PRISMA
BY PALO ALTO NETWORKS

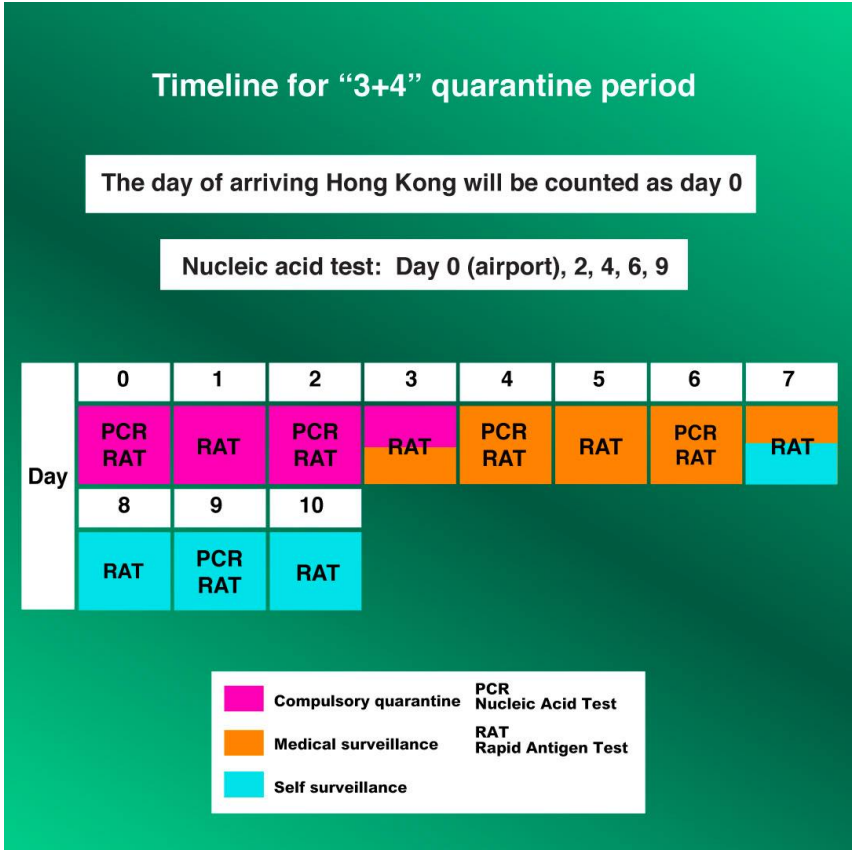
Cloud Security with “0+3” approach

October 2022

HARRY PUN
Cloud Security Lead

paloalto NETWORKS

Timeline for “3+4” Arrangements



Timeline for “0+3” Arrangements

The day of arriving Hong Kong will be counted as day 0

Nucleic acid test: Day 0 (airport), 2, 4, 6

Day	0	1	2	3	4	5	6	7
	PCR RAT	RAT	PCR RAT	RAT	PCR RAT	RAT	PCR RAT	RAT

Medical surveillance — PCR Nucleic Acid Test

Self surveillance — RAT Rapid Antigen Test

SAST

DAST

Zero Trust

PRISMA
BY PALO ALTO NETWORKS

Top 5 Cloud Native Risks

DevSecOps Is Critical to Protecting Applications from Build to Runtime

paloalto NETWORKS

OVERVIEW

The overall problem(s): The cloud has changed the game for everyone. Today, nearly 70% of organizations host more than half their workloads in the cloud, up from just 31% in 2020.

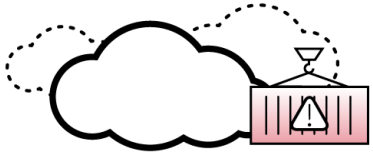
And yet, Gartner says 50% of organizations indicate a lack of internal knowledge about cloud-native security, never mind the risks.

With cloud innovation come security challenges

Insecure Configurations

42%

of CloudFormation templates are insecure



Vulnerable Defaults

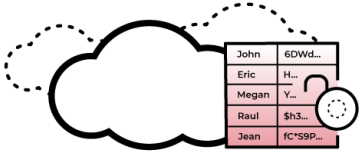
51%

of exposed Docker containers use insecure defaults

Host Vulnerabilities

24%

of exposed cloud hosts have known vulnerabilities



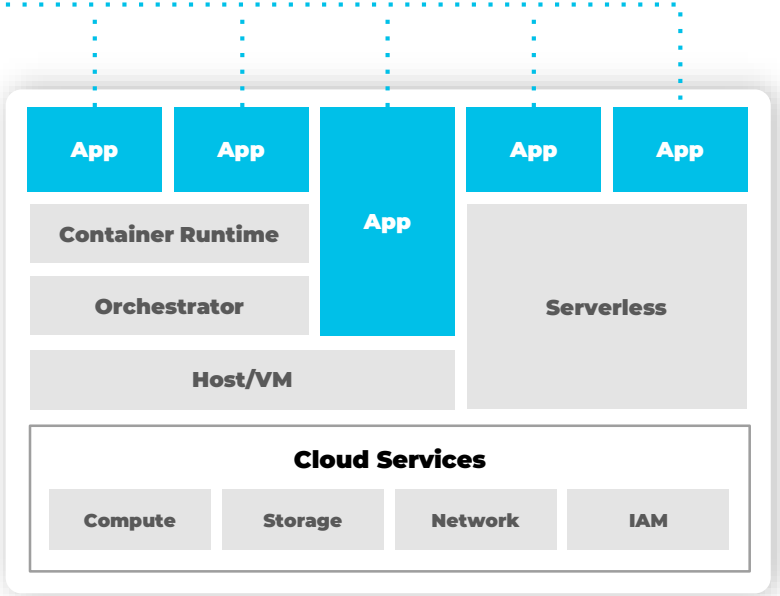
Compliance Risks

43%

of cloud databases are not encrypted

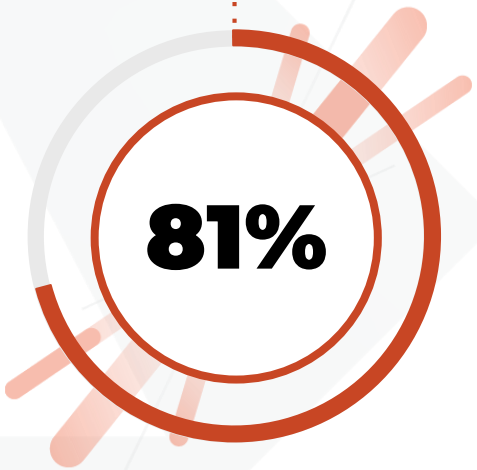
A majority of the code in the average application is open source

of application code is open source[1]

