Q4 Fiscal Year 2023
Earnings Call & Medium Term Update
Safe Harbor

This presentation contains “forward-looking” statements within the meaning of Section 27A of the Securities Act and Section 21E of the Exchange Act, including statements related to our financial guidance for the first quarter of fiscal 2024 and fiscal year 2024, our financial estimates for fiscal years 2023 through 2026, our modeling points, our strategic plans, our achievements, our growth rates and growth prospects, our estimates of market sizes and opportunities, the performance and benefits of our products, our product development expectations, anticipated trends, business and economic conditions and challenges, and other financial, operational and business expectations. Many of these assumptions relate to matters that are beyond our control and changing rapidly.

There are a significant number of factors that could cause actual results to differ materially from forward-looking statements made in this presentation, including: developments and changes in general market, political, economic, and business conditions; risks associated with managing our growth; risks associated with new product, subscription and support offerings; shifts in priorities or delays in the development or release of new product or subscription offerings, or the failure to timely develop and achieve market acceptance of new products and subscriptions as well as existing products, subscription and support offerings; rapidly evolving technological developments in the market for security products, subscription and support offerings; our customers’ purchasing decisions and the length of sales cycles; our competition; our ability to attract and retain new customers; our ability as an organization to acquire and integrate other companies, products, or technologies in a successful manner; our debt repayment obligations; and our share repurchase program, which may not be fully consummated or enhance shareholder value, and any share repurchases which could affect the price of our common stock. Further information on these and other factors that could affect the forward-looking statements we make in this presentation can be found in the documents that we file with or furnish to the U.S. Securities and Exchange Commission, including Palo Alto Networks’ most recent Quarterly Report on Form 10-Q filed for the quarter ended April 30, 2023, which is available on our website at investors.paloaltonetworks.com and on the SEC’s website at www.sec.gov. Additional information will also be set forth in other filings that we make with the SEC from time to time. All forward-looking statements in this presentation are based on our current beliefs and on information available to management as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

All information in this presentation is as of August 18, 2023. This presentation contains non-GAAP financial measures and key metrics relating to the company’s past and expected future performance. We have not reconciled diluted non-GAAP earnings per share guidance to GAAP earnings per diluted share, non-GAAP operating margin to GAAP operating margin or adjusted free cash flow margin guidance to GAAP net cash from operating activities because we do not provide guidance on GAAP net income (loss) or net cash from operating activities and would not be able to present the various reconciling cash and non-cash items between GAAP and non-GAAP financial measures, including share-based compensation expense, without unreasonable effort.
Over the last 5 years, the cybersecurity market has evolved significantly

<table>
<thead>
<tr>
<th>TAM ’23 ('18-’23 CAGR)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$29B (35%)</td>
<td>New segments</td>
</tr>
<tr>
<td></td>
<td>SASE, Cloud Security, IoT Security</td>
</tr>
<tr>
<td>$72B (19%)</td>
<td>Segments undergoing transformation</td>
</tr>
<tr>
<td></td>
<td>Endpoint / XDR, SecOps (+SIEM), Network Security</td>
</tr>
<tr>
<td>$31B (13%)</td>
<td>Largely steady segments</td>
</tr>
<tr>
<td></td>
<td>Identity, App Security, Data Security, Email Security</td>
</tr>
<tr>
<td>$81B (7%)</td>
<td>Services</td>
</tr>
</tbody>
</table>

**Enterprise Cybersecurity Market**


All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.
Looking back, we envisioned three transformations:

1. **The network would need to be reimagined**
   - $19B
   - Network Security 2018 TAM

2. **Public Cloud adoption would scale rapidly**
   - $2B
   - Cloud Security 2018 TAM

3. **AI & ML would be THE way we ‘solve’ security**
   - $17B
   - Security Ops 2018 TAM

*Note: the size of the bubbles in the chart is not adjusted to scale*
These transformations ended up driving rapid growth in cybersecurity.

- **$19B**
  - Network Security
  - 2018 TAM

- **$2B**
  - Cloud Security
  - 2018 TAM

- **$17B**
  - Security Ops
  - 2018 TAM

**Note:** the size of the bubbles in the chart is not adjusted to scale.

These transformations ended up driving rapid growth in cybersecurity.
These transformations ended up driving rapid growth in cybersecurity.

$45B
Network Security 2023 TAM

$11B
Cloud Security 2023 TAM

$48B
Security Ops 2023 TAM

Note: the size of the bubbles in the chart is not adjusted to scale
What we have achieved in the last 5 years

- Proved **Platforms** are the way to deliver security outcomes
- Made **Innovation** the lifeblood of our multi-product business
- Executed “**Build & Buy**” strategy to become the largest cyber player

- **20+ Industry Recognitions**
- **180+ major releases since FY19**
- **~3.5x Market Cap growth**

---

1. Average market cap for the first 15 days in August 2018 to the first 15 days in August 2023; source: Bloomberg
Looking ahead

Shift to more real-time and autonomous security

The future will require ubiquitous platformization to deliver real-time security outcomes
Our addressable market continues to expand

Zero Trust Platform
~$80B by 2028
Security for network traffic managed comprehensively via a single pane of glass

Code to Cloud Platform
~$40B by 2028
Scalable and comprehensive security across the cloud app development lifecycle

Autonomous Security Ops Platform
~$90B by 2028
Security reaching ‘real-time’ using the power of AI to contend with agile bad actors
Our strategy to win

Be an evergreen innovation company
Fortify our multi-category lead

Make our platforms more comprehensive & ubiquitous
Deliver near real-time security outcomes

Leverage AI across our portfolio
Supercharge our Products, Processes & People

Amplify our go-to-market to deliver our ambition
Drive ubiquity across customers

Be the best place to work in cybersecurity
Build the most capable and motivated team
Our strategy to win

- Innovation
- Platformization
- Leverage AI
- Go-To-Market
- Team
To stay ahead of relentless adversaries, we must be an innovation-led cybersecurity company

Our innovation pipeline drove our success...
Number of major product releases by year

...and we plan to accelerate the pace

Underpinning ML/AI across our portfolio

Expanding sensors into new parts of the estate like OT

Scouting externally for next-level capabilities & modules

Investing in leading edge R&D, from AI threats to quantum

Enhanced by Acquisitions
We are enhancing our platforms to deliver real-time security outcomes

**ZERO TRUST PLATFORM**
Radically more integration across form-factors...
Comprehensiveness across form-factors enabling Zero Trust
‘Single pane of glass’ offering instantaneous visibility & response

**CODE TO CLOUD PLATFORM**
Security will be at the ‘speed of Cloud’...
Traceability through integration across the app lifecycle
‘Block in real-time’ and ‘fix at the source’

**AUTONOMOUS SECOPS PLATFORM**
MTTR will need to go from Days to Minutes...
‘Real-time remediation’ by stitching data across sources and using AI
All security products will either provide data or act as enforcement points
We will leverage AI across our entire portfolio

Unique Assets

- Sensors installed across ~48k customers

- 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
Continued evolution of our Go-To-Market model...

