paloalto® NETWORKS

Q4 Fiscal Year 2023

Earnings Call & Medium Term Update

Q4 Fiscal Year 2023 Earnings Call

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.

Nikesh Arora

CEO & Chairman

Q4 capped a strong year of execution

TOTAL REVENUE

$1.95B
+26% y/y

OPERATING MARGIN (NON-GAAP)

28.4%
+760 bps y/y

TOTAL BILLINGS

$3.16B
+18% y/y

ADJ. FREE CASH FLOW (NON-GAAP)

$388M
+46% y/y on trailing 12-month basis

REMAINING PERFORMANCE OBLIGATION

$10.6B
+30% y/y

EPS (NON-GAAP)

$1.44
+80% y/y

DELIVERED AT OR ABOVE ALL INITIAL FY'23 GUIDANCE TARGETS

	GUIDANCE AS OF 8/22/22	ACTUAL RESULTS	
Total Billings [1]	**$8.95B - $9.05B** +20%-21% yr/yr	**$9.19B** +23% yr/yr	✓
Total Revenue	**$6.85B - $6.90B** +25% yr/yr	**$6.89B** +25% yr/yr	✓
EPS (Non-GAAP)	**$3.13 - $3.17** [2] +24%-26% yr/yr	**$4.44** +76% yr/yr	✓
Adj. FCF Margin (Non-GAAP)	**33.5-34.5%**	**38.8%**	✓

[1] Total billings is a key financial metric calculated as total revenue plus change in total deferred revenue, net of total acquired deferred revenue.
[2] Non-GAAP Earnings Per Share for period Q4'22 adjusted to reflect the effect of the stock split executed on September 13, 2022
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.

5

Continued strong demand for cybersecurity drove our NGS business

We achieved key milestones

SASE
>$1B in FY'23 bookings

Cortex
>$1B in FY'23 bookings

Prisma Cloud
>$500M in ARR in Q4 [2]

Q4'23 NGS ARR [1]

$2.95B

Q4'23 NGS ARR growth y/y

+56%

Net New NGS ARR q/q

+$381M

Largest Net New ARR in PANW history

Largest Net New ARR of any pure-play cybersecurity company [3]

Platformization continues to drive large deal momentum

Six out of top-10 deals were Driven by NGS

Deal[1] size (TCV)

Top 10 Q4'23 deals

- ✓ Deal 1
- ✓ Deal 2
- ✓ Deal 3
- ✓ Deal 4
- ✓ Deal 5
- ✓ Deal 6
- ✓ Deal 7
- ✓ Deal 8
- ✓ Deal 9
- ✓ Deal 10

- ● % of Deal - non-NGS
- ● % of Deal - NGS
- **Deal** Top-10 deal driven by NGS
- ✓ Have Purchased all 3 NGS Areas [2]

Large deal growth

+37% y/y

Number of Deals [1]
>$10M

+43% y/y

Number of Deals [1]
>$20M
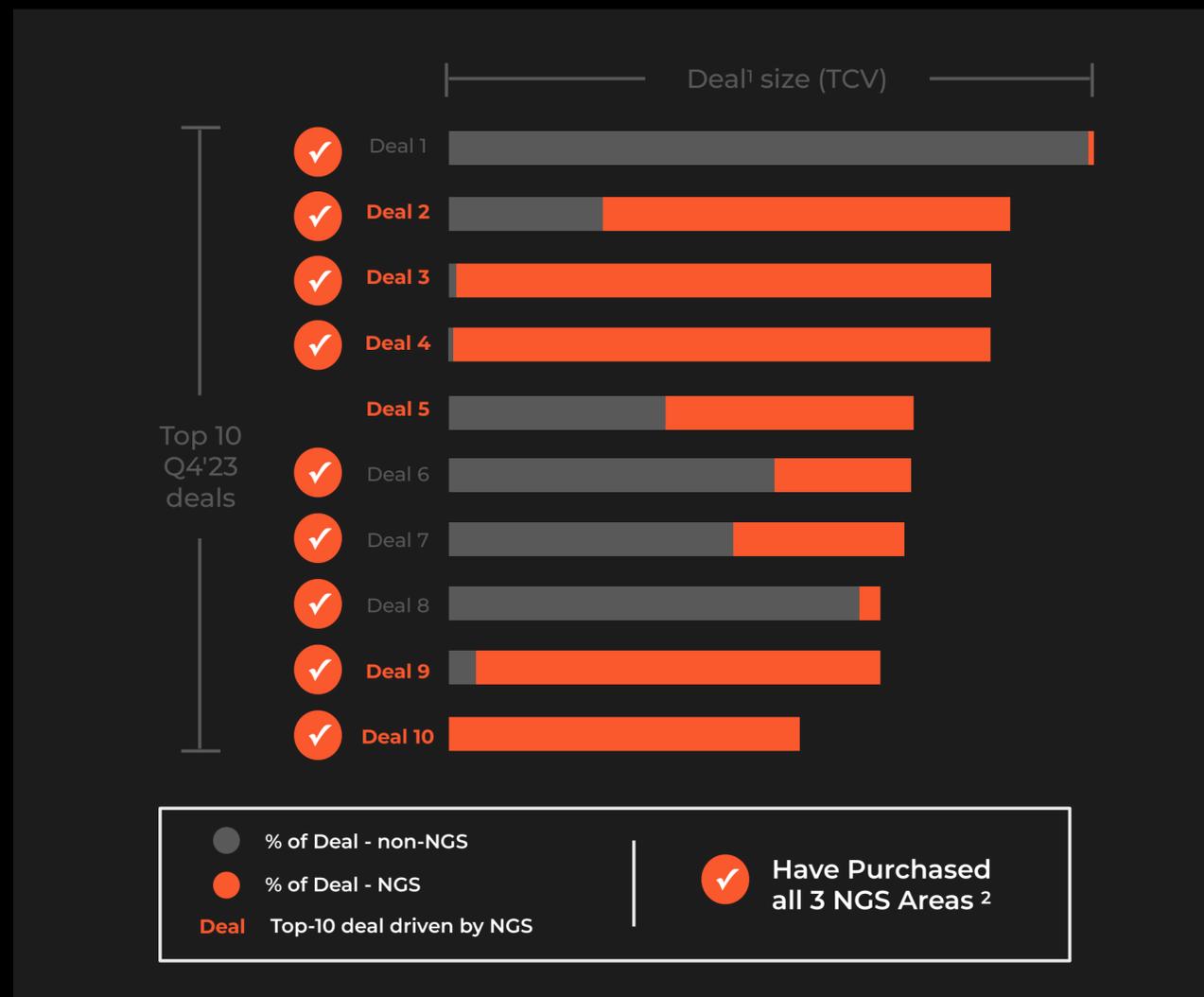
[1] Deal represents the total bookings from a single customer, within the stated period.
[2] Have made a purchase of SASE, Cortex, and Prisma Cloud, life to date.

XSIAM traction amplifying Cortex trajectory

>$200M

XSIAM Bookings within first year of release

XSIAM Transactions are Large and Strategic

3-5 Year
customer commitments

>$1M
Average ACV [1]

Driving MTTR [2] from days to hours / minutes

Cortex Active Customers

Q4'23 Average Cortex Deal Size

>5K
+28% y/y

+50%
y/y

Driven by XDR customer adds and market-leading XSOAR

8

◀◀ SASE

SASE continues to display strong performance

Q4'23 SASE ARR Growth

~60% y/y

FY'23 Bookings [1]

>$1B

Two new SASE leadership position

FORRESTER®

A **Leader** in Forrester Zero Trust Enterprise Wave

☰IDC

Leader in IDC ZTNA MarketScape

5

Total SASE & Zero Trust Category Leadership Positions

Increasing leadership recognition is contributing to our customer wins

Marquee deals in Q4

$43M
New win with a Business Consulting and Services Company

$26M
Expansion with a US Technology Company

$21M
Expansion with a European Food and Beverages company

$11M
Expansion with a US Financial Services Company

SASE continues to display strong performance

Q4'23 SASE ARR Growth

~60% y/y

FY'23 Bookings [1]

>$1B

Two new SASE

FORRESTER®

A **Leader** in Forrester Zero Trust Enterprise Wave

Leader in IDC ZTNA MarketScape

5

Total SASE & Zero Trust Category Leadership Positions

Increasing leadership recognition is contributing to our customer wins

Marquee deals in Q4

$43M
New win with a Business Consulting and Services Company

Expansion with a US Technology Company

Expansion with a European Food and Beverages company

$11M
Expansion with a US Financial Services Company

BREAKING NEWS

Gartner®

Single Vendor SASE Magic Quadrant

Published: August 16th, 2023

[1] Prisma SASE includes Prisma Access and Prisma SD-WAN, PANOS SD-WAN and SaaS Security subscriptions.

10

PRISMA® CLOUD

Sustained credit consumption propels Prisma Cloud through $500M in ARR [1]

Growth in multi-module adoption customers [2]

+31% y/y — 2+ modules

+57% y/y — 3+ modules

+179% y/y — 5+ modules

Extending Platform Lead in Q4
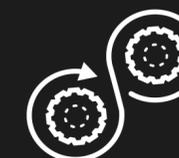
Enhancing Cloud Security capabilities

API Change Detection

Agentless CWP

Launched 11th module based on Cider acquisition

CI/CD Security

FY23: Successful execution through a tough macro environment

Platformization

Go to market transformation

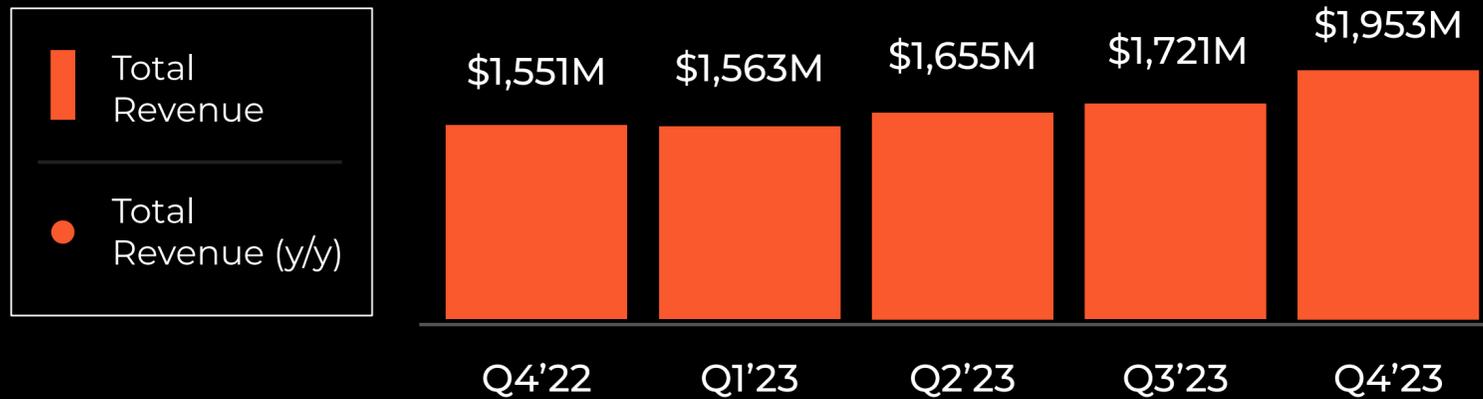Strong product innovation

Driving efficiency and leverage

Dipak Golechha

Chief Financial Officer

Strong top-line growth at industry leading scale

Total Revenue

	27%	25%	26%	24%	26%
	$1,551M	$1,563M	$1,655M	$1,721M	$1,953M
	Q4'22	Q1'23	Q2'23	Q3'23	Q4'23

Legend:
- Total Revenue
- Total Revenue (y/y)

Next-Gen Security ARR

	60%	67%	63%	60%	56%
	$1,893M	$2,111M	2,332M	2,574M	$2,955M
	Q4'22	Q1'23	Q2'23	Q3'23	Q4'23

Legend:
- Next-Gen Security ARR
- Next-Gen Security ARR (y/y)

Total Billings

	44%	27%	26%	26%	18%
	$2,685M	$1,749M	2,029M	2,256M	$3,160M
	Q4'22	Q1'23	Q2'23	Q3'23	Q4'23

Legend:
- Total Billings
- Total Billings (y/y)

Remaining Performance Obligation

	40%	38%	39%	35%	30%
	$8.2B	$8.3B	$8.8B	$9.2B	$10.6B
	Q4'22	Q1'23	Q2'23	Q3'23	Q4'23

Legend:
- Remaining Performance Obligation
- Remaining Performance Obligation (y/y)

Managing through the impact of the rising cost of money

% of Bookings under Deferred Payment Plans [1]

Q4'22	Q1'23	Q2'23	Q3'23	Q4'23

% of Bookings under deferred payment plans

Remaining Performance Obligation

40%	38%	39%	35%	30%

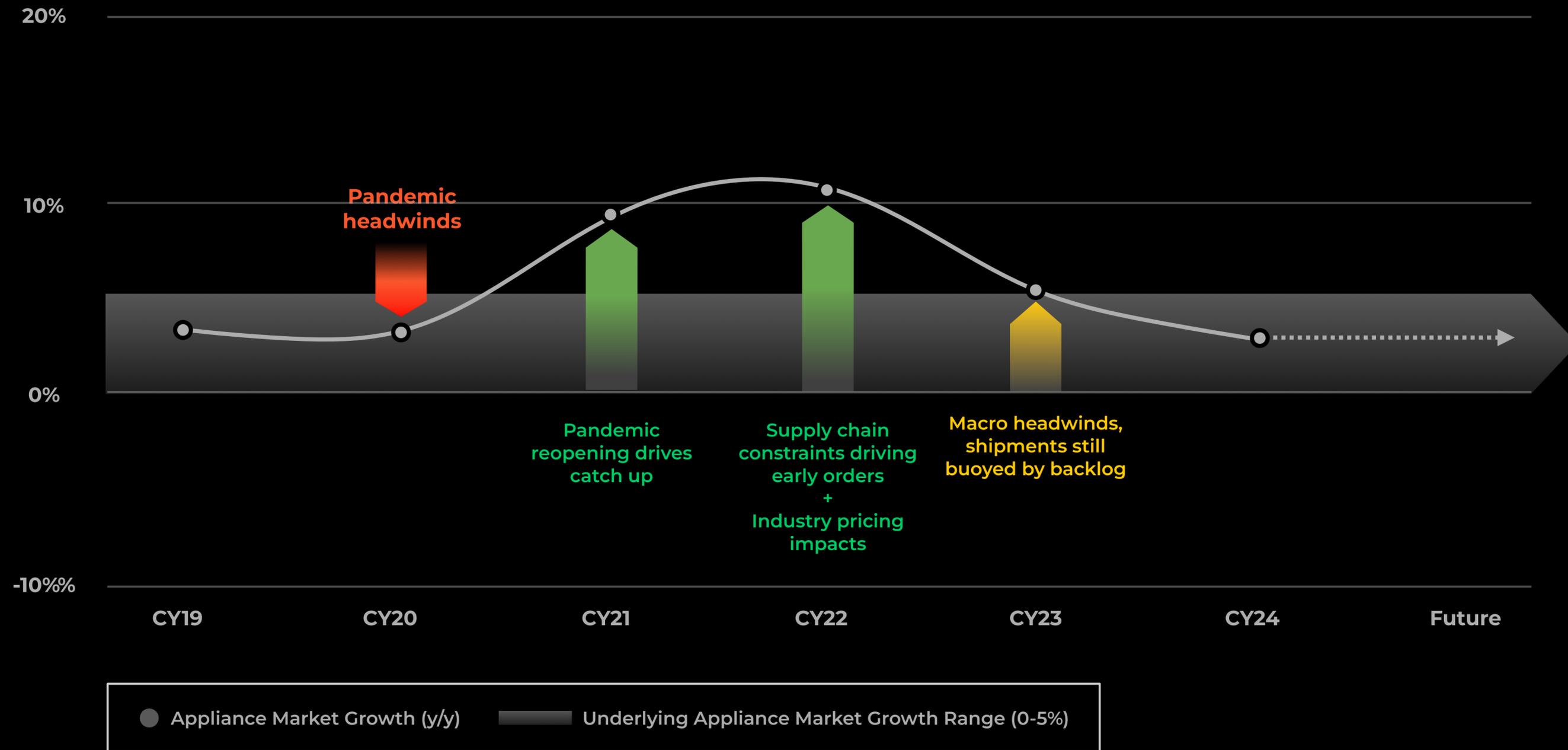| $8.2B	$8.3B	$8.8B	$9.2B	$10.6B
Q4'22	Q1'23	Q2'23	Q3'23	Q4'23

