
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT241

SPONSORED BY PALO ALTO NETWORKS

Avalon Healthcare Solutions secures AWS deployments with Palo Alto Networks

Tanya Shastri

SVP of Product Management – Next Gen Firewall
Palo Alto Networks

Jesse Webb

SVP, Security and Technology
Avalon Healthcare Solutions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Avalon

AWS

Why NGFWs are needed in the public cloud

Anatomy of the Log4J attack

Palo Alto Networks platform approach

Cloud NGFW overview

Avalon’s outcome with Cloud NGFW

Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

World’s first lab insights company

Avalon is pioneering a **new era of value-driven care** by unlocking the potential of lab results to generate actionable lab-driven insights in real time to proactively ensure appropriate care and enhance clinical outcomes



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Avalon’s lab insights system

CRITICAL INSIGHTS AT EACH STEP TO DELIVER VALUE-DRIVEN CARE

RIGHT TEST



- Evidence-based lab policies
- Policy enforcement
- Prior authorization
- Lab network

RIGHT DATA



- Lab results capture
- Digitized lab results, across network in real time
- Prior authorization and payment decisions

RIGHT INTEL



- Lab insights engine
- Early detection of disease
- Performance reporting
- Clinical decision support

RIGHT CARE



- Lab-informed treatment
- Clinical pathway adherence
- Optimized outcomes
- Lower healthcare costs

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

About Avalon: Lab science is our true north

6–12%
Proven savings

- ✓ Clinical data & science depth
- ✓ Independent clinical advisory board

200+
Dedicated Avalonians

- ✓ Technologists
- ✓ Biostatisticians
- ✓ Clinicians

>40M
Health plan members

- ✓ Curated network
- ✓ Genetic and routine

140+
Evidence-based lab policies

>120
Independent labs

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Avalon security strategies

Zero Trust/negative security model
- Hyper network and environment segmentation
- Workflow and system isolation
- Restricted access for systems and users

HIPAA minimum necessary rule
- Harden systems to minimum function
- Retain minimum data needed to provide service
- User access minimized to their job roles

Defense in depth/layered security
- Assume a “breach” – Reduce shared-fate failure designs
- Assume a “zero day” – Reduce surface area of attack
- Assume the “user will click the link!” – layer the defense

Build security into the culture
- Leadership makes compliance and security #1 goal
- Make security part of every IT job – Linux Security Admin
- Have HR add security reporting and monitoring to JDs

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Security must be job zero!”

Andy Jassy
CEO, Amazon

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Avalon security strategies

Zero Trust/negative security model
- Hyper network and environment segmentation
- Workflow and system isolation
- Restricted access for systems and users

HIPAA minimum necessary rule
- Harden systems to minimum function
- Retain minimum data needed to provide service
- User access minimized to their job roles

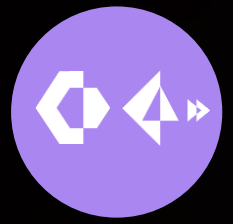
Defense in depth/layered security
- Assume a “breach” – Reduce shared-fate failure designs
- Assume a “zero day” – Reduce surface area of attack
- Assume the “user will click the link” – layer the defense

Build security into the culture
- Leadership makes compliance and security #1 goal
- Make security part of every IT job – Linux security admin
- Have HR add security reporting and monitoring to JDs

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

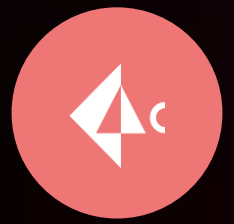
Palo Alto Networks offers enhanced protection for AWS deployments

INTEGRATED WITH AWS



Network security

Deliver advanced network and threat protection (NGFWs) on AWS



Prisma Cloud

Secure any tech stack and any application components running on AWS



SOC security

Automate incident response to eliminate manual work and speed response

All flagship Palo Alto Networks cloud security products integrate with AWS

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

paloalto NETWORKS

Strong collaboration with AWS

aws PARTNER

- Public Sector
- AWS Outposts Ready
- AWS Marketplace Seller
- DevOps Software Competency
- Security Software Competency
- Networking Software Competency
- Containers Software Competency



