PRISMA
BY PALO ALTO NETWORKS

# Prisma Cloud 3.0
## Best-In-Class Cloud Native Application Protection Platform

Presented By

Sebastian Straube
Lead Cloud Solution Architect DACH

sstraube@paloaltonetworks.com
linkedin.com/in/sebastianstraube

paloalto NETWORKS

# We’re trusted by the world’s most valuable enterprises to keep them secure.

## Securing more than 85,000+ customers globally

9 of 10
of the Fortune 10

10 of 10
Largest Utilities in the World

8 of 10
Largest Manufacturing Companies in the World

8 of 10
Largest U.S. Banks

6 of 10
Largest Oil & Gas in the World

7 of 10
Top U.S. Hospitals

 © 2022 Palo Alto Networks, Inc. All rights reserved.

# Prisma Cloud

Top customers worldwide **trust us** to secure their cloud environments

| | |
|---|---|
| BANKING & FINANCE |         |
| TECHNOLOGY |         |
| HEALTHCARE |       |
| MEDIA & RETAIL |         |
| GOVERNMENT |          |
| INDUSTRIAL & TELECOM |       |

 © 2022 Palo Alto Networks, Inc. All rights reserved.

# Log4j Vulnerability and Threat Prevention Response Timeline

**2021-12-09 21:14 -** *signature 91991 published as part of content update 8498*

A remote code execution (RCE) vulnerability in Apache log4j was identified being exploited in the wild.

**Dec. 9, 2021**

**2021-12-10 15:50 -** *updated signature 91991 published as part of content update 8499*


NIST publishes CVE-2021-44228 Critical Alert with CVSS of 10.

**Dec. 10, 2021**

**2021-12-12 17:06 -** *signatures 91994 and 91995 published as part of content update 8500*

Apache releases updates 2.15.0, 2.15.1, and 2.16.0

**Dec. 16 - 13, 2021**

**2021-12-14 12:00 -** *updated signatures 91994 and 91995 published as part of content update 8501*

**2021-12-14 21:54 -** *signature 92001 and updates to 91994 and 91995 published as part of content update 8502*

**2021-12-16 21:37 -** *signatures 92006 and 92007 added and updates to 92001 published as part of content update 8504*

Apache updates CVE-2021-45046 to include another Critical RCE vulnerability in 2.15.1

**Dec. 17, 2021**

**2021-12-17 18:35 -** *updated signature 92007 to Critical as part of content update 8505*

**2021-12-18 23:18 -** *signature 92012 to cover new vuln and update to 91991 published in 8506*

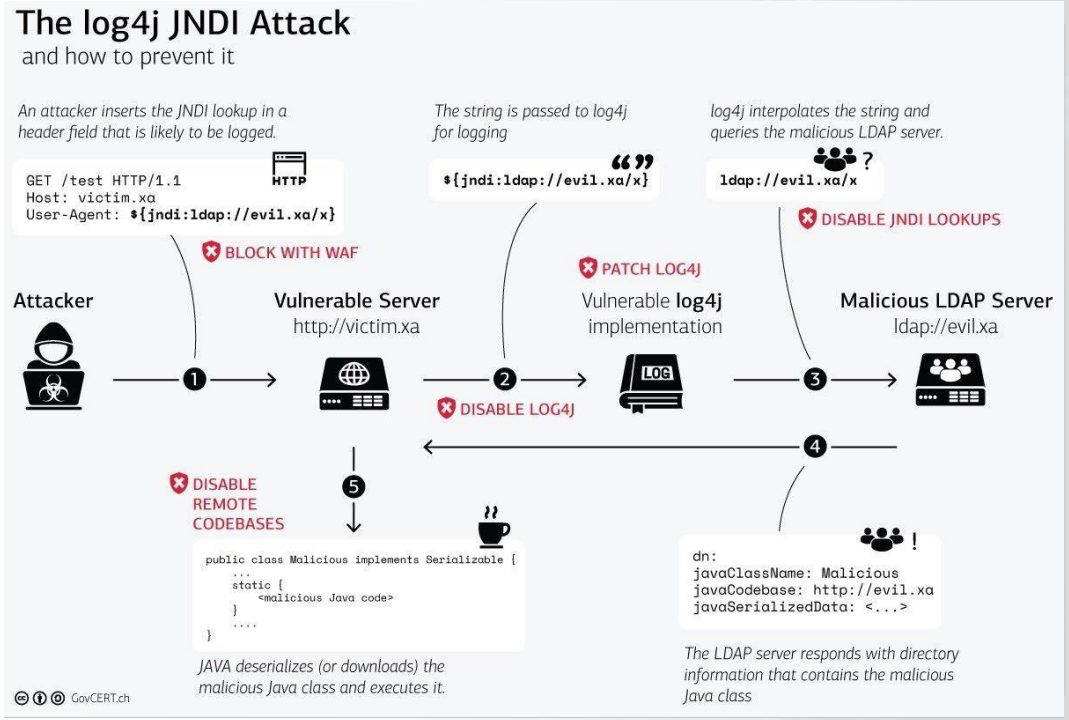
Apache releases log4j 2.17.0 to address CVE-2021-45105, High severity DoS vulnerability in 2.16.0

**Dec. 18, 2021**

**Widespread scanning, confirmed coin miners / botnets**

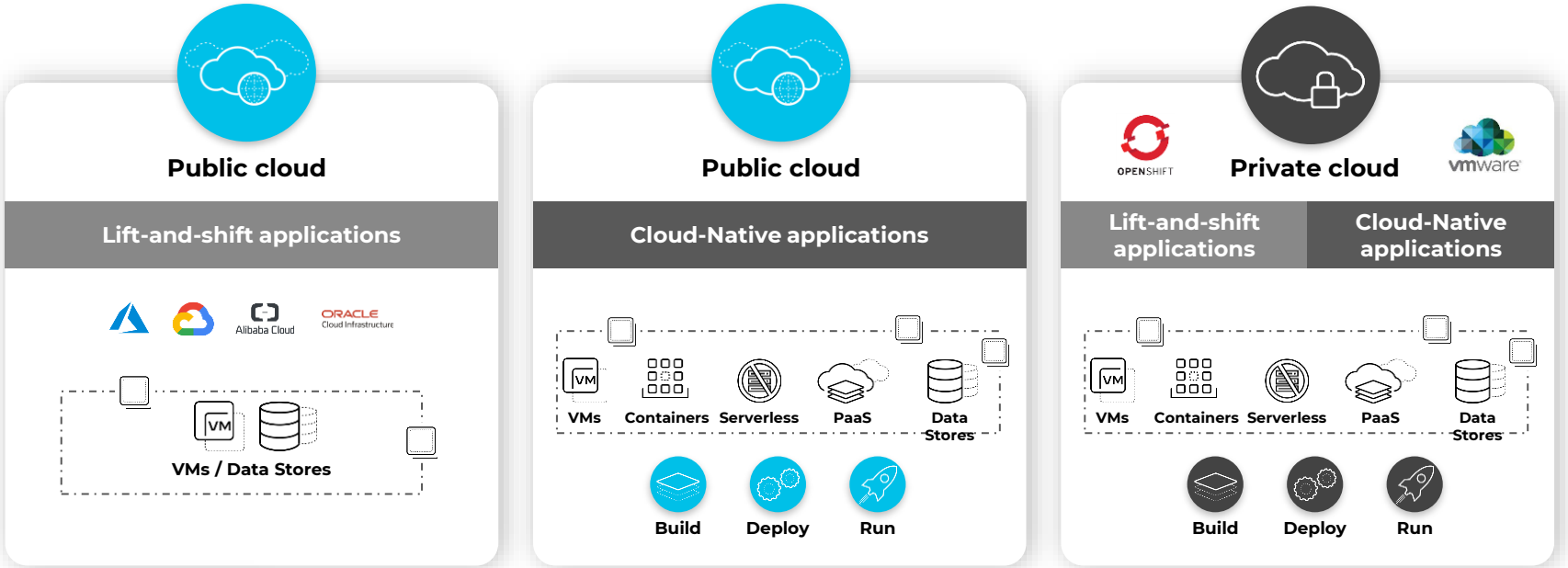
# CVE-2021-44228
# Apache Log4j Vulnerability

- **Software:** Log4j
- **Severity:** Critical
- **Versions:** Log4j 2.x through 2.15.0-rc1
- **Usage:** Attackers submitting a specially crafted request to a vulnerable system, depending on how the system is configured, an attacker is able to instruct that system to download and subsequently execute a malicious payload.




 © 2022 Palo Alto Networks, Inc. All rights reserved.