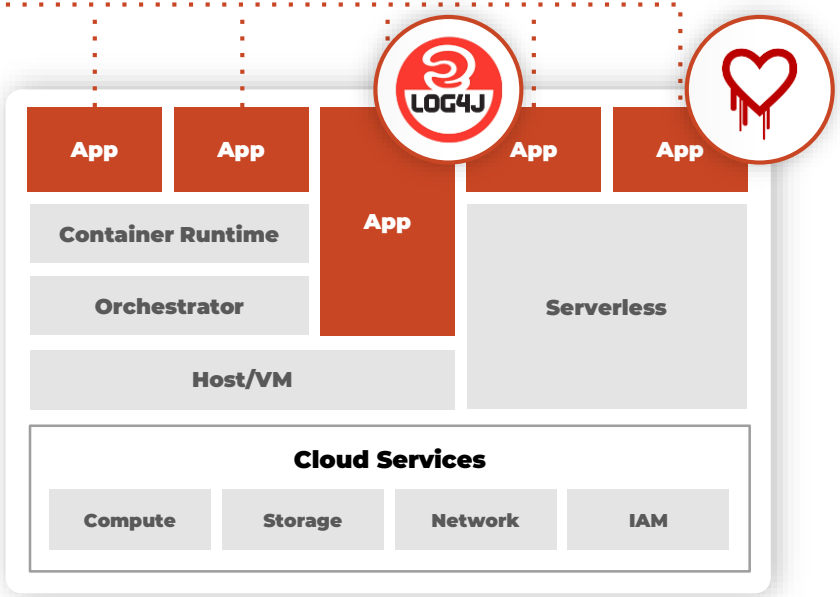


1. Forrester's The State of Application Security, 2022

Open source code is vulnerable to attack

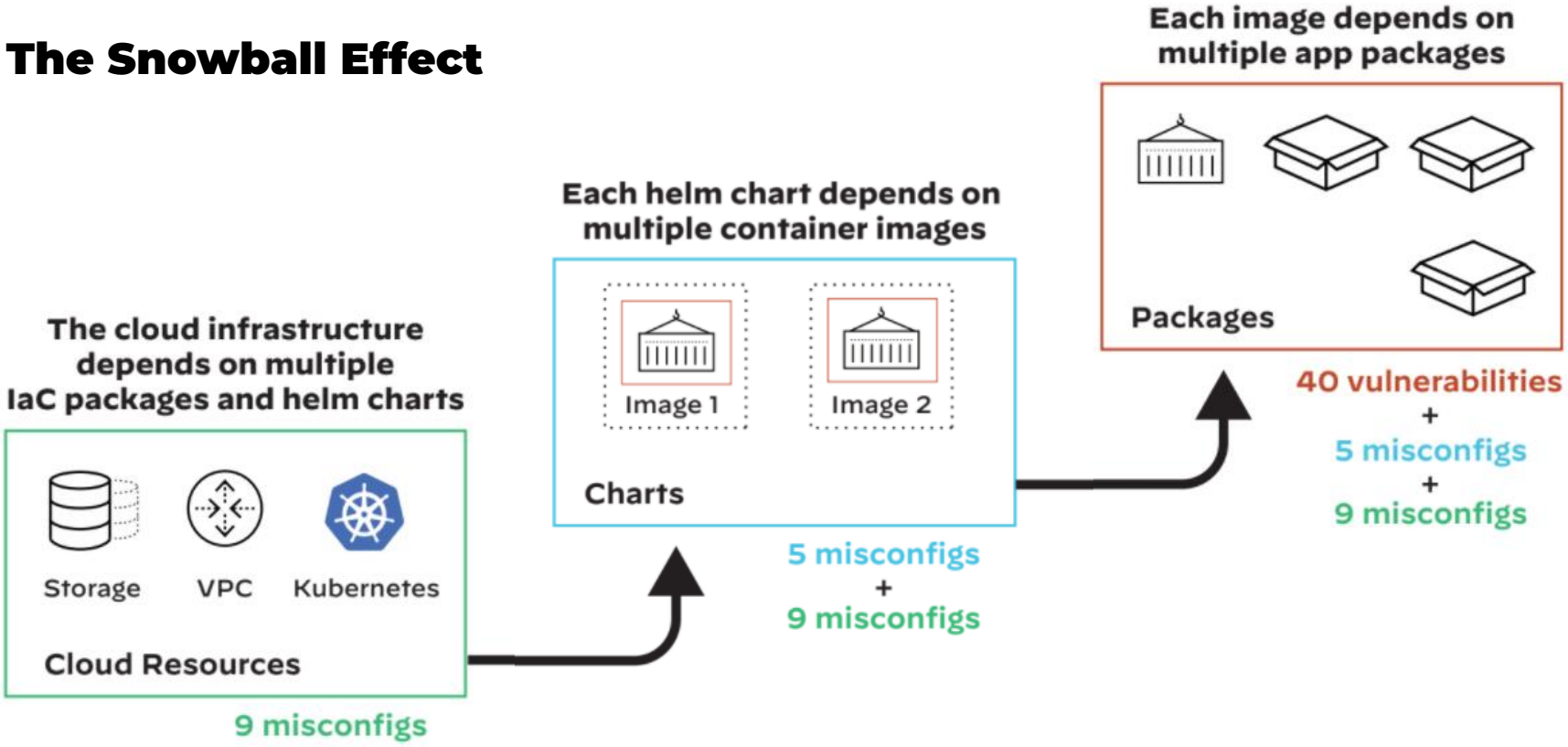


of codebases contain an OSS vulnerability**



1. Unit 42 Cyber Intelligence

The Snowball Effect



Cloud Infrastructure Provisioning → Kubernetes Application Deployment → Container Image Instantiation

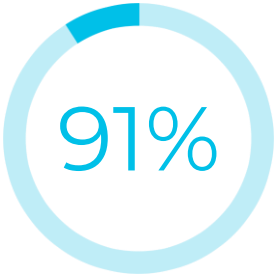
Cloud Native Risk # 1:

Application Vulnerabilities

(CWP + Code Security)

- There's an increasing need for developer-friendly approaches that help identify security issues in code (application and cloud configurations), while also providing automation and best practices.

of third-party container applications deployed in cloud infrastructure were found to contain known vulnerabilities



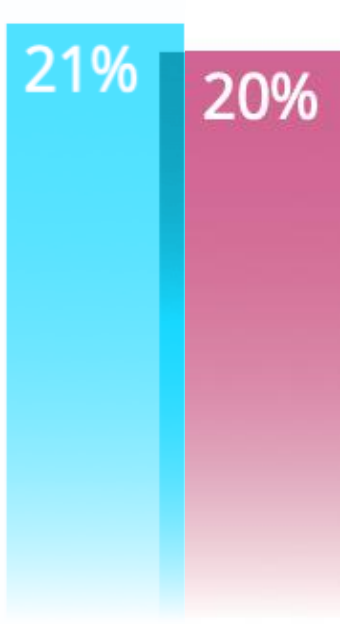
contain at least one "critical" or "high" vulnerability in the images

Cloud Native Risk # 2:

Infrastructure Misconfigurations

(CSPM)

- Misconfigurations leave the door open for network attacks and exploits. The most common is leaving ports open. Any port left open to the internet provides hackers with an attack vector.



