



# AI-powered Next-generation Security Platform

Jon Li,  
Director, System Engineer

# Palo Alto Networks Corporate Overview

Palo Alto Networks, the global cybersecurity leader, continually delivers innovation to enable secure digital transformation—even as the pace of change is accelerating

## Palo Alto Networks, Inc. Common Stock (PANW)

Nasdaq Listed Nasdaq 100

\$231.90 +5.11 (+2.25%)  
CLOSED AT SEP 27, 2023 4:00 PM ET

\$230.04 -1.86 (-0.80%)

Bid: \$231.00 x 1

Ask: \$231.99 x 76

Volume: 6,308

SEP 28, 2023 9:23 AM ET

 + ADD TO WATCHLIST + ADD TO PORTFOLIO

### QUOTES

#### Summary

Real-Time

After-Hours

Pre-Market LIVE

Charts

### NEWS & ANALYSIS

News

Press Releases

Analyst Research

Dividend History

Historical Quotes

Historical NOCP

Financials

Earnings

P/E & PEG Ratios

Option Chain

Institutional Holdings

Insider Activity

SEC Filings

Revenue EPS

Sep 27, 2023

PREVIOUS  
CLOSE  
\$226.79

1D 5D 1M 6M YTD 1Y **5Y** MAX



# KEY TRENDS IMPACTING CYBERSECURITY



The shift to the cloud has gone mainstream

**188%**

YoY increase in Cloud incidents



The nature of work has changed fundamentally

**61%**

of organizations say they are struggling to secure the hybrid workforce



The threat landscape continues to escalate

**53%**

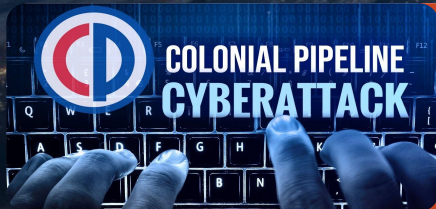
of organizations turn to AI for more effective threat detection

Palo Alto Networks *What's Next in Cyber* survey

## Recent Examples of **High Profile Attacks**



CVE-2022-26134, a remote code execution vulnerability was reported in Confluence Server and Data Center products. This vulnerability was actively exploited by Ransomware gangs such as AvosLocker and Cerber after proof-of-concept exploits were leaked online



Leveraged ransomware-as-a-service (RaaS) variant (DarkSide). DarkSide attackers typically first gain initial access through phishing and use Cobalt Strike to obscure their C2 operations



CVE-2021-44228, a JNDI injection flaw in Apache's widely deployed open-source Log4j logging library—present in everything from web and email servers—allows remote, unauthenticated attackers to take control of vulnerable targets

# AI will transform the threat landscape

WSJ

## With AI, Hackers Can Simply Talk Computers Into Misbehaving

Using a technique called 'prompt injections', hackers can break AI systems using plain English

Aug 10, 2023

### And many, many more use cases

- AI-generated malware
- AI-enhanced social engineering attacks
- Malicious code injection into model repos
- AI-driven botnets

### The threat future, powered by AI

#### Increased speed to near real-time

Decreased time from compromise to exfiltration  
CVE exploitation in record time

#### Increased scope

Any "vulnerable population" targeted

#### Dark motivations

Attacks to disrupt essential services

#### Huge "opportunity"

\$10.5T<sup>1</sup> cybercrime "market" in 2025

---

## WHAT WE KNOW

# The costs of inaction are...

**Breaches  
guaranteed**

**96%**

The percentage of organizations attacked in the last year

Source: Palo Alto Networks What's Next In Cyber

**Operational  
disruption**

**33%**

Of security professionals experienced operational disruption as a negative consequence of a breach

Source: Palo Alto Networks What's Next In Cyber

**Financial and  
business impacts**

**\$2.4M**

The average cost associated with recovering from a breach.

Source: Forrester

# Cybersecurity transformation has become imperative for all of us

---

## WHAT WE KNOW

**Best of  
Breed**

**and  
~~or~~**

**Platform  
Approach**

It's not just our view...