FROM

Transactional vendor  \rightarrow  Strategic partner helping customers on their transformation journey

Selling products  \rightarrow  Architecting outcomes jointly with ecosystem solution providers

Reactive help  \rightarrow  “In it together” mindset - driving success for every customer
Delivering on our strategy is only possible with the best team

We will attract the best...

with opportunity to **make an impact**, **flexibility** to get the job done and challenging work to **grow and develop**

...and empower them

by radically **eliminating friction**, providing **information at their fingertips** and driving **autonomy with accountability**

Built on our Brand and Reputation

Supercharged by Generative AI

**40+ Employer Awards in FY23**
The continued business transformation of Palo Alto Networks...

Strong & sustained top-line growth

- Target markets undergoing inflection
- Relentless innovation across all 3 platforms
- Closer GTM partnerships to expand platform reach
- Software & Cloud increasingly fueling growth

Unique opportunity to deliver leverage beyond expectations

- Integrated salesforce with scale across platforms
- Platform and scale benefits within R&D
- GenAI-enabled employee & operational productivity
- AI-driven technical support transformation
Innovating our way to three leading platforms
Lee Klarich

Chief Product Officer
The threat landscape is intensifying

Elevated attacker motivation

$8T cost of cybercrime

Integral part of modern warfare

Nation-state economic gain

Tech is enabling attacks at scale

Automated attacks executed across regions within 1 hour of initial compromise

>10 million people and >1,700 organizations affected by supply chain attacks in 2022

Near-instant “trickle down” of attack techniques

Organizations are heavily impacted... and it’s getting worse

20x increase to 1.3 billion new malicious programs since 2014

Sources:
2. Unit 42 research: https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/

© 2023 Palo Alto Networks, Inc. All rights reserved.
Attacks are happening faster than organizations can respond

**Average Days from “Compromise” to “Exfil”**

- **2021**: 44 days
- **2022**: 30 days
- **2023**: 5 days

**Latest attacks**

**Industry average**

- **6 DAYS** to remediate
- **4 DAYS** to disclose material cybersecurity incident

**Sources:**

1. Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience
2. Under the new SEC Rules, the occurrence of a cybersecurity incident must be reported within four business days of when the incident is determined to be material by the reporting company.
AI will transform the threat landscape

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

WSJ

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”
$10.5T¹ cybercrime “market” in 2025

Sources:
¹ https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
Threat trends demand a high-powered innovation engine

4,400+ product team drives innovation

From single-product to 3 leading platforms in 5 years

While leveraging the broader market

Continuously identifying great tech to include in our journey

Embracing AI from the early days

AI used in all 3 platforms, across 30+ products and modules

~250

Private cybersecurity companies evaluated annually

Cumulative number of Palo Alto Networks products that use AI

*Some still in development
We will continue to be leading innovators

4,400+ product team drives innovation
From single-product to 3 leading platforms in 5 years

Accelerated pace of innovation

13 22 29 49 2023
2019 2020 2021 2022

While leveraging the broader market
Continuously identifying great tech to include in our journey

While leveraging the broader market

While leveraging the broader market

2019 2020 2021 2022 2023

Embracing AI from the early days
AI used in all 3 platforms, across 30+ products and modules

Evolution into an AI-first company

Private cybersecurity companies evaluated annually

2019 2020 2021 2022 2023

Cumulative number of Palo Alto Networks products that use AI

*Some still in development
Data, architecture, expertise key to being an AI-first company

The most security data per customer
Each day we analyze and detect 750M+ new and unique events
We secure 4.7B billion cloud resources
4.86PB/day ingested across XDR and XSIAM

The right architecture
All services running in the cloud
Enforcement points leveraged as data sensors
Designed for scale

Deep expertise
~150 AI experts across product organization
Proven tech leadership in the foundation of our next AI transformation
The industry approach leads to point product proliferation

~$210B
to “solve” the problem

Source: All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.
The industry approach leads to point product proliferation

Source: All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.
Only a platform approach will work

**Zero Trust Platform**
Network security that ensures every connection is secure

**Code to Cloud Platform**
Cloud security that ensures every cloud application is secure

**AI-Driven Security Operations Platform**
SecOps that is powered by a real-time security engine

*Source: All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.*
Not all platforms are created equal

1. Innovation-Led
2. Comprehensive
3. Integrated
4. Real-Time

© 2023 Palo Alto Networks, Inc. All rights reserved.
Zero Trust Platform
Network Security: Increased integration for real-time security

Network traffic will continue to increase; all traffic must be inspected

Users will remain hybrid, network needs to be protected everywhere

Point products will increase complexity & manual effort

Enterprises need a consolidated solution

Threat sophistication will necessitate faster response

AI enables self remediation

New use cases emerge — Passwordless, quantum (& PQC), BYOD

New trends will propel platformization and AI

Real-time in-line security for every connection

Great user experience across self-healing network

Single pane of glass for network and security

Our opportunity as TAM grows to ~$80B by 2028

Source: All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.
Network security has become increasingly complex

- Campus
- Branch
- Mobile
- Home
- Data Center
- Internet
- Public cloud
- SaaS

Hardware Security Stack
Software Security Stack
SASE Security Stack

One Platform, One Security Stack, One User Experience, One Security Policy

Network security has become increasingly complex.
What if we could take a radically new approach?

One Platform, One Security Stack,
One User Experience, One Security Policy

Unified Security Stack

Enterprise-wide Zero Trust Platform
Over the last 5 years, we have developed a Zero Trust Platform with best-in-class products.
Best-in-class form factors — Hardware, Software and SASE

Unified Management & Experience

Cloud-Delivered Security Services

NGFW
A Leader in Gartner Magic Quadrant Network Firewalls
Gartner

Zero Trust
A Leader in Forrester Zero Trust xTended Ecosystem Platform Providers Wave

SSE
A Leader in Gartner Magic Quadrant Security Service Edge

SD-WAN
A Leader in Gartner Magic Quadrant WAN Edge Infrastructure

Sources:
1. Gartner® Magic Quadrant for Network Firewalls, 19 December 2022
2. The Forrester Wave™: Zero Trust xTended Ecosystem Platform Providers, Q3 2020
3. Gartner® Magic Quadrant for Security Service Edge, 10 April 2023, Gartner® Magic Quadrant for SD-WAN, 12 September 2022
4. Gartner® Magic Quadrant for SD-WAN, 12 September 2022