# Application and Infrastructure security dependencies are stretched across multi-cloud and hybrid-cloud environments




Gartner

**81% of organizations** are working with two or more public cloud providers.

 © 2022 Palo Alto Networks, Inc. All rights reserved.

paloalto NETWORKS

# Public cloud security is a shared responsibility

**Customers**

Responsible for security **in** the cloud

- Data
- Hosts, Containers, Functions
- Networks
- Users & Credentials
- Resource Configurations

**Cloud Service Provider**

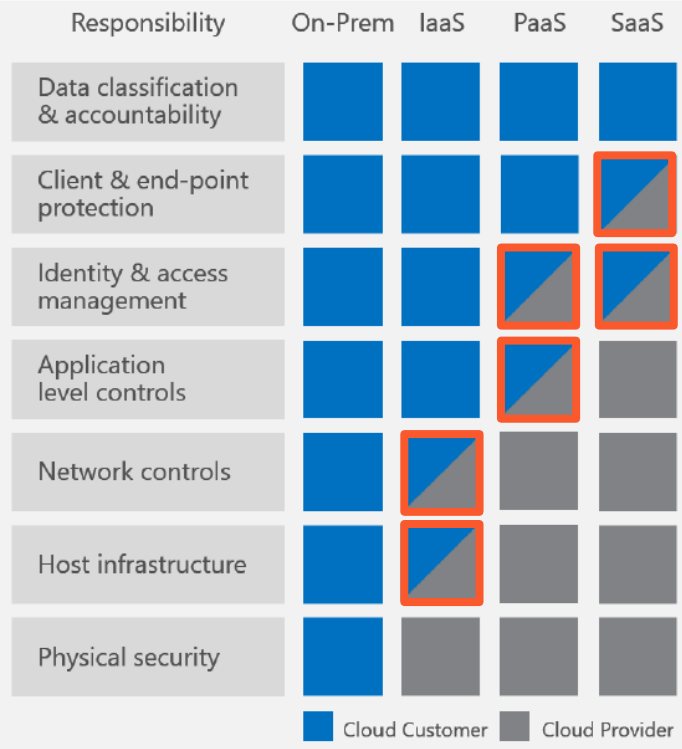
Responsible for security **of** the cloud

- Routers
- Switches
- Hypervisor
- Hubs
- Data Center

aws Azure ORACLE Cloud Infrastructure Alibaba Cloud

 © 2022 Palo Alto Networks, Inc. All rights reserved.

# Impact of Shared Responsibility - What is the cloud customer in charge of?

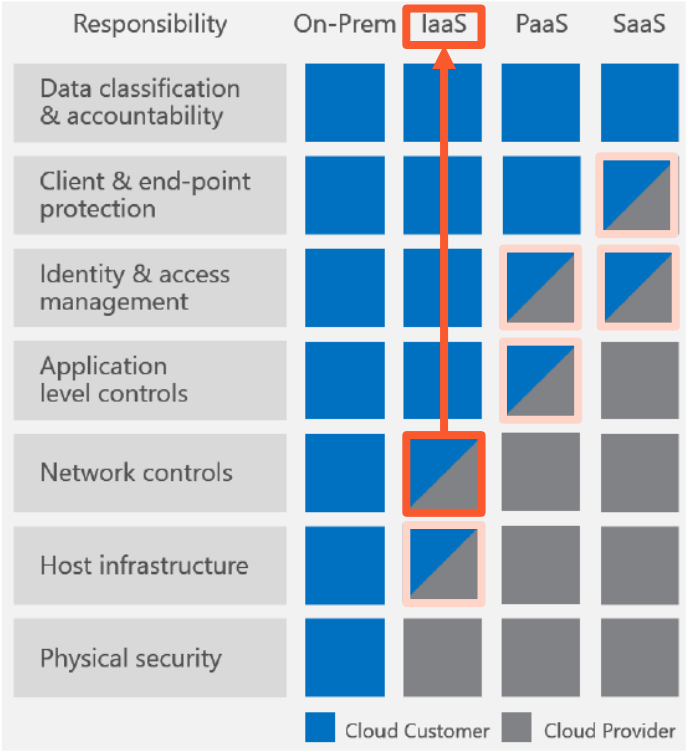



Cloud Environments

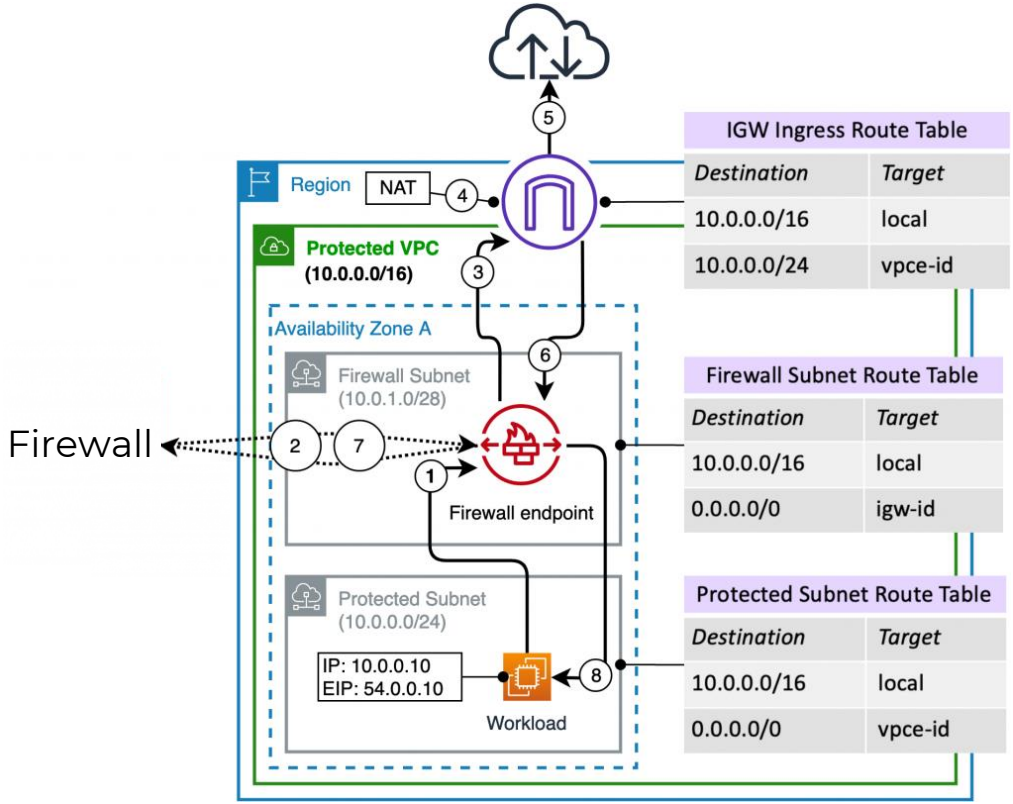
- Corner case create security gaps that are hard to detect
- Configuration of different layers and the interaction between them is hard to manage
- Responsibility for the cloud provider is clear > AGB, the customer is in charge.

 © 2019 Palo Alto Networks. All Rights Reserved.

# Impact of Shared Responsibility

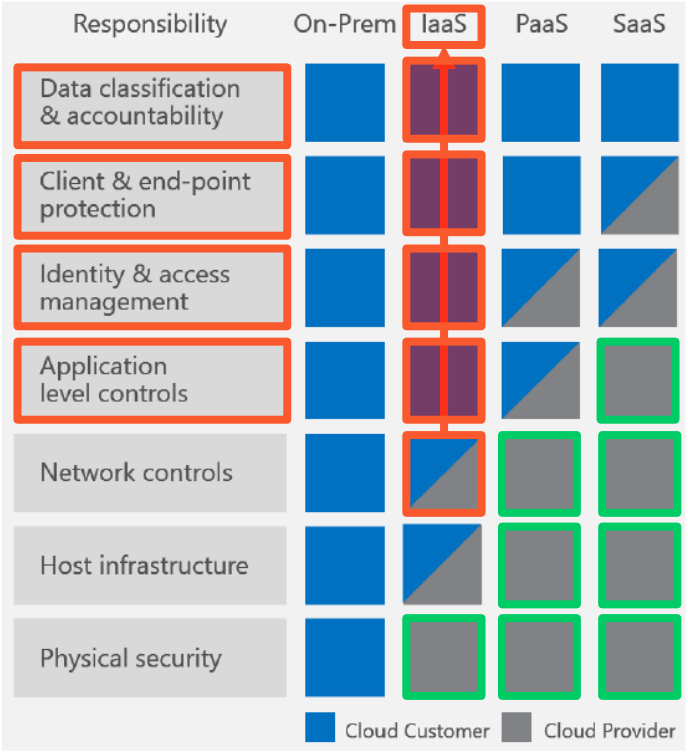



Cloud Network Security POC configuration

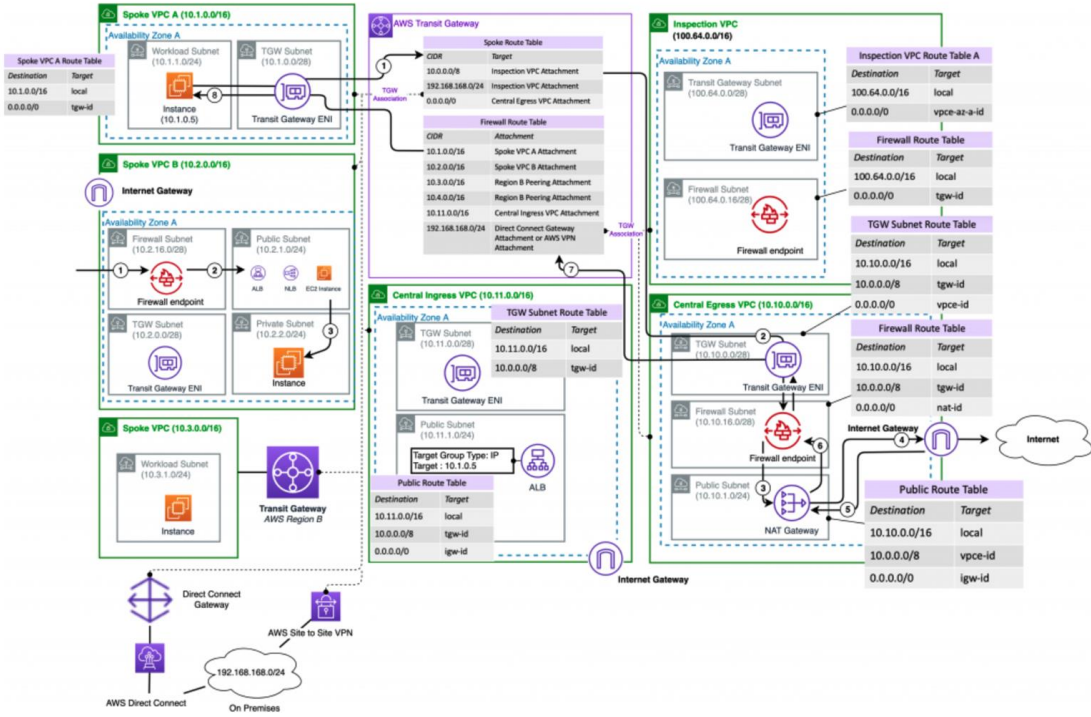



 © 2019 Palo Alto Networks. All Rights Reserved.