21% of the security scans run against the large SaaS provider's customer's development environment resulted in misconfigurations or vulnerabilities (industry average 20%)

Cloud Native Risk # 3:

Malware

(CWP + Data Security)

- Malware isn't new, but it is evolving at breakneck speed in the cloud. Consider cryptojacking–containers offer attackers a simple way to distribute malicious cryptominers

An in-depth look into Docker Hub found **30 malicious images** downloaded **20 million times**

Cloud Native Risk #4:

Overprovisioned Access

(CIEM)

- Overprovisioned access opens your organization up to two major cloud security threats–malicious insiders and, more frequently, account takeovers.
- One recent global study found that 99% of cloud users, roles, services and resources were granted excessive permissions.

Cloud Native Risk #5:

Insecure APIs

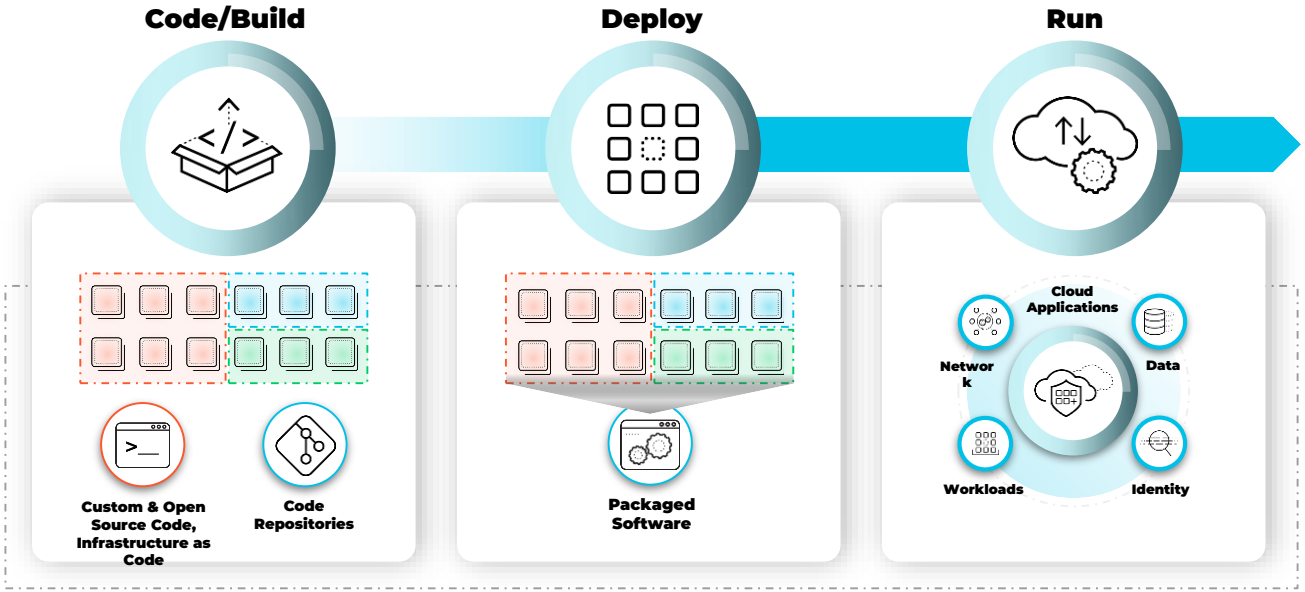
(WAAS + CNS)

- APIs are the lifeblood of cloud-native and app-based economies. Failing to protect them creates new challenges.
  - Who is using what APIs?
  - Are your APIs updated?
  - Has your organization formalized the way it evaluates API security?

CLOUD APPLICATIONS ARE CREATED DIFFERENTLY

THE APPLICATION LIFECYCLE

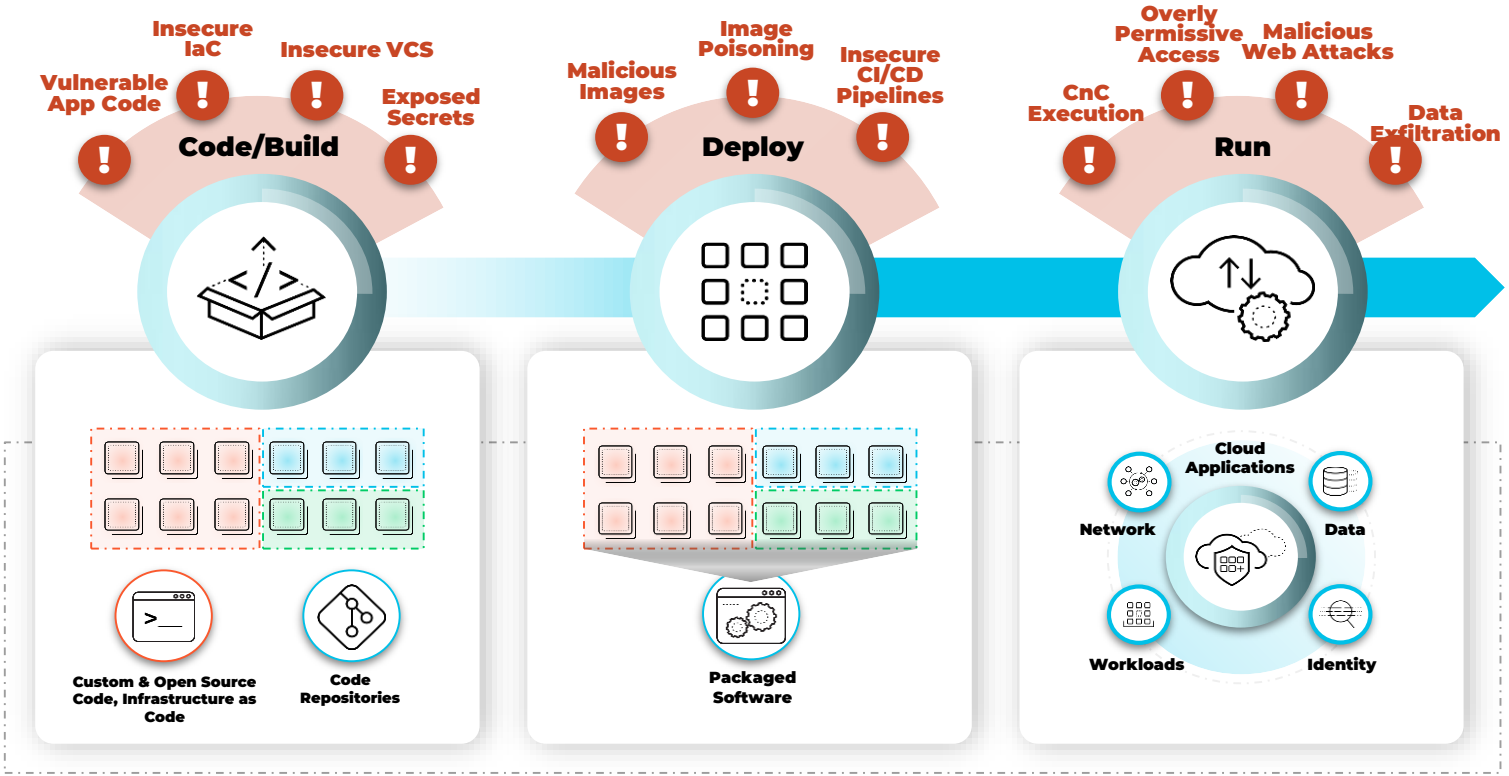
- Designed for rapid iteration and continuous application rollouts
- Highly automated builds to reduce time to market
- Improves app team / developer productivity