**77%**

Of security executives think it is critical to reduce the number of security solutions and services they use

Source: Palo Alto Networks *What's Next in Cyber* survey

# WHAT WE PROVIDE

## Our next-gen platforms enable cyber transformation



### Network Security

STRATA | PRISMA SASE

Best-in-class security delivered across hardware, software and SASE



### Cloud Security

PRISMA CLOUD

Comprehensive platform to secure everything that runs in the cloud



### Security Operations

CORTEX

A new approach to SOC with fully integrated data, analytics and automation




### Threat Intelligence and Advisory Services


World-renowned threat intelligence, cyber risk management and advisory services



# SIMPLIFY SECURITY WITH OUR BEST OF BREED PLATFORMS

SUB-CATEGORY	ZERO TRUST
Firewall	 <p><b>Network Security Platform</b></p>
Intrusion Detection	
URL Filtering	
Sandbox Detection	
DNS Security	
IoT Security	
Data Loss Prevention	
Cloud Access Security Broker	
Posture and Health Management	
Remote Access for Users	
SWG	
SD-WAN	

SUB-CATEGORY	CODE TO CLOUD
Cloud Security Posture Management	 <p><b>Cloud Security Platform</b></p>
Cloud Workload Protection	
Identity & Access Management	
Code Security	
Web Application / API Security	

SUB-CATEGORY	AUTONOMOUS SECOPS
Security Information & Event Management	 <p><b>AI-Driven Security Operations Platform</b></p>
Endpoint + EDR	
NTA / UEBA	
SOAR	
Attack Surface Management	