# Cloud Network Security and Impact of Shared Responsibility



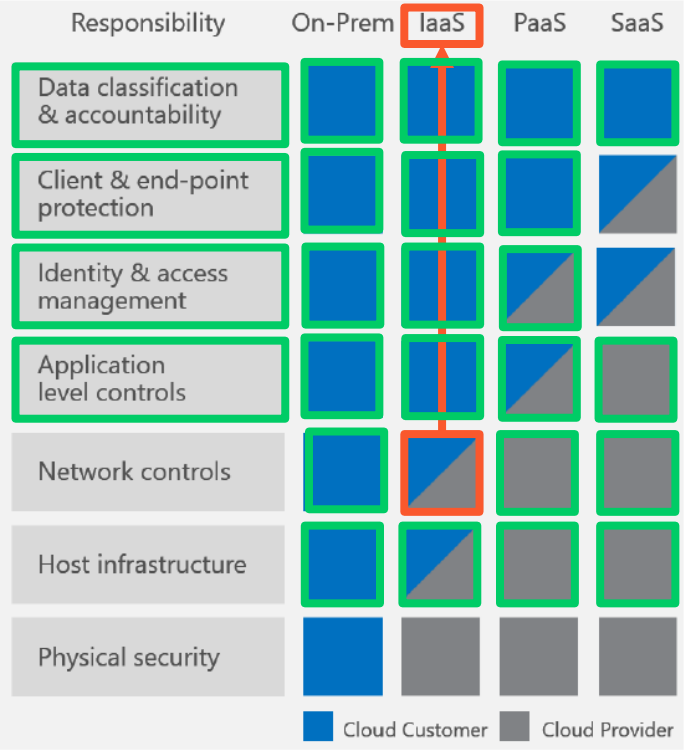

It is complicated to configure and to maintain




 © 2019 Palo Alto Networks. All Rights Reserved.

paloalto NETWORKS

# Impact of Shared Responsibility



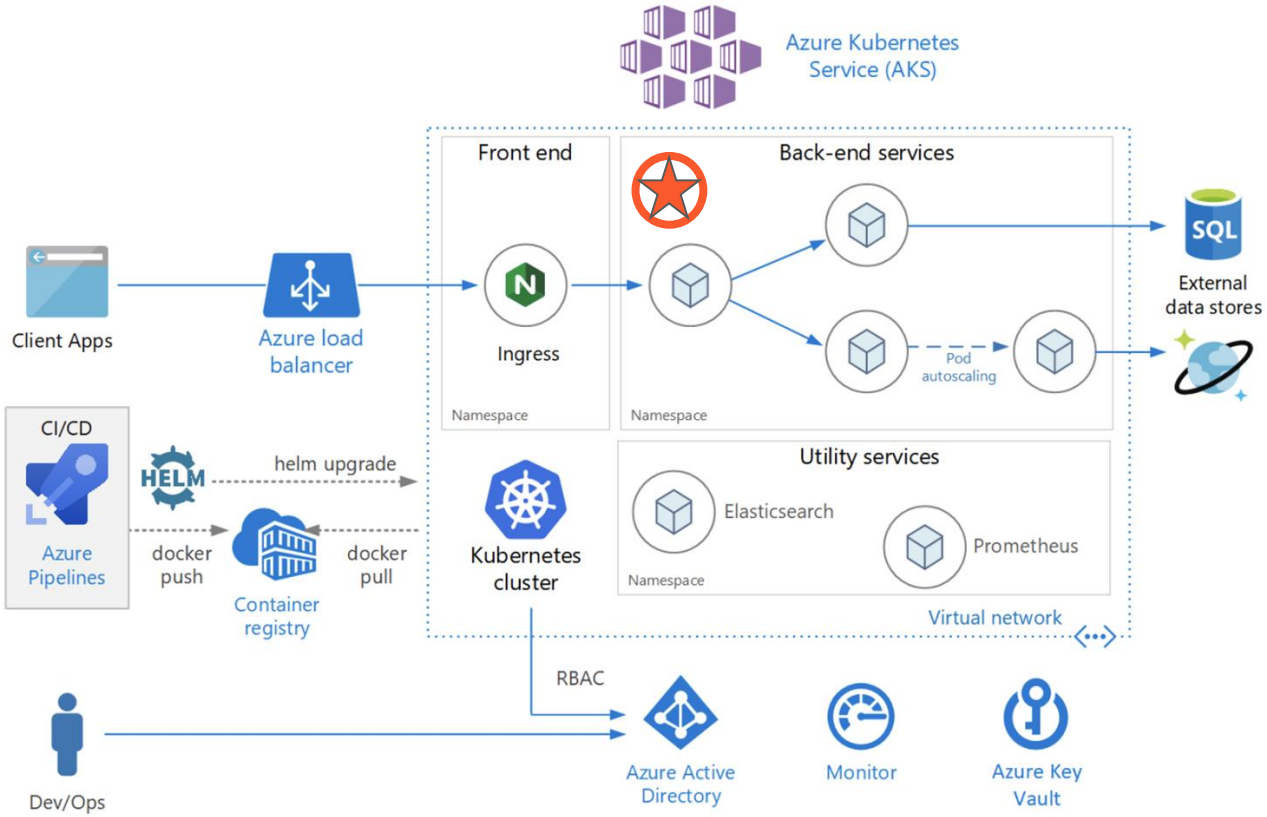

Prisma Cloud

- Provides compliance checks and configuration visibility against best practices checks
- Prevents Attacks and Intrusions in app from L7 into infrastructure stack
- Provides Confidence detecting breaches and incidents from inside and outside
- Enables Shift-Left Security for Dev(Sec)Ops Teams
- We check identities and least privileges configurations

 © 2019 Palo Alto Networks. All Rights Reserved.

# Audit Trail through Cloud Native Services and App Infrastructure

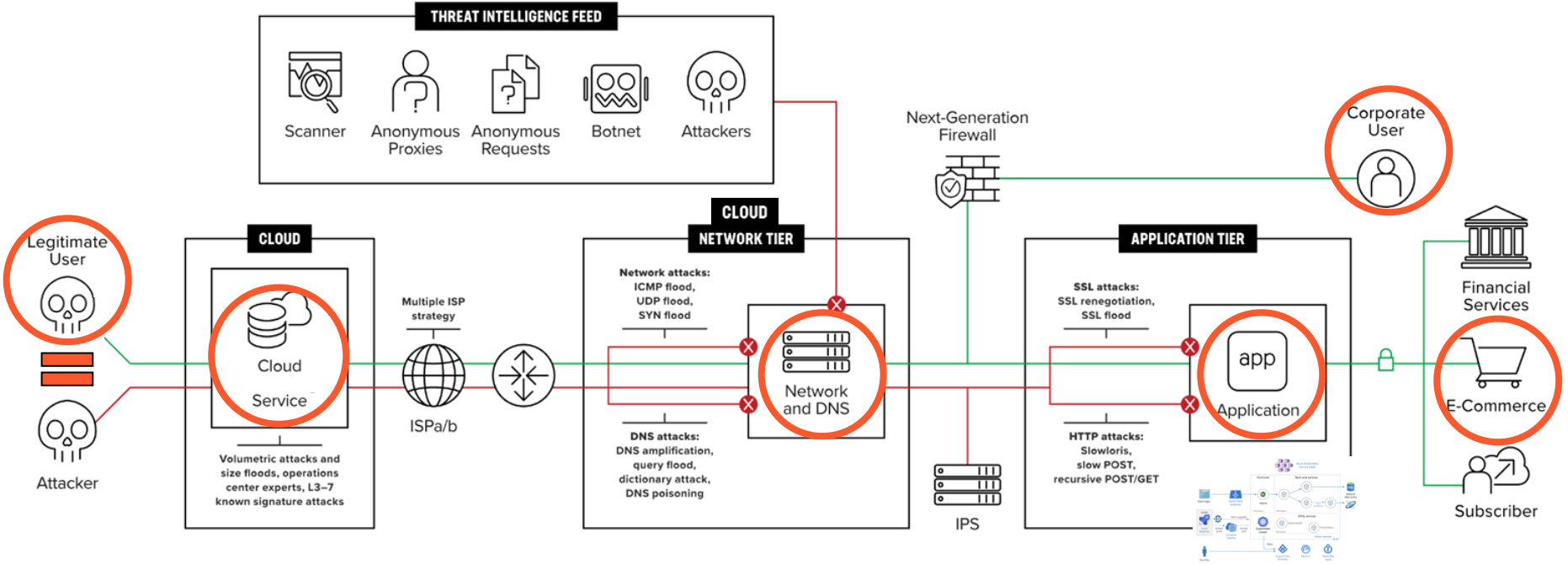
- We can identify and alert  in real time the cloud resource in which the incident happened
- We check in realtime from inside app (OS and infrastructure) and outside the app (network activities and misconfigurations)
- We provide the ability for top5 (AWS, Azure, GCP, OCI, Alibaba) cloud provider




 © 2019 Palo Alto Networks. All Rights Reserved.