2017: Security launch partner for Amazon GuardDuty



2018: Security launch partner for AWS Security Hub



2019: Security launch partner for Amazon VPC Traffic Mirroring



2020: Security launch partner for Gateway Load Balancer

2021: Panorama automates software firewall insertion on AWS

2021: CN-Series PAYG on AWS Marketplace for Containers Anywhere



2022: Cloud NGFW for AWS – managed by Palo Alto Networks

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

paloalto NETWORKS

Avalon’s environment growth

Avalon was born in the cloud and is 100% based on AWS; AWS has provided the flexibility and enterprise scalability our startup required

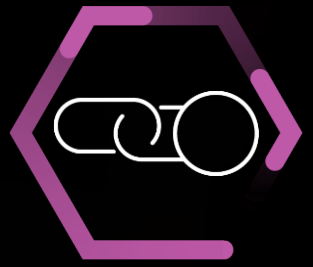
2015	US-East-1; 1 OU; 4 VPCs; 4 firewalls from previous provider
2017	US-East-1; 2 OUs; 8 VPCs; 4 firewalls from previous provider, 4 Palo Alto firewalls, 1 Panorama
2022	US-East-1; 6 OUs; AWS Transit Gateway; Palo Alto Networks Cloud NGFW
2023	US-East-1; 6 OUs; AWS Transit Gateway; Palo Alto Networks Cloud NGFW US-East-2; 1 OUs; AWS Transit Gateway; Palo Alto Networks Cloud NGFW US-West-1; 6 OUs; AWS Transit Gateway; Palo Alto Networks Cloud NGFW

Avalon’s growth strategy to expand into multiple AWS Regions was hindered by the rising cost of resources, the ability to scale securely, and the management of existing and new infrastructure

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why are NGFWs useful in the public cloud?

Risk



Outbound connections

When connections to the internet are allowed, acts such as crypto-mining, command and control (C&C), and data exfiltration can occur



Unknown and unpatched vulnerabilities

Unknown or unpatched vulnerabilities (such as Log4J) can be exploited by third parties before updates become available



Lateral movement

Applications connected to the internet can be a risk that can spread laterally to other applications

How does a next-generation firewall (NGFW) address this risk?



The NGFW provides the next layer of workload inspection for potential malware or threats, and can block malicious connections



While WAFs secure HTTP connections, inbound connections protected by an NGFW block outside parties from exploiting vulnerabilities while you work on patching



NGFW enables a Zero Trust strategy by protecting inbound connections from the Internet, as well as connections from other applications