# We leverage AI across our entire portfolio

## Unique Assets



Sensors installed  
across ~48k customers <sup>1</sup>



4.86 PBs of high quality  
data collected per day



Out-of-the-box automation  
to take real-time action

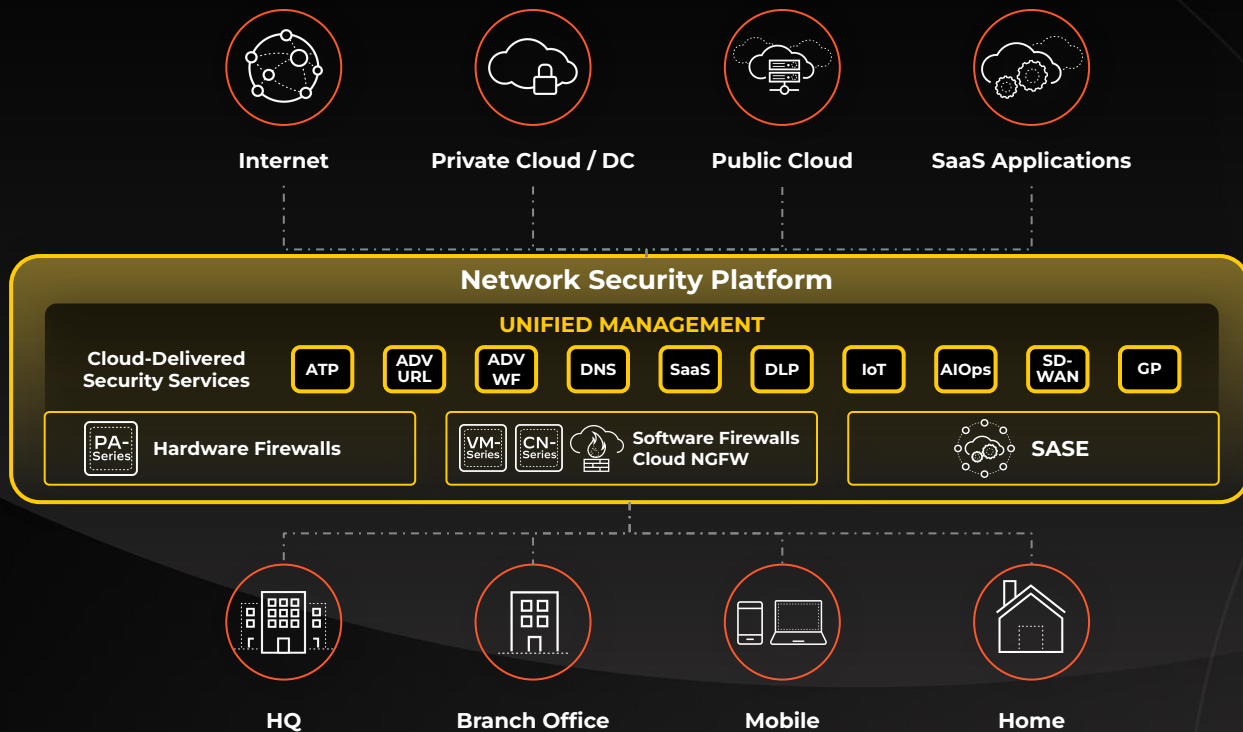
## Precision AI

Precision AI will allow us to deliver unparalleled detection and response to achieve near real-time security

## Generative AI

Generative AI will redefine and simplify how customers engage with our products and services

# BEST-IN-CLASS NETWORK SECURITY FOR ALL USERS ACCESSING ALL APPLICATIONS



## BENEFITS

**Safer**

**48%**

more zero-day attacks stopped in real-time with inline deep learning, compared to legacy vendors

**Always-On**

**99.999%**

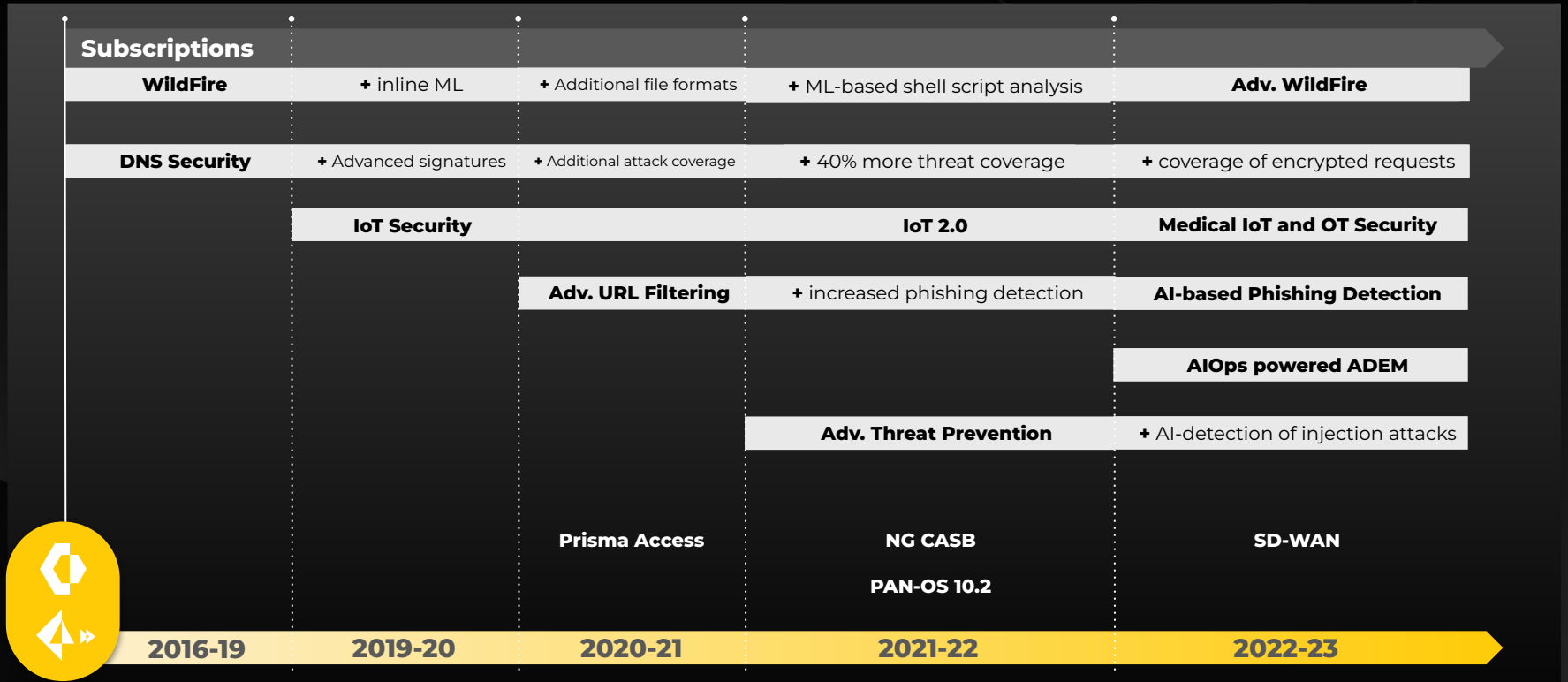
availability with industry-leading ZTNA 2.0