# Cloud Native Service and App Security Controls

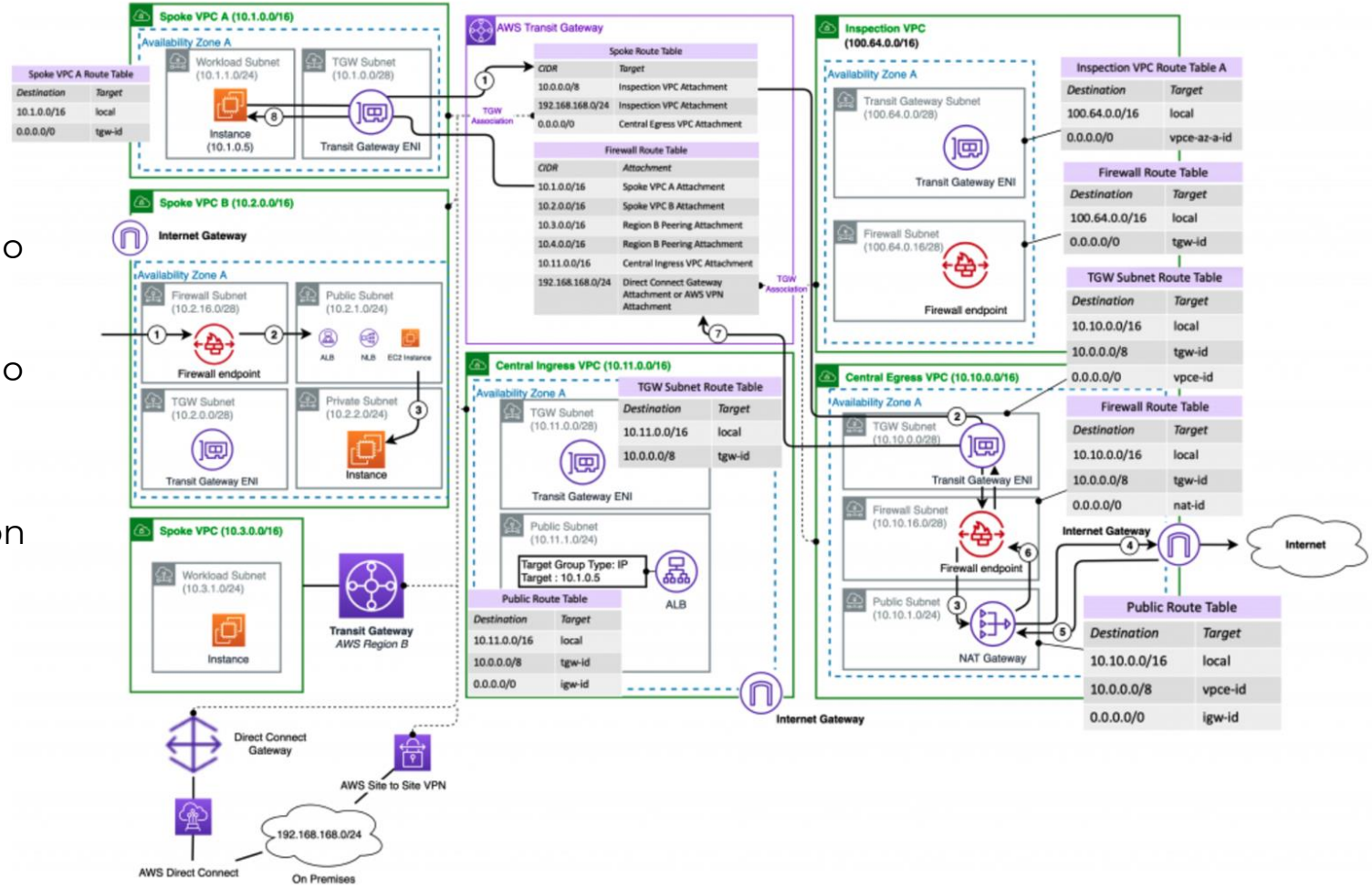
- What happens when the attacker breaches into the app environment - e.g. through  XSS, Hijack, code injection
- We search for relevant data points of the incident in network configurations, cloud infrastructure, user behaviour, user identity and application infrastructure




 © 2019 Palo Alto Networks. All Rights Reserved.

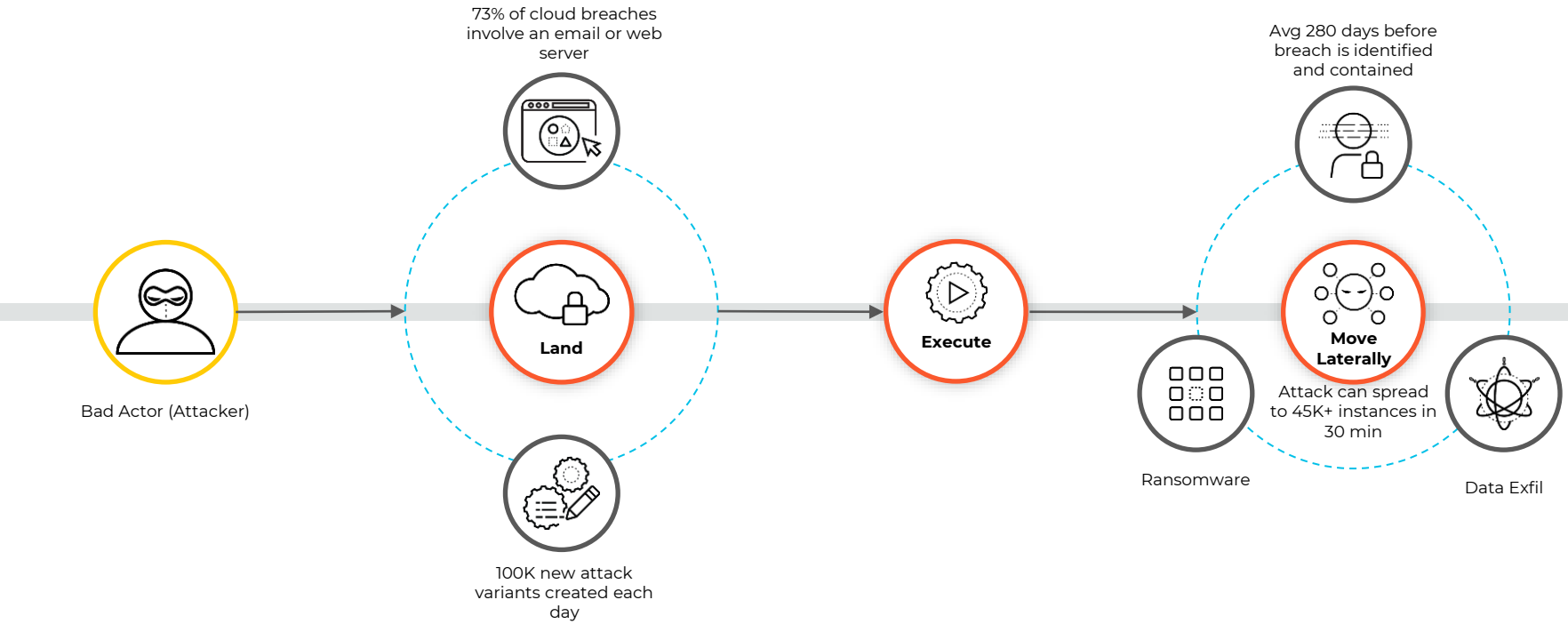
# Cloud Network Security configuration of a small environment

- Misconfigurations are easily possible
- Misconfigurations lead to security breaches and data exfiltration




 © 2019 Palo Alto Networks. All Rights Reserved.

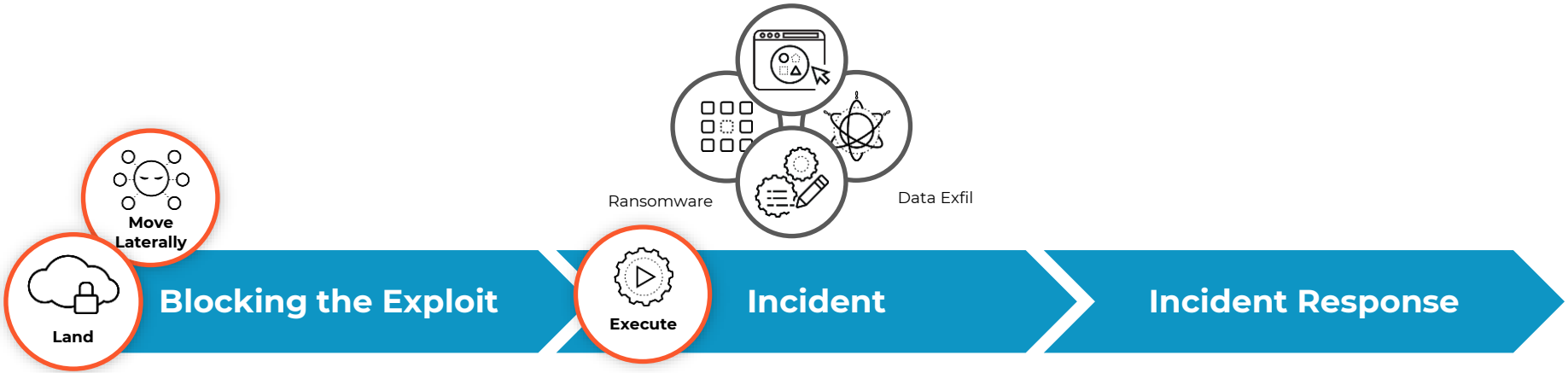
# Vulnerabilities and Misconfiguration lead to compromised infrastructure




| Attack Lifecycle: | 1. Penetrate | 2. Execute | 3. Move Laterally |
|---|---|---|---|