© 2023 Palo Alto Networks, Inc. All rights reserved.
Best-in-class security services — Infused with AI for near real-time protection

Unified Management & Experience

Hardware Firewalls

Software Firewalls

SASE

Core Security

Inline deep learning models detect 96% of web-based Cobalt Strike

76% of malicious URLs discovered 24 hours before other vendors

99% prevention of known and unknown malware and 60X faster signature delivery

IOT

90% of devices discovered in 48 hours, protect seen and unseen devices

Data Security

80% higher data classification with ML-based detection
Best-in-class security services — Extended to AI-powered operations

Unified Management & Experience

- GlobalProtect
  - 86M users leverage GlobalProtect for securing remote access

- AIOps
  - Predict 51% of network disruptions before any customer impact

- ADEM
  - Quickly identify the problem segment and reduce IT escalations by 46%

Hardware Firewalls

Software Firewalls

SASE
The next transformation in network security — Unified management and experience

Zero Trust Network Security Platform

Unified Management & Experience

Cloud-Delivered Security Services

Hardware
Firewalls

VM-Series
CN-Series

Software
Firewalls

SASE
Is my environment impacted by CVE-2022-31706?
Guided remediation to secure against threats with “one click”
Best Practices

✓ Committed successfully. All security profiles are now following best practice recommendations.
Network Security
Copilot
Hello, Anand!

In the last 24 hours: Processed 32TB of data and blocked 54K threats to provide secure access to all 150K users.

- 4 Critical Open Incidents
- 140K/150K Users with Good Experience
- 327 Malicious Files Blocked
- 1100 Malicious URLs Blocked
Why are 10k users in my organization having degraded experience?
Why are 10k users in my organization having degraded experience?

Current Status

- 150k Users
- Good: 30k (99.36%)
- Degraded: 12k (6.7%)

Historical Trend (Last 24 hours)

10k users connecting to PA location US East US Southeast are having degraded experience while accessing Jira application.

Prisma Access is healthy. Jira application is reachable from the Prisma Access location and the authentication server deployed in your datacenter is reachable. All the 10k users impacted are having auth failures. This is mostly likely due to AAA service which requires further investigation.

ServiceNow ticket is already opened for this issue and NOC analyst has scheduled AAA service restart which should restore Jira application access.
Are users in my organization accessing any risky applications?
Are users in my organization accessing any risky applications?

There are 3135 users working from campus, remote locations and branch offices accessing 6 risky applications in last 7 days with total data transfer of 44.4 GB.

How can I block access to above risky applications?
Are users in my organization accessing any risky applications?

There are 3136 users working from campus, remote locations and branch offices accessing 6 risky applications in last 7 days with total data transfer of 44.9 GB.

<table>
<thead>
<tr>
<th>App Name</th>
<th>Risk Score</th>
<th>Usage</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>RoadWarrior</td>
<td>9</td>
<td>9.2 GB</td>
<td>900</td>
</tr>
<tr>
<td>Netify</td>
<td>9</td>
<td>8.4 GB</td>
<td>852</td>
</tr>
<tr>
<td>PDFElement</td>
<td>9</td>
<td>8.3 GB</td>
<td>752</td>
</tr>
<tr>
<td>Eventable</td>
<td>9</td>
<td>7.2 GB</td>
<td>632</td>
</tr>
<tr>
<td>InfowInventory</td>
<td>9</td>
<td>6.1 GB</td>
<td>551</td>
</tr>
<tr>
<td>AfterCollege</td>
<td>9</td>
<td>5.2 GB</td>
<td>231</td>
</tr>
</tbody>
</table>

How can I block access to above risky applications?

Type your question here
Are users in my organization accessing any risky applications?

There are 3,335 users working from campus, remote locations and branch offices accessing 6 risky applications in last 7 days with total data transfer of 48.1 GB.

How can I block access to above risky applications?

Following the best practice recommendations will block access to risky applications in your organization.
Best practice security recommendation ready for commit.

How you want to proceed?

- [ ] Review Changes
- [ ] Commit Changes
How can I block access to above risky applications?

Following the best practice recommendations will block access to risky applications in your organization.

Best practice security recommendation ready for commit.

How you want to proceed?

- [ ] Review Changes
- [x] Commit Changes

Commit successful. All security profiles are following best practice recommendations.
The opportunity ahead

Uniquely positioned to deliver Enterprise wide Zero Trust

Opportunity compounded by the adoption of integrated security services

- Deliver near real time security outcomes with Zero-trust platform
- Consolidate additional security services
- Deliver operational simplicity with AI

Customers with full network security platform

- 2021: ~800
- 2023: ~1,700
- 2028: 10,000+

# of services attached

- 2021: 2.8
- 2023: 3.4
- 2028: 5+
Code-to-Cloud Platform
Cloud Security: Only an integrated platform can secure from code to cloud

Organizations are building and using more applications

- 500M+ cloud-native applications globally
- 33M devs building apps, and growing
- 90% deploy applications in 2+ clouds

Securing Applications requires a Code to Cloud approach

- Applications are increasingly assembled - 75% of cloud code bases consist of open source
- 80% of open source contain at least 1 vulnerability
- Applications must be protected when Running, but also Secure by Design

Our opportunity: Deliver a AI-driven cloud security platform

- Today, securing code and cloud requires 15+ tools
- Continued evolution of cloud technologies will increase this count
- Preventing Breaches in Cloud and Fixing at the Source represents a ~$40B TAM in 2028

Sources:
1. IDC FutureScape;
2. State of the Developer Nation report, SlashData;
3. ESG 2023 Technology Spending Intentions Survey of 742 enterprises; Worldwide IT Industry 2020 Predictions;
Cloud applications are assembled in multiple stages
Security risks multiply across the application lifecycle
Security risks go unaddressed as the industry delivers multiple point products.
Our Code-to-Cloud Platform approach prevents risks & breaches in near real-time

Integrated context helps prioritize actions to Fix at Source and Block in Runtime
Our strategy is resonating well

- **Code**: Secure the source
  - 20% use Code Modules
  - **CNAPP LEADER**
    - Global CNAPP Radar 2022

- **Cloud Infrastructure**: Secure the infrastructure
  - 68% use infrastructure modules
  - **CSPM LEADER**
    - CSPM 2022 Radar
  - **Vuln Mgmt LEADER**
    - Vuln Mgmt 2021 Radar

- **Cloud Runtime**: Secure the runtime
  - 54% use Cloud runtime modules
  - **CWP LEADER**
    - Cloud Workload Security 2022 Forrester Wave

- **16%** use the Full Platform

---

**Code-to-Cloud Platform**
- SCA
- IaC Security
- SAST
- Secrets Scanning
- CICD Security
- CSPM
- CIEM
- CDS
- API
- Vulnerability Management
- CWP
- WAAS
- CNS
- CDR