**Faster**

**<10 seconds**

from threat detection to threat prevention. 180x faster than competing products

# Significant Acceleration in AI-based Innovation



# AI Drives Tangible Customer Outcomes at Scale

## ADVANCED THREAT PREVENTION

Exploits & C2 sessions prevented inline per day

**8.3B**\*

**34.3M** suspicious sessions analyzed in the cloud

## ADVANCED WILDFIRE

Malware attacks prevented inline per day

**79.4M**\*

**29.4M** new files analyzed  
**165K** zero-day malware detected

## ADVANCED URL FILTERING

Web-based attacks prevented inline per day

**78.2M**\*

**280.6M** new URLs analyzed  
**417K** new malicious URLs attacks blocked

## DNS SECURITY

DNS-based attacks prevented inline per day

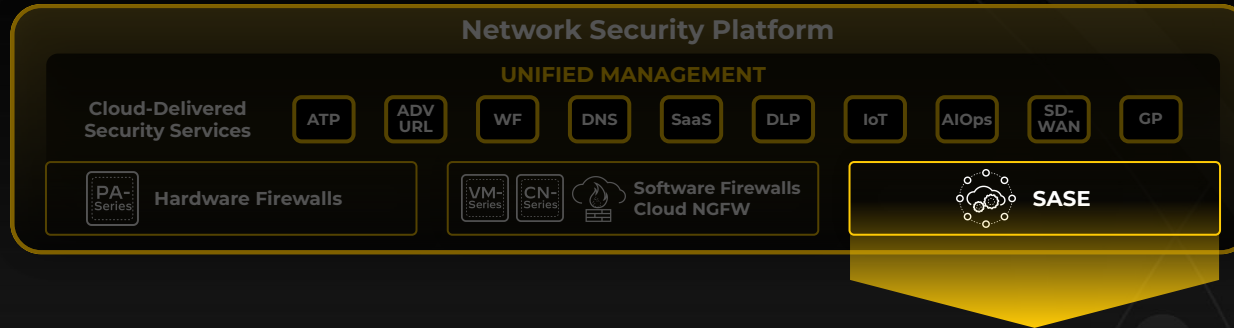
**143M**\*

**394M** new domains analyzed  
**936K** new malicious domains blocked

# Using AI & Data to Revolutionize User Experience



# PRISMA SASE: ZERO TRUST WITH ZERO EXCEPTION



## • Delivering ZTNA 2.0

- Least-Privilege Access
- Continuous Trust Verification
- Continuous Security Inspection
- Protect All Data
- Secures All Apps