 |

THE INTRODUCTION OF RISK AT EVERY STAGE

THE APPLICATION LIFECYCLE IS VULNERABLE FROM DEV TO OPS



 |

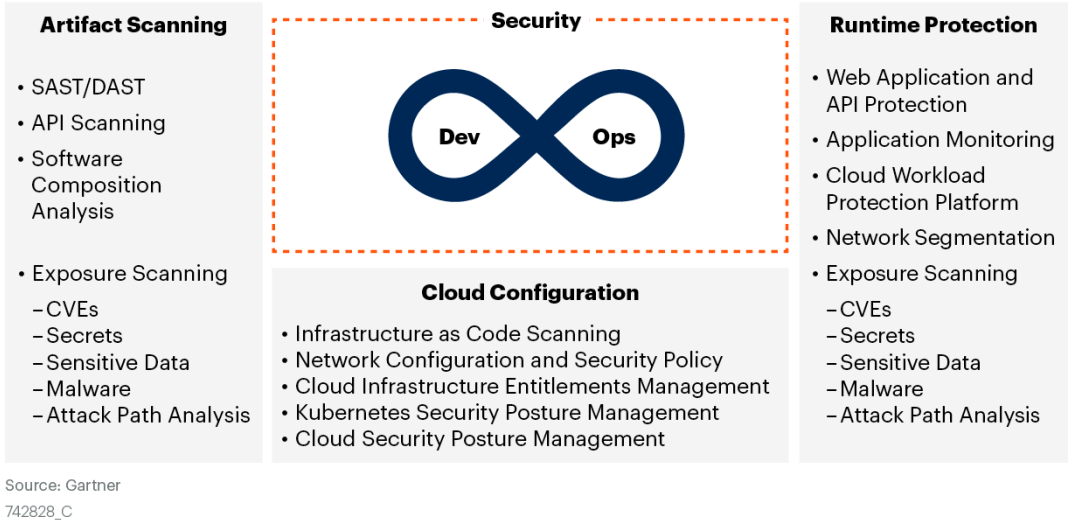
Cloud Native Application Protection Platform (CNAPP)

*Optimal security of cloud-native applications requires an **integrated approach** that starts in **development** and extends to **runtime protection** - Gartner (Aug 2021)*

CNAPP consolidates a large number of siloed capabilities:

- Development artifact scanning, including containers
- Cloud security posture management (CSPM)
- IaC Scanning
- Cloud infrastructure entitlements management (CIEM)
- Runtime cloud workload protection platform (CWPP)

Detailed CNAPP Capabilities



Source: Gartner
742828_C

Source: Innovation Insight for Cloud-Native Application Protection Platforms by Gartner
Download from: https://www.paloaltonetworks.com/blog/prisma-cloud/gartner-know-cloud-native-application-protection-platforms/

THE FUTURE OF SECURE CLOUD APPLICATIONS

GO FROM POINT SECURITY TOOLS TO BEST-IN-CLASS, COMPREHENSIVE CNAPP

POINT PRODUCTS	CODE-TO-CLOUD CNAPP
Protection Focused on Runtime	**Comprehensive Security from Code to Cloud**
Visibility Without Prevention	**Prevention-First Approach**
Infrequent Scans Lead to Blind Spots	**Continuous, Real Time Visibility**
Tool Proliferation	**Platform with Choice For Every Cloud Journey**
Scale Issues, Performance Impacts	**Cloud Scale Security**

 |

Prisma Cloud
Introduction

 |

PRISMA® CLOUD

CODE TO CLOUD

PREVENTION FIRST

CONTINUOUS REAL TIME VISIBILITY

SECURITY CHOICE

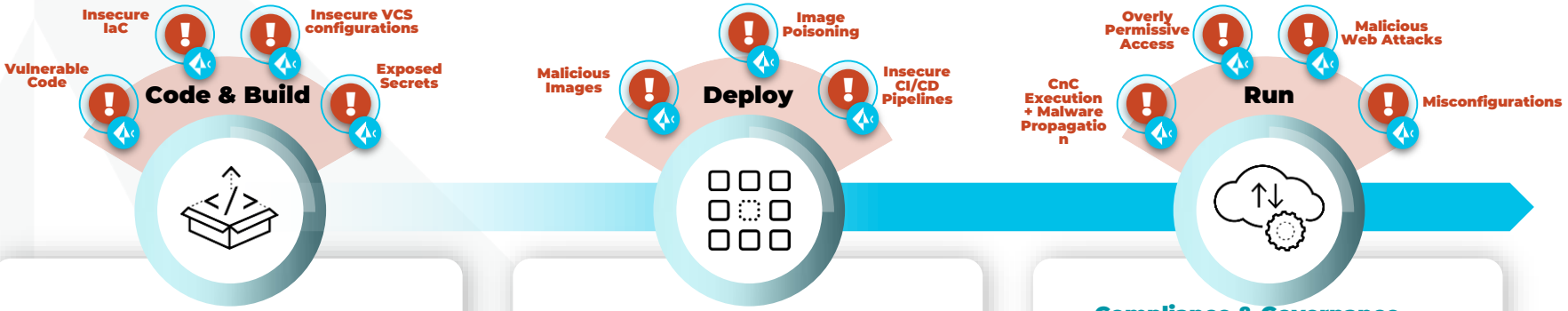
SECURITY AT ANY SCALE

THE INDUSTRY'S MOST COMPREHENSIVE CODE-TO-CLOUD CNAPP

 |

paloalto NETWORKS

PRISMA CLOUD CAPABILITIES



- IaC Security (CCS)
- Software Composition Analysis (CCS)
- Secrets Scanning (CCS)
- Supply Chain Security (CCS)