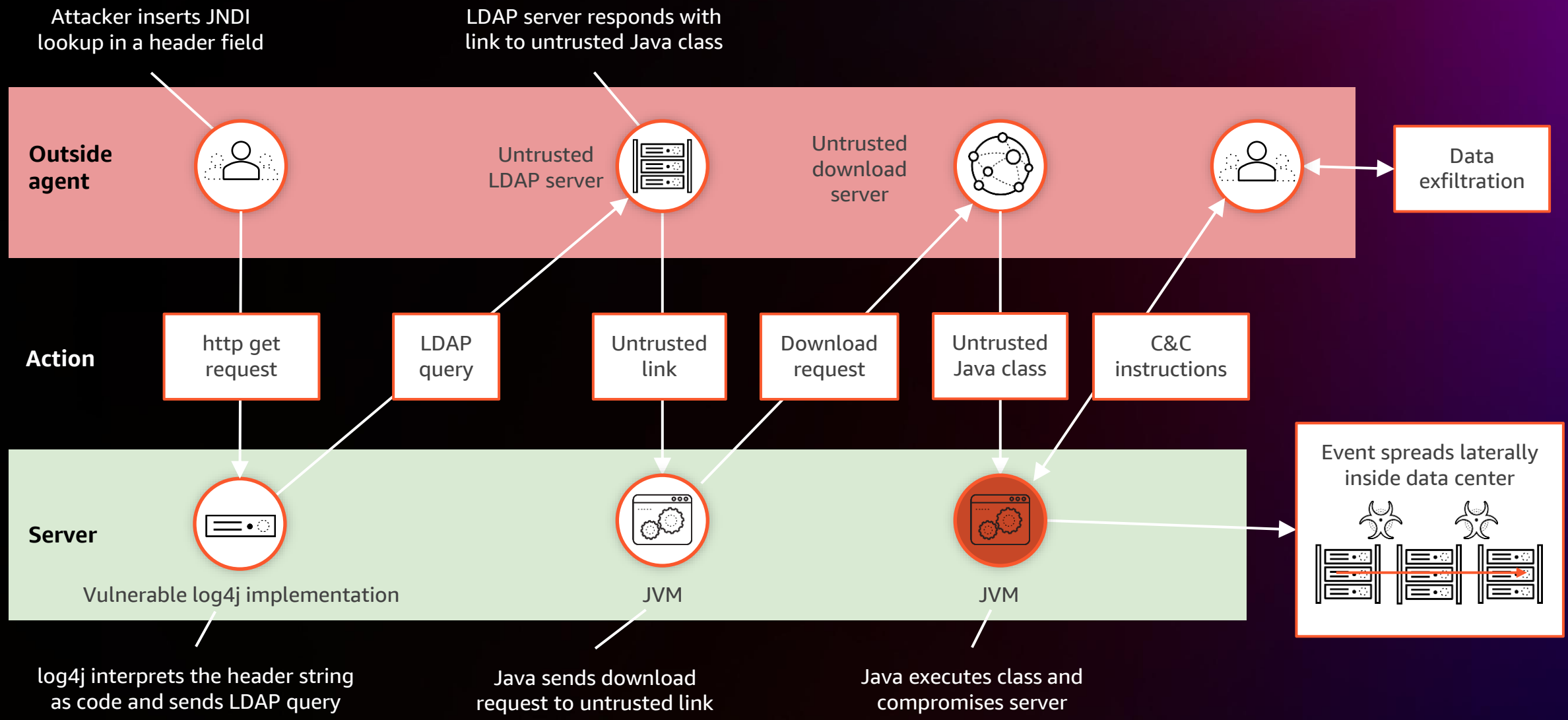
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of the Log4J incident