Sources: Unit 42 Research

# Palo Alto Networks Portfolio Protects Customers from the Apache Log4j Vulnerability




### Stop-Gaps While Patching

Prisma Cloud
WAF + API Security
MicroSegmentataion

### Investigate Vulnerable Assets

Prisma Cloud
Workload Protection
Cloud Posture

### Remove Risk and Exposure

Prisma Cloud
Historical Audit Trial
Forensic Data

## Customers Need to Patch!

# Customers need a growing number of capabilities to secure their cloud environments

**Visibility, Compliance, Governance**

Misconfigurations

Compliance

Advanced threats (Cryptomining, Account Compromise)

**Workload Security**

Vulnerabilities - Host, Container, Serverless

Runtime Threats

Web Application & API Protection

**Network Security**

Cloud-Native Network Segmentation

Network Threat Prevention / NGFW

**Identity Security**

Identity and Access Misconfiguration

Over-Privileged Access

**Application Lifecycle Security**

Code vulnerabilities, CI / CD pipeline vulnerabilities

 © 2020 Palo Alto Networks, Inc. All rights reserved.

# 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 integrated in CI/CD Pipeline

### Cloud Security Posture Management

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

Visibility, Compliance & Governance

Threat Detection

Data Security

### Cloud Workload Protection

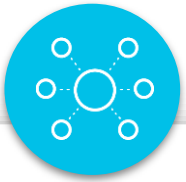
Secure hosts, containers, and serverless across the application cycle

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

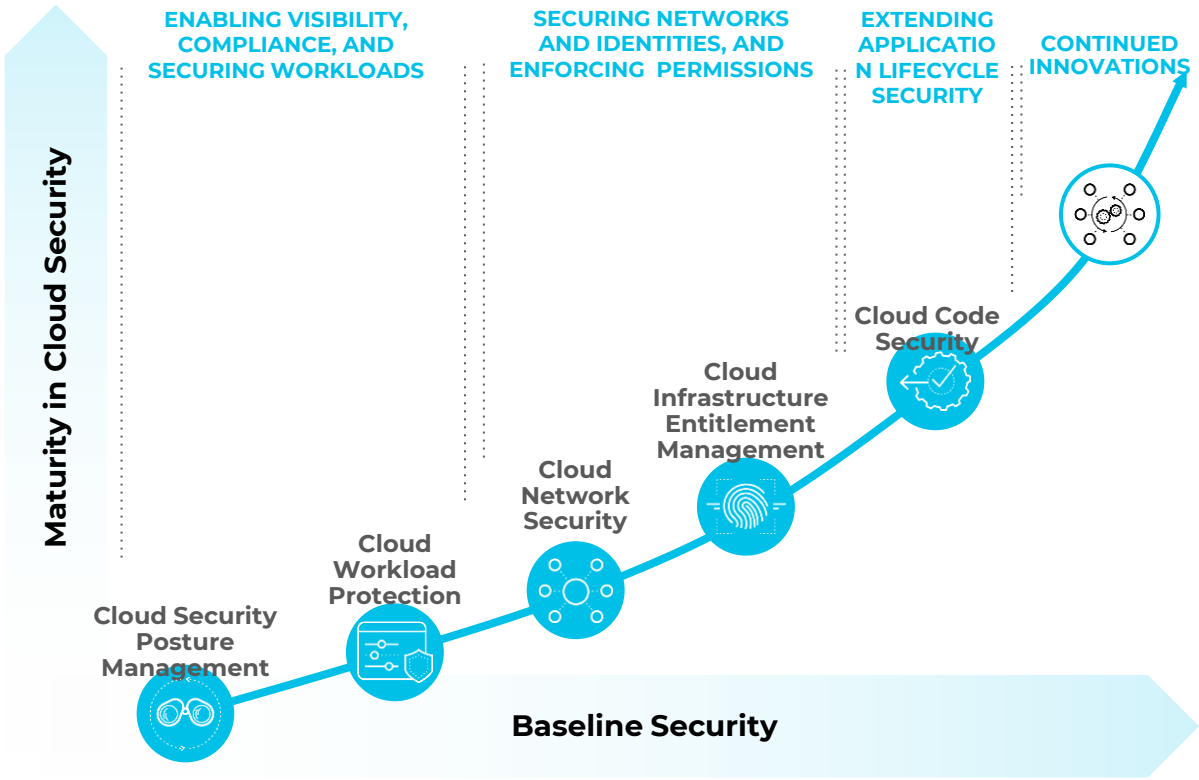
Enforce permissions and secure identities across workloads and clouds

Cloud Infrastructure Entitlement Management

**Cloud Native Application Lifecycle Security through Build-Deploy-Run Phase**

 © 2022 Palo Alto Networks, Inc. All rights reserved.

# Cloud Security: step by step approach

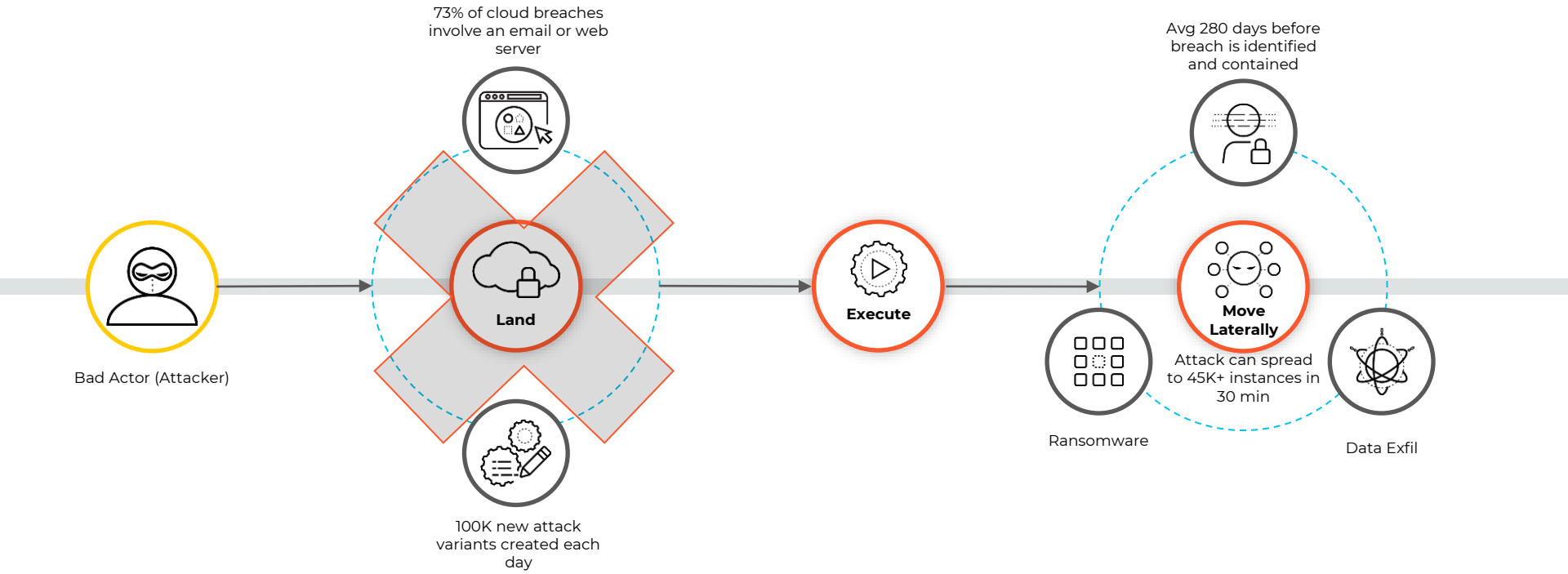



## Key Value

- All Security Use-Cases Integrated in one platform
- Common alerting and routing of security incidents
- Workload protection based on real time and snapshots
- Raise cross-organizational maturity against security threats

 | © 2022 Palo Alto Networks, Inc. All rights reserved.