---

1, 2, 3 - Customers using at least one module within Code / Infrastructure / Runtime categories
4 - Customers using at least one module each of Code, Infrastructure, and Runtime categories
The opportunity ahead

Customers expand rapidly into multiple modules as they adopt the full platform

Credit consumption grows with expansion across multiple modules

We are in the early innings of customers using multiple modules
AI-Driven Security Operations Platform
Security Operations: fundamental transformation needed for real-time outcomes

Fragmented stack leaves processing to a human analyst (93% of SOCs dependent on manual processes) ¹

Ever-faster threats (months → days → hours → minutes)

Not enough SOC analysts globally to keep pace with the threats

Today's human-driven SOC tools are far too slow

AI is the “only option” for near real-time attack detection and remediation

The SOC needs to be rebuilt from the ground up to enable AI

Order of magnitude more data, fully normalized, instantly accessible to precision AI models

Common platform needed to achieve the “self-driving SOC”

Large, previously independent categories driven to integrate

AI & automation to replace a portion of human-powered security services

Security Operations TAM will double to ~$90B by 2028

Source:
¹ IDC In Cybersecurity Every Alert Matters, October 2021
The human-driven SOC architecture doesn’t work

Every tool was built to perform one function.

No holistic end-to-end management of detection, investigation, and response.

Teams try to solve for highest-priority issues

Impossible to have real-time responses for all incidents with current tool stack

Sources:
2. IDC: In Cybersecurity Every Alert Matters, October 2021
3. ESG: SOC Modernization and the Role of XDR, October 2022

Impossible to have real-time responses for all incidents with current tool stack

~11K 1 ALERTS PER DAY
~93% 2 SOCS STILL DEPENDENT ON MANUAL PROCESSES
~23% 3 ALERTS GET IGNORED / NOT INVESTIGATED
Real-time Security Operations requires a single data platform powered by AI and Automation

- Massive data enhanced with stitching and correlation dramatically reduces the # of alerts
- Machines automate detection, investigation, and response and make recommendations
- Empowered analysts become more proactive

Detect, Investigate, Respond

Network
Endpoint
Identity
Cloud
Attack Surface
Other

Analytics (AI/ML)

Stitch and Normalize Data

Automation
We’ve built category-leading products to help the SOC for the past 5 years

Cortex XDR
Collect, stitch & analyze data in real time

 FY19  FY20  FY21  FY22  FY23
XDR 1.0  Threat Hunting  XDR Cloud  MDR  ITDR

Cortex XSOAR
Automating attack response actions

 Demisto acquisition  Threat Intel  Threat Intel 2.0  1,000+ Integrations  XSOAR Saas

Cortex XPANSE
Proactively shrink the attack surface

 Expanse acquisition  Xpanse Assess  Xpanse 2.0 Active ASM

Sources:
1 The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021; 2 GigaOm Radar for Security Orchestration, Automation, and Response v2.0 (Sept. 2022); 3 GigaOm Radar for Attack Surface Management v2.01 (Feb. 2023).

Recognized Leadership

FORRESTER
A Leader in Forrester Endpoint Security Software As A Service Wave 1

GIGAOM
Leader in GigaOm’s Security Orchestration, Automation and Response Radar 2

GIGAOM
Leader in GigaOm’s Attack Surface Management Radar 3
Cortex XSIAM

Security operations platform to enable near real-time outcomes
Detecting attacks with siloed tools and data is impossible

Unusual user login
Happens 50 times per day

Events in isolation can be suspicious...
Detecting attacks with siloed tools and data is impossible

...but they are common, and overwhelm the SOC.
Detecting attacks with siloed tools and data is impossible

This means attacks are missed…
Detecting attacks with siloed tools and data is impossible

...because of a low confidence to act on any one alert.
Cortex XSIAM collects complete context and uses the power of AI to detect attacks that siloed tools miss.

Stitching and normalizing alerts, augmented with contextual data...
Cortex XSIAM collects complete context and uses the power of AI to detect attacks that siloed tools miss

- Network
- Endpoint
- Identity
- Cloud
- Attack Surface
- Other

...enables us to automatically respond with high confidence.
XSIAM completely reimagines how the SOC works, built with AI on a common data platform
### Ingested Data per day

| Ingested Data per day | 75 TB |

### Incidents flagged per day*

| Incidents flagged per day* | 133 |

### Incidents resolved with automation*

| Incidents resolved with automation* | 100% |

### Incidents close out rate

| Incidents close out rate | 100% |

### Mean Time to Respond*

| Mean Time to Respond* | 1 MIN (HIGH SEVERITY ALERTS) |

---

*Incidents flagged* - potential security events flagged that requires automated or manual investigation. Incidents resolved with automation - partially or fully addressed with automation. Mean Time to Respond - time from incident creation to incident assignment.
And XSIAM is already driving amazing outcomes for our customers

<table>
<thead>
<tr>
<th>Before XSIAM</th>
<th>Early XSIAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzing more data ...</td>
<td>~230 GB per day (In prior SIEM)</td>
</tr>
<tr>
<td>with fewer false positives...</td>
<td>~290</td>
</tr>
<tr>
<td>and closing far more via automation...</td>
<td>Minimal</td>
</tr>
<tr>
<td>leading to all incidents getting addressed.</td>
<td>&lt;20% when not using MSSP</td>
</tr>
<tr>
<td>Most importantly, getting ahead of attackers</td>
<td>MTTR* 2-3 Days, sometimes even &quot;months&quot;</td>
</tr>
</tbody>
</table>

*Median Time To Resolve (time from incident creation to incident resolution). Incidents Resolved by automation partially or fully addressed with automation. Source: XSIAM customer interviews and XSIAM product telemetry for customers.

"XSIAM is the best single pane of glass I’ve seen in cybersecurity. We went from looking at 10 data stores to just XSIAM in our investigations."

– SOC Leader, XSIAM Customer
The opportunity ahead

Cortex customers, by fiscal year

\[\begin{array}{ccc}
\text{FY21A} & \text{FY23A} & \text{FY28F} \\
>2,600 & >5,100 & 10,000+ \\
\end{array}\]

- **$200M** XSIAM bookings in FY23
- **>3x** ARR Expansion when existing Cortex customers move to XSIAM
- **4** Customers booking >$20M on XSIAM in FY23

Continue taking share with our XDR, XSOAR, and Xpanse offerings...

...while building on our phenomenal XSIAM launch...