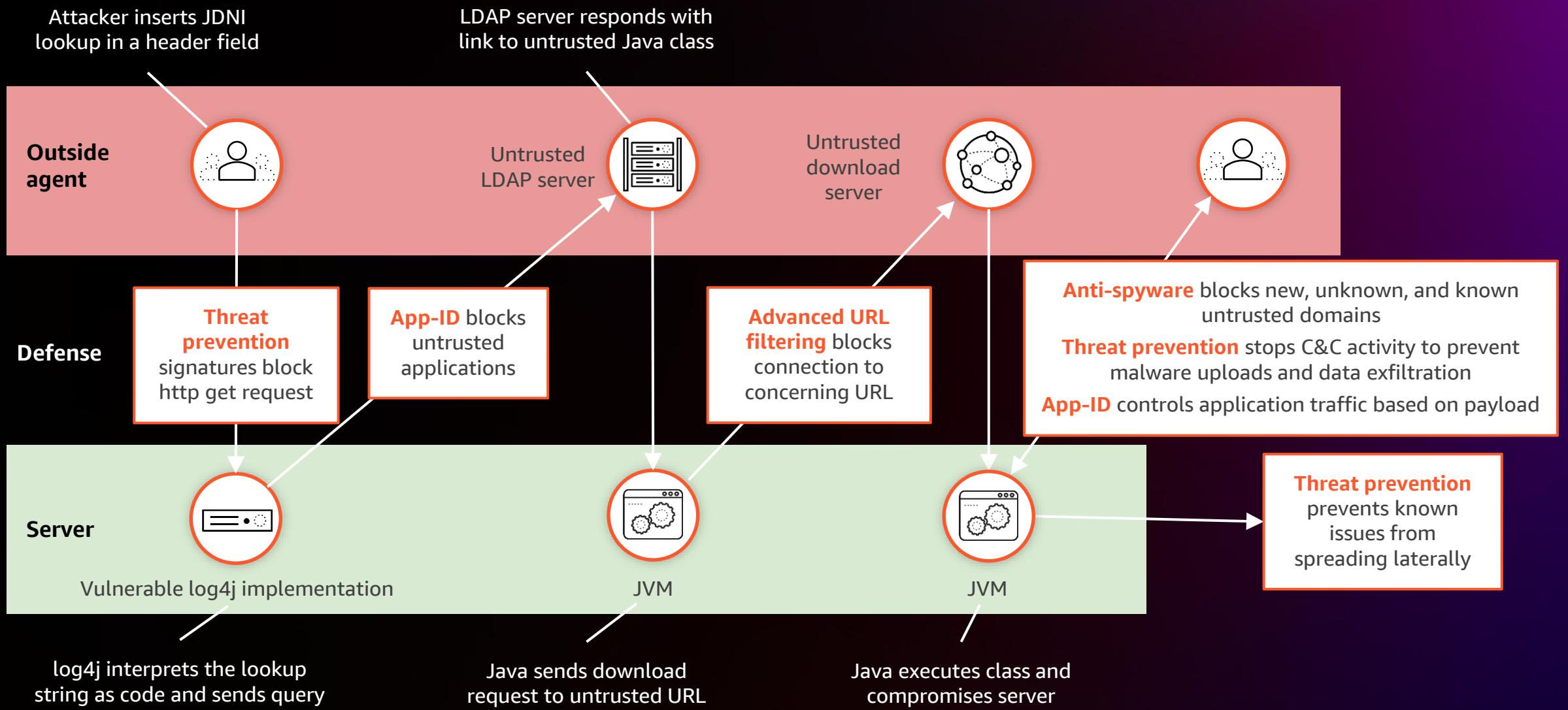
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Apache Log4j incident sequence



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How network security can address a Log4j event



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Avalon’s Log4J Patch Nightmare

- 4 patching cycles
- Some third party elements still not patch
- Mitigation became the strategy
- AWS WAF & PAN Firewall recognition of attack vectors became key defense to buy time for remediation, removal, or replacement

** Vulnerability Mitigation is a KEY reason we chose to use Palo Alto Networks NGFW as the go forward strategy of protection of our environments **