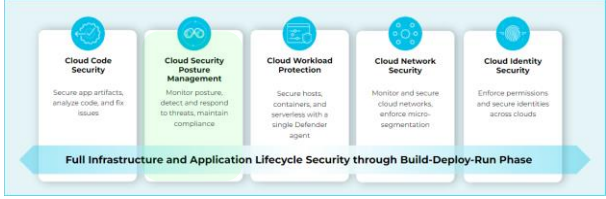
# Vulnerabilities and Misconfiguration lead to compromised infrastructure




| Attack Lifecycle: | 1. Penetrate | 2. Execute | 3. Move Laterally |
|---|---|---|---|

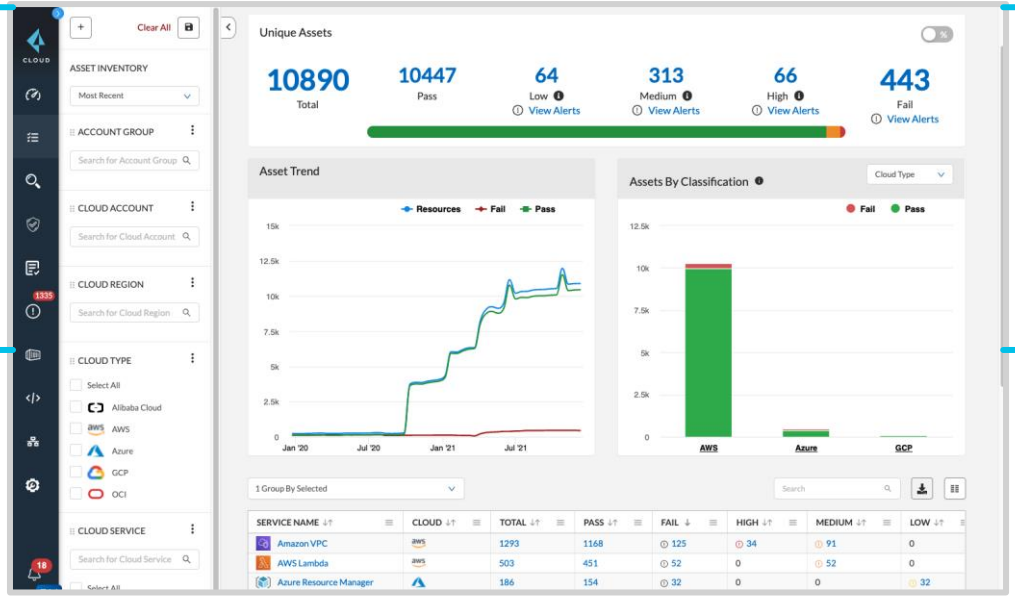
Sources: Unit 42 Research

# Cloud Security Posture Management to achieve compliance and secure multi-cloud environments




**Multi-cloud visibility and security**
Support for the world's 5 largest clouds, including AWS, Azure, Google Cloud, Alibaba Cloud, and OCI

**Optimized compliance**
Real-time and historical compliance with over 40 pre-build frameworks



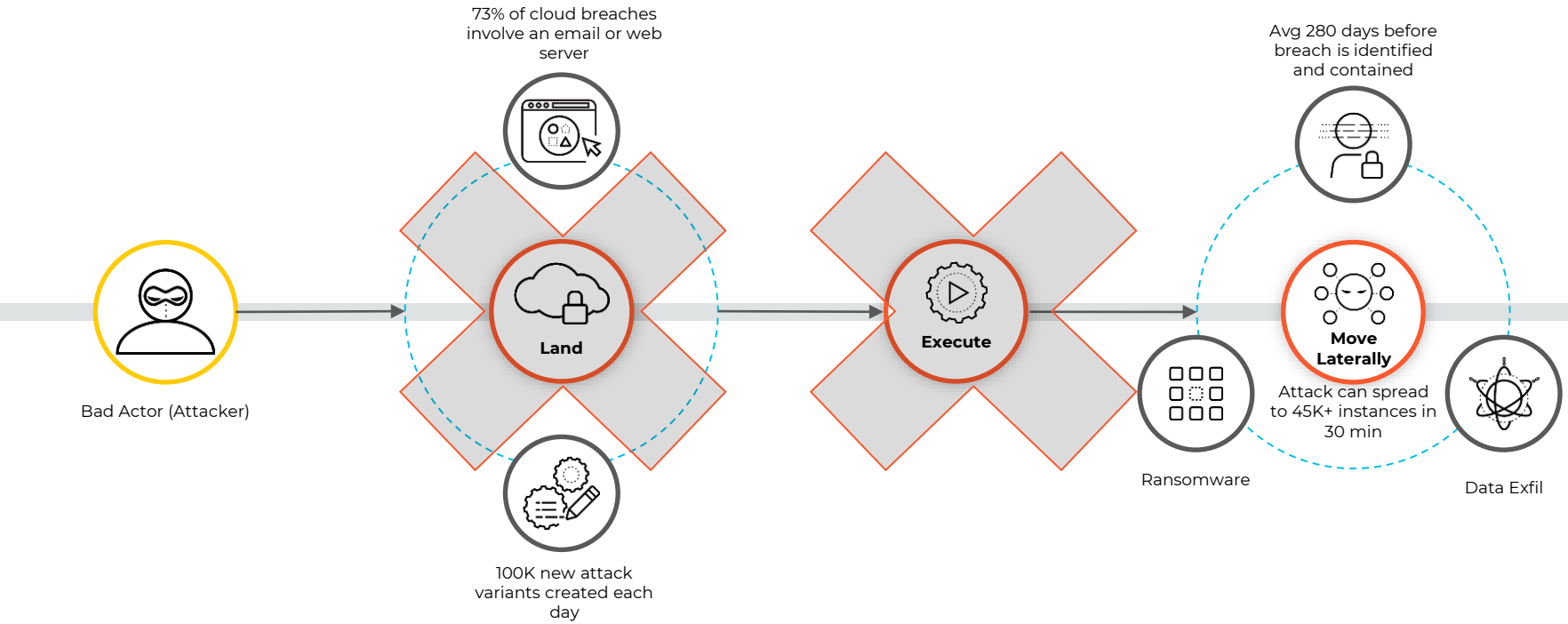

**Integrated threat detection**
Monitor and analyze cloud audit logs and network flow logs to detect and prevent threats

**Scan and secure public cloud data**
Audit cloud storage and identify personal information and malware, integrated with WildFire

**Easy onboarding and proven scalability**
Unify users and cloud accounts in a single UI for managing and enabling cloud security

 © 2022 Palo Alto Networks, Inc. All rights reserved.

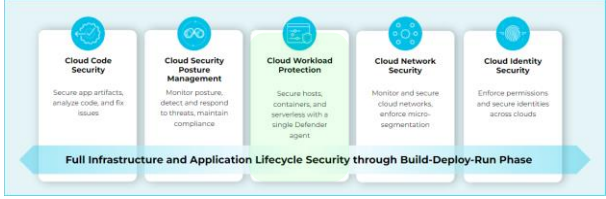
# Vulnerabilities and Misconfiguration lead to compromised infrastructure



