security Centre, July 28, 2021

Threats Take Over Legitimate Tools

Cobalt Strike

Cybersquatting is not limited to cryptojacking. Consider Cobalt Strike, a legitimate, commercially available simulation software security testers use to emulate threat actor activity in networks. Ironically, threat actors have discovered the utility of the tool can be used to penetrate vulnerable systems, deploy malware, and then depart the scene of the crime with no artifacts left in system memory.

One example of Cobalt Strike's use in the field was the threat actor TA511's use of the program in its Hancitor campaign. Starting in October 2020, TA511 began incorporating Cobalt Strike within Hancitor, a malware used for exfiltrating data and downloading more malware.[16] This led to attacking and infecting the more vulnerable endpoints in a network, including those in Kubernetes infrastructures. Once deployed, Hancitor would use Cobalt Strike to noisily ping victims' networks, and grant the threat actor full visibility into network topologies, for access to more vulnerable hosts to steal confidential data.

CN-Series customers need not fear for this threat, as the Threat Prevention service prevents network spam and other Cobalt Strike operations.

BotNet C2

Botnets are a network of malware-infected computers assembled under the control of a single attacker. Botnets steal compute power and resources to perform whatever nefarious operation the attacker desires, such as performing distributed denial-of-service(DDoS) attacks or mass cryptomining campaigns.

In September 2021, the Meris BotNet shocked the world when 250,000 IoT compromised devices were coordinated to perform massive DDoS attacks against the Russian Internet Search company, Yandex.[17] At its peak, it launched roughly 17 million fake requests-per-second. For context, Cloudflare only serves 25 million HTTP requests per second.

CN-Series customers can stop their containers from BotNet targeting through multiple Palo Alto Networks security services. Threat Prevention, for example, prevents the infiltration of the malware componentry. Meanwhile, DNS Security and Advanced URL Filtering prevent containers from beaconing out to malicious domains.

To stop DDoS attacks from affecting their infrastructure, CN-Series customers can set up traffic profiles to observe and control the floods of specific traffic such as SYN, UDP, and ICMP floods.[18]

CN-Series: NGFW for Your Containerized Infrastructure

The Palo Alto Networks CN-Series container firewall is the industry's first next-generation firewall (NGFW) delivered in a container form factor and natively integrated into Kubernetes. CN-Series provides protection against threats that have historically targeted legacy infrastructure, as well as against the new, emerging threats, which help criminals make and demand more money than ever.[19]

And to gain a better understanding of how this NGFW can protect dynamic container environments, sign up for the in-depth CN-Series lab to get started protecting innovation at DevOps speed.

16. Hancitor's Use of Cobalt Strike and a Noisy Network Ping Tool, Unit 42, Palo Alto Networks, April 1, 2021
17. "Meet Meris, the new 250,000-strong DDoS botnet terrorizing the internet," The Record, September 9, 2021
18. "What is a Distributed Denial of Service Attack (DDoS)?" Cyberpedia, Palo Alto Networks
19. "Highlights from the 2021 Unit 42 Ransomware Threat Report," Unit 42, Palo Alto Networks, March 17, 2021

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