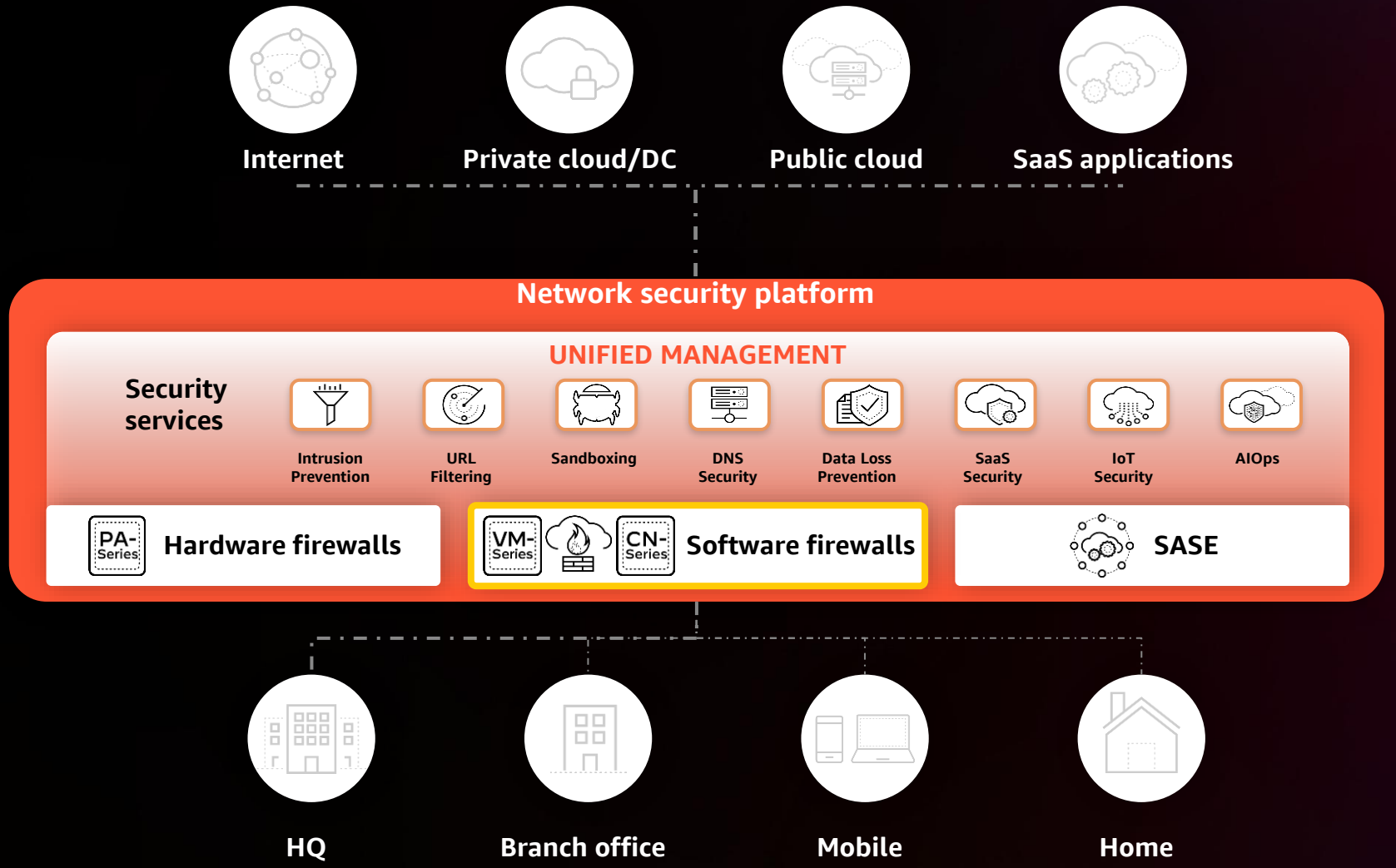
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Platform approach

For the best security posture

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Palo Alto Networks solution



- Best-in-class security for all users and applications
- Integrated security services across hardware, software, and SASE
- Optimized end user experience at all locations
- Unified security operations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud NGFW for AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enterprises need best-in-class security and cloud-native ease of use



Best-in-class security

- Layer 7 firewall controls traffic at the application layer
- Real-time updates protect against the latest concerns
- ML-powered threat prevention protects against zero-day events



Cloud-native ease of use

- Zero maintenance with no infrastructure to manage
- Built-in scalability and resiliency
- Integration with AWS services for automation of end-to-end workflows

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.
paloalto NETWORKS

Cloud NGFW for AWS

BEST-IN-CLASS SECURITY MEETS CLOUD-NATIVE EASE OF USE



Best-in-class security

Built to stop zero-day concerns

+



Cloud-native ease of use

Designed for the way you work with AWS

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

paloalto NETWORKS

Cloud NGFW key capabilities



Cloud NGFW

Best-in-class NGFW delivered as a fully managed cloud-native service for AWS

- Managed cloud-native service
- Deploy in just a few clicks
- Best-in-class security
- Integrated with AWS Firewall Manager

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud NGFW best-in-class security
built to stop zero-day threats



App-ID

Reduce the attack surface by controlling traffic based on patented layer 7 traffic classification

Threat prevention

Automatically stop malware, vulnerability issues, and command and control traffic

Advanced URL filtering

Prevent known and zero-day web-based events and control web traffic with URL categories

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

paloalto NETWORKS

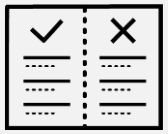
Cloud NGFW delivered as a managed cloud-native service