Remaining Performance Obligation

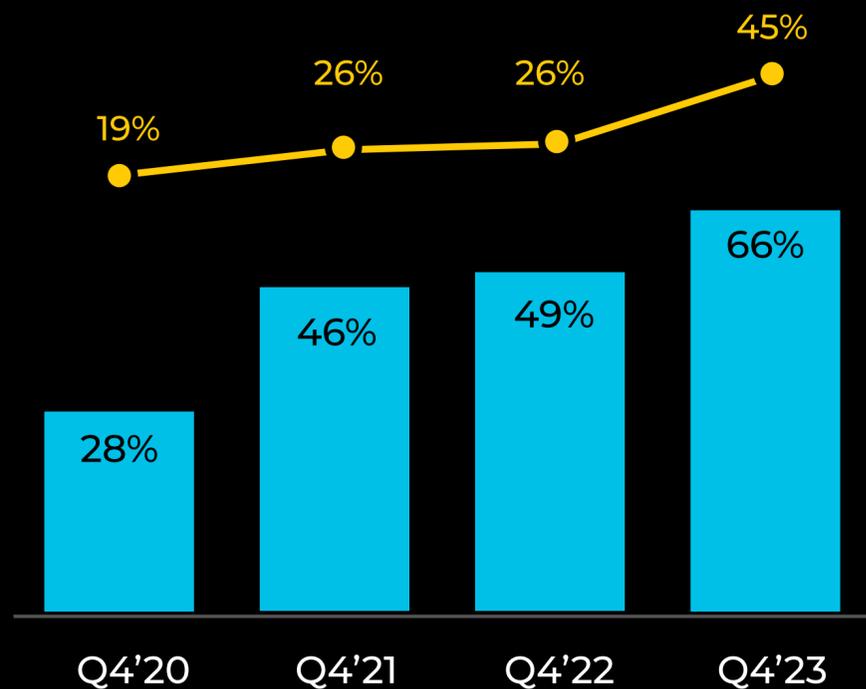**Remaining Performance Obligation (y/y)**
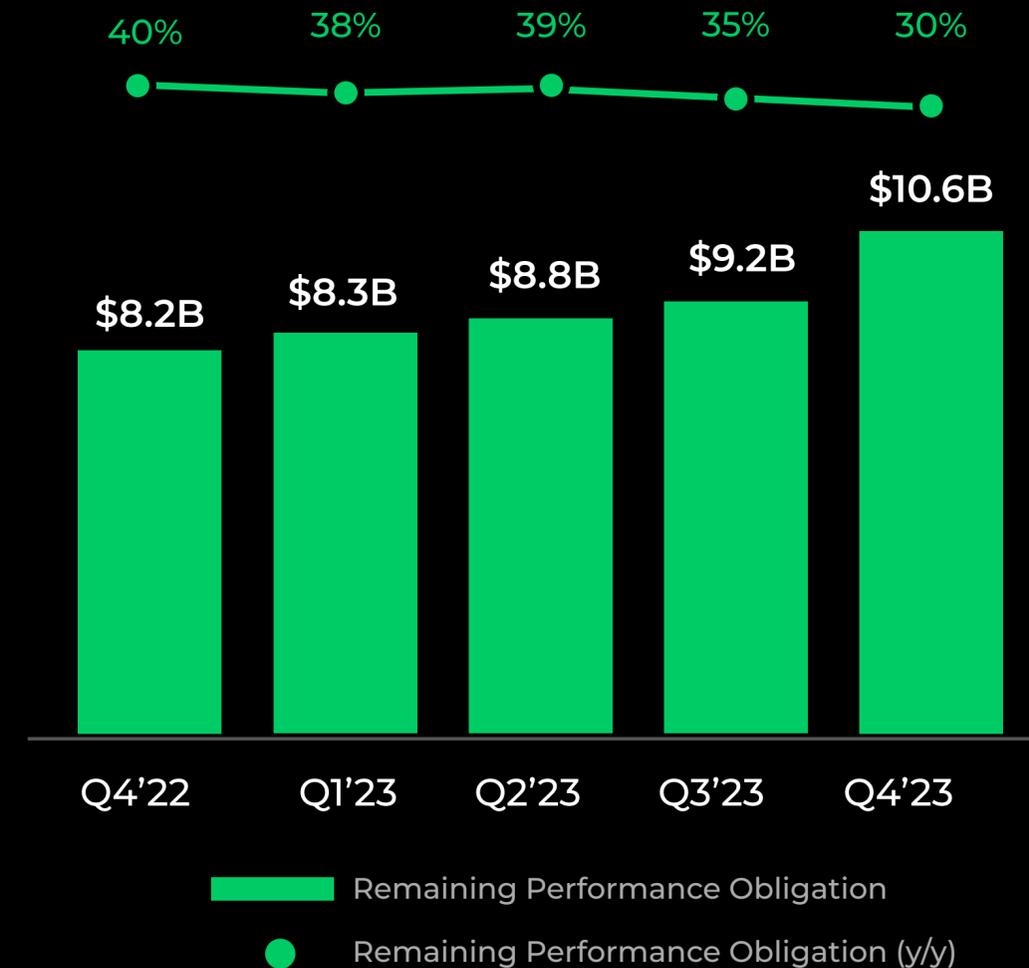
[1] Deferred payment plans include any deals under Billings Plans & Palo Alto Networks Financial Service
Fiscal year ending on July 31.

15

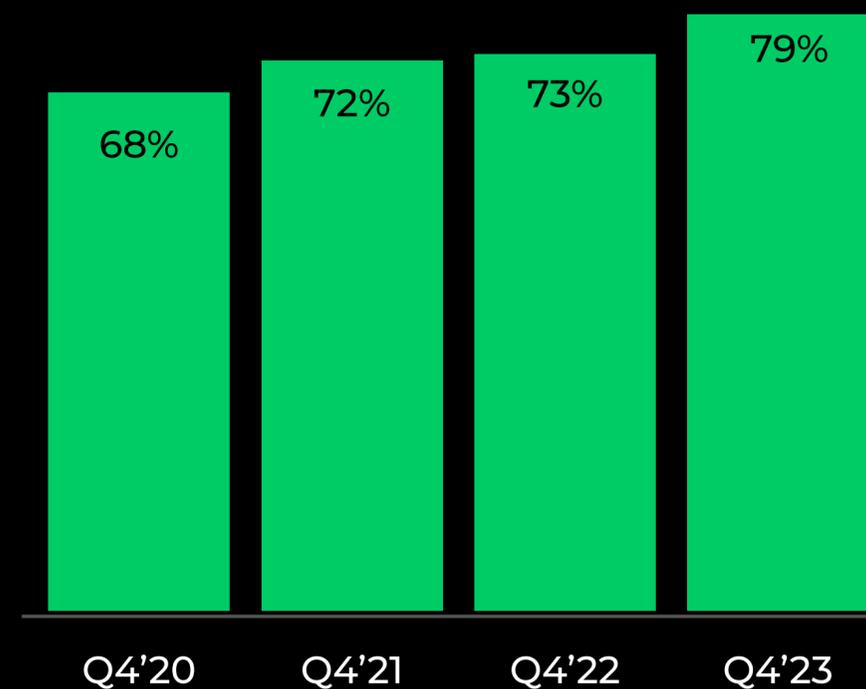# Industry hardware growth trend is returning to expected baseline level

Appliance Market Growth (y/y)

Underlying Appliance Market Growth Range (0-5%)

Pandemic headwinds

Pandemic reopening drives catch up

Supply chain constraints driving early orders + Industry pricing impacts

Macro headwinds, shipments still buoyed by backlog

CY19 CY20 CY21 CY22 CY23 CY24 Future

20% 10% 0% -10%%

Software transition and NGS growth is driving more recurring revenue

FWaaP Billings Growth & SW as a % of FWaaP

	Q4'20	Q4'21	Q4'22	Q4'23
SW % of FWaaP Billings	28%	46%	49%	66%
FWaaP Billings Growth y/y	19%	26%	26%	45%

Legend:
- SW % of FWaaP Billings
- FWaaP Billings Growth y/y

Recurring Revenue as a % of Total Revenue

	Q4'20	Q4'21	Q4'22	Q4'23
Recurring Revenue[3] % of Total Revenue	68%	72%	73%	79%

Legend:
- Recurring Revenue[3] % of Total Revenue

[1] Firewall as a Platform (FWaaP) billings is a key financial and operating metric defined as publicly reported product billings, together with the services billings for Prisma Access, VM-Series, and SD-WAN offerings, during the period stated.
[2] SW % of Total FWaaP billings is the billings for the Prisma Access and VM-series offerings, and the non-hardware portion of SD-WAN offerings, as a percentage of total Firewall as a Platform billings, during the period stated.
[3] Recurring Revenue represents Total Revenue less hardware and professional services revenue.
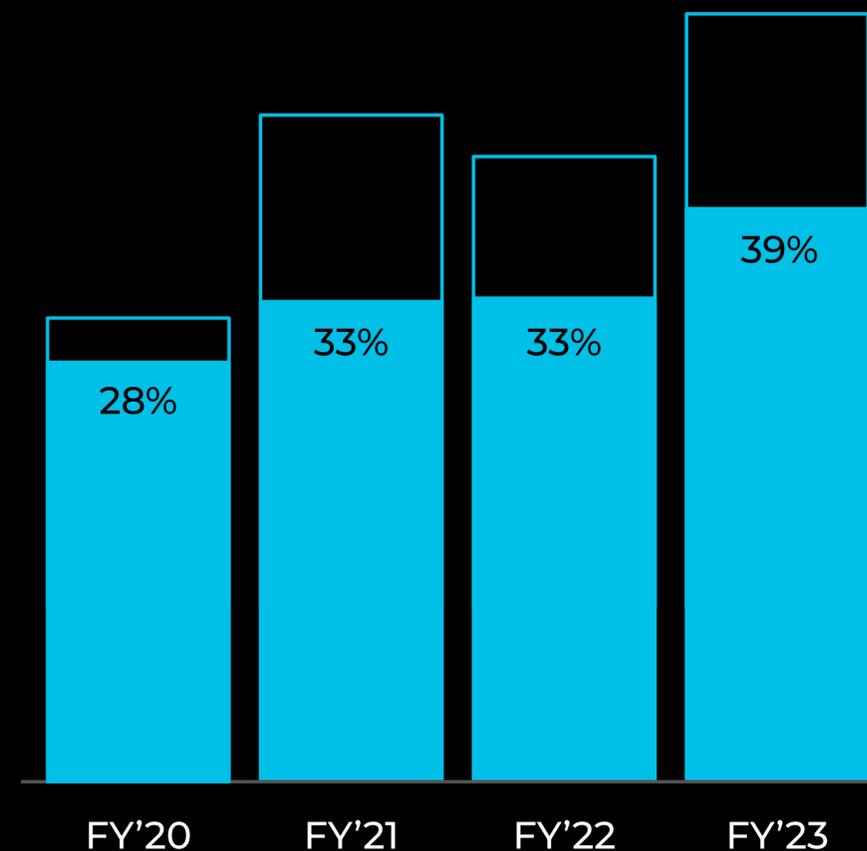Fiscal year ending on July 31.

Profitability supporting a higher free cash flow baseline

Operating Income Growth & Margin (Non-GAAP)

-6%
34%
30%
59%

18%
19%
19%
24%

FY'20   FY'21   FY'22   FY'23

■ Operating Margin (Non-GAAP)
● Operating Income Growth y/y (Non-GAAP)
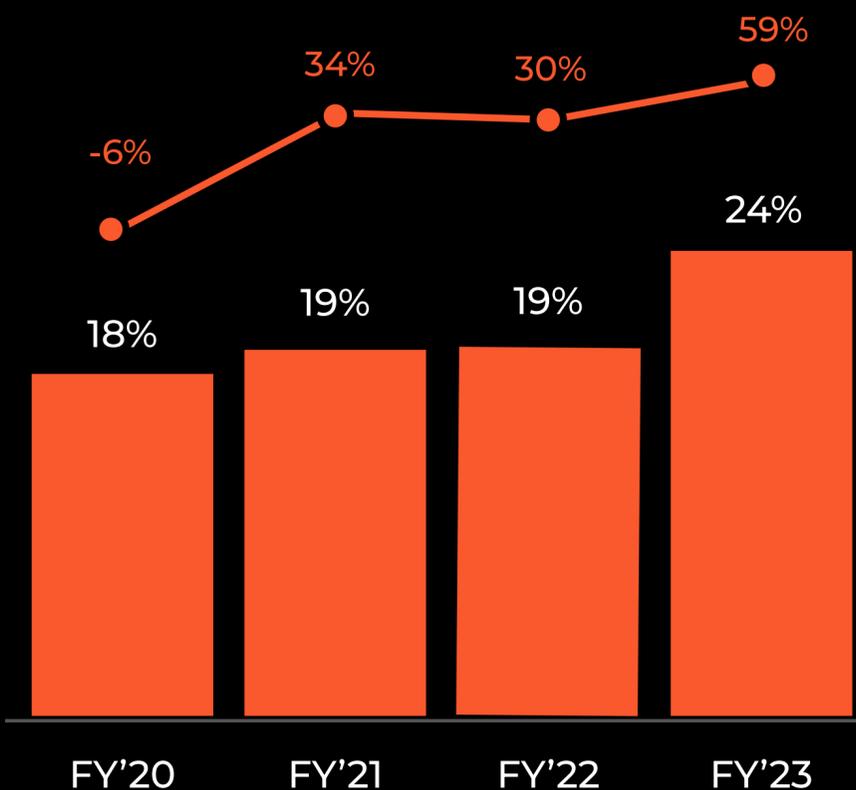
Fiscal Year Adjusted Non-GAAP Free Cash Flow Margin

28%
33%
33%
39%

FY'20   FY'21   FY'22   FY'23

■ Adjusted Non-GAAP Free Cash Flow Margin
▢ Impact to adjusted non-GAAP Free Cash Flow Margin when removing the impact of Deferred Payment Plans

% of Bookings on Deferred Payment Plans[1]

FY'20   FY'21   FY'22   FY'23

■ % of Bookings under deferred payment plans

[1] Deferred payment plans include any deals Billings Plans & Palo Alto Networks Financial Services. Fiscal year ending on July 31.

Q4 Results Summary

	Q4'23 Guidance (as of 5/23/23)	Q4'23 Actual	
Total Billings	$3.15B-$3.20B 17%-19% yr/yr	$3.16B 18% yr/yr	✓
Total Revenue	$1.937B-$1.967B 25%-27% yr/yr	$1.95B 26% yr/yr	✓
Product Revenue		$507M 24% yr/yr	
Remaining Performance Obligation		$10.6B 30% yr/yr	
Next-Gen Security ARR		$2.95B 56% yr/yr	
Gross Margin (Non-GAAP)		77.3% +410 bps yr/yr	
Operating Income (Non-GAAP)		$554M 71% yr/yr	
Operating Margin (Non-GAAP)		28.4% +760 bps yr/yr	
EPS (Non-GAAP)	$1.26-$1.30	$1.44	✓
EPS (GAAP)		$0.64	
Adj. Free Cash Flow (Non-GAAP)		$388M	

Fiscal Year 2024 Guidance

	FY 2023 Actuals	FY 2024 Guidance as of 8/18/23
Total Billings	$9.19B +23% yr/yr	$10.9B - $11.0B +19%-20% yr/yr
Next-Gen Security ARR	$2.95B +56% yr/yr	$3.95B - $4.00B +34%-36% yr/yr
Total Revenue	$6.89B +25% yr/yr	$8.15B - $8.20B +18%-19% yr/yr
Op Margin (Non-GAAP)	24.1%	25.0-25.5%
EPS (Non-GAAP)	$4.44 +76% yr/yr	$5.27 - $5.40 +19%-22% yr/yr
Adj. FCF Margin (Non-GAAP)	38.8%	37-38%

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.

Q1 Fiscal 2024 Guidance

	Q1'24 Guidance as of 8/18/23
Total Billings	**$2.05B - $2.08B** 17%-19% yr/yr
Total Revenue	**$1.82B - $1.85B** 16%-18% yr/yr
EPS (Non-GAAP)	**$1.15 - $1.17** 39%-41% yr/yr

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.

Modeling Points

Q1'24 and FY24 non-GAAP effective tax rate: 22%

Cash taxes for FY24 of $230-280M

Q1'24 net interest and other income of $50M – $55M

Q1'24 diluted shares outstanding 336 – 339 million

FY24 diluted shares outstanding 338 – 343 million

Q1'24 capital expenditures of $40M – $45M

FY24 capital expenditures of $160M – $170M

Q&A

Nikesh Arora

CEO & Chairman

Over the last 5 years, the cybersecurity market has evolved significantly

Enterprise Cybersecurity Market

TAM '23
('18-'23 CAGR)

$29B
(35%)

New segments
SASE, Cloud Security, IoT Security

$72B
(19%)

Segments undergoing transformation
Endpoint / XDR, SecOps (+SIEM), Network Security

$31B
(13%)

Largely steady segments
Identity, App Security, Data Security, Email Security

$81B
(7%)

Services

$213B

Looking back, we envisioned three transformations

The network would need to be reimagined

$19B
*Network Security
2018 TAM*

Public Cloud adoption would scale rapidly

$2B
*Cloud Security
2018 TAM*

AI & ML would be THE way we 'solve' security

$17B
*Security Ops
2018 TAM*

These transformations ended up driving rapid growth in cybersecurity

Adv. Threat

VPN

SWG   DLP   IoT / OT

ZTNA   AIOps

SD-WAN

SASE

CASB

ADEM

$19B
Network Security
2018 TAM

SCA   CNS

CWP

SAST   IaC

CDS

CIEM   Secrets Scanning

CI/CD

WAAS

Web App FW

$2B
Cloud Security
2018 TAM

SIEM

XDR   MTH

Threat Intel.   ASM

Network Intel.   SOAR

Vuln. Mgmt.