- Container Access Control (CWP)
- CD Security (CWP)
- Trusted Images (CWP)
- Image Analysis Sandbox (CWP)

- Compliance & Governance (CSPM)
- Misconfig & Threat Detection (CSPM)
- Vulnerability management & Runtime Security (CWP)
- Web App & API Security (WAAS)
- IAM Security (CIEM)
- Data Security (CSPM)
- Network Security (CNS)

SaaS Platform

- Cloud Scale SaaS Platform
- Integrated experience from Code to Cloud
- Easy to Adopt and Operationalize

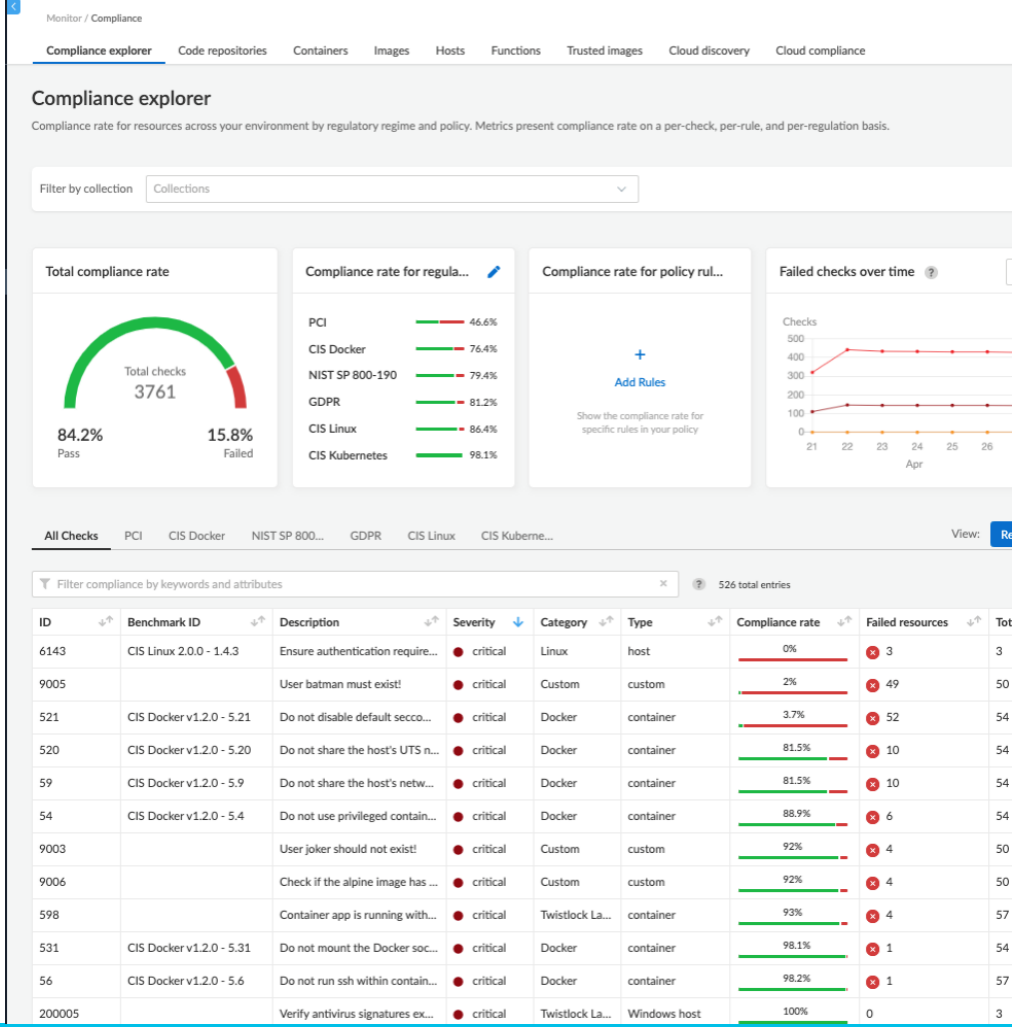
 |

Prisma Cloud Typical Use Cases

1. Continuous compliance / best practices / company policies assessment => eliminate manual efforts and reduce time to risk mitigation
2. Out-of-the-box risky cloud configuration identification => reduced cost and complexity in risk analysis
3. Threat detection in public cloud => uniform detection capabilities across multiple public cloud environments
4. DevSecOps => automated risk detection across the application lifecycle (build, deploy, run)
5. Application runtime visibility and protection => automated app profiling, suspicious activities and OWASP Top 10 risks detection and prevention

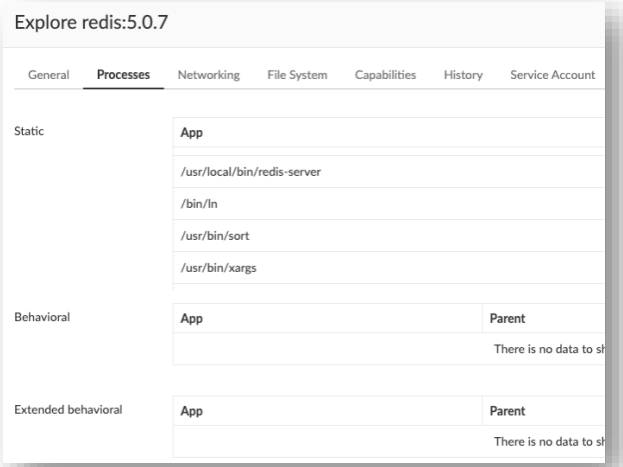
Compliance

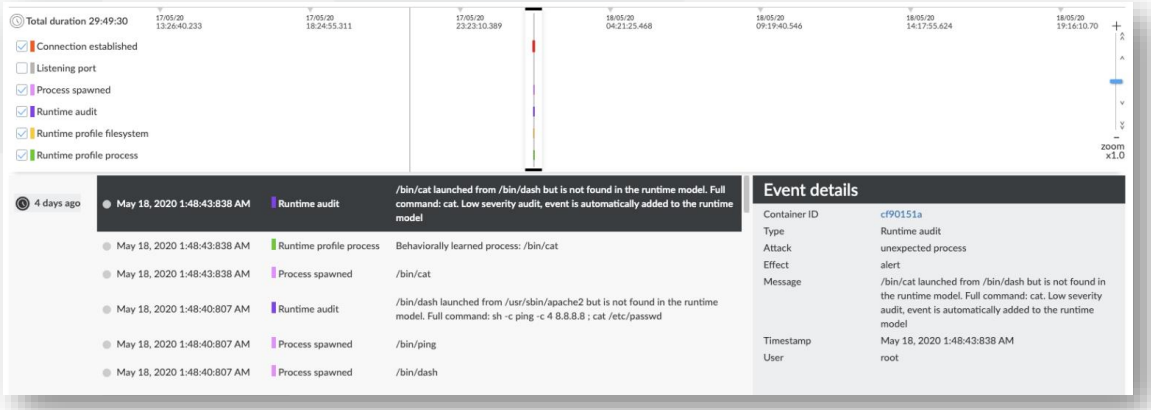
- One-click enforcement for CIS, PCI-DSS, HIPAA, GDPR, NIST SP 800-190, DISA STIG
- Custom compliance checks