...and adding more modules to our AI-driven SecOps platform

**XSIAM Modules**

Over next 3-5 years
(both from Palo Alto Networks and our partners)

- **10+ additional XSIAM modules**
- EDR
- NTA
- ITDR
- TIP
- ASM
- SOAR
- SIEM

Customers booking >$20M on XSIAM in FY23

>2,600

>5,100

10,000+

Today

>3x

FY21A

FY23A

FY28F

Customers booking

$200M

$20M

>$20M

>$200M

>$20M

100
Go To Market
BJ Jenkins
President
Customers have tried to solve cybersecurity challenges by buying point solutions.

Security in customers’ estates is fragmented...

Average number of cybersecurity solutions at large companies

~75

Complexity
Customers are burdened with stitching together disparate products and data

Duplication
Multiple vendors’ products overlap and “do not talk to each other”

Most are buying cybersecurity ineffectively

1 Microsoft Study: “Microsoft Security Reaches Another Milestone - Comprehensive Customer Centric Solutions Drive Results”
As an industry, we need to get better at helping our customers

<table>
<thead>
<tr>
<th>FROM</th>
<th>TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactional vendor</td>
<td><strong>Strategic partner</strong> helping customers on their transformation journey</td>
</tr>
<tr>
<td>Selling products</td>
<td><strong>Architecting outcomes</strong> jointly with ecosystem solution providers</td>
</tr>
<tr>
<td>Reactive help</td>
<td><strong>“In it together”</strong> mindset - driving success for every customer</td>
</tr>
</tbody>
</table>
We are well on our journey to becoming a strategic partner

<table>
<thead>
<tr>
<th>Historical Motion</th>
<th>Evolving Motion across ~3,000 Sellers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engaged by technical domain experts</td>
<td>Engaged by CxOs looking to transform</td>
</tr>
<tr>
<td>Pre-defined product requirements</td>
<td>Strategic discussions focused on security outcomes</td>
</tr>
<tr>
<td>Focus on price negotiation</td>
<td>‘Seat at the table’ for architectural choices</td>
</tr>
<tr>
<td>Ends with a transactional product sale</td>
<td>Trusted relationship and multi-year roadmap</td>
</tr>
</tbody>
</table>
We will accelerate **solution selling in partnership with the broader ecosystem**

<table>
<thead>
<tr>
<th>Five Years Ago</th>
<th>Today</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sold a single product as part of a larger partner-delivered motion</td>
<td>Co-lead sales motions with our partners and deliver joint solutions</td>
<td>Architect integrated offerings with partners to improve client outcomes</td>
</tr>
</tbody>
</table>

~70% of route-to-market business was transactional **1**

~150 $10M+ strategic partners today **2**

~$10B+ in business from top 30 partners **3**

---

**1** Based on deal registration status for ecosystem sales

**2** Refers to number of partners (Value Added Resellers, SIs, SPs, and CPs) achieving $10M+ in sales in the FY23 fiscal year

**3** From top 30 partners sales across Value Added Resellers (VAR), System Integrators (SI), Service Providers (SP), and Cloud Providers (CP)
We are ‘in it together’ with our customers

Our customers have 90%+ CSAT today...

...and we plan to make it better

### Rapid AI-Driven Issue Resolution
In-product support, empowered by AI
*Targeting 65%+ reduction in Mean Time to Resolution (MTTR)*

### Accelerated Deployment
Scale global network of fully-certified delivery partners
*Starting from a base of 300+ today¹*

### Increased Adoption
Stick with the customer throughout their journey
*600+ CS professionals with deep expertise²*

---

¹ Includes CPSP (Certified Professional Services Partner) and PSDP (Professional Services Delivery Partner)
² Includes PANW branded employees and contractors
The opportunity in front of us is extensive...

We serve ~80% of G2K but only ~54% have begun the journey across all 3 platforms...

Note: Size of the bar is not to scale and for illustrative purposes only

FY23 Sales per G2K customer who have purchased 1, 2, or all 3 platforms defined as: Strata, Prisma, Cortex.

We have ample potential to expand the breadth & depth of our platforms...

Breadth
Land every platform across our installed base

Depth
Increase penetration by covering full estate of every customer
Our model is ready to scale and deliver real-time security outcomes for every customer through the power of our platforms.
Finance
Bringing it all Together
Dipak Golechha

Chief Financial Officer
We have shown we can capitalize on an expanding TAM

Expanding Platform TAMs

<table>
<thead>
<tr>
<th>Year</th>
<th>Cortex TAM</th>
<th>Prisma Cloud Security TAM</th>
<th>PANW share of Cortex TAM</th>
<th>PANW share of Cloud TAM</th>
<th>Network Security TAM</th>
<th>PANW share of NetSec TAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>$38B</td>
<td>$8B</td>
<td>$5B</td>
<td>$14B</td>
<td>$25B</td>
<td>$5B</td>
</tr>
<tr>
<td>2023</td>
<td>$104B</td>
<td>$20B</td>
<td>$26B</td>
<td>$72B</td>
<td>$40B</td>
<td>$10B</td>
</tr>
<tr>
<td>2026</td>
<td>$163B</td>
<td>$30B</td>
<td>$38B</td>
<td>$116B</td>
<td>$55B</td>
<td>$14B</td>
</tr>
</tbody>
</table>

Market share leaders in other IT categories

- ITOM: 36%
- CRM: 34%
- Database Mgmt Systems: 25%
- ERP SW: 17%

Our ~7% share of TAM remains well below that of leaders in other markets

1 All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.
Our platform leadership and innovation will fuel our growth and key metrics

- **Zero Trust**
  - FWaaP growth
  - Market share gains

- **Code-to-Cloud**
  - Credit consumption
  - New Module Adoption

- **Autonomous SecOps**
  - Growth in customers
  - Growth in large deals
Our go-to-market evolution enables us to execute on the larger opportunity.

- Become our customers’ strategic partner
- Deliver security outcomes
- Integrate into the ecosystems
- ‘In it together’ with our customers

### Large deal momentum over time (>10M+ deals)
- FY19: 15
- FY20: 32
- FY21: 42
- FY22: 67
- FY23: 110

### Increasing core productivity and driving growth in new channels
- >5% core sales productivity improvement annually, over the last 3 years
- ~75% growth in Cloud Service Provider (CSP) bookings in FY23
Growing revenue ahead of our markets through FY26 while increasing predictability

- **17-19%**
  - 3-yr revenue and billings CAGR
  - FY23-26

- **25%**
  - Growth in RPO through FY26

- **$6.5B**
  - NGS ARR exiting FY26

**FY26 Revenue Profile**

- ~10% of revenue from Hardware
- >55% Year end NGS ARR as % of total revenue
- ~2/3rs Proportion of revenue from prior year cRPO
We can deliver steady gross margin while investing in cloud