$17B
Security Ops
2018 TAM

These transformations ended up driving rapid growth in cybersecurity

$45B
Network Security
2023 TAM

$11B
Cloud Security
2023 TAM

$48B
Security Ops
2023 TAM

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]

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

Code to Cloud Platform

~$40B

by 2028

Autonomous Security Ops Platform

~$90B

by 2028

Security for network traffic managed comprehensively via a single pane of glass

Scalable and comprehensive security across the cloud app development lifecycle

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
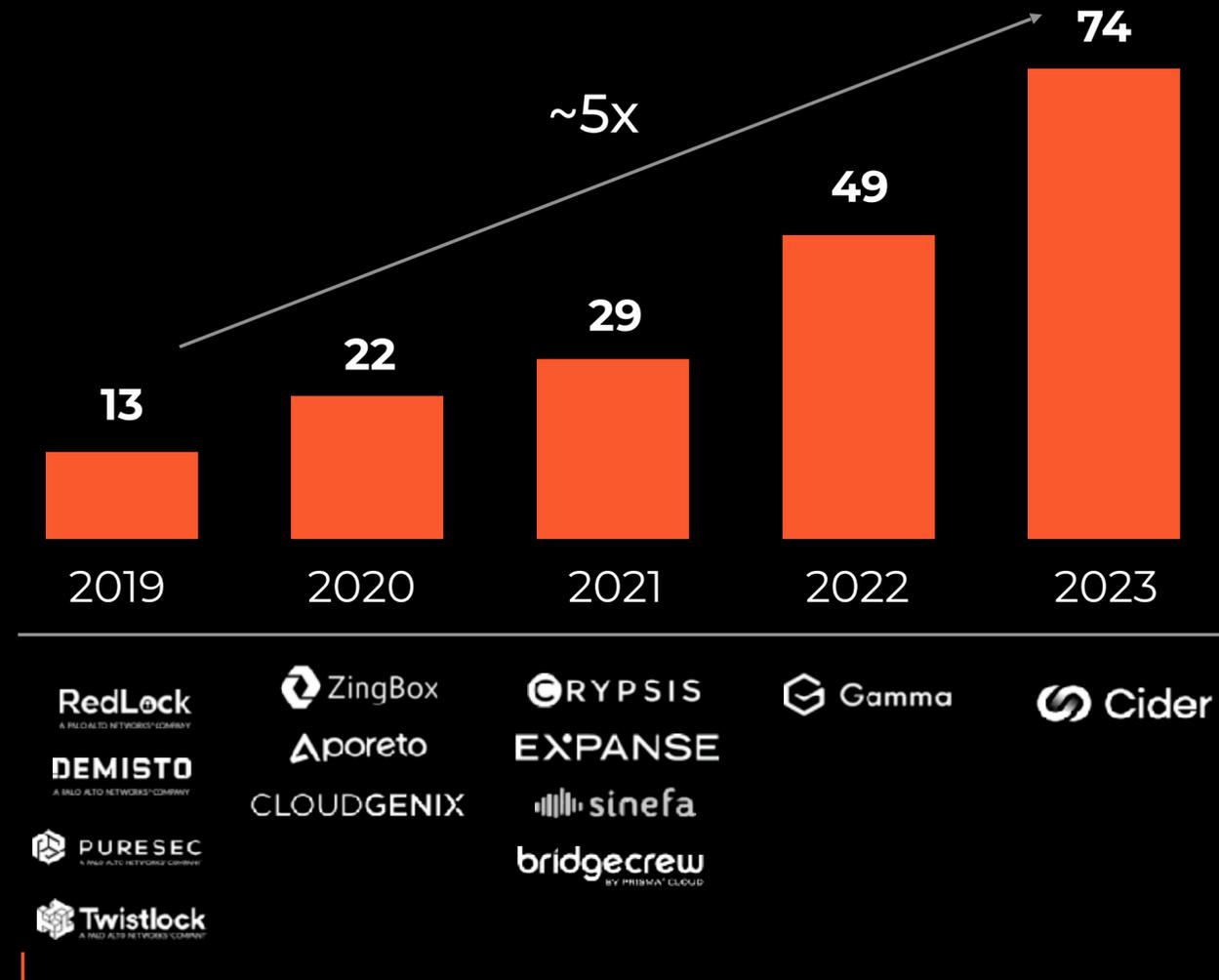Build the most capable and motivated team

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

~5x

Year	Releases
2019	13
2020	22
2021	29
2022	49
2023	74

RedLock
A PALO ALTO NETWORKS COMPANY

ZingBox

CRYPSIS

Gamma

Cider

DEMISTO
A PALO ALTO NETWORKS COMPANY

Aporeto

EXPANSE

CLOUDGENIX

sinefa

PURESEC
A PALO ALTO NETWORKS COMPANY

bridgecrew
BY PRISMA CLOUD

Twistlock
A PALO ALTO NETWORKS COMPANY

Enhanced by Acquisitions

...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

34

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

CODE TO CLOUD PLATFORM

ZERO TRUST PLATFORM

AUTONOMOUS SECOPS PLATFORM
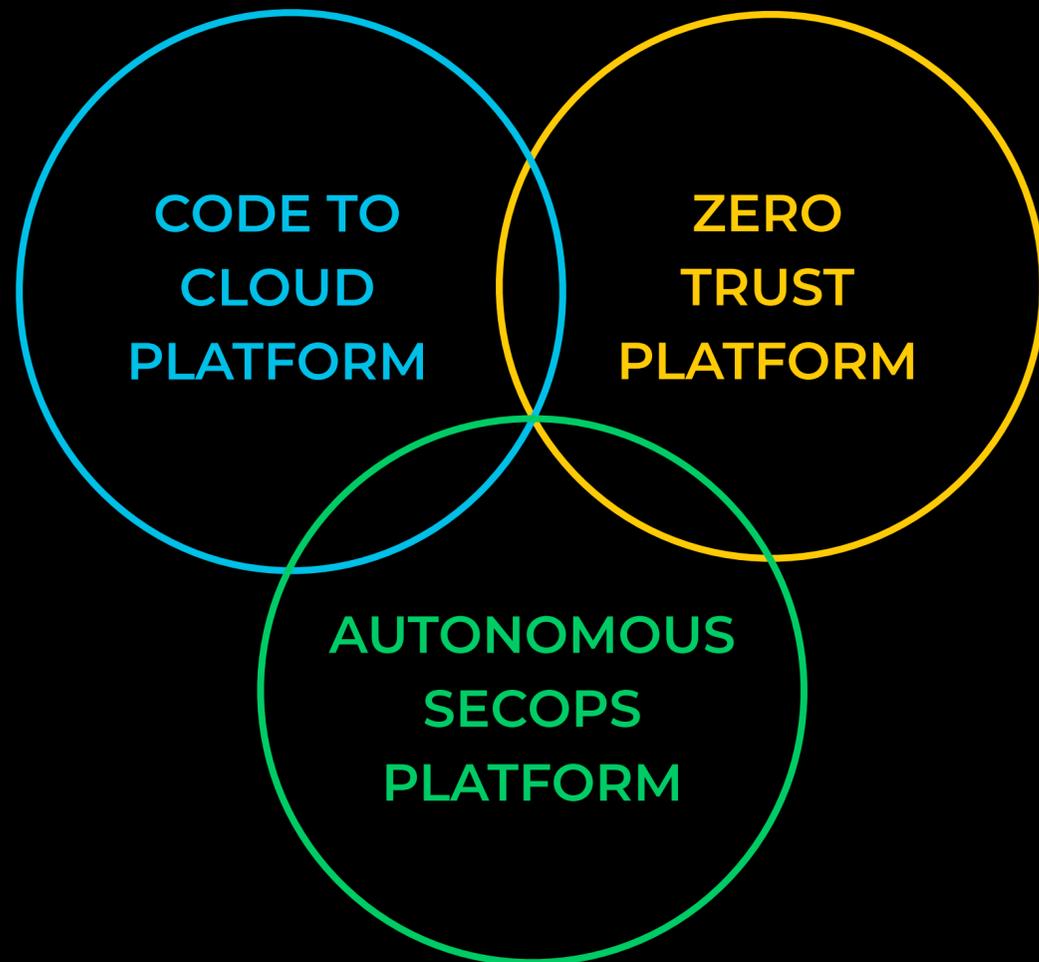
ZERO TRUST PLATFORM
Radically more integration across form-factors…

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 [1]

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

TO

Transactional vendor 〉 **Strategic partner** helping customers on their transformation journey

Selling products 〉 **Architecting outcomes** jointly with ecosystem solution providers

Reactive help 〉 **"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**

Built on our Brand and Reputation

…and empower them

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

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

paloalto
NETWORKS®

The threat landscape is intensifying

Elevated attacker motivation

$8T cost of cybercrime [1]

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 [2]

>10 million people and >1,700 organizations affected by
supply chain attacks in 2022 [3]

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 [4]
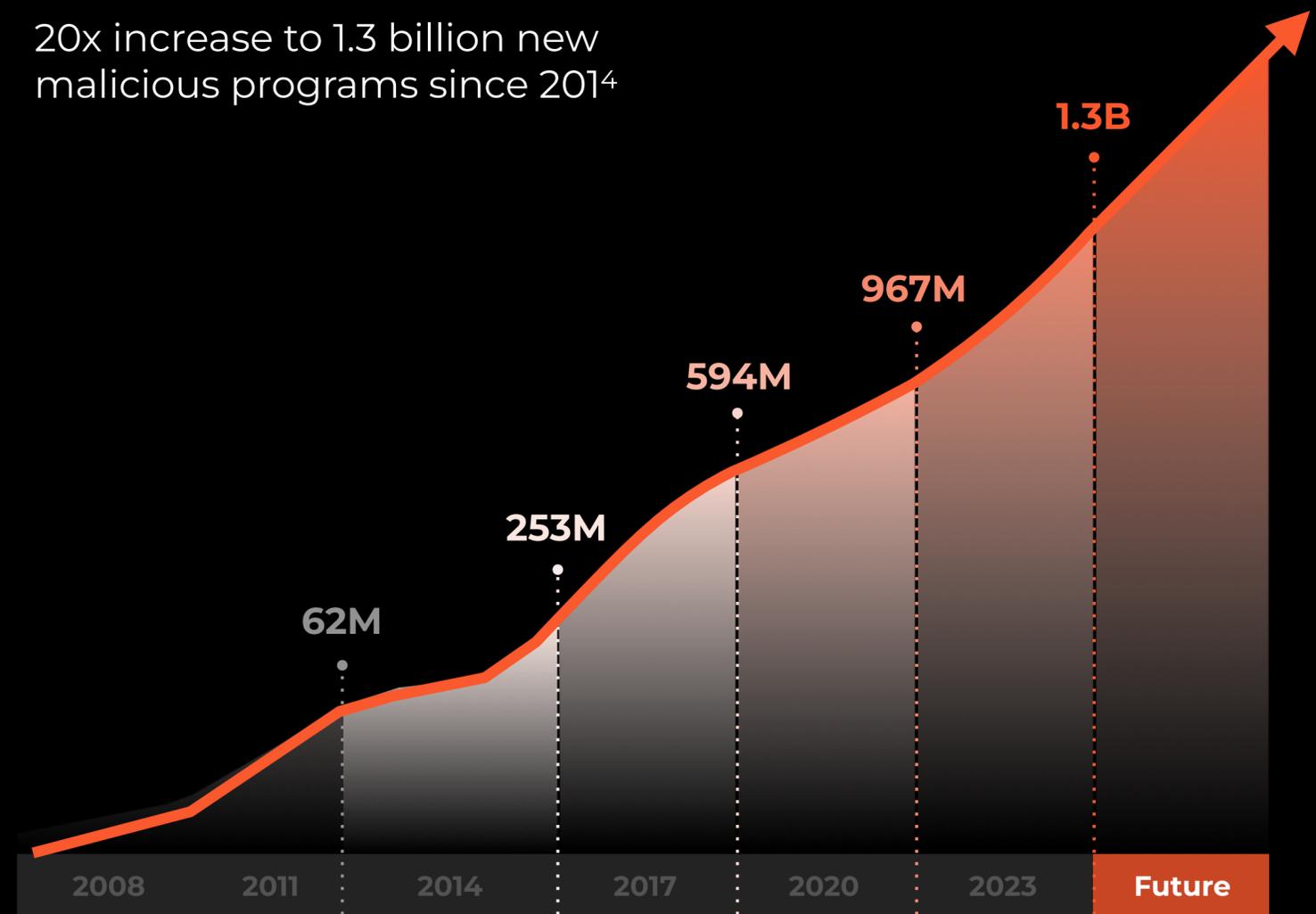
1.3B

967M

594M

253M

62M

| 2008 | 2011 | 2014 | 2017 | 2020 | 2023 | Future |

Attacks are happening faster than organizations can respond

Average Days from "Compromise" to "Exfil" [1]

44 days
2021

30 days
2022

5 days
2023

Hours
Latest attacks

Industry average
6 DAYS
to remediate

SEC adopted rule
4 DAYS
to disclose material cybersecurity incident[2]

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

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[1] cybercrime "market" in 2025

Threat trends demand a high-powered innovation engine

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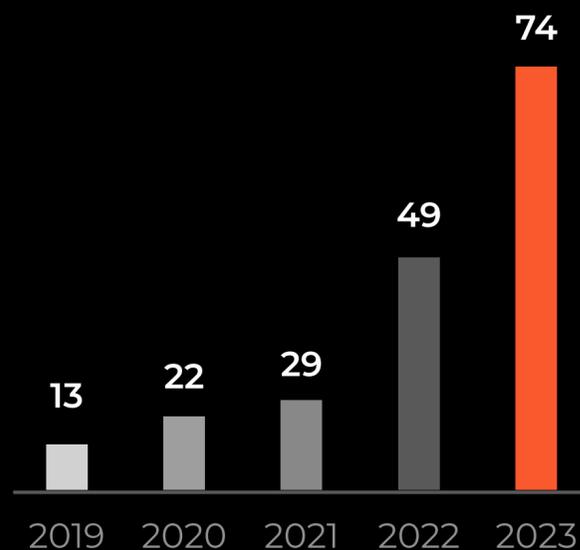
From single-product to 3 leading platforms in 5 years

74

49

29

22

13

2019 2020 2021 2022 2023

Major releases per fiscal year
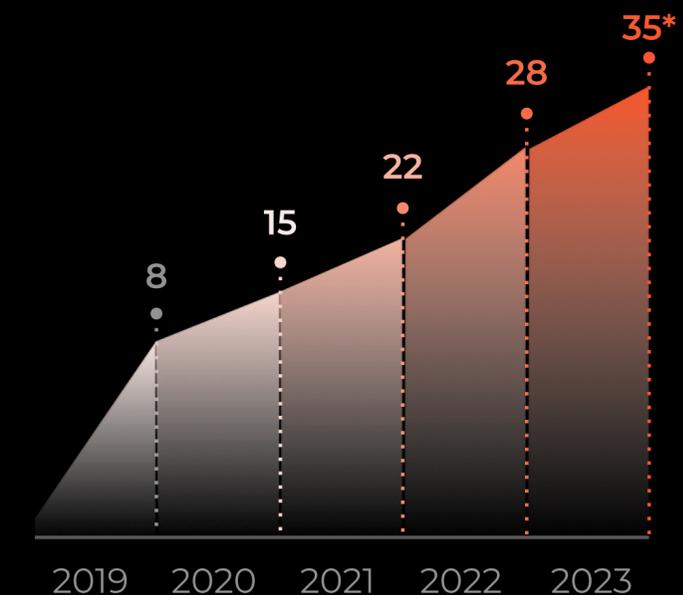
While leveraging the broader market

Continuously identifying great tech to include in our journey

~250

Private cybersecurity companies evaluated annually

Embracing AI from the early days

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

35*

28

22

15

8

2019 2020 2021 2022 2023
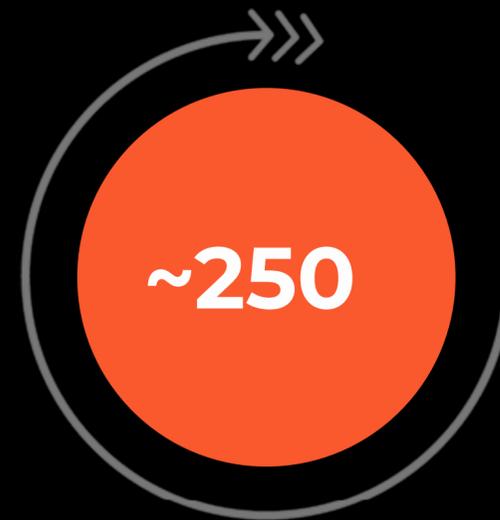
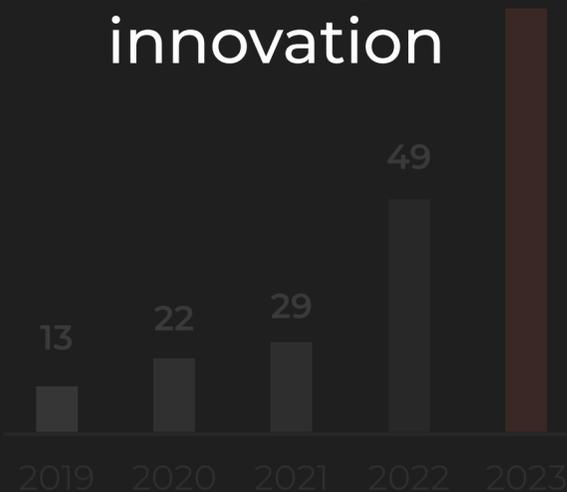Cumulative number of Palo Alto Networks products that use AI

*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

49
29
22
13

2019 2020 2021 2022 2023

Major releases per fiscal year

While leveraging the broader market

Continuously identifying great tech to include in our journey
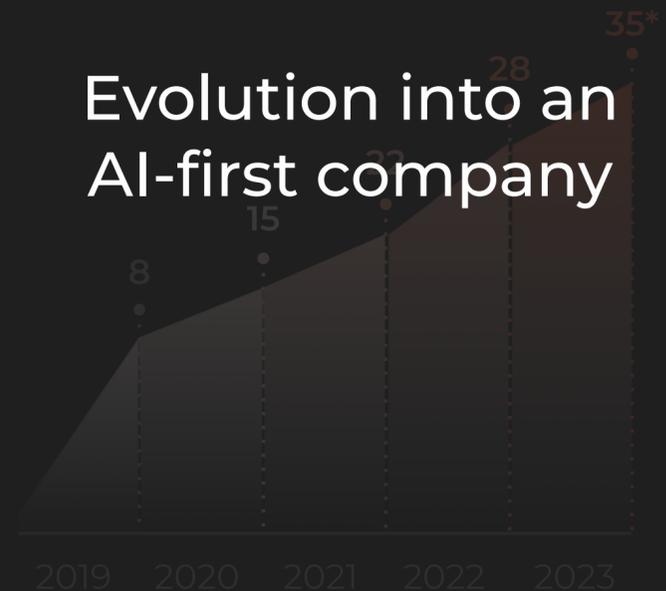
Proven playbook sets us up well

~250

Private cybersecurity companies evaluated annually

Embracing AI from the early days

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

Evolution into an AI-first company

35*
28
15
8

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

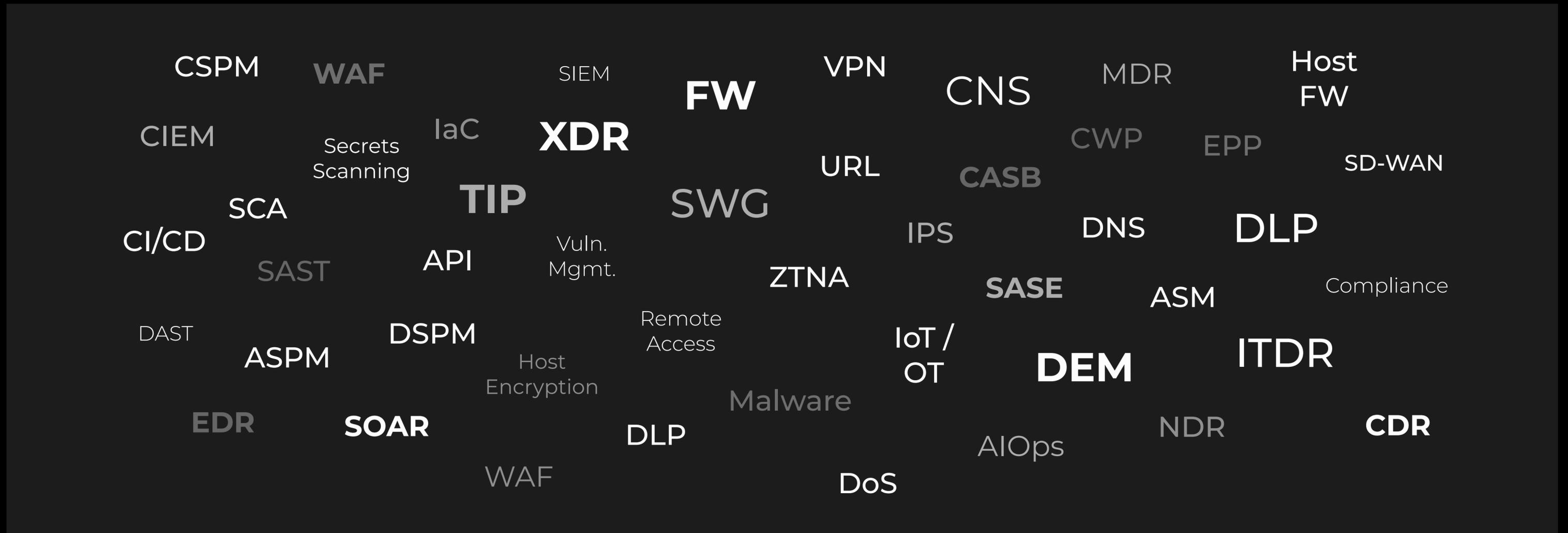## Deep expertise

~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

# The industry approach leads to point product proliferation

CSPM WAF SIEM FW VPN CNS MDR Host FW

CIEM IaC XDR CWP EPP SD-WAN

Secrets Scanning URL CASB

SCA TIP SWG IPS DNS DLP

CI/CD SAST API Vuln. Mgmt. ZTNA SASE ASM Compliance

DAST DSPM Remote Access IoT / OT DEM ITDR

ASPM Host Encryption

EDR SOAR DLP Malware AIOps NDR CDR

WAF DoS
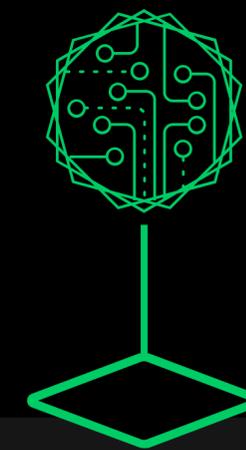
Only a platform approach will work