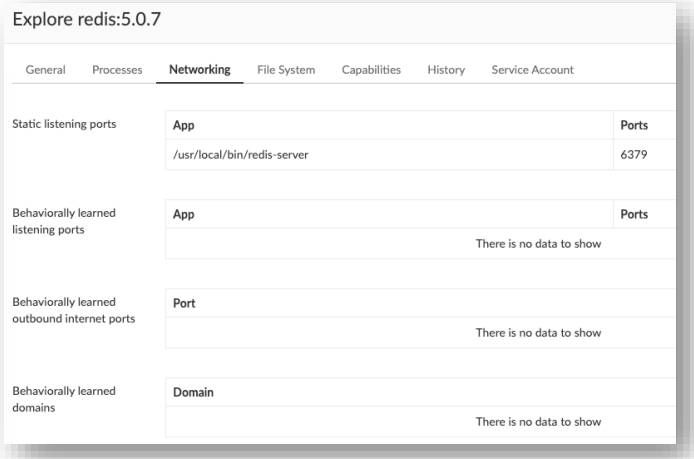


Runtime Defense

- Automatic modeling of explicit ‘allow lists’ for every app
- Automated incident detection and prevention based on model and threat indicators
- Continuous forensics for every container and host in your environment



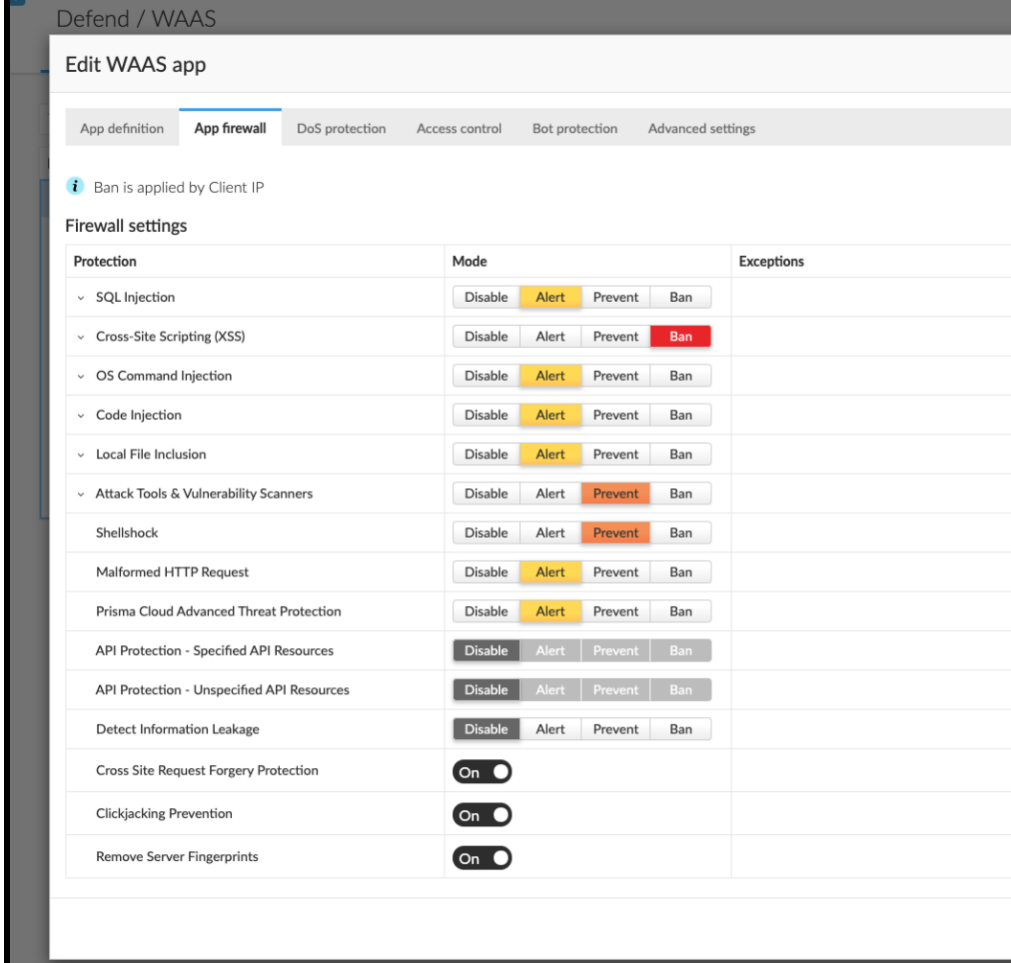




Protection for the OWASP Top 10

Protect cloud native applications against top attacks, including SQLi, XSS, LFI, Shellshock, and more

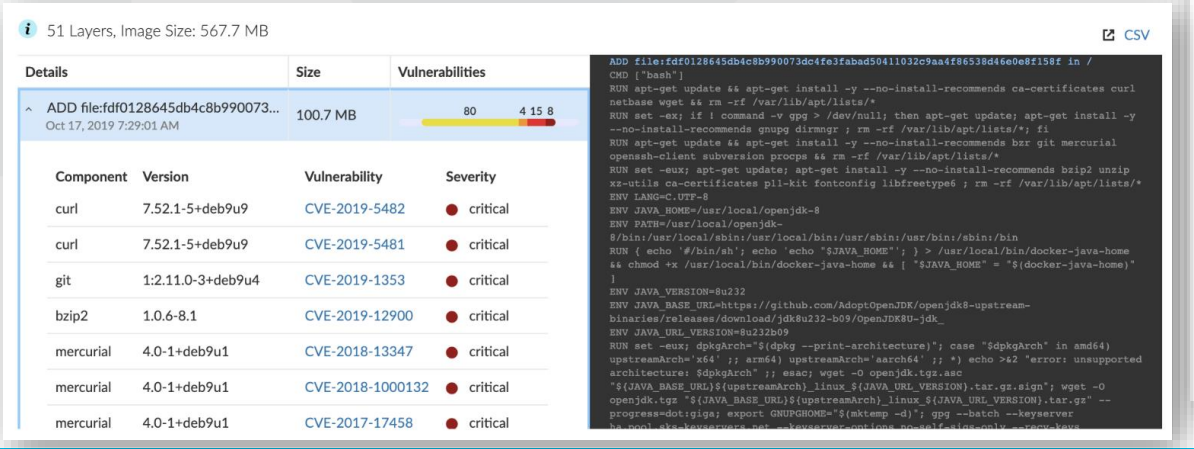
Fully-configurable protection for each application