## • Seamless User Experience

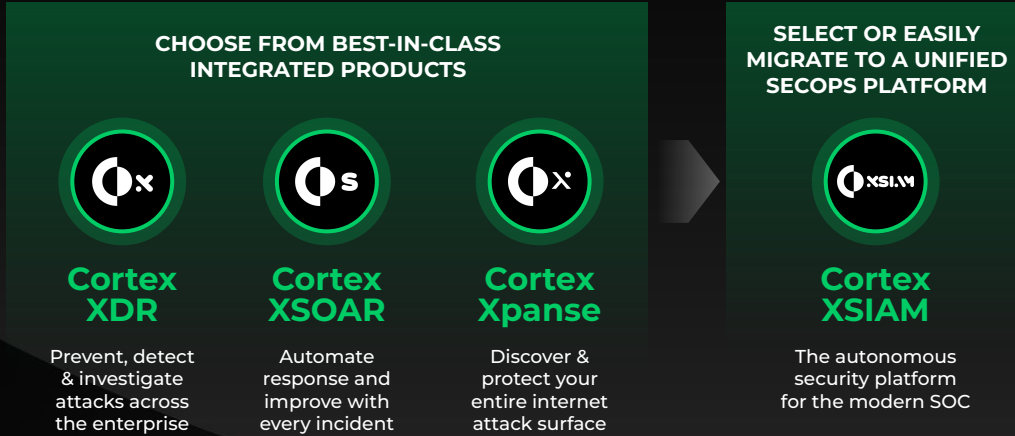
- High availability
- Cloud-Scale Architecture
- Data Plane Isolation
- Industry leading SLAs

## • Unified Best-of-Breed Capabilities

- Firewall as a Service (FWaaS)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA)
- Software-defined WAN (SD-WAN)
- Native Visibility (ADEM)

# CORTEX - POWERING UP THE MODERN SOC

## WHAT'S POSSIBLE WITH THE AUTOMATED SOC



Events .....

**36 B Events**

Alerts / Incidents .....

**133 Alerts**  
**7 Incidents**

Automated / Manual Analysis .....

**125 Automated**  
**8 Manual**

Major Incidents .....

**0**

**10**  
SECONDS

**Mean Time to Detect**

**1**  
MINUTE

**Mean Time to Respond**  
(High priority)



# UNIT 42: DATA-DRIVEN THREAT INTELLIGENCE & RESPONSE



## Assess

### CYBER RISK MANAGEMENT

**Assess** and test your controls against real-world threats targeting your organization, then communicate your security risk posture to your board and key stakeholders.

## Transform

### CYBER RISK MANAGEMENT & THREAT INTEL

**Transform** your security strategy with a threat-informed approach to tighten alignment across your people, processes, technology and governance.

## Respond

### INCIDENT RESPONSE & MANAGED DETECTION & RESPONSE

**Respond** in record time by quickly investigating, eradicating and remediating even the most advanced attacks.

# BEST OF BREED ACROSS THE BOARD

## LEADING THE WAY IN CYBERSECURITY INNOVATION

### ACROSS 15 CATEGORIES



#### More leadership categories:

- A Leader in Forrester **Zero Trust Extended Ecosystem Wave**
- Frost & Sullivan Global Company of the Year Award for **SASE**
- A Leader in GigaOm **Developer Security Tools Radar**
- A Leader in GigaOm **OT Security Radar**
- A Leader in Forrester **Cloud Workload Security Wave**
- Outperformer Leader in GigaOm **Vulnerability Management Radar**
- Leader in KuppingerCole **Security Orchestration Automation & Response Leadership Compass**
- Outperformer Leader in GigaOm **Attack Surface Management Radar**

### Leadership In Critical Third Party Assessments

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner content described herein (the "Gartner Content") represent(s) research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. ("Gartner"), and are not representations of fact. Gartner Content speaks as of its original publication date (and not as of the date of this analyst day), and the opinions expressed in the Gartner Content are subject to change without notice.

## WHY PALO ALTO NETWORKS

# We are the cybersecurity partner of choice

Securing tens of thousands of customers globally

**10 of 10**

of the Fortune 10

**8 of 10**

Largest U.S. Banks

**9 of 10**

Largest Manufacturing  
Companies in the  
World

**9 of 10**

Largest Utilities  
in the World

**7 of 10**

Largest Oil & Gas  
in the World

**9 of 10**

Top U.S. Hospitals





Cybersecurity  
Partner of Choice

# THANK YOU