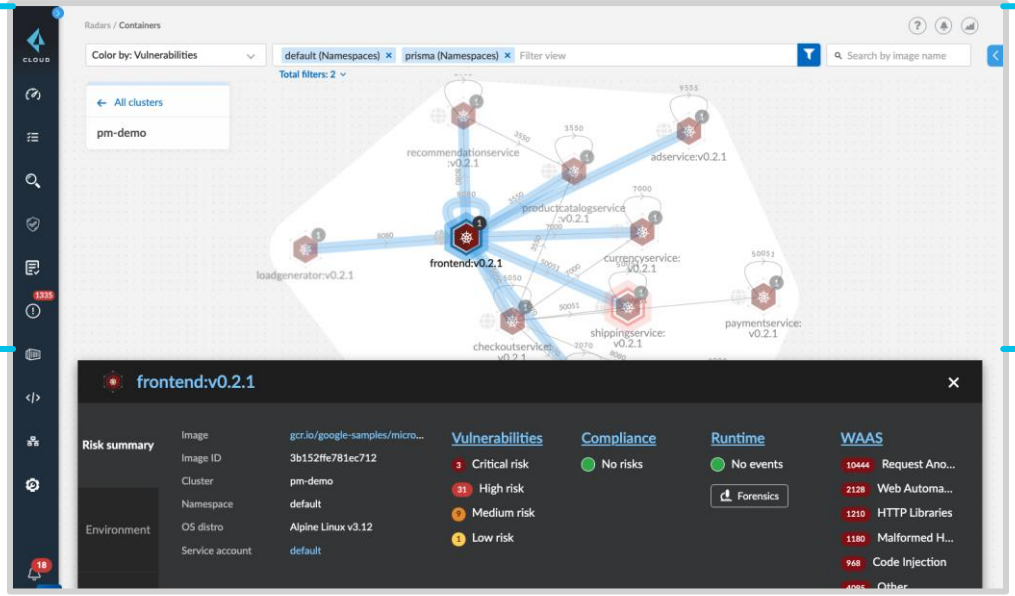

**Attack Lifecycle:** | **1. Penetrate** | **2. Execute** | **3. Move Laterally**

Sources: Unit 42 Research

# Cloud Workload Protection to secure hosts, containers, and Serverless-Functions




**Agent-based protection and Agentless scanning**
Protect hosts, containers, and serverless all from a central Console




**Runtime protection and forensics**
Secure all application tech stacks and investigate events and incidents

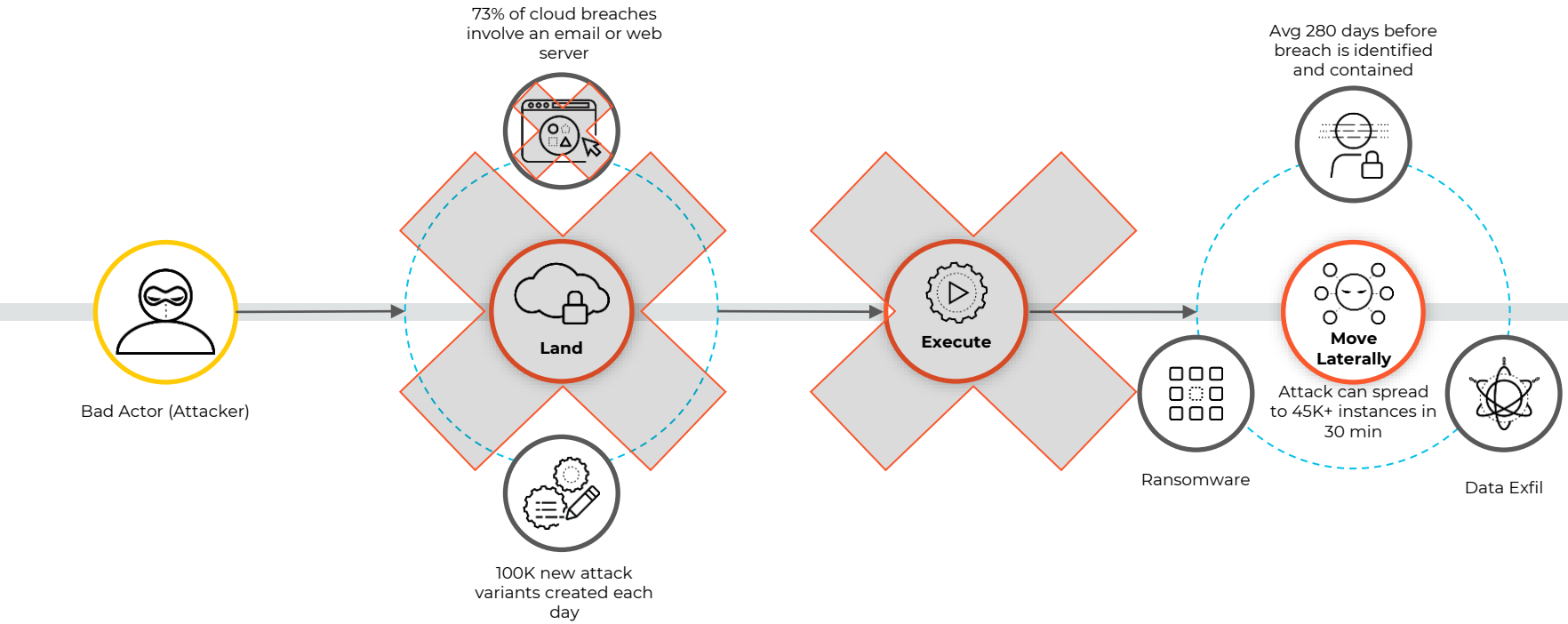
**Accurate vulnerability management**
Recognized Leader in vulnerability management and risk prioritization across OS, images, and functions

**Cloud native compliance**
400+ checks covering the Linux, Docker, and Kubernetes CIS Benchmarks, plus Windows and Istio

**Integrated Web Application & API Security**
Protection including OWASP Top 10, API protection, bot risk management, and more

 © 2022 Palo Alto Networks, Inc. All rights reserved.

# Vulnerabilities and Misconfiguration lead to compromised infrastructure

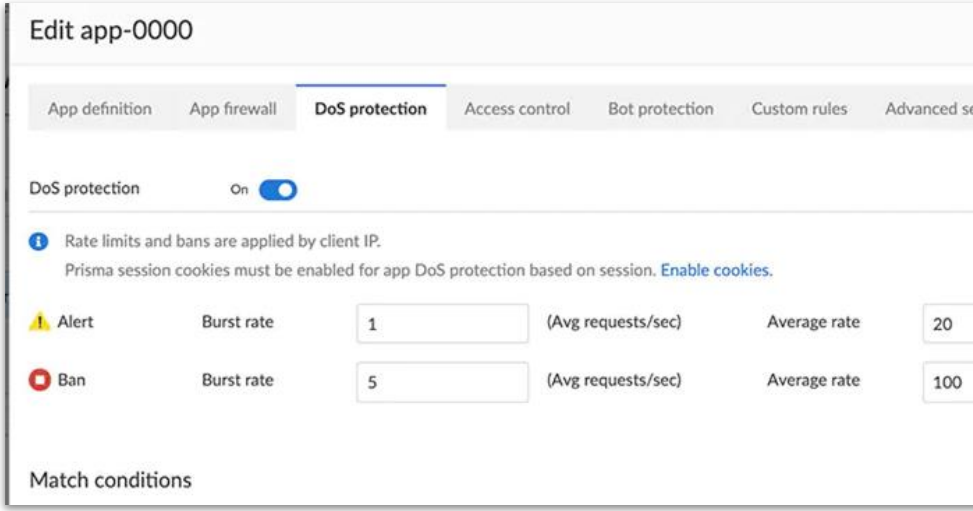



Sources: Unit 42 Research

# Web Application and API Security - Protect web applications and APIs across any public or private cloud.

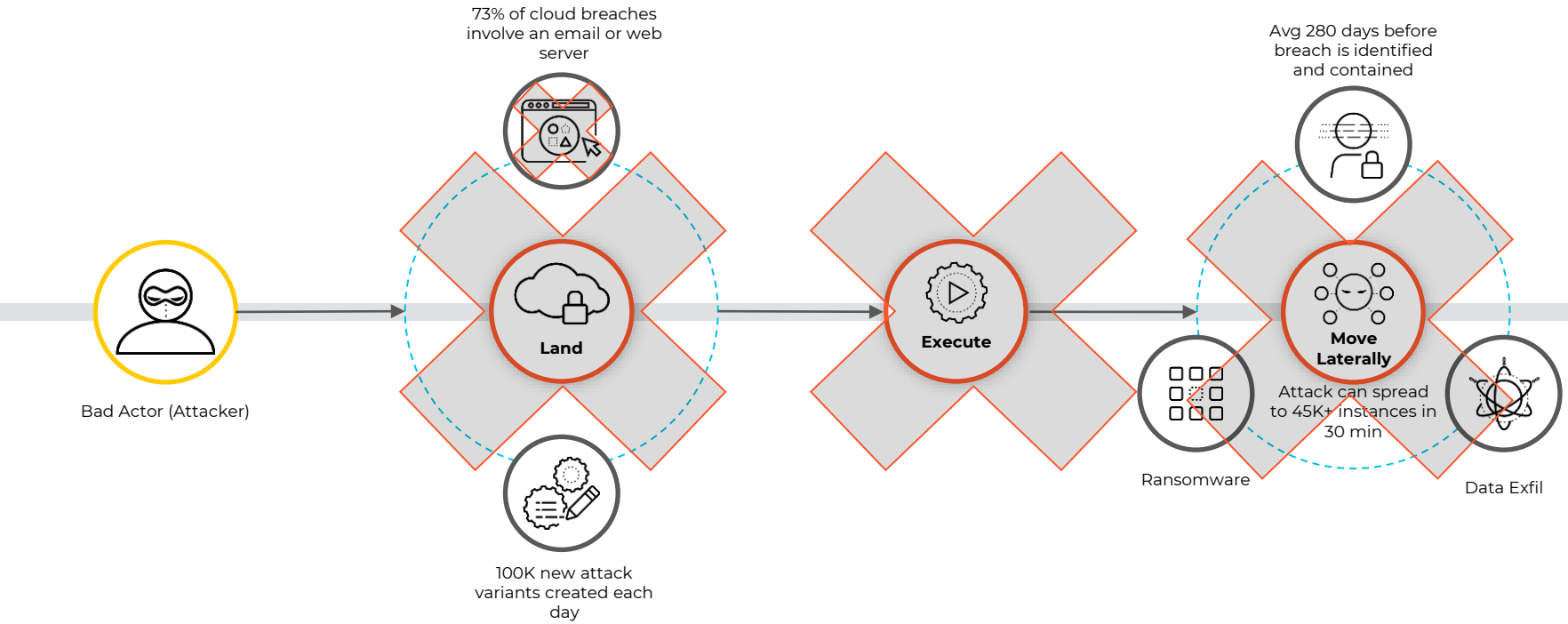

Prisma® Cloud WAAS provides an integrated approach to Web Application and API Security as part of our Cloud Native Security Platform, supporting the OWASP Top 10 and API protection, along with capabilities like Vulnerability Management, Compliance, and Runtime Defense. The WAAS module automatically detects and protects microservices-based web applications and APIs in cloud and on-premises environments.

- OWASP Top 10 protection
- Application and API Protection
- Bot risk management
- Virtual patching (using Custom Rules)
- Application DoS protection
- Continuous Event visibility




 © 2020 Palo Alto Networks, Inc. All rights reserved.

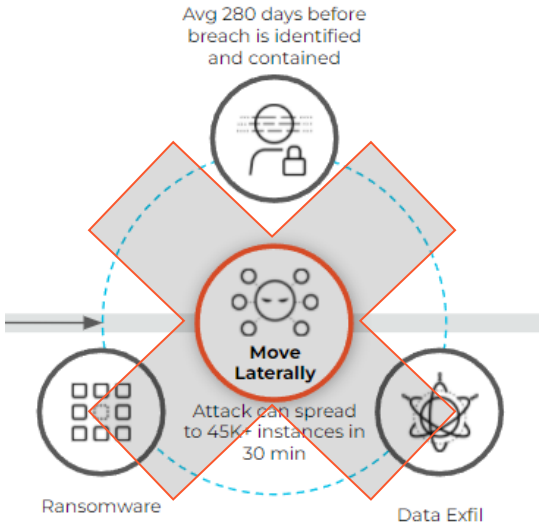
# Vulnerabilities and Misconfiguration lead to compromised infrastructure