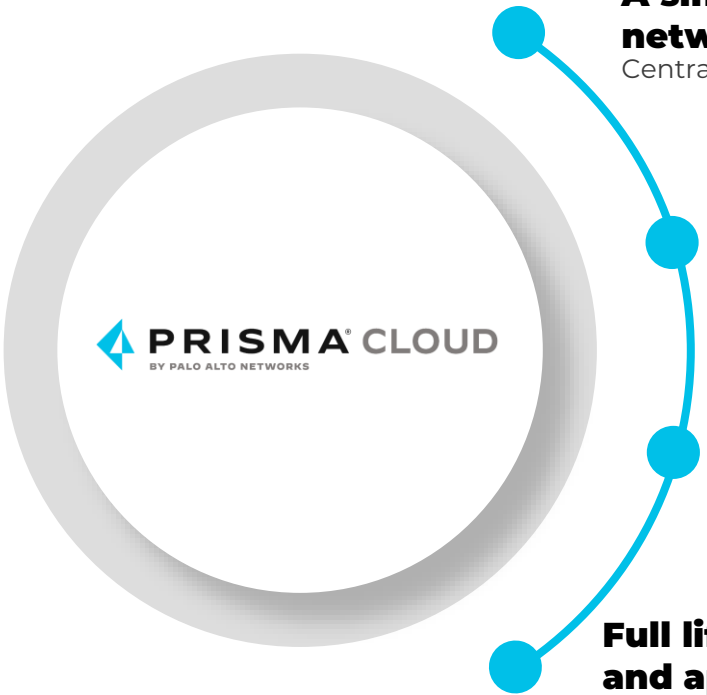
Vulnerability Management

- Industry leading precision across hosts, images, containers and serverless functions
- Automated prioritization of vulnerabilities based on your unique environment
- Layer analysis identifying vulnerabilities introduced in each layer
- Prevent running vulnerable software across your environment

Prioritize vulnerabilities based on the running environment



Prisma Cloud: Defining Cloud Native Application Protection Platforms



A single user experience to secure infra, apps, identities, networks, and data

Centralized policy management, auditing and protection instead of point solutions

Unified agentless and agent-based protection for Hosts, Containers and Serverless

Vulnerability management, compliance, and runtime protection spanning popular architectures

Integrated with SecOps tools to address issues and alerts

Security posture dashboards, or send results to SIEM, SOAR, or ChatOps systems

Full lifecycle security from code to cloud for infrastructure and applications

Identify vulnerabilities and misconfigurations, integrated with code repos, CI tools, CD workflows, and runtime

Prisma Cloud

Integrated capabilities for complete cloud native application protection

Cloud Code Security

Secure app artifacts, analyze code, and fix issues

Infrastructure as Code (IaC) Security

Cloud Security Posture Management

Monitor cloud security posture, detect and respond to threats, maintain compliance

Visibility, Compliance & Governance

Threat Detection

Cloud Workload Protection

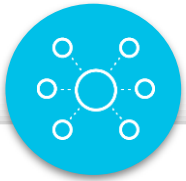
Secure hosts, containers, and serverless across the application cycle

Host Security

Container Security

Serverless Security

Web App & API Security



Cloud Network Security

Monitor and secure cloud networks, enforce microsegmentation

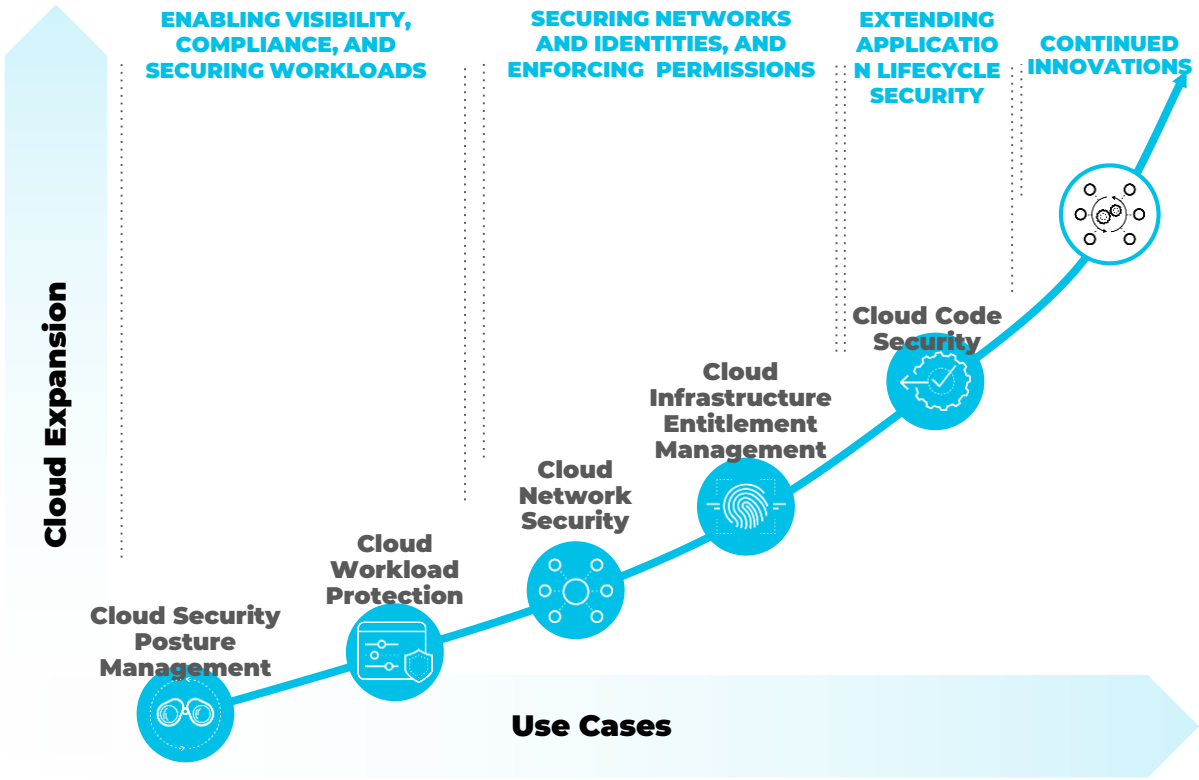
Identity-Based Microsegmentation

Cloud Identity Security

Enforce permissions and secure identities across workloads and clouds

Cloud Infrastructure Entitlement Management

Delivering integrated, best-in-class capabilities



Key Customer Value Drivers

- Integrated in one platform
- Common onboarding of resources
- Agentless and Agent-based protection
- Unified security scenarios