Security management

Customer responsibility



Create firewall rules



Route traffic to endpoint



Manage using AWS Firewall Manager*



Infrastructure management

paloalto NETWORKS

Automatically deploy firewalls and dependencies

Continuously update firewalls with threat signatures



Cloud NGFW
Cloud-native NGFW

Automatically scales with traffic up to 45 Gbps

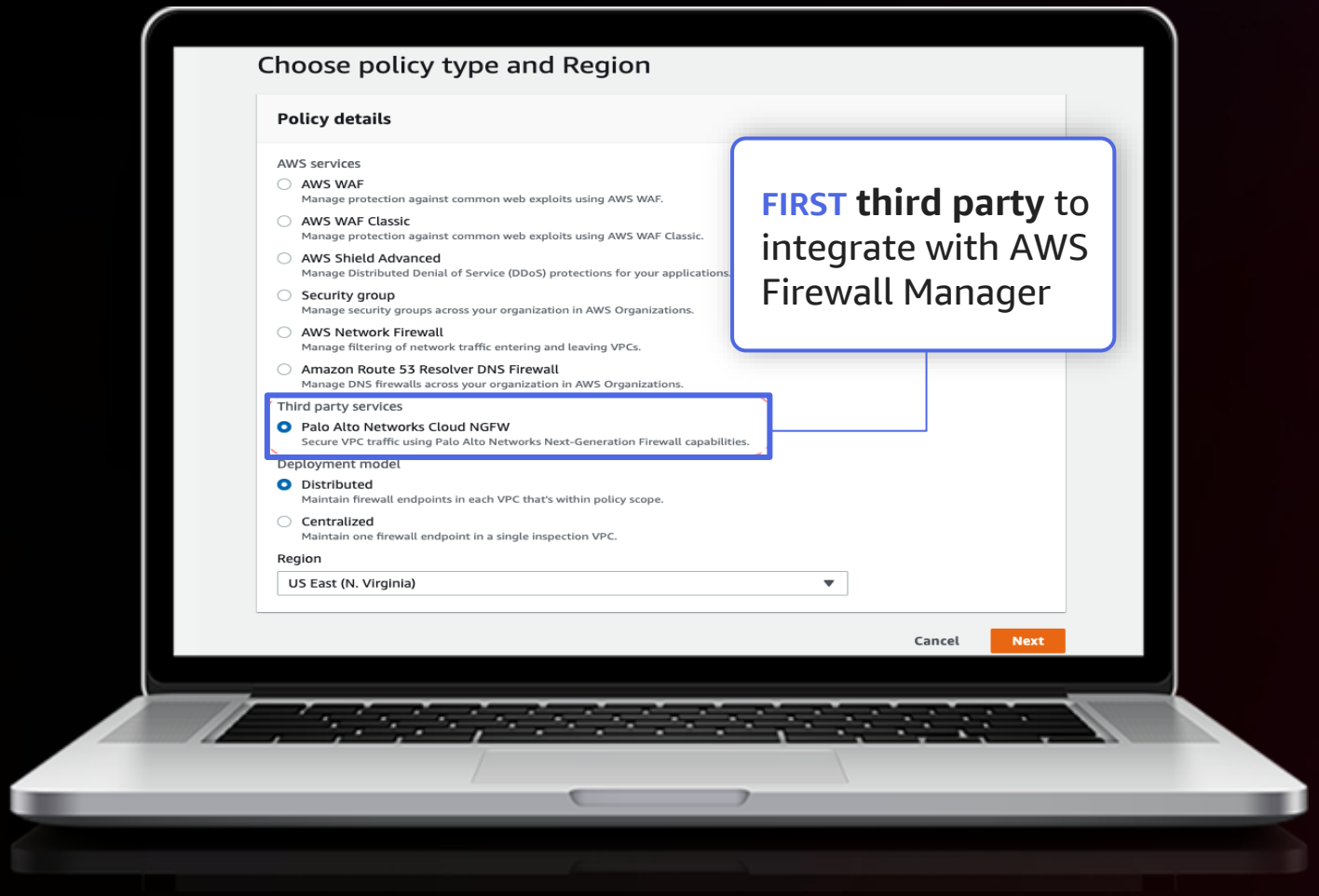
Highly resilient (99.99% SLA)

aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

*Optional. All users must use Cloud NGFW management.