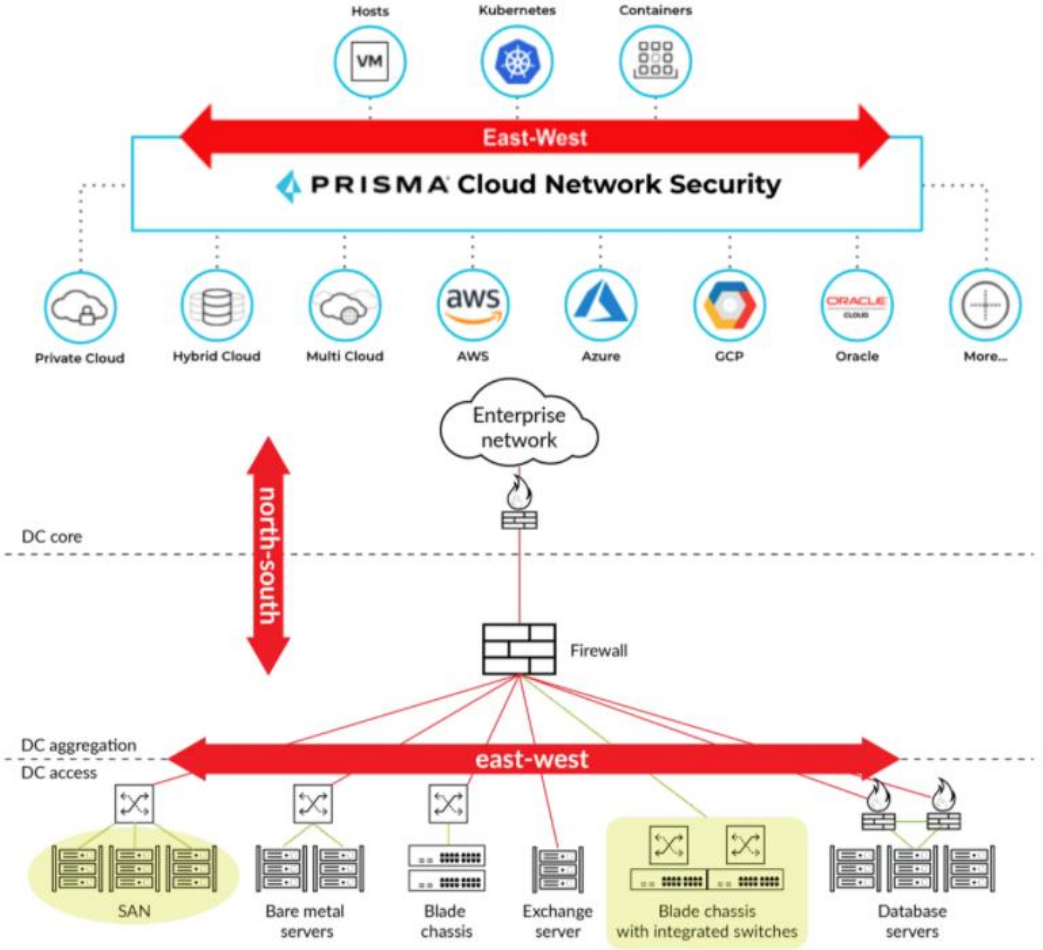



**Attack Lifecycle:** | **1. Penetrate** | **2. Execute** | **3. Move Laterally**

Sources: Unit 42 Research

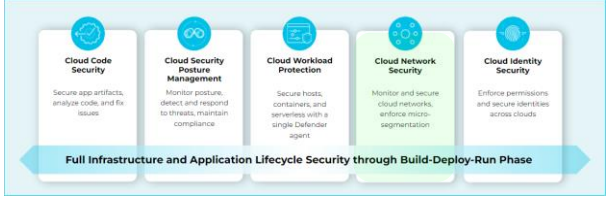
# Zero-Trust Cloud Native Network Security



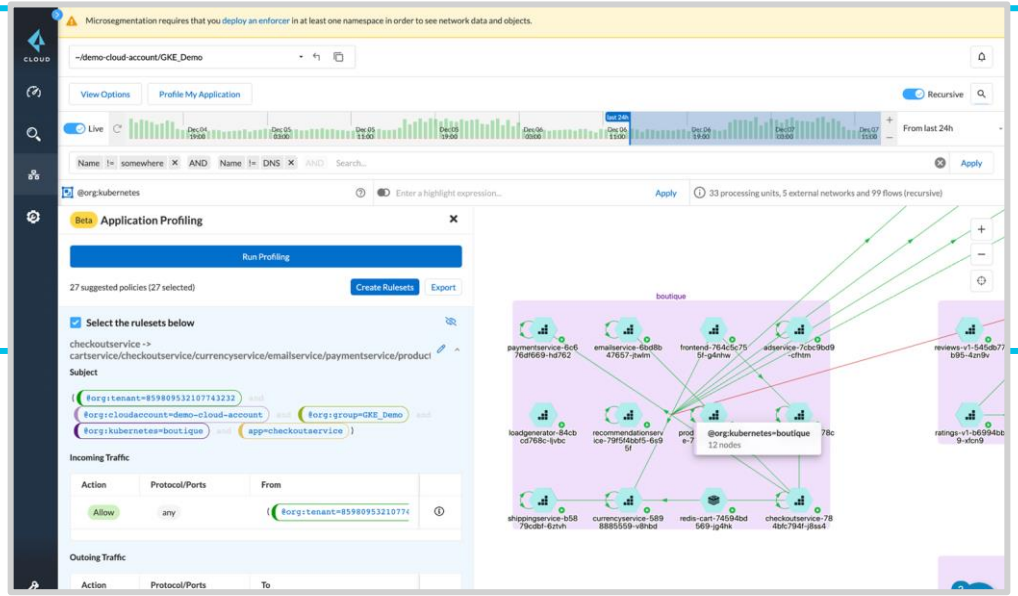

 © 2019 Palo Alto Networks. All Rights Reserved.

# Cloud Network Security to secure workloads by removing lateral communication flows




**App dependency mapping**
Visualize network flows across workloads

**Automatic app profiling**
Generate least-privilege microsegmentation rules based on learned traffic patterns



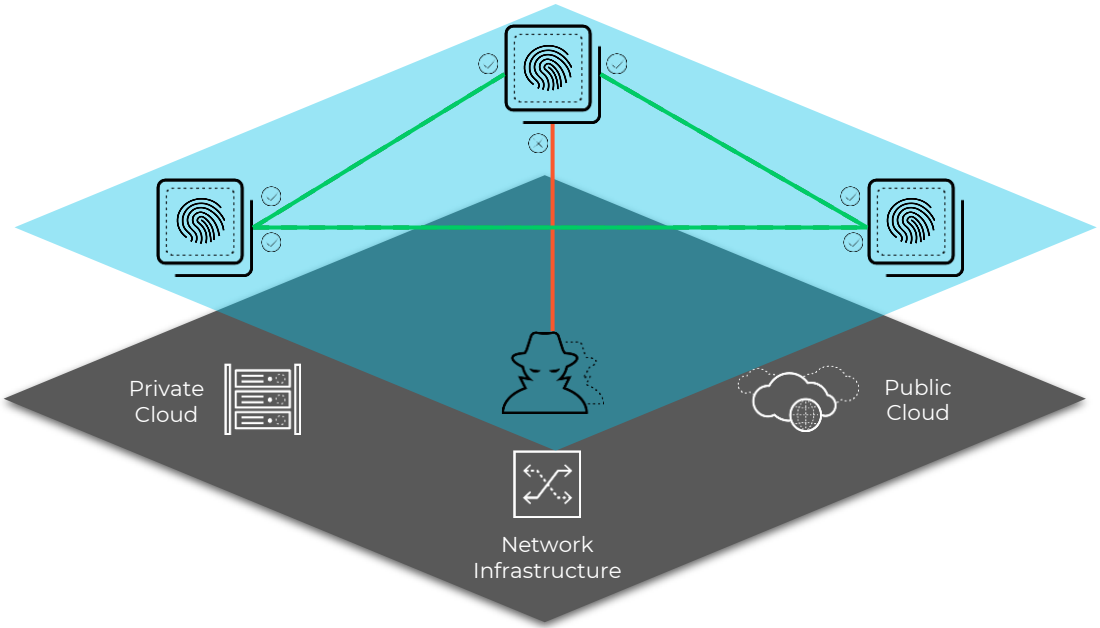

**True internet exposure**
Analyze cloud network configurations and assess network-based risk

**Agent-based security**
Microsegmentation for hosts and containers across private and public clouds

**Identity-based microsegmentation**
Prevent lateral movement of threats and achieve zero trust and compliance goals

 © 2022 Palo Alto Networks, Inc. All rights reserved.

# Our Unique Approach




1. Decouple security from the network. Identity becomes the security perimeter, no IP addresses or ACLs
2. Discover and learn application communications inside and across clouds in real time using a map
3. Implement and test segmentation policies safely.
4. Authenticate and authorize connection requests using distributed, identity-based enforcement. Deny unknown requests

**Zero Trust Network Segmentation purpose built for any cloud**

# Prisma Cloud Proof of Concept

## Integrated capabilities for complete cloud native application protection

### Cloud Code Security

Secure app artifacts, analyze code, and fix issues

Infrastructure as Code (IaC) Security integrated in CI/CD Pipeline

### Cloud Security Posture Management

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

Visibility, Compliance & Governance

Threat Detection

Data Security

### Cloud Workload Protection

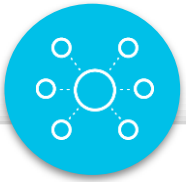
Secure hosts, containers, and serverless across the application cycle

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

**Qualify Opportunity, Execute Evaluation (30 days), Close the Deal**

 © 2022 Palo Alto Networks, Inc. All rights reserved.

PRISMA
BY PALO ALTO NETWORKS

# Thank you

Sebastian Straube
Lead Cloud Solution Architect DACH

sstraube@paloaltonetworks.com
linkedin.com/in/sebastianstraube

paloalto NETWORKS