Zero Trust Platform

Network security that ensures every connection is secure
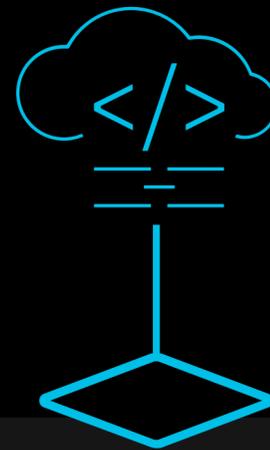
Code to Cloud Platform

Cloud security that ensures every cloud application is secure

AI-Driven Security Operations Platform

SecOps that is powered by a real-time security engine

Not all platforms are created equal

1
Innovation-Led

2
Comprehensive

3
Integrated

4
Real-Time

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

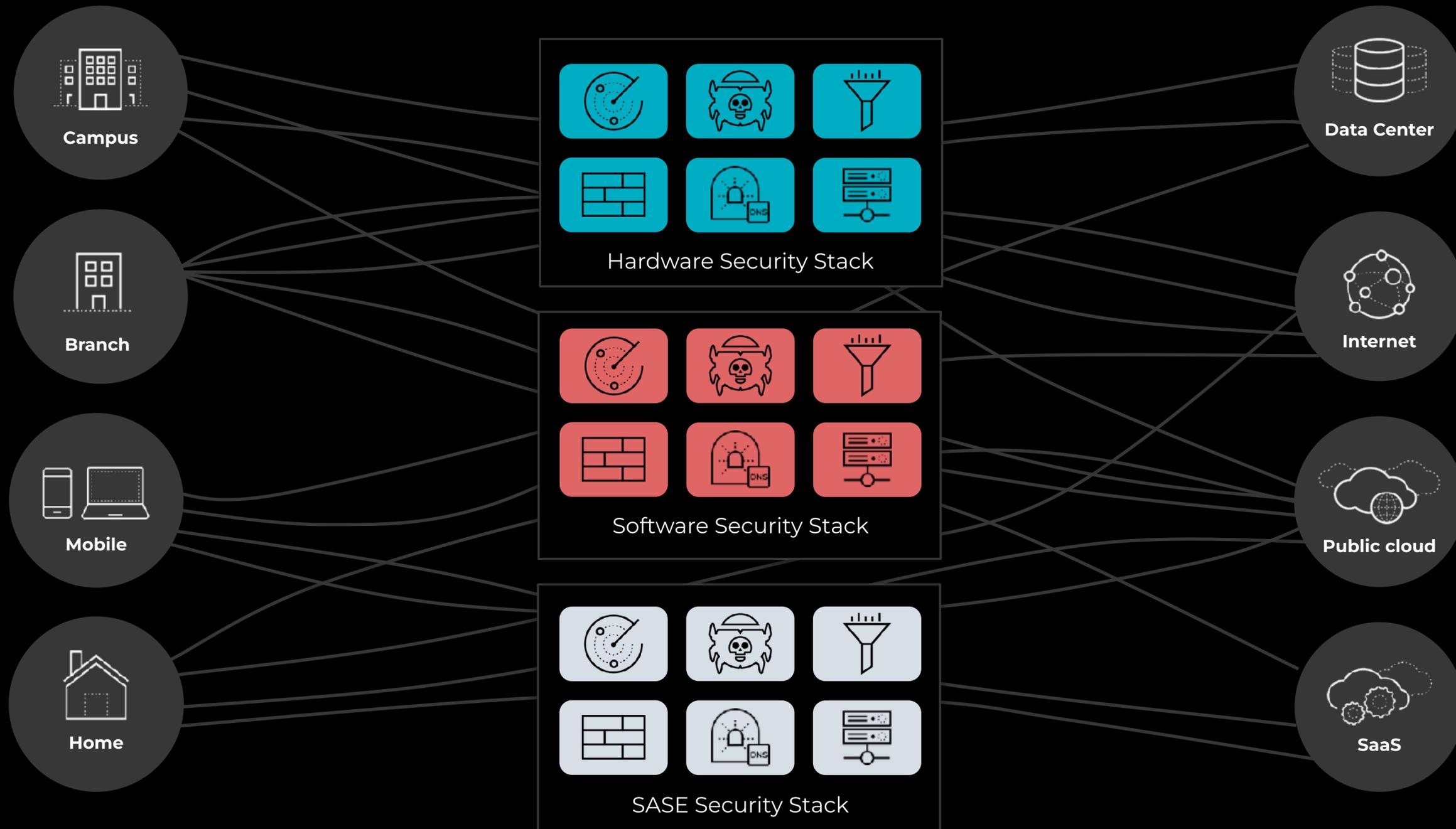**New trends will propel platformization and AI**

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[1]

Network security has become increasingly complex

Campus

Branch

Mobile

Home

Hardware Security Stack

Software Security Stack

SASE Security Stack

Data Center

Internet

Public cloud

SaaS

What if we could take a radically new approach?

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

Campus

Branch

Mobile

Home

Unified
Security Stack

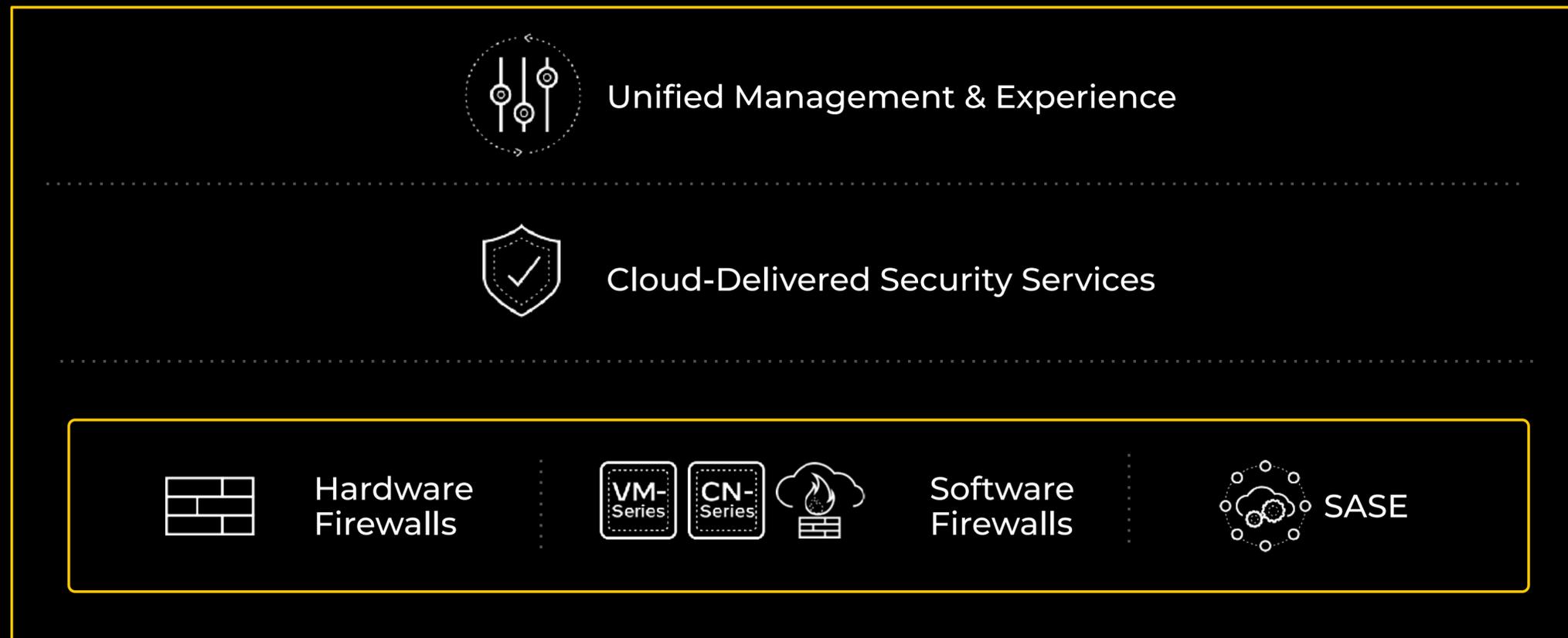Data Center

Internet

Public cloud

SaaS

Enterprise-wide Zero Trust Platform

Over the last 5 years, we have developed a Zero Trust Platform with best-in-class products

Zero Trust Network Security Platform

Unified Management & Experience

ADV TP · ADV URL · ADV WF · DNS · IoT · DLP · NG CASB · GP · AIOps · ADEM

Cloud-Delivered Security Services

Hardware Firewalls · VM-Series · CN-Series · Software Firewalls · SASE
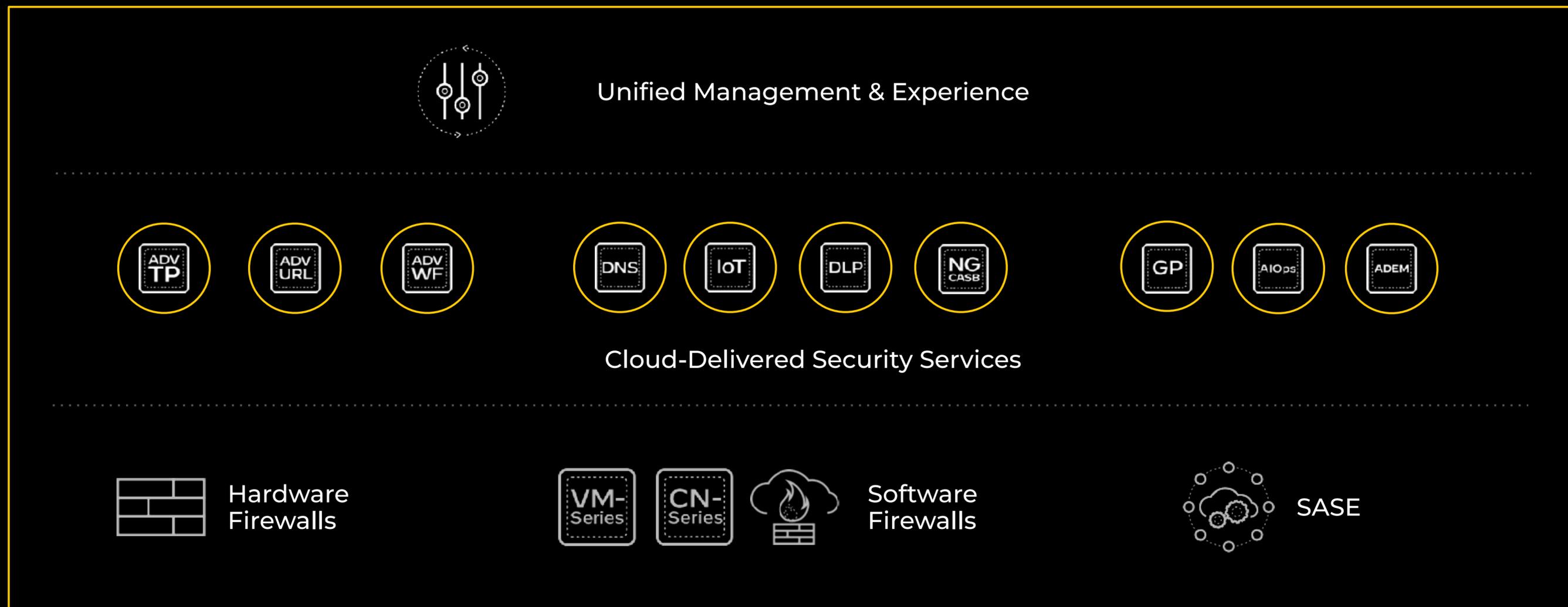
Best-in-class form factors — Hardware, Software and SASE

Unified Management & Experience

Cloud-Delivered Security Services

| Hardware Firewalls | VM-Series CN-Series | Software Firewalls | SASE |

NGFW

A **Leader** in Gartner Magic Quadrant Network Firewalls [1]

Gartner.

Zero Trust

A **Leader** in Forrester Zero Trust eXtended Ecosystem Platform Providers Wave [2]

FORRESTER

SSE

A **Leader** in Gartner Magic Quadrant Security Service Edge [3]

Gartner.

SD-WAN

A **Leader** in Gartner Magic Quadrant WAN Edge Infrastructure [4]
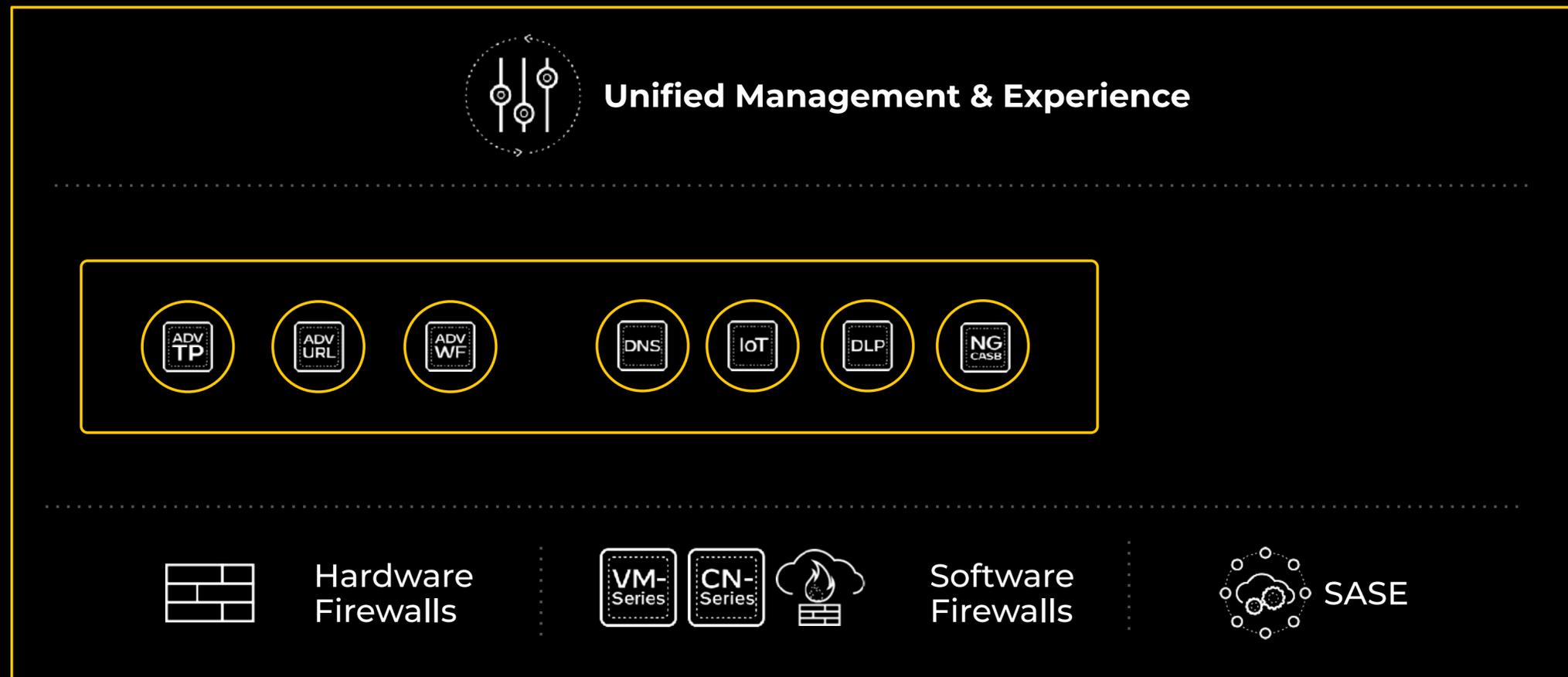
Gartner.

Sources:
[1] Gartner® Magic Quadrant for Network Firewalls, 19 December 2022
[2] The Forrester Wave™: Zero Trust eXtended 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.

57

Best-in-class security services —
Infused with AI for near real-time protection

Unified Management & Experience

ADV TP · ADV URL · ADV WF · DNS · IoT · DLP · NG CASB

Hardware Firewalls · VM-Series · CN-Series · Software Firewalls · SASE

Core Security			**IOT**	**Data 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	**90%** of devices discovered in 48 hours, protect seen and unseen devices	**80%** higher data classification with ML-based detection

Best-in-class security services — Extended to AI-powered operations

Unified Management & Experience

ADV TP · ADV URL · ADV WF · DNS · IoT · DLP · NG CASB · GP · AIOps · ADEM

Hardware Firewalls

VM-Series · CN-Series · Software Firewalls

SASE
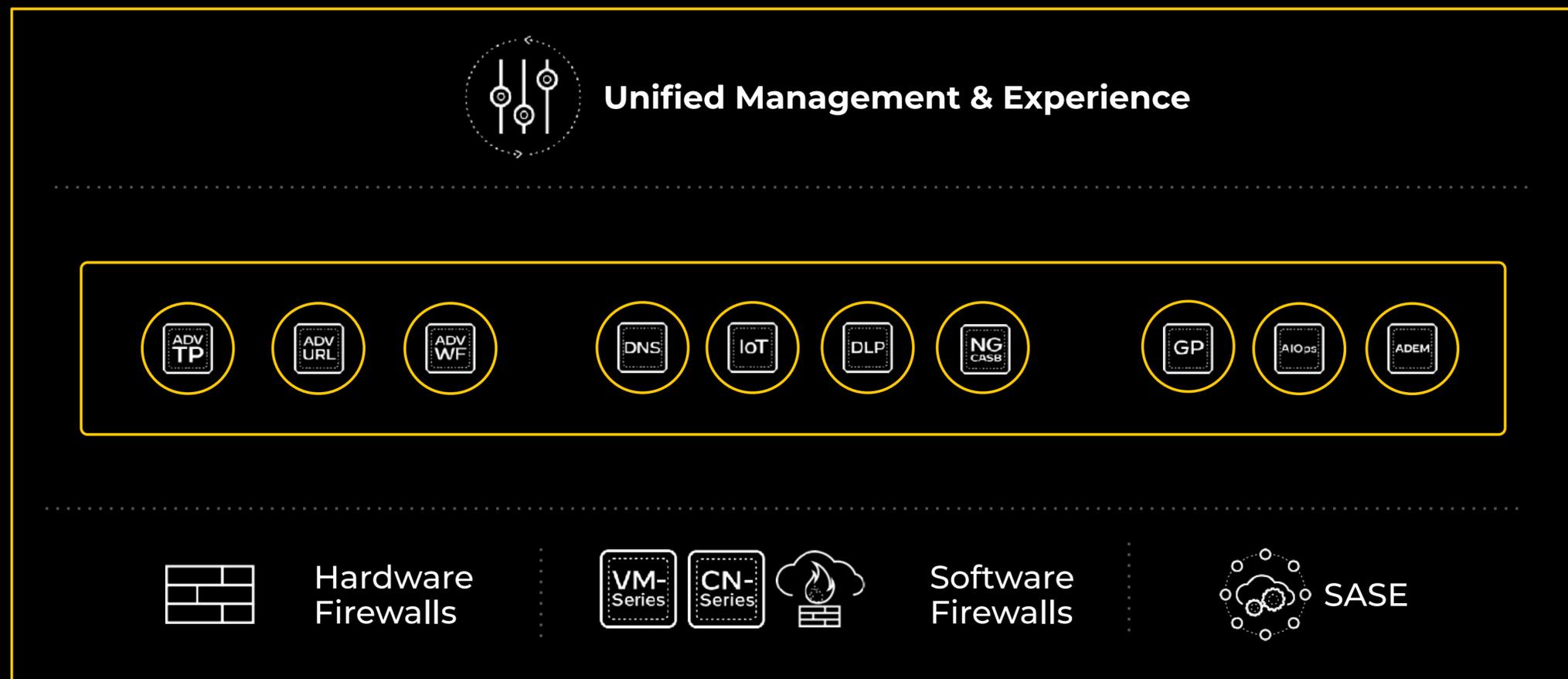
GlobalProtect	**AIOps**	**ADEM**
86M users leverage GlobalProtect for securing remote access	Predict **51%** of network disruptions before any customer impact	Quickly identify the problem segment and reduce IT escalations by **46%**

The next transformation in network security — Unified management and experience
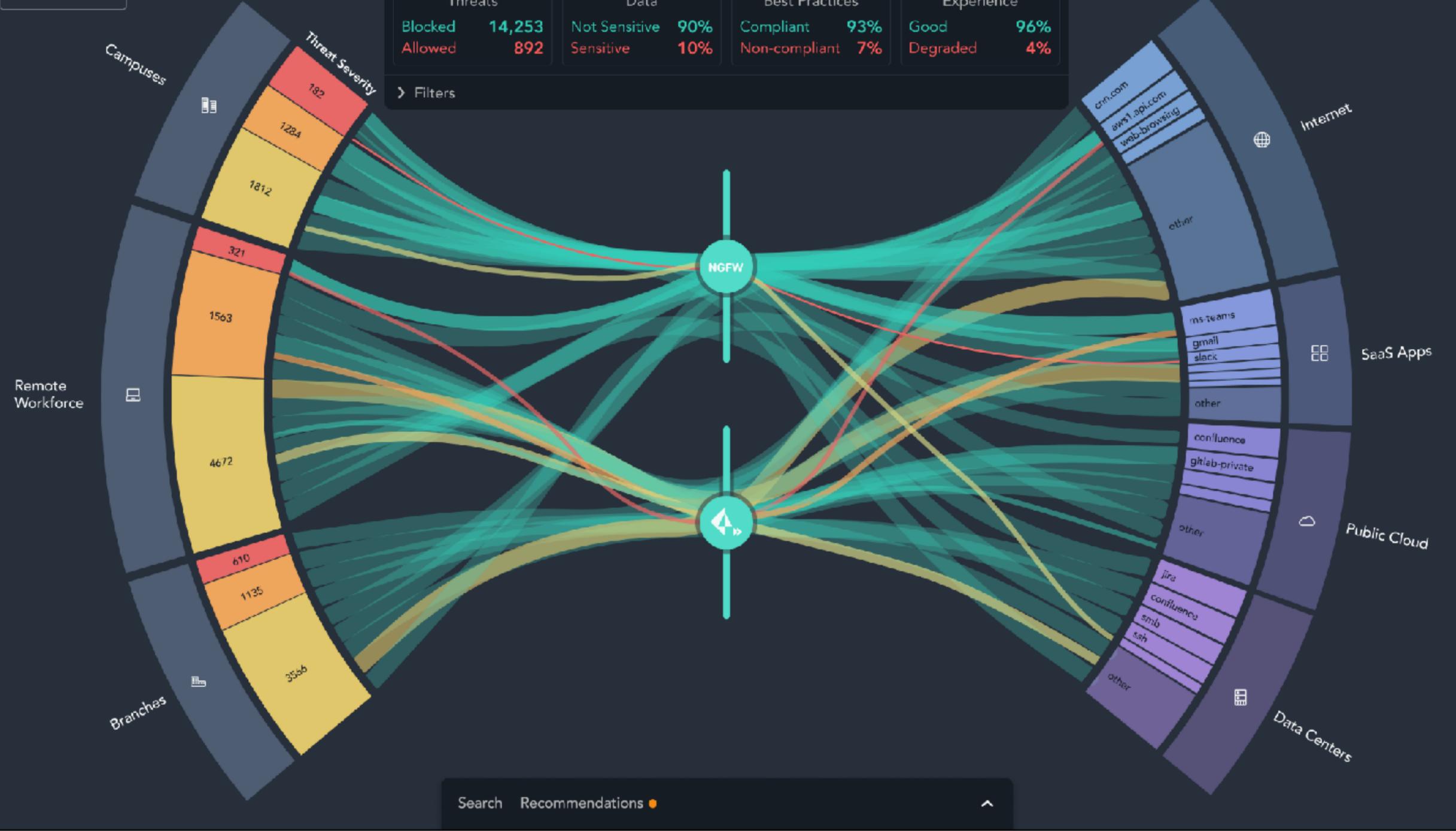
Zero Trust Network Security Platform

Unified Management & Experience

ADV TP · ADV URL · ADV WF · DNS · IoT · DLP · NG CASB · GP · AIOps · ADEM

Cloud-Delivered Security Services

Hardware Firewalls

VM-Series · CN-Series · Software Firewalls

SASE

61

Guided remediation to secure against threats with "one click"

65

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

7% ↓

327
Malicious Files Blocked

1100
Malicious URLs Blocked
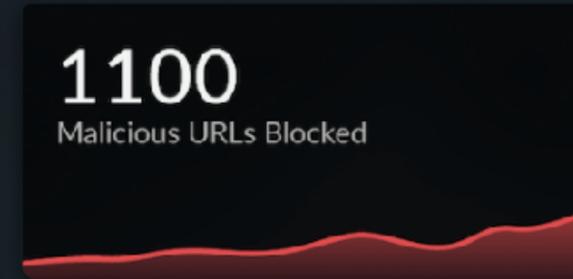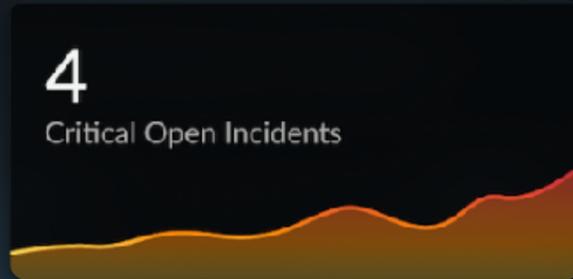
Search "health and usage of my network"
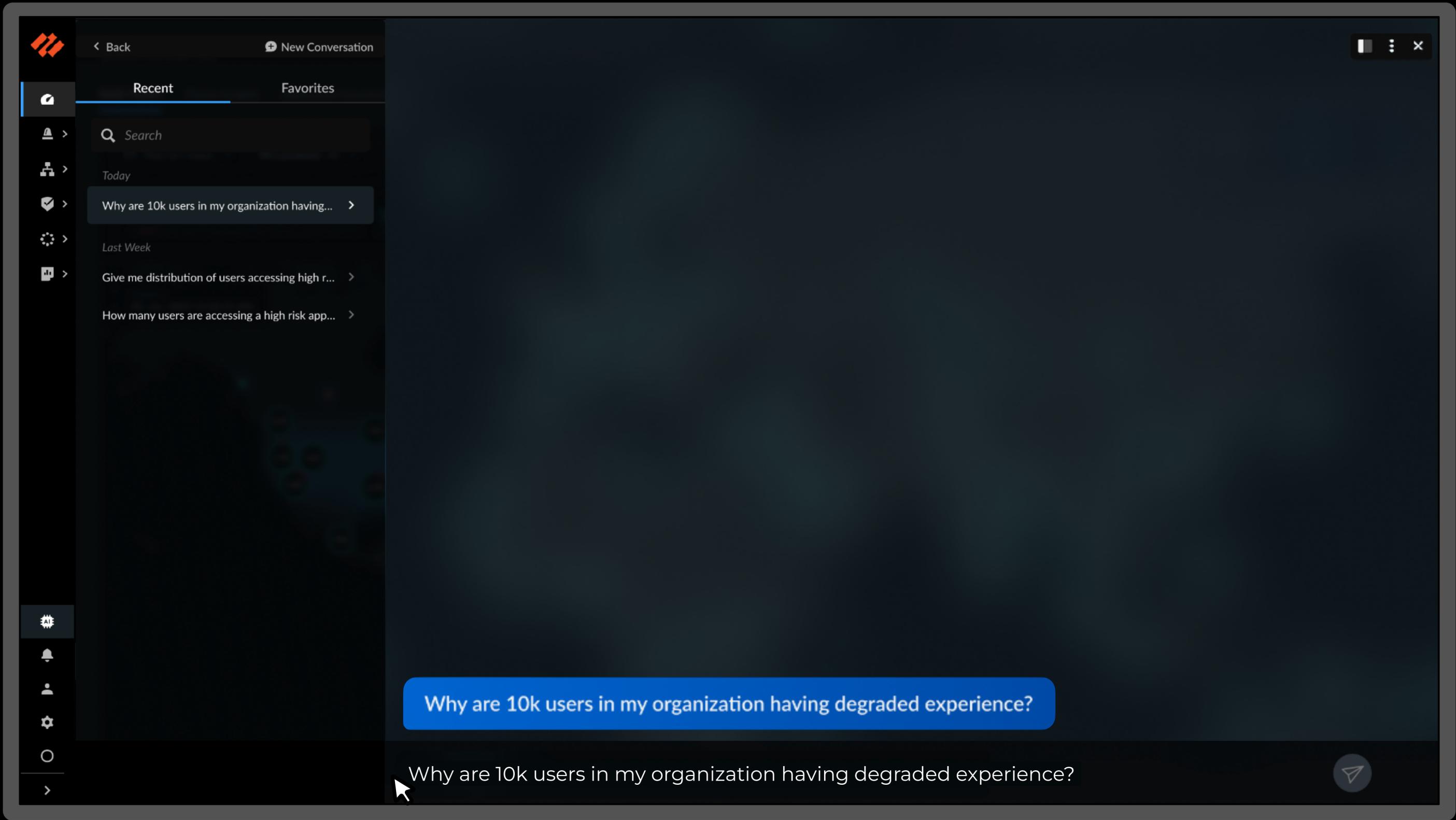
Back   ⊕ New Conversation

Recent   Favorites

🔍 Search

Today

Why are 10k users in my organization having...   ›

Last Week

Give me distribution of users accessing high r...   ›

How many users are accessing a high risk app...   ›

Why are 10k users in my organization having degraded experience?

Why are 10k users in my organization having degraded experience?

Why are 10k users in my organization having degraded experience?

Current Status

Degraded
10k | 6.7%

Good
149k | 99.3%

150k
Users

Historical Trend (Last 24 hours)

- Connected Users
- Good Experience
- Degraded Experience

User Count: 200k, 150k, 100k, 50k, 0

Time: 9 PM, 12 PM, 3 AM, 6 AM, 9 AM

10k users connecting to PA location US East, US Southeast are having degraded experience while accessing Jira application.
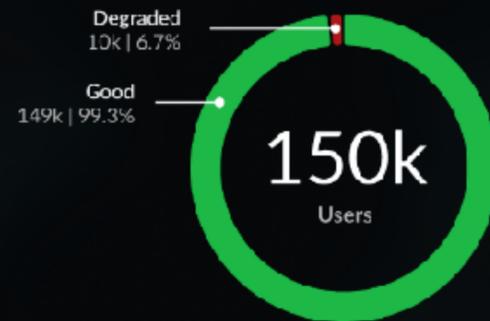
Prisma Access is healthy. Jira application is reachable from the Prisma Access location and the authentication server deployed in your datacenter is reachable. All the 10k users impacted are having auth failures. This is most likely due to "AAA" service, which requires further investigation.

Servicenow ticket is already opened for this issue and NOC analyst has scheduled AAA service restart which should restore Jira application access.

Type your question here

Are users in my organization accessing any risky applications?

Back   ⊕ New Conversation

Recent   Favorites

🔍 Search

Today

Are users in my organization accessing any ris...

Why are 10k users in my organization having...

Last Week

Give me distribution of users accessing high r...

How many users are accessing a high risk app...

Are users in my organization accessing any risky applications?

App Name	Risk Score	Usage	Users
RoadWarrior	9	9.2 GB	900
Netify	9	8.4 GB	852
PDFElement	9	8.3 GB	752
Eventable	9	7.2 GB	632
inFlowInventory	9	6.1 GB	551
AfterCollege	9	5.2 GB	231

5.2 AfterCollege
6.1 GB inFlowInventory
9.2 GB RoadWarrior
7.2 GB Eventable
6 Risky Applications
8.3 GB PDFElement
8.4 GB Netify

There are 3136 users working from campus, remote locations and branch offices accessing 6 risky application in last 7 days with total data transfer of 44.4 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]

Type your question here

Recent   Favorites

🔍 Search

Today

Are users in my organization accessing any ris... ›

Why are 10k users in my organization having... ›

Last Week

Give me distribution of users accessing high r... ›

How many users are accessing a high risk app... ›

5.2 AfterCollege

6.1 GB inFlowInventory

7.2 GB Eventable

8.3 GB PDFElement

6
Risky Applications

9.2 GB RoadWarrior

8.4 GB Netify
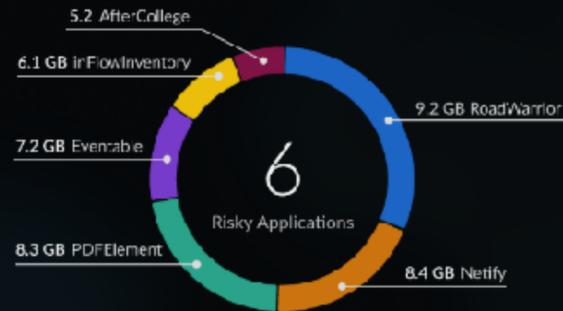
App Name	Risk Score	Usage	Users
RoadWarrior	9	9.2 GB	900
Netify	9	8.4 GB	852
PDFElement	9	8.3 GB	752
Eventable	9	7.2 GB	632
inFlowInventory	9	6.1 GB	551
AfterCollege	9	5.2 GB	231

There are 3136 users working from campus, remote locations and branch offices accessing 6 risky application in last 7 days with total data transfer of 44.4 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

👍 👎

Commit successful. All security profiles are following best practice recommendations.

👍 👎

Type your question here

The opportunity ahead

10,000+
potential
customers

~1,700

~800

| 2021 | 2023 | 2028 |

Customers with full
network security platform
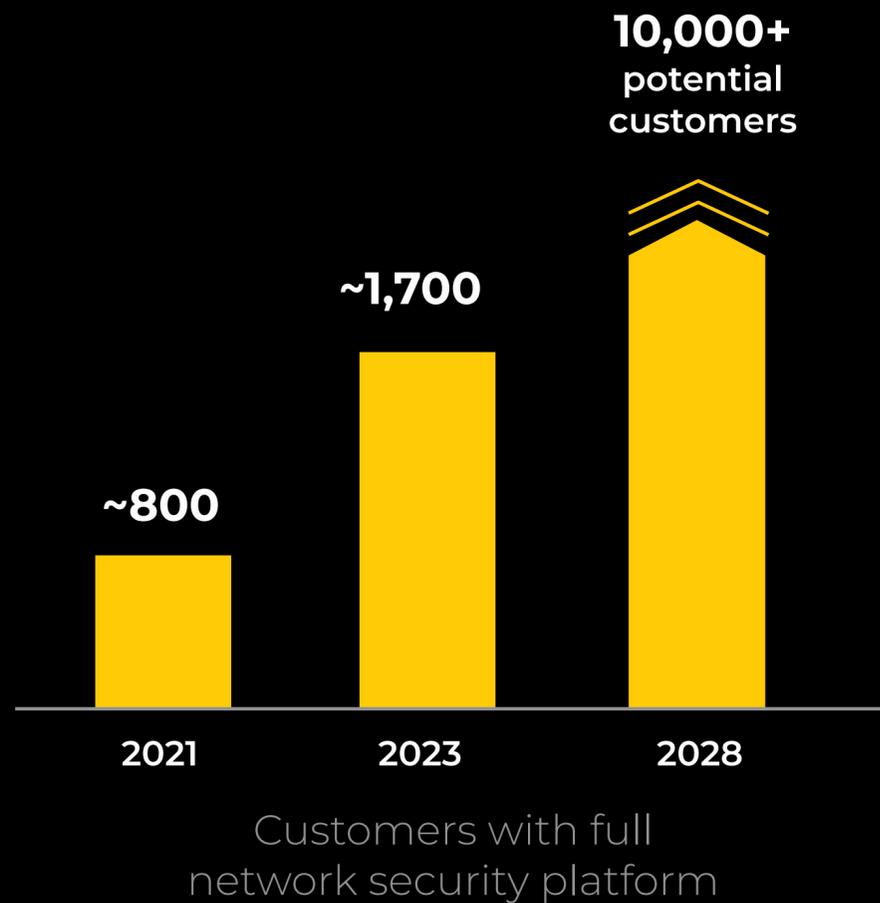
Uniquely positioned to deliver
Enterprise wide Zero Trust

5+

3.4

2.8

| 2021 | 2023 | 2028 |

# of services attached
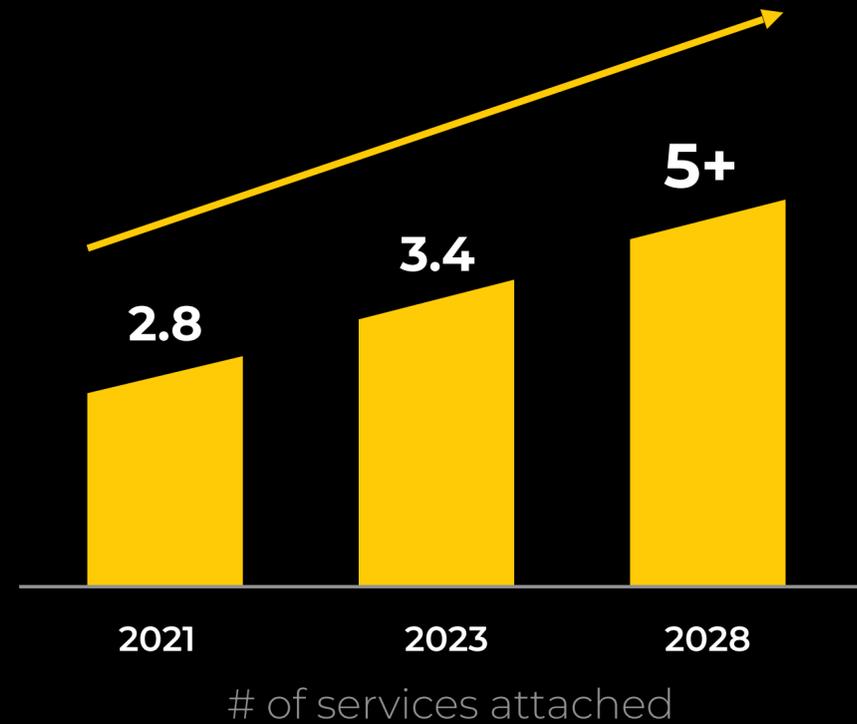
Opportunity compounded by
the adoption of integrated
security services

✓ **Deliver near real time
security outcomes with
Zero-trust platform**

✓ **Consolidate additional
security services**

✓ **Deliver operational
simplicity with AI**

Code-to-Cloud Platform
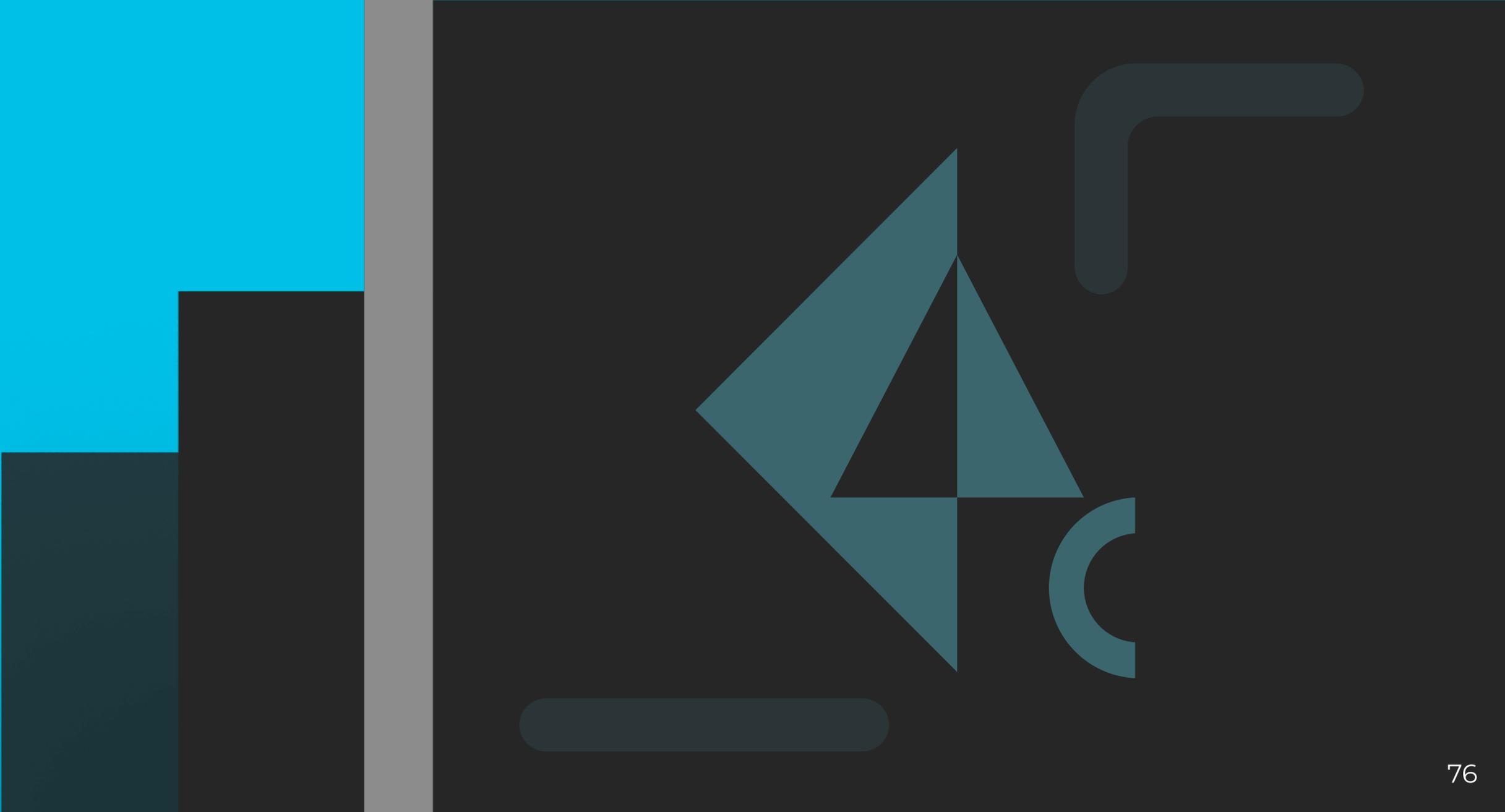
Cloud Security: Only an integrated platform can secure from code to cloud

500M+ cloud-native applications globally [1]

33M devs building apps, and growing [2]

90% deploy applications in 2+ clouds [3]

Organizations are building and using more applications

Applications are increasingly assembled - 75% of cloud code bases consist of open source [4]

80% of open source contain at least 1 vulnerability [4]

Applications must be protected when Running, but also Secure by Design

Securing Applications requires a Code to Cloud approach

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

Our opportunity: Deliver a AI-driven cloud security platform

Cloud applications are assembled in multiple stages

Code

Cloud Application

Custom   Open Source   IaC

CI/CD pipeline →

Cloud Infrastructure

VMs   Serverless   Containers

DBaaS   PaaS   Identity

CI/CD pipeline →

Cloud Runtime

Payments

Catalog   Billing

Shipping   Analytics

Security risks multiply across the application lifecycle

Code

Cloud Application

Custom Open Source IaC

CI/CD pipeline

Cloud Infrastructure

VMs Serverless Containers

DBaaS PaaS Identity

CI/CD pipeline

Cloud Runtime

Payments

Catalog Billing

Shipping Analytics

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

Code
Secure the source

Cloud Infrastructure
Secure the infrastructure

Cloud Runtime
Secure the runtime

Cloud Application

Custom
Open Source
IaC

VM
VMs

Serverless

Containers

DBaaS

PaaS

Identity

CI/CD pipeline

CI/CD pipeline

Payments

Catalog

Billing

Shipping
Analytics

| SCA | IaC Security | SAST | Secrets Scanning | CI/CD Security | CSPM | CIEM | CDS | API | Vulnerability Management | CWP | WAAS | CNS | CDR |

Code-to-Cloud Platform

Our strategy is resonating well
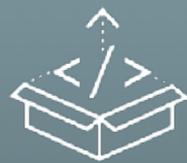
Code
Secure the source

GIGAOM

DevSecOps
LEADER
Dev Security Tools 2021 Radar

Code Security
LEADER
Policy as Code 2022 Report

Cloud Infrastructure
Secure the infrastructure

GIGAOM

CSPM
LEADER
CSPM 2022 Radar

Vuln Mgmt
LEADER
Vuln Mgmt 2021 Radar

Cloud Runtime
Secure the runtime

FORRESTER

CWP
LEADER
Cloud Workload Security 2022 Forrester Wave

FROST & SULLIVAN
CNAPP LEADER
Global CNAPP Radar 2022

20%[1] use Code Modules

68%[2] use Infrastructure modules

54%[3] use Cloud runtime modules

16%[4] use the Full Platform

| SCA | IaC Security | SAST | Secrets Scanning | CI/CD Security | | CSPM | CIEM | CDS | API | Vulnerability Management | | CWP | WAAS | CNS | CDR |

Code-to-Cloud Platform

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

Demo

The opportunity ahead

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

4x

2x

1x

	8 MODULES
5 MODULES	
2 MODULES	
2021	2022	2023
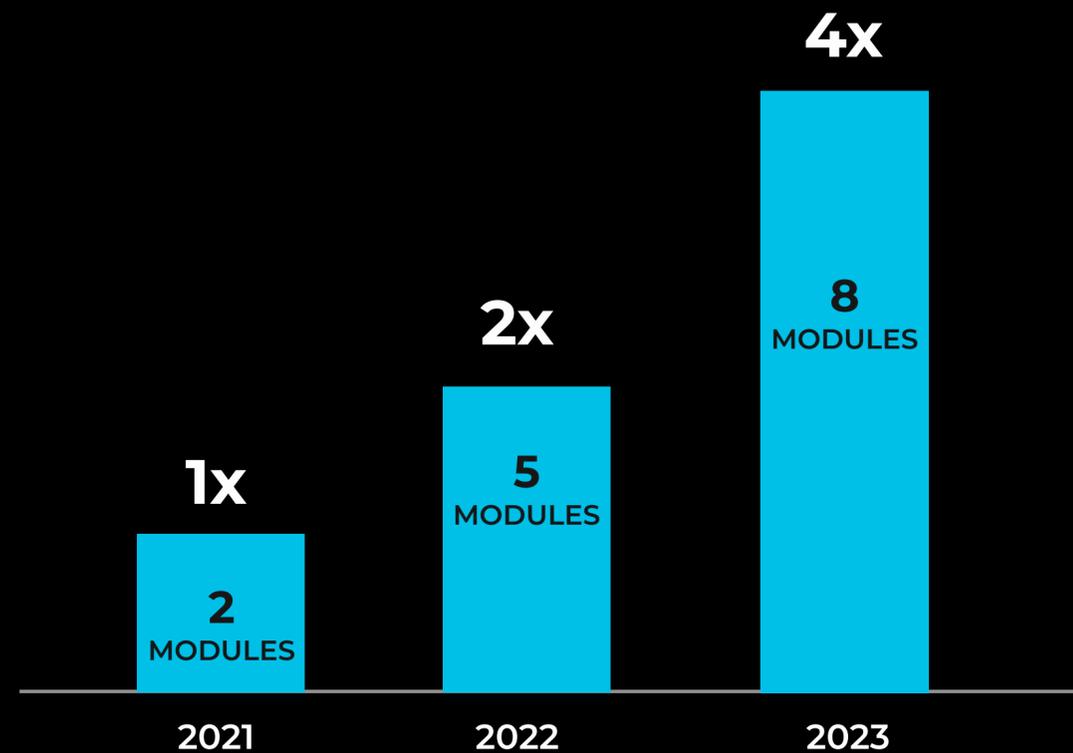
Credit consumption growth - evolution of current 8-module customers

Credit consumption grows with expansion across multiple modules

>7,000
Potential customers

~400

~80

| 2021 | 2023 | 2028 |
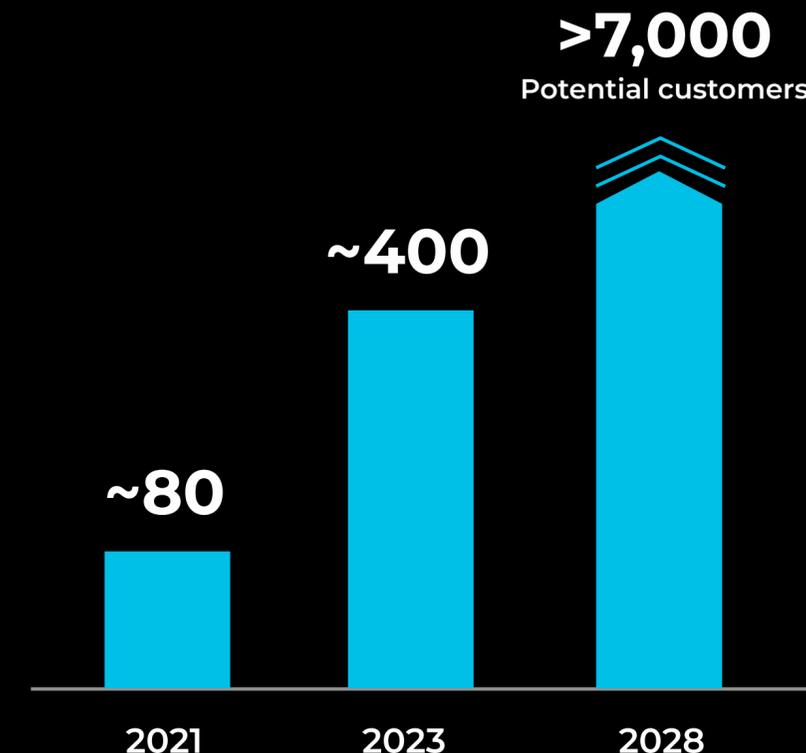
Number of customers using 5+ modules

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

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

Large, previously independent **categories driven to integrate**

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

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

Common platform needed to achieve the "self-driving SOC"

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

The human-driven SOC architecture doesn't work

UEBA

EDR

NTA

CDR

TIP

ASM

SOAR

SIEM

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

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

~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

ANALYTICS (AI/ML)

NETWORK

ENDPOINT

IDENTITY

CLOUD

ATTACK SURFACE

OTHER

STITCH AND NORMALIZE DATA

DETECTION

INVESTIGATION

RESPONSE
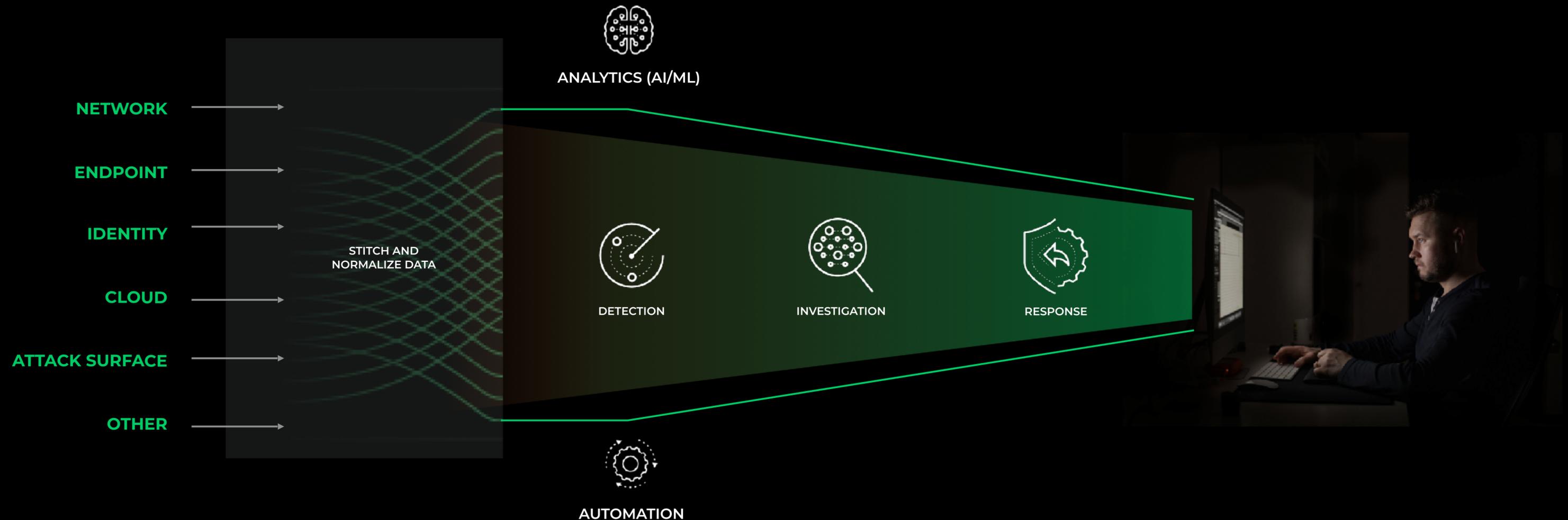
AUTOMATION

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

	FY19	FY20	FY21	FY22	FY23
Cortex XDR Collect, stitch & analyze data in <u>real time</u>	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 <u>Proactively</u> shrink the attack surface			Expanse acquisition	Xpanse Assess	Xpanse 2.0 Active ASM
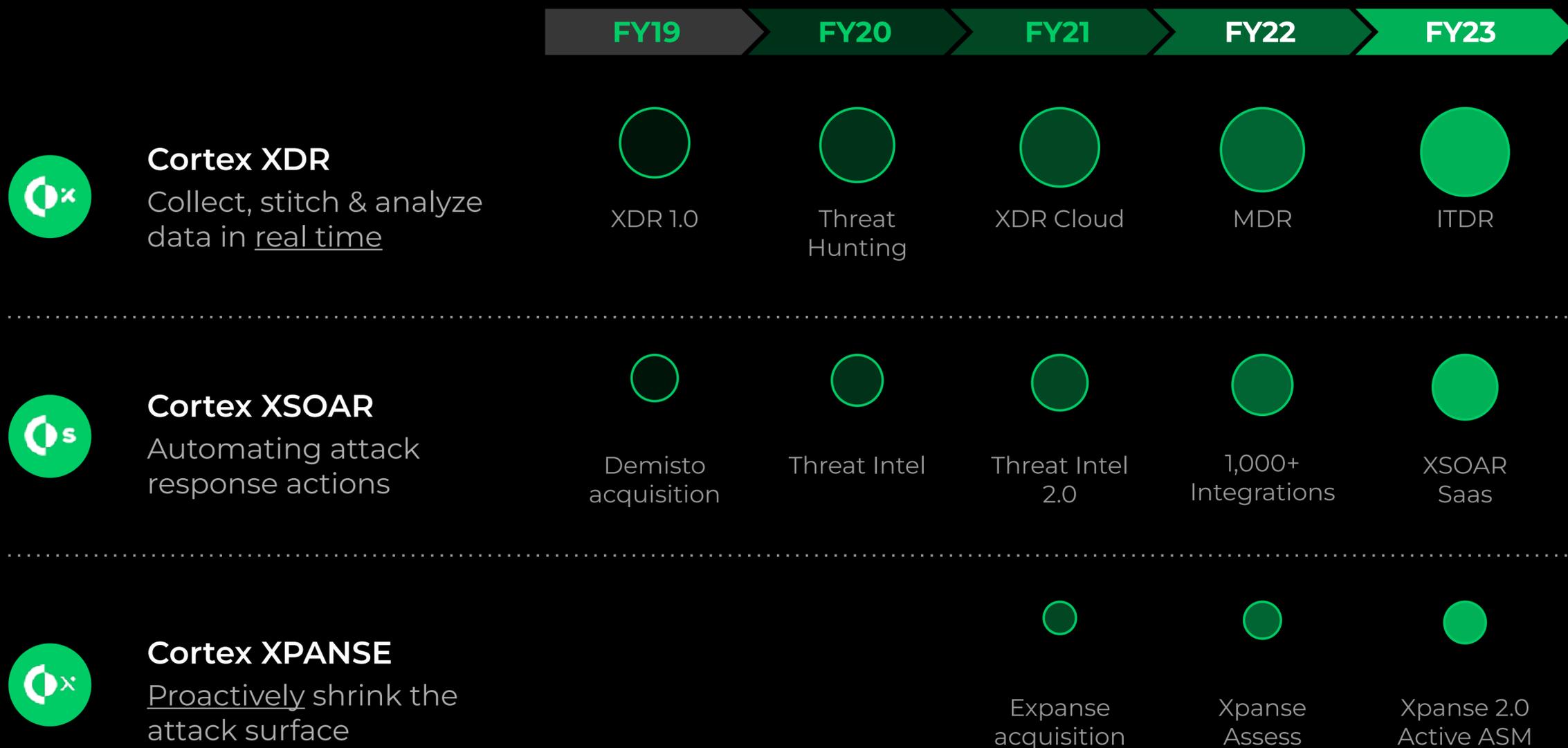
Recognized Leadership

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]

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).

Cortex XSIAM

Security operations platform to enable near real-time outcomes

90

Detecting attacks with siloed tools and data is impossible

Unusual user login
Happens 50 times per day
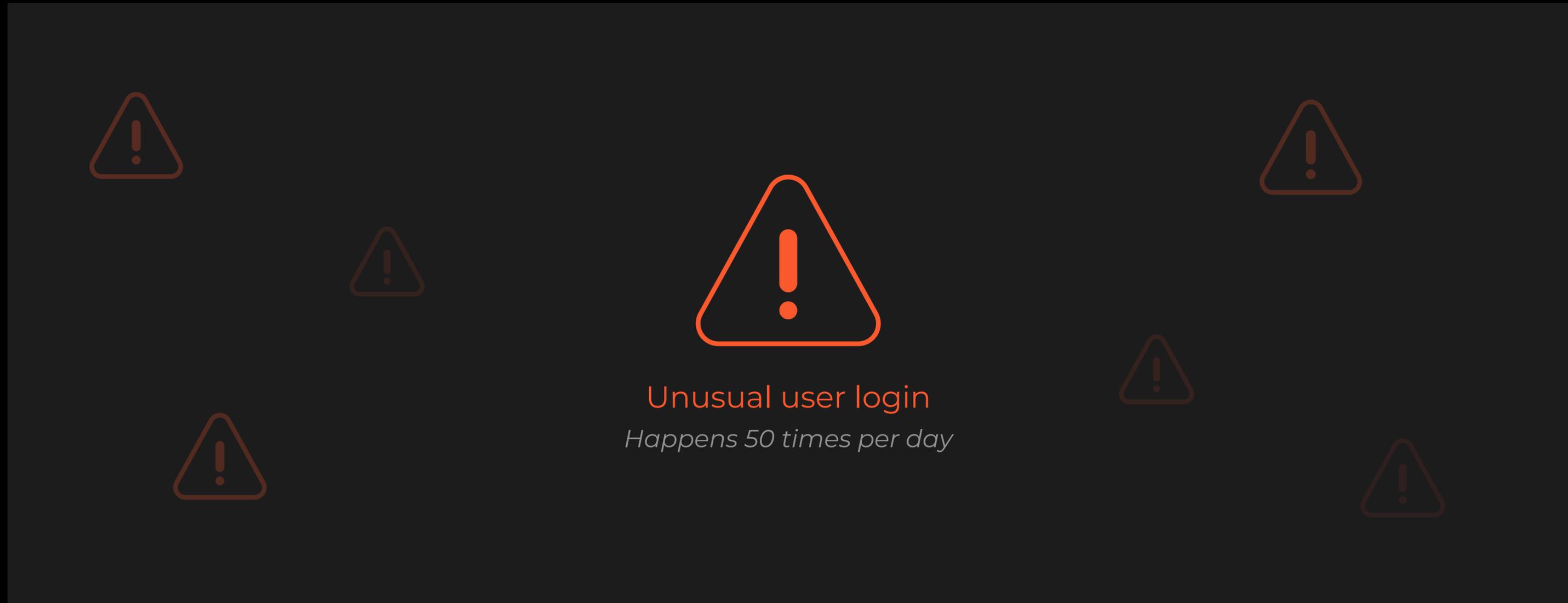
Events in isolation can be suspicious...

Detecting attacks with siloed tools and data is impossible

New application connection
Happens 600 times per day

...but they are common, and overwhelm the SOC.

Detecting attacks with siloed tools and data is impossible

Active directory access from new computer

Happens 300 times per day
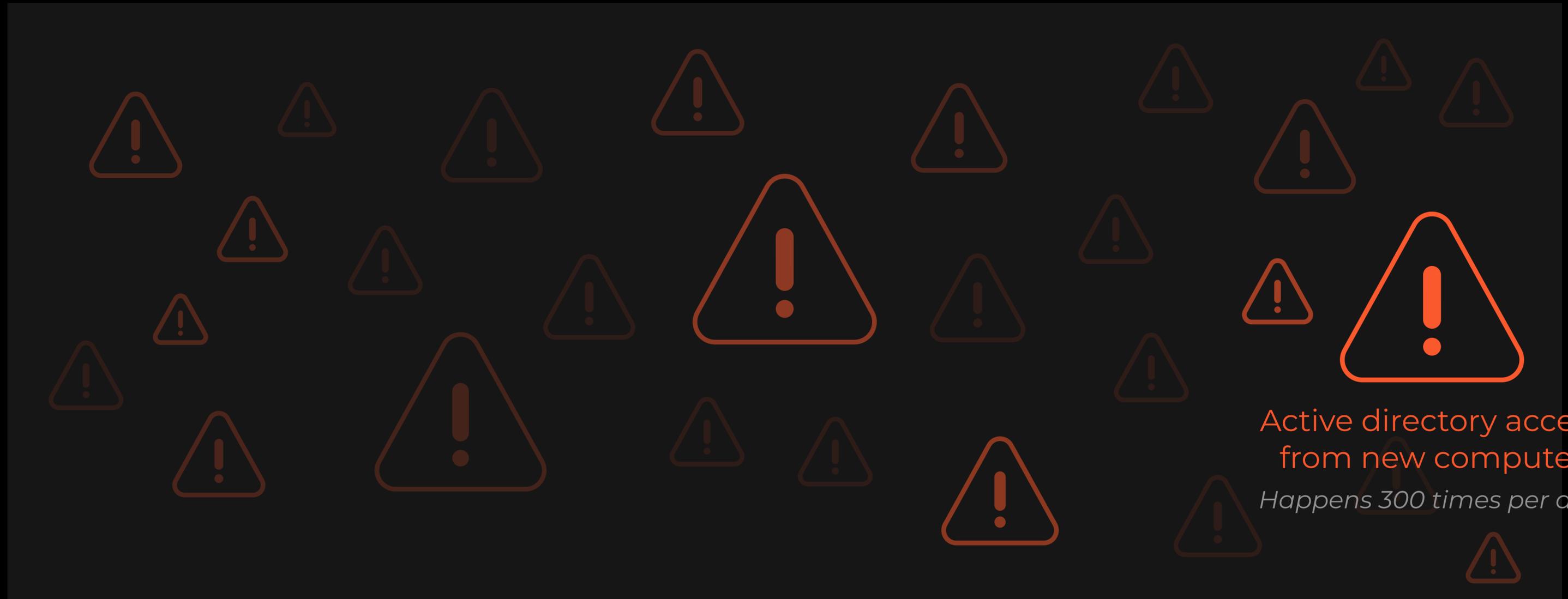
This means attacks are missed...

Detecting attacks with siloed tools
and data is impossible

Privilege escalation
Happens 100 times per day
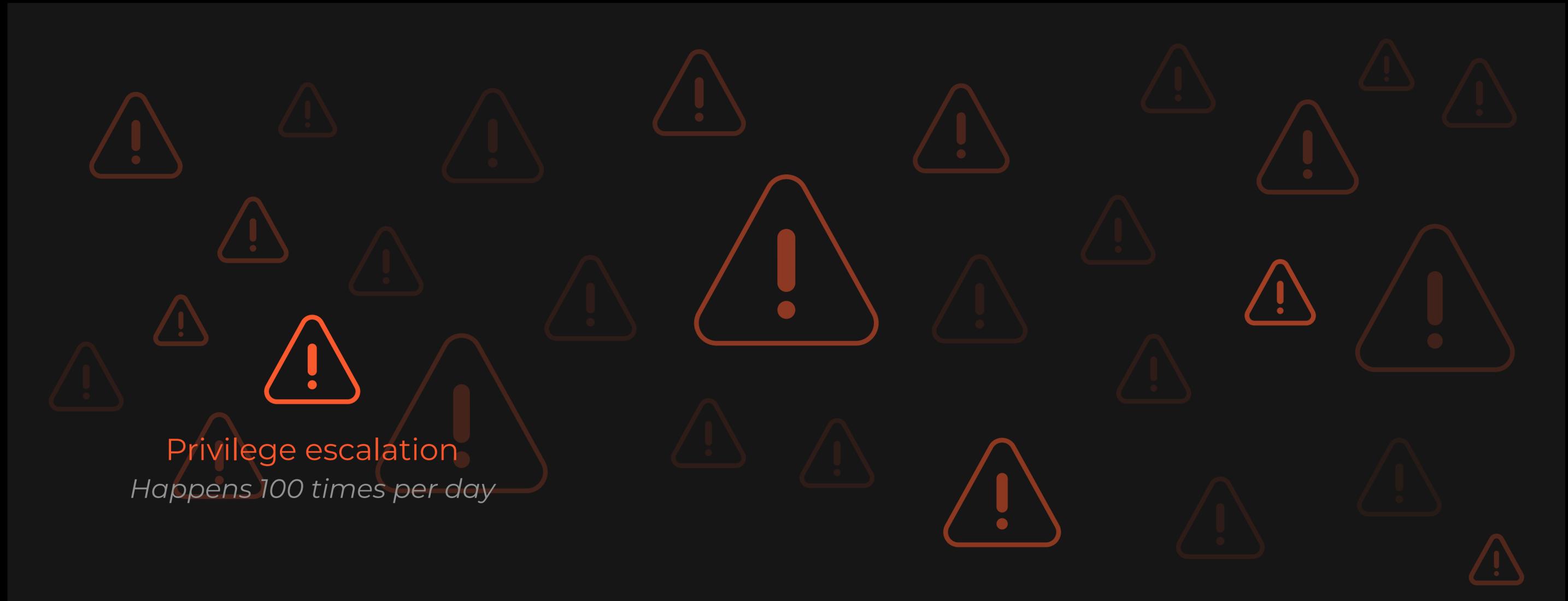
...because of a low confidence to act on any one alert.

Cortex XSIAM collects complete context and uses the power of AI to detect attacks that siloed tools miss

Network →

Endpoint →

Identity →

Cloud →

Attack Surface →

Other →

⚠️ Unusual user login   ⚠️ Privilege escalation

⚠️ Active directory access from new computer   ⚠️ New application connection
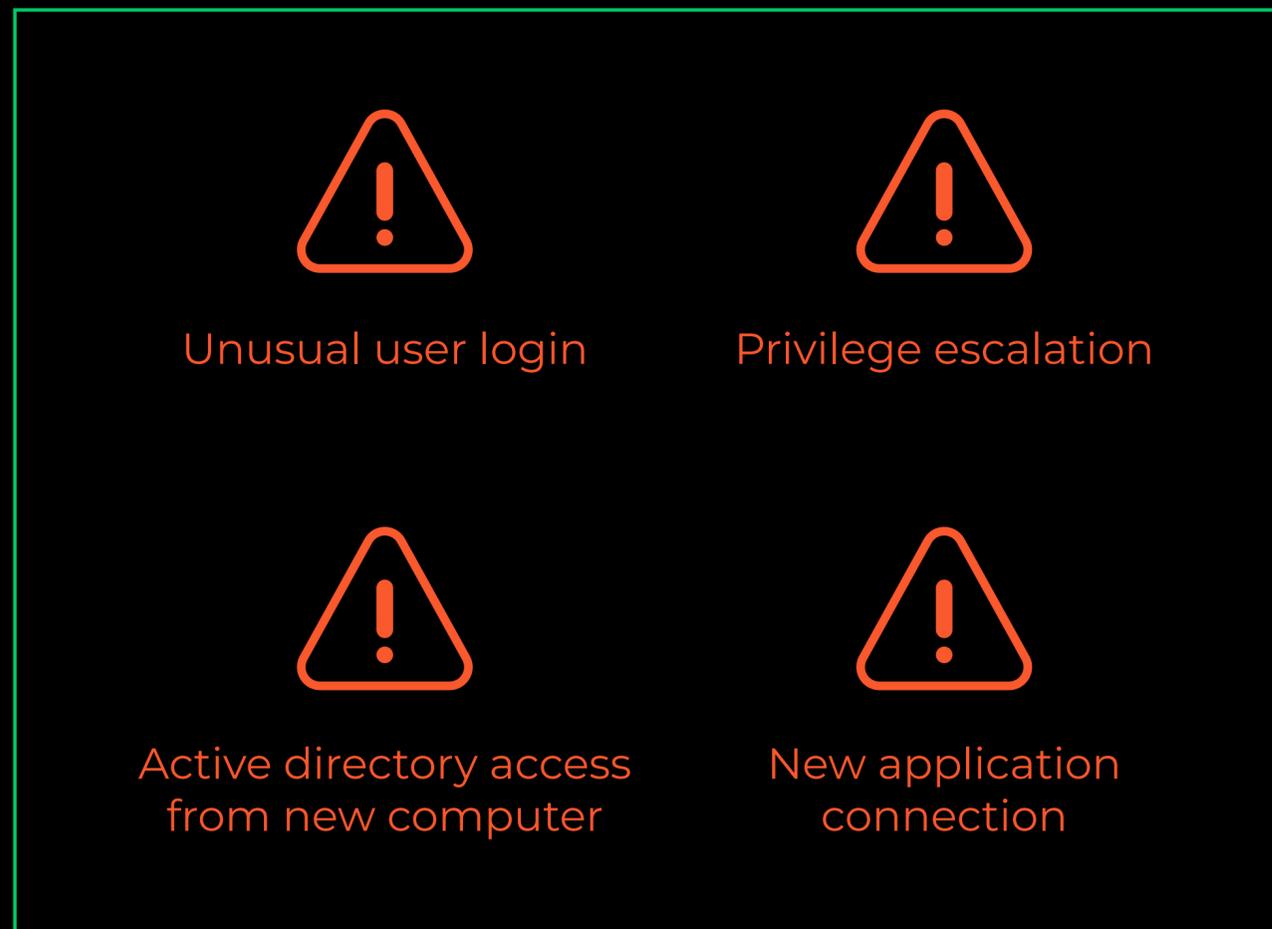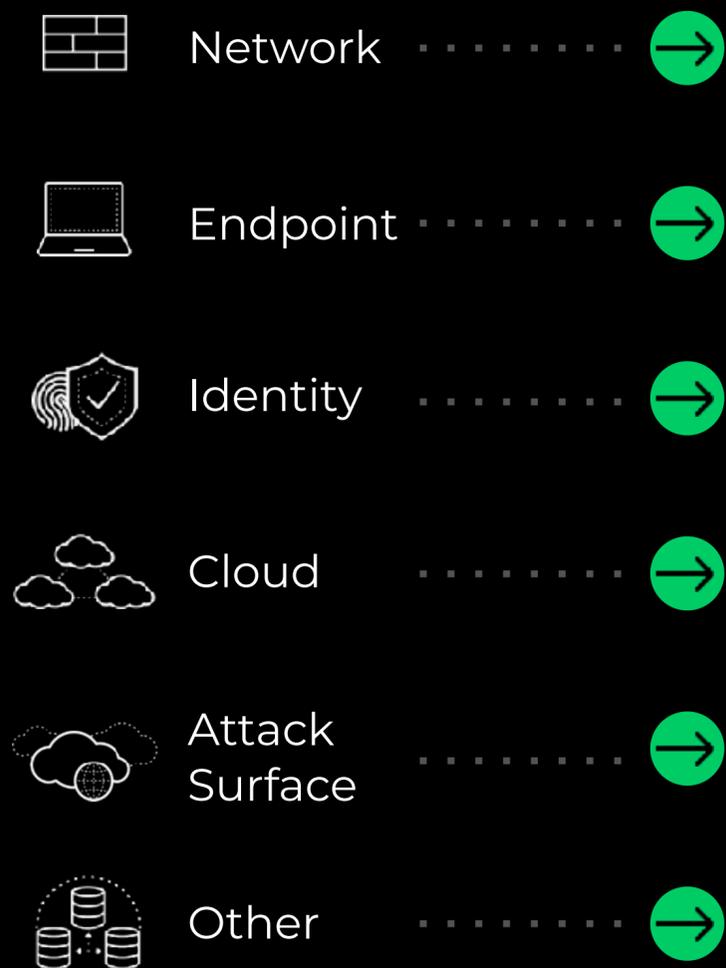
Stitching and normalizing alerts, augmented with contextual data...

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 ----→

⚠ Unusual user login   ⚠ Privilege escalation

⚠ Active directory access from new computer   ⚠ New application connection
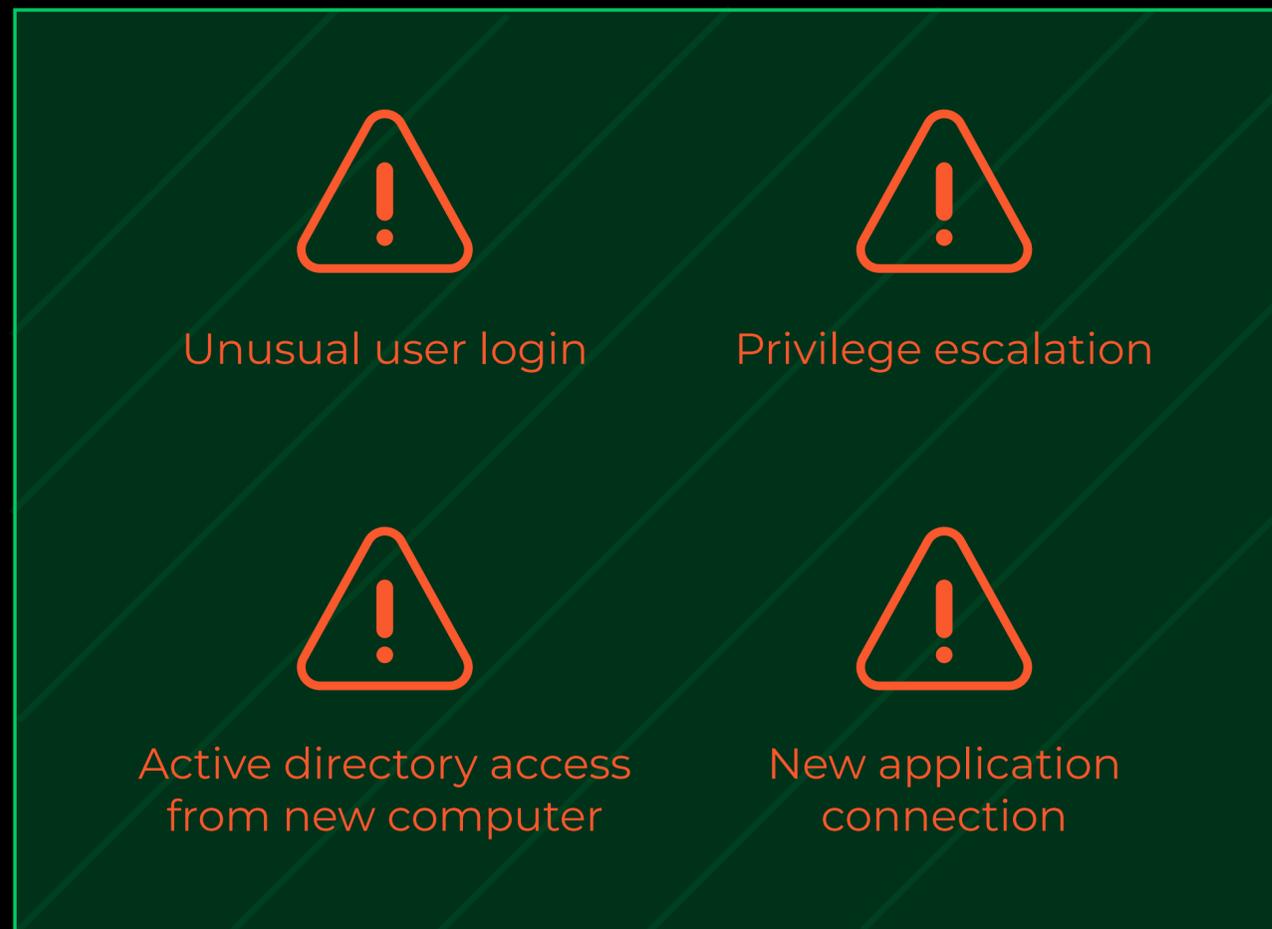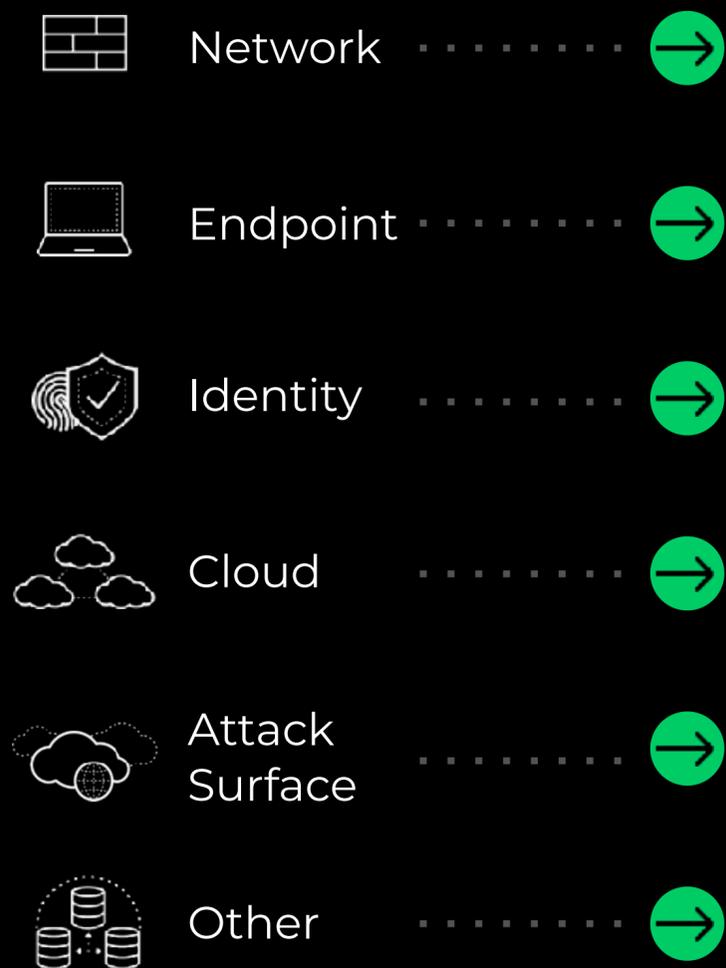
...enables us to automatically respond with high confidence.

XSIAM completely reimagines how the SOC works, built with AI on a common data platform

97
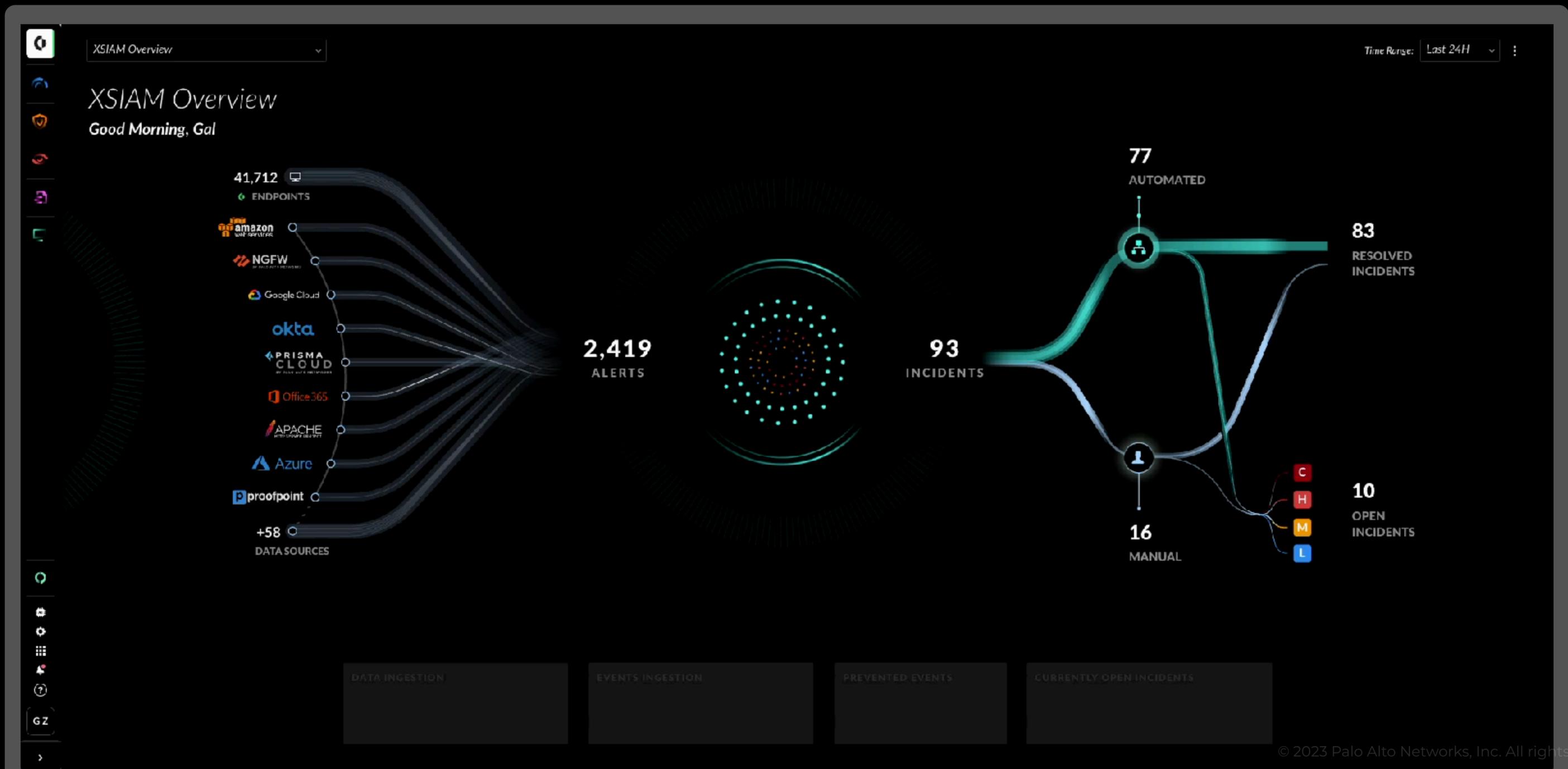
XSIAM is driving incredible outcomes for the SOC at Palo Alto Networks

A day in the life of the Palo Alto Networks internal SOC

Ingested Data per day	**75 TB**
Incidents flagged per day*	**133**
Incidents resolved with automation*	**100%**
Incidents close out rate	**100%**
Mean Time to Respond*	**1 MIN (HIGH SEVERITY ALERTS)**
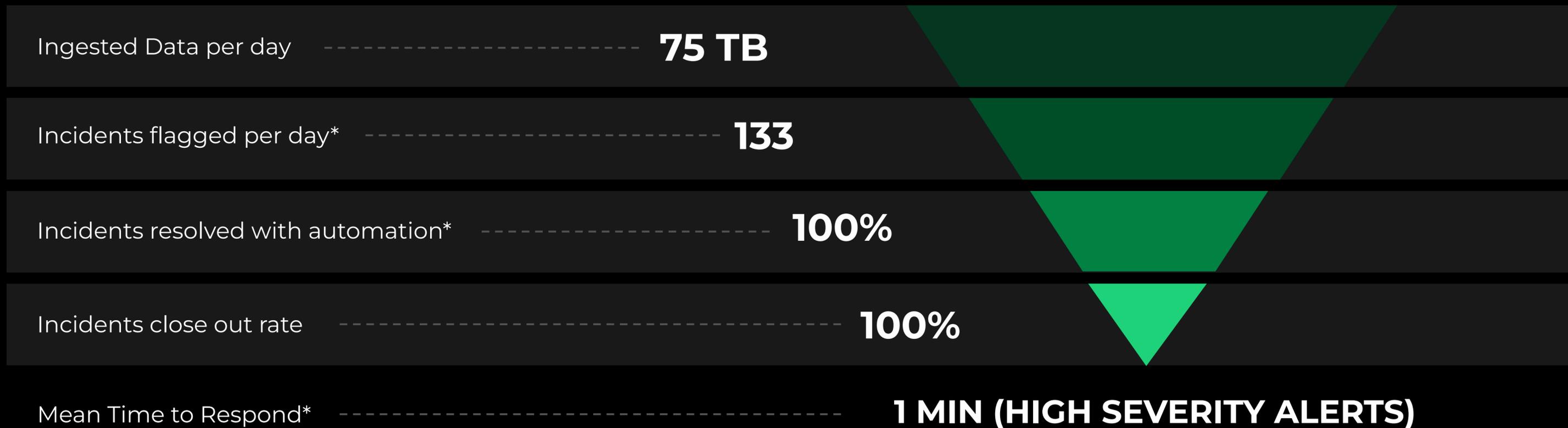
*Incidents flagged= potential security events flagged that requires automated or manual investigation. Incidents Resolved with automation: partially or fully addressed with automation. Mean Time to Respond (time from incident creation to incident assignment.

And XSIAM is already driving amazing outcomes for our customers

	Before XSIAM	**Early XSIAM**	
	(Average across initial implemented customers)	*(Average across initial implemented customers)*	
Analyzing more data ...	**~230 GB per day** *(In prior SIEM)*	**~1400 GB per day** *(In XSIAM)*	
with fewer false positives...	**~290**	**~80**	Incidents per day
and closing far more via automation...	**Minimal**	**High Majority**	Resolved using automation*
leading to all incidents getting addressed.	**<20%** when not using MSSP	**~100%**	Incidents closed out
Most importantly, getting ahead of attackers	MTTR* 2-3 Days, sometimes even "months"	MTTR* 16 mins-5 Hours	

> " 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

*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

The opportunity ahead

XSIAM Modules

10,000+

>5,100

>2,600

FY21A   FY23A   FY28F

Cortex customers, by fiscal year

>$200M   XSIAM bookings in FY23

>3x   ARR Expansion when existing Cortex customers move to XSIAM

4   Customers booking >$20M on XSIAM in FY23

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

10+ additional XSIAM modules

EDR   **NTA**

ITDR   **TIP**

ASM   **SOAR**

SIEM

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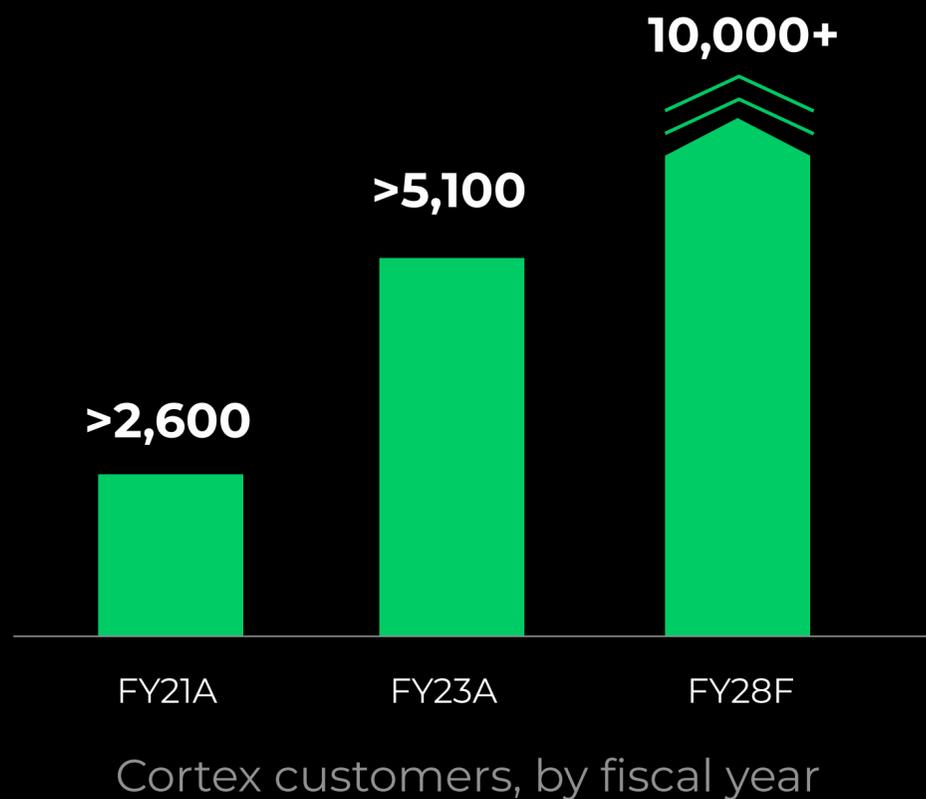
Continue taking share with our XDR, XSOAR, and Xpanse offerings...

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

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

Go To Market

BJ
Jenkins

President

Customers have tried to solve cybersecurity challenges by buying point solutions

Security in customers' estates is fragmented...

~75

Average number of cybersecurity solutions at large companies [1]

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

As an industry, we need to get better at helping our customers

FROM		TO
Transactional vendor	〉	**Strategic partner** helping customers on their transformation journey
Selling products	〉	**Architecting outcomes** jointly with ecosystem solution providers
Reactive help	〉	**"In it together"** mindset - driving success for every customer

We are well on our journey to becoming a **strategic partner**

Historical Motion

Engaged by technical domain experts

Pre-defined product requirements

Focus on price negotiation

Ends with a transactional product sale

Evolving Motion across ~3,000 Sellers

Engaged by CxOs looking to transform

Strategic discussions focused on security outcomes

'Seat at the table' for architectural choices

Trusted relationship and multi-year roadmap

We will accelerate solution selling in partnership with the broader ecosystem

Five Years Ago

Sold a single product as part of a larger partner- delivered motion

↓

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

Today

Co-lead sales motions with our partners and deliver joint solutions

↓

~150 $10M+ strategic partners today [2]

Future

Architect integrated offerings with partners to improve client outcomes

↓

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

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+ today [1]

Increased Adoption
Stick with the customer throughout their journey

600+ CS professionals with deep expertise [2]

[1] Includes CPSP (Certified Professional Services Partner) and PSDP (Professional Services Delivery Partner)
[2] Includes PANW badged employees and contractors

The opportunity in front of us is extensive…

Palo Alto Networks G2K Customers [1]

All 3 Platforms
$4.1M per customer [2]

2 Platforms
$418K per customer [2]

1 Platform
$86K per customer [2]

Platform Breadth

Platform Depth

Untapped Potential