paloalto NETWORKS

Cloud NGFW integrates into the way you work with AWS today



FIRST third party to integrate with AWS Firewall Manager

Infrastructure-as-code (IaC) capabilities

- Application programming interface
- AWS CloudFormation template
- Terraform provider
- AWS CLI*
- AWS SDK*

*AWS Firewall Manager only

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud NGFW: Cloud-native ease of use

Easy setup



Procure through AWS Marketplace and set up in minutes

Zero maintenance



Highly resilient cloud service with dynamic scaling

Scalable policy management



AWS Firewall Manager integration provides simple, consistent management across multiple AWS accounts and VPCs

Automated NGFW provisioning



Automate workflows using CloudFormation and Terraform (infrastructure as code)

Embed network security into the CI/CD pipeline

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

paloalto NETWORKS

Avalon's outcome with Cloud NGFW for AWS



- Reduces Amazon EC2, AWS networking, and firewall licensing cost
- Reduces engineering resource loads and staffing needs
- Reduces complexity of managing multiple firewalls
- Increases security manageability
- Condense 8 firewalls to one HA scalable system per Region
- Provides the ability to secure our multiple AWS Region environment strategy



AWS Firewall Manager and Palo Alto Networks Cloud NGFW delivers results

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Palo Alto Networks cloud network security is . . .



Best-in-class security

Consistent, best-in-class network security for all your applications



Cloud-integrated

Deep integrations with clouds and hypervisors, cloud-native form factors, and cloud-like consumption



Automated

Easy integration into DevOps processes for automated deployment and scaling



Easy to manage

Centralized management for all your private and public cloud needs

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Backed by one of the industry's largest security platforms