CUSTOMER SUCCESS STORIES

 |

Industry: Entertainment | **Region:** Global

Background

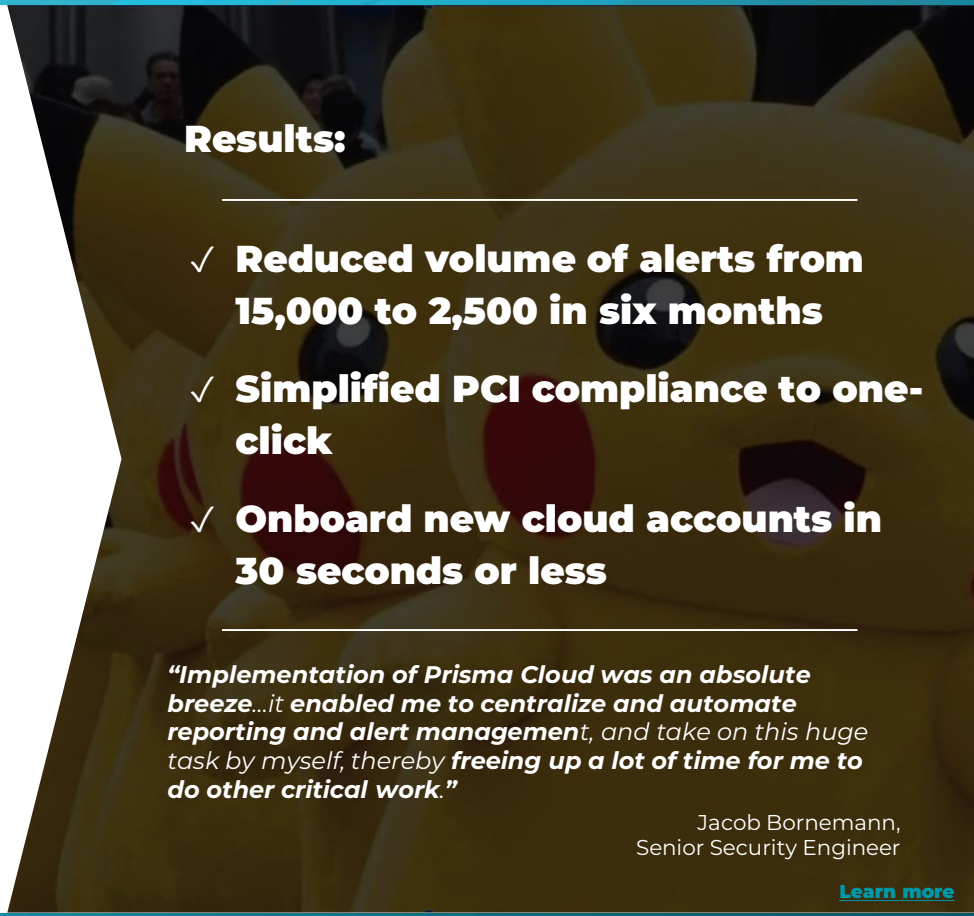
- Release of Pokémon GO drove an exponential explosion in digital traffic. Not built to handle the surge, the company looked to the cloud

Customer Challenges

- Protect the company's AWS cloud deployments, meet compliance, and scale to support rapid expansion and growing global user base

Security Solution

- Prisma Cloud: CSPM, Container Security, Host Security
- Gain complete visibility into their cloud environment
- Centrally manage security configurations across the diverse set of cloud applications and resources
- Effectively meet new, stringent PCI compliance requirements



Results:

- ✓ **Reduced volume of alerts from 15,000 to 2,500 in six months**
- ✓ **Simplified PCI compliance to one-click**
- ✓ **Onboard new cloud accounts in 30 seconds or less**

***"Implementation of Prisma Cloud was an absolute breeze**...it **enabled me to centralize and automate reporting and alert management**, and take on this huge task by myself, thereby **freeing up a lot of time for me to do other critical work**."*

Jacob Bornemann,
Senior Security Engineer

Learn more

 |

paloalto NETWORKS

IRON MOUNTAIN®

Industry: Technology | **Region:** USA

Background

- Iron Mountain stores and protects billions of valued assets, including critical business information, highly sensitive data, and cultural and historical artifacts.

Customer Challenges

- Gain comprehensive visibility and security across multi-cloud infrastructure, maintain compliance, and scale quickly and efficiently.

Security Solution

- Prisma Cloud: CSPM, Container Security, Host Security
- Shift left and integrate security throughout the CI/CD pipeline, without adding friction
- Continuously monitor for compliance violations in a cloud-agnostic manner

Results:

✓ **Unified view of all deployed resources across multi-cloud environment**

✓ **Reduces time gathering evidence for compliance audits by 2 hours**

✓ **Enables DevSecOps with robust shift-left capabilities**

"Prisma Cloud not only made my job and my team's jobs so much easier; it made our jobs possible. *We didn't have this type of insight into our environment... now, we have a solution with everything laid out in one place where we can dive deeper and see a robust picture."*

David Williams
Cloud Manager

Learn more

 |

paloalto NETWORKS

Leader: Forrester Wave™: Cloud Workload Security, Q1 2022

"While point solution providers are still relevant for technical innovation, Forrester sees end-user organizations increasingly preferring suite providers."

Top scores in 18 categories including:

- High availability/data sovereignty, scalability
- Agent deployment, malware, memory integrity
- Reputation services, log inspection, supported OSs
- Azure coverage
- Infrastructure-as-Code (IaC)
- Integrations
- CWP, CIEM, and Container Protection future plans

SOURCE: Forrester Wave™: Cloud Workload Security, Q1 2022

 |

OUR BEST-IN-CLASS PLATFORMS

We provide next-gen cybersecurity to enable transforming enterprises

Security Analytics and Automation

Network Security

Best-in-class Network Security Platform across hardware, software and SASE - securing hybrid workforces and complex infrastructures of today

Cloud Security

Comprehensive cloud-native application protection platform from development to runtime, across multi-cloud and hybrid environments

Endpoint Security

The next-generation SOC platform with unparalleled threat visibility, detection and response

Threat Intelligence and Incident Response

THANK YOU

 |