**Platform drivers**
- Higher software mix
- Public cloud scale
- Cross-company and platform Global Customer Support

**Cost / Efficiency initiatives**
- Supply chain normalizing
- Broad procurement efficiency
- Increasingly global support workforce
- AI-based automation in Support

Steady gross margin as we drive core improvements and invest in new cloud-based offerings
Platform and efficiency opportunities driving operating leverage

- **Platform drivers**
  - Core sellers always have more to sell and becoming more productive
  - Shared R&D platform and innovation spend
  - Increasing leverage in overhead functions

- **Efficiency initiatives**
  - Broad procurement efficiency
  - Consolidation of Sales Specialists
  - Leveraging global footprint

**AI-based automation in S&M and G&A**

**Continued opportunity for leverage in our operating expense, led by sales and marketing**
Significant operating margin expansion through FY26

- **Steady Gross Margin**: 28-29% FY26 non-GAAP operating margin
- **Low to Mid 30s**: Long-term non-GAAP operating margin potential
- **20%+**: non-GAAP EPS CAGR FY23-26

A reconciliation of forward-looking non-GAAP financial measures to the corresponding GAAP measures has not been provided as it is not available without unreasonable effort. Fiscal year ending on July 31.
Steady free cash flow margin with flexibility to navigate the environment

<table>
<thead>
<tr>
<th>Leverage drivers</th>
<th>FY’23 Drivers</th>
<th>FY’24 - FY’26 Net new drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong top-line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating margin leverage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Driving to best in class working capital management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low CAPEX requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Higher interest rates on cash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increase in % of bookings with deferred payments vs. FY23 levels</td>
<td></td>
<td>Accounting for higher cash taxes</td>
</tr>
</tbody>
</table>

Accounting for business shifts
We have already delivered strong cash flow while managing through an increase in deferred payments.

Increased deals with Deferred Payments

Robust Free Cash Flow Margins

Deferred payments will contribute ~$1B in FY24 free cash flow (2x vs. FY23)
Aspiring to the ‘rule of 60’

17%-19%
3-yr revenue and billings CAGR (FY23-26)

37%+
Adjusted non-GAAP FCF margin sustained FY24-26

Peer group-leading combination of growth and cash flow while having the flexibility to navigate the current environment
Driving optimal balance of capital allocation

$2.5B
In cash used for M&A over last 5 years

Continue focus on acquiring emerging leaders and boosting with our GTM

$1.7B
FY23 convertible note repaid

Maintenance capital structure that allows flexibility & minimizes dilution

$3.9B
In cash used for share repurchase over last 5 years

Planning to settle $2.0B FY25 convertible note with cash

Opportunistic buyback

$3.9B
In cash used for share repurchase over last 5 years
Bringing it all together into an attractive financial profile

**Top Line**

17%-19% revenue CAGR, from FY23-FY26  
17%-19% billings CAGR, from FY23-FY26  
$6.5B in NGS ARR, exiting FY26  
25% RPO CAGR, from FY23-FY26  
~10% of revenue from hardware, by FY26

**Non-GAAP operating income**

28%-29% FY26 Non-GAAP Operating Margin  
Low to mid-30%, Long-term Non-GAAP Operating Margin potential

**Non-GAAP EPS**

20%+ non-GAAP EPS CAGR, from FY23-FY26

**Adjusted Non-GAAP free cash flow**

37%+ adjusted non-GAAP FCF margin, sustained from FY24-26

A reconciliation of forward-looking non-GAAP financial measures to the corresponding GAAP measures has not been provided as it is not available without unreasonable effort. Fiscal year ending on July 31.
Thank you for watching
Appendix
## Calculation of Billings

<table>
<thead>
<tr>
<th></th>
<th>Q422</th>
<th>Q123</th>
<th>Q223</th>
<th>Q323</th>
<th>Q423</th>
<th>FY'22</th>
<th>FY'23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total revenue</td>
<td>$1,550.5</td>
<td>$1,563.4</td>
<td>$1,655.1</td>
<td>$1,720.9</td>
<td>$1,953.3</td>
<td>$5,501.5</td>
<td>$6,892.7</td>
</tr>
<tr>
<td>Add: change in total deferred revenue, net of acquired deferred revenue</td>
<td>1,134.6</td>
<td>185.6</td>
<td>374.0</td>
<td>535.3</td>
<td>1,206.8</td>
<td>1,970.0</td>
<td>2,301.7</td>
</tr>
<tr>
<td>Total billings</td>
<td>$2,685.1</td>
<td>$1,749.0</td>
<td>$2,029.1</td>
<td>$2,256.2</td>
<td>$3,160.1</td>
<td>$7,471.5</td>
<td>$9,194.4</td>
</tr>
</tbody>
</table>
GAAP to Non-GAAP Reconciliations

Gross Margin

$ In millions

<table>
<thead>
<tr>
<th>Non-GAAP gross profit and gross margin:</th>
<th>Q422</th>
<th>%</th>
<th>Q423</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAAP gross profit and gross margin</td>
<td>$1,058.2</td>
<td>68.2%</td>
<td>$1,446.5</td>
<td>74.1%</td>
</tr>
<tr>
<td>Share-based compensation-related charges</td>
<td>36.0</td>
<td>2.3%</td>
<td>41.8</td>
<td>2.1%</td>
</tr>
<tr>
<td>Amortization expense of acquired intangible assets</td>
<td>25.8</td>
<td>1.7%</td>
<td>19.3</td>
<td>1.0%</td>
</tr>
<tr>
<td>Litigation-related charges⁽¹⁾</td>
<td>1.7</td>
<td>0.1%</td>
<td>1.7</td>
<td>0.1%</td>
</tr>
<tr>
<td>Restructuring and other costs⁽²⁾</td>
<td>14.0</td>
<td>0.9%</td>
<td>-</td>
<td>0.0%</td>
</tr>
<tr>
<td>Non-GAAP total gross profit and gross margin</td>
<td>$1,135.7</td>
<td>73.2%</td>
<td>$1,509.3</td>
<td>77.3%</td>
</tr>
</tbody>
</table>

⁽¹⁾ Consists of the amortization of intellectual property licenses and covenant not to sue.
⁽²⁾ Consists of manufacturing related charges and other costs.

Fiscal year ends on July 31.
GAAP to Non-GAAP Reconciliations
Operating Margin

$ In millions

<table>
<thead>
<tr>
<th>Non-GAAP operating income and operating margin:</th>
<th>Q422</th>
<th>Q423</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAAP operating income and operating margin</td>
<td>$15.4</td>
<td>1.0%</td>
</tr>
<tr>
<td>Share-based compensation-related charges</td>
<td>251.3</td>
<td>16.1%</td>
</tr>
<tr>
<td>Acquisition-related costs⁽¹⁾</td>
<td>2.4</td>
<td>0.2%</td>
</tr>
<tr>
<td>Amortization expense of acquired intangible assets</td>
<td>31.2</td>
<td>2.0%</td>
</tr>
<tr>
<td>Litigation-related charges⁽²⁾</td>
<td>1.7</td>
<td>0.1%</td>
</tr>
<tr>
<td>Restructuring and other costs⁽³⁾</td>
<td>21.2</td>
<td>1.4%</td>
</tr>
<tr>
<td>Non-GAAP operating income and operating margin</td>
<td>$323.2</td>
<td>20.8%</td>
</tr>
</tbody>
</table>

⁽¹⁾ Consists of acquisition transaction costs, share-based compensation related to the cash settlement of certain equity awards, and costs to terminate other contracts of the acquired companies.
⁽²⁾ Consists of the amortization of intellectual property licenses and covenant not to sue.
⁽³⁾ Consists of manufacturing related charges, loss on the closure of an office facility, and other costs.

Fiscal year ends on July 31.
### GAAP to Non-GAAP Reconciliations

#### Operating Margin

<table>
<thead>
<tr>
<th>Non-GAAP operating income and operating margin:</th>
<th>FY’20</th>
<th>FY’21</th>
<th>FY’22</th>
<th>FY’23</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAAP operating income (loss) and operating margin</td>
<td>($179.0)</td>
<td>($304.1)</td>
<td>($188.8)</td>
<td>$387.3</td>
</tr>
<tr>
<td>Share-based compensation-related charges</td>
<td>685.5</td>
<td>936.5</td>
<td>1,072.0</td>
<td>1,145.1</td>
</tr>
<tr>
<td>Acquisition-related costs⁽¹⁾</td>
<td>15.7</td>
<td>46.1</td>
<td>5.5</td>
<td>19.5</td>
</tr>
<tr>
<td>Amortization expense of acquired intangible assets</td>
<td>76.4</td>
<td>116.7</td>
<td>125.8</td>
<td>103.1</td>
</tr>
<tr>
<td>Litigation-related charges⁽²⁾</td>
<td>3.6</td>
<td>7.1</td>
<td>7.1</td>
<td>7.1</td>
</tr>
<tr>
<td>Restructuring and other costs⁽³⁾</td>
<td>(3.1)</td>
<td>-</td>
<td>21.2</td>
<td>(2.2)</td>
</tr>
<tr>
<td>Non-GAAP operating income and operating margin</td>
<td>$599.1</td>
<td>$802.3</td>
<td>$1,042.8</td>
<td>$1,659.9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$ in millions</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY’20</td>
</tr>
<tr>
<td>$</td>
</tr>
<tr>
<td>($179.0)</td>
</tr>
<tr>
<td>685.5</td>
</tr>
<tr>
<td>15.7</td>
</tr>
<tr>
<td>76.4</td>
</tr>
<tr>
<td>3.6</td>
</tr>
<tr>
<td>(3.1)</td>
</tr>
<tr>
<td>$599.1</td>
</tr>
</tbody>
</table>

⁽¹⁾ Consists of acquisition transaction costs, share-based compensation related to the cash settlement of certain equity awards, and costs to terminate certain employment, operating lease, and other contracts of the acquired companies.

⁽²⁾ Consists of the amortization of intellectual property licenses and covenant not to sue.

⁽³⁾ Consists of manufacturing related charges, (gain) loss on the closure of certain office facilities, other costs, and related adjustments.

Fiscal year ends on July 31.
## GAAP to Non-GAAP Reconciliations

### EPS

<table>
<thead>
<tr>
<th>Non-GAAP net income per share, diluted:</th>
<th>Q422</th>
<th>Q123</th>
<th>Q223</th>
<th>Q323</th>
<th>Q423</th>
<th>FY’22</th>
<th>FY’23</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAAP net income (loss) per share, diluted</td>
<td>$0.01</td>
<td>$0.06</td>
<td>$0.25</td>
<td>$0.31</td>
<td>$0.64</td>
<td>($0.90)</td>
<td>$1.28</td>
</tr>
<tr>
<td>Share-based compensation-related charges</td>
<td>0.78</td>
<td>0.87</td>
<td>0.94</td>
<td>0.91</td>
<td>0.86</td>
<td>3.42</td>
<td>3.59</td>
</tr>
<tr>
<td>Acquisition-related cost⁽¹⁾</td>
<td>0.01</td>
<td>0.00</td>
<td>0.04</td>
<td>0.02</td>
<td>0.00</td>
<td>0.02</td>
<td>0.06</td>
</tr>
<tr>
<td>Amortization expense of acquired intangibles assets</td>
<td>0.09</td>
<td>0.08</td>
<td>0.07</td>
<td>0.07</td>
<td>0.07</td>
<td>0.43</td>
<td>0.30</td>
</tr>
<tr>
<td>Litigation-related charges⁽²⁾</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.00</td>
<td>0.02</td>
<td>0.02</td>
</tr>
<tr>
<td>Restructuring and other costs⁽³⁾</td>
<td>0.06</td>
<td>(0.01)</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.08</td>
<td>(0.01)</td>
</tr>
<tr>
<td>Non-cash charges related to convertible notes⁽⁴⁾</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.00</td>
<td>0.02</td>
<td>0.02</td>
</tr>
<tr>
<td>Foreign currency gain (loss) associated with non-GAAP adjustments</td>
<td>0.00</td>
<td>(0.01)</td>
<td>0.01</td>
<td>0.00</td>
<td>0.00</td>
<td>(0.01)</td>
<td>0.00</td>
</tr>
<tr>
<td>Income tax and other tax adjustments⁽⁵⁾</td>
<td>(0.17)</td>
<td>(0.18)</td>
<td>(0.28)</td>
<td>(0.23)</td>
<td>(0.13)</td>
<td>(0.56)</td>
<td>(0.82)</td>
</tr>
<tr>
<td>Non-GAAP net income per share, diluted</td>
<td>$0.80</td>
<td>$0.83</td>
<td>$1.05</td>
<td>$1.10</td>
<td>$1.44</td>
<td>$2.52</td>
<td>$4.44</td>
</tr>
</tbody>
</table>

⁽¹⁾ Consists of acquisition transaction costs, share-based compensation related to the cash settlement of certain equity awards, and costs to terminate certain employment, operating leases, and other contracts of the acquired companies.

⁽²⁾ Consists of the amortization of intellectual property licenses and covenant not to sue.

⁽³⁾ Consists of manufacturing related charges, loss on the closure of an office facility, other costs, and related adjustments.

⁽⁴⁾ Consists primarily of non-cash interest expense for amortization of debt issuance costs related to our convertible senior notes.

⁽⁵⁾ Consists of income tax adjustments related to our long-term non-GAAP effective tax rate. In Q2’23, it included a tax benefit from a release of tax reserves related to uncertain tax positions resulting from a tax settlement.

Fiscal year ends on July 31.
### GAAP to Non-GAAP Reconciliations

#### Adjusted Free Cash Flow

<table>
<thead>
<tr>
<th>Free cash flow and adjusted free cash flow (non-GAAP):</th>
<th>Q423</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net cash provided by operating activities</td>
<td>$414.1</td>
</tr>
<tr>
<td>Less: purchases of property, equipment, and other assets</td>
<td>37.2</td>
</tr>
<tr>
<td>Free cash flow (non-GAAP)</td>
<td>$376.9</td>
</tr>
<tr>
<td>Add: cash payment related to tax settlement</td>
<td>10.9</td>
</tr>
<tr>
<td>Adjusted free cash flow (non-GAAP)</td>
<td>$387.8</td>
</tr>
</tbody>
</table>

$ In millions
GAAP to Non-GAAP Reconciliations

Adjusted Free Cash Flow

$ In millions

<table>
<thead>
<tr>
<th>Free cash flow and adjusted free cash flow (non-GAAP):</th>
<th>FY’20</th>
<th>FY’21</th>
<th>FY’22</th>
<th>FY’23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net cash provided by operating activities</td>
<td>$1,035.7</td>
<td>$1,503.0</td>
<td>$1,984.7</td>
<td>$2,777.5</td>
</tr>
<tr>
<td>Less: purchases of property, equipment, and other assets</td>
<td>214.4</td>
<td>116.0</td>
<td>192.8</td>
<td>146.3</td>
</tr>
<tr>
<td>Free cash flow (non-GAAP)</td>
<td>$821.3</td>
<td>$1,387.0</td>
<td>$1,791.9</td>
<td>$2,631.2</td>
</tr>
<tr>
<td>Add: capital expenditures for headquarters⁽¹⁾</td>
<td>94.3</td>
<td>-</td>
<td>38.9</td>
<td>-</td>
</tr>
<tr>
<td>Add: cash payment related to tax settlement</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>39.8</td>
</tr>
<tr>
<td>Add: repayments of convertible senior notes attributable to debt discount</td>
<td>-</td>
<td>0.1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Add: litigation related payment⁽²⁾</td>
<td>50.0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Less: cash payment related to landlord lease amendment⁽³⁾</td>
<td>(2.0)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Adjusted free cash flow (non-GAAP)</td>
<td>$967.6</td>
<td>$1,387.1</td>
<td>$1,830.8</td>
<td>$2,671.0</td>
</tr>
</tbody>
</table>

Adjusted free cash flow margin (non-GAAP)

<table>
<thead>
<tr>
<th></th>
<th>FY’20</th>
<th>FY’21</th>
<th>FY’22</th>
<th>FY’23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjusted free cash flow margin (non-GAAP)</td>
<td>28.4 %</td>
<td>32.6 %</td>
<td>33.3 %</td>
<td>38.8 %</td>
</tr>
</tbody>
</table>

⁽¹⁾ Consists of capital expenditures for our headquarters including a land purchase of $51.7 million in Q3’20 and $38.9 million in Q2’22.
⁽²⁾ Consists of a one-time payment in Q3’20 related to covenant not to sue.
⁽³⁾ During Q3’19, we received an upfront cash reimbursement of $58.2 million from our landlords in connection with the exercise of their option to amend the lease payment schedules and eliminate the rent holiday periods under certain of our lease agreements. The upfront cash reimbursement was applied against increased rental payments totaling $38.2 million due in FY’18 through Q1’20 under the amended lease agreements. Adjusted free cash flow for the periods presented reflects adjustments for these increased rental payments made during the respective periods.

Fiscal year ends on July 31.
Reports

Third-party data from the reports listed below was used as a basis for the estimates and figures in this presentation related to total addressable markets, market or segment sizes or similar data (“TAM Data”). All TAM Data is for calendar years. For the purposes of this presentation, we sometimes refer to a “Network Security,” “Cloud Security,” or “Security Operations” segment. The “Network Security” segment includes the following segments described in this presentation: SASE, Network Security, Data Security and IoT Security. The “Cloud Security” segment includes the following segments described in this presentation: cloud security and a portion of the application security segment estimated to be attributable to security tools used for cloud applications. The “Security Operations” segment includes the following segments described in this presentation: SecOps [+SIEM] and Endpoint / XDR.

For estimates and figures related to calendar years 2018 and 2020:
- Omdia, Network Security Appliances and Software Market Tracker, 1Q23 Database (June 30, 2023)
- Omdia, Content Security Gateway Appliances, Software, and SaaS Market Tracker, 1Q23 Database (June 13, 2023)
- Dell’Oro Group, Network Security Forecast Tables, July 2023
- Gartner, Forecast: Public Cloud Services, Worldwide, 2018-2024, Q420 Update (December 21, 2020)
- Gartner, Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2021-2027, 2Q23 Update (June 29, 2023)
- Gartner, Market Databook, Q420 Update (Forecast for IT Worldwide, 2018-2024) (December 22, 2022)
- International Data Corporation, Worldwide Semiannual Security Product Tracker (June 2023)
- International Data Corporation, Worldwide Security Spending Guide (July 2023)
- Palo Alto Networks estimates

For estimates and figures related to calendar years 2023 and 2026:
- Omdia, Network Security Appliances and Software Market Tracker, 1Q23 Database (June 30, 2023)
- Omdia, Content Security Gateway Appliances, Software, and SaaS Market Tracker, 1Q23 Database (June 13, 2023)
- Dell’Oro Group, Network Security Forecast Tables, July 2023
- Gartner, Forecast: Information Security and Risk Management, Worldwide 2021-2027, 2Q23 Update (June 29, 2023)
- Gartner, Forecast: Public Cloud Services, Worldwide, 2021-2027, 2Q23 Update (July 10, 2023)
- Gartner, Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2021-2027, 2Q23 Update (June 29, 2023)
- Gartner, Market Databook, 2Q23 Update, Worldwide, IT, 2021-2027 (June 30, 2023)
- Gartner, Forecast: Enterprise Infrastructure Software, Worldwide, 2021-2027, 2Q23 Update (June 29, 2023)
- International Data Corporation, Worldwide and US Comprehensive Security Services Forecast, 2023-2027 (June 2023)
- International Data Corporation, Worldwide Semiannual Security Product Tracker (June 2023)
- International Data Corporation, Worldwide OT Security Forecast, 2022-2026 (July 2022)
- International Data Corporation, Worldwide Security Spending Guide (July 2023)
- Palo Alto Networks estimates

For estimates and figures related to calendar year 2028:
- Palo Alto Networks estimates