224

billion

threats blocked per day

4.3

million

unique security updates per day

200

researchers

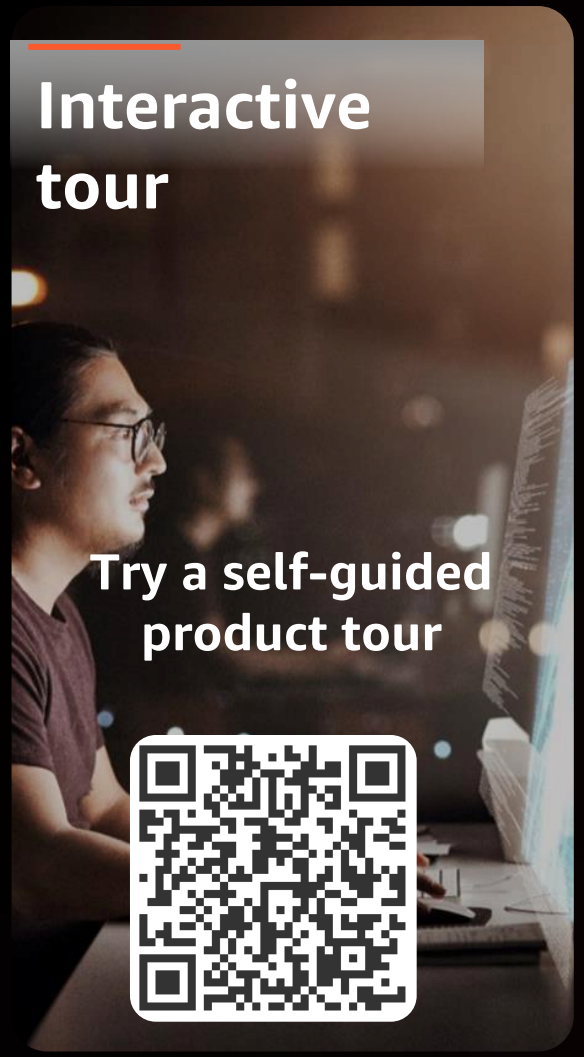
for threat intelligence

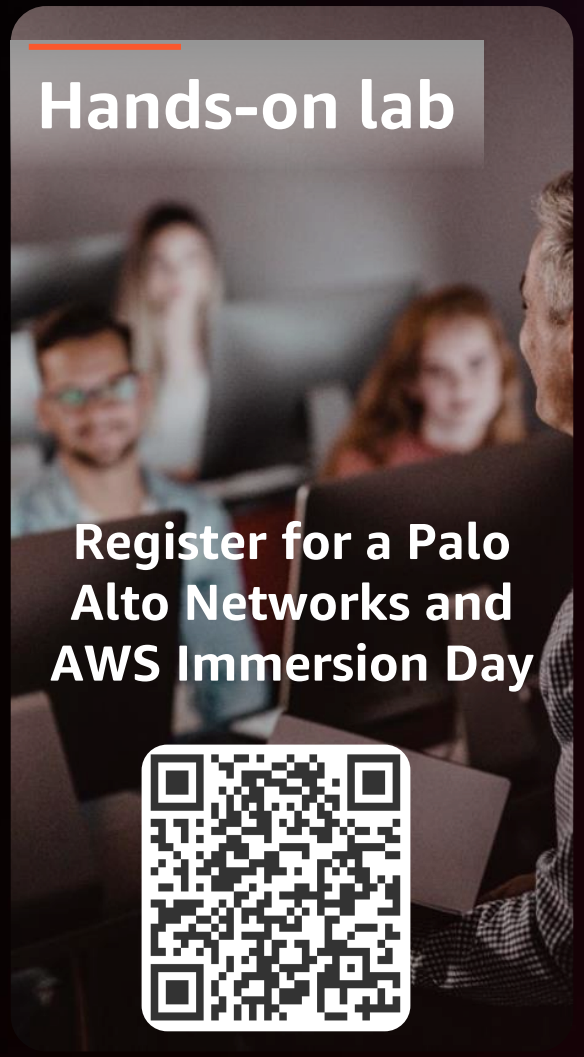
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

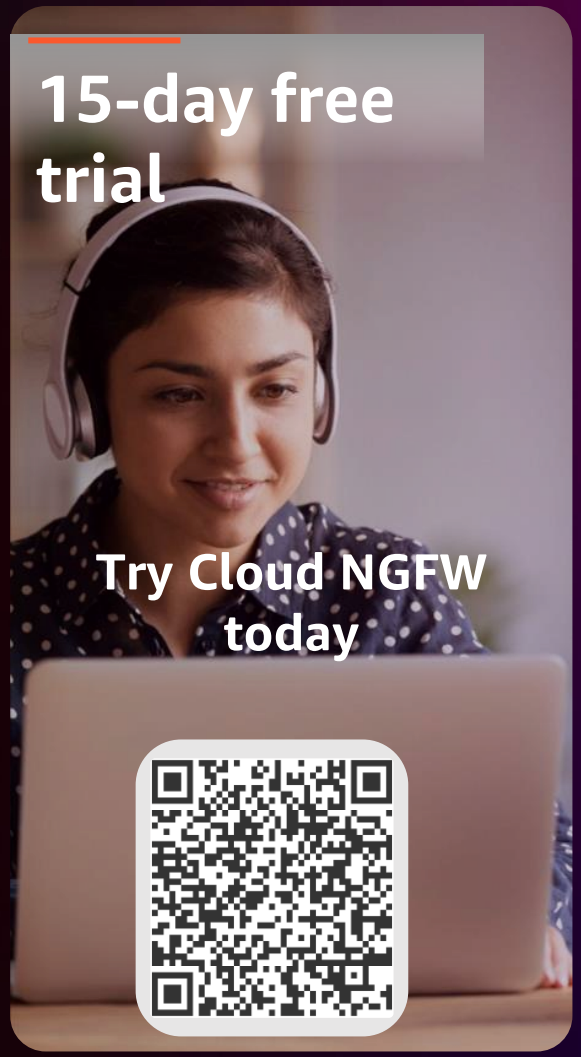
Any questions?
We have answers!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Get your hands on Cloud NGFW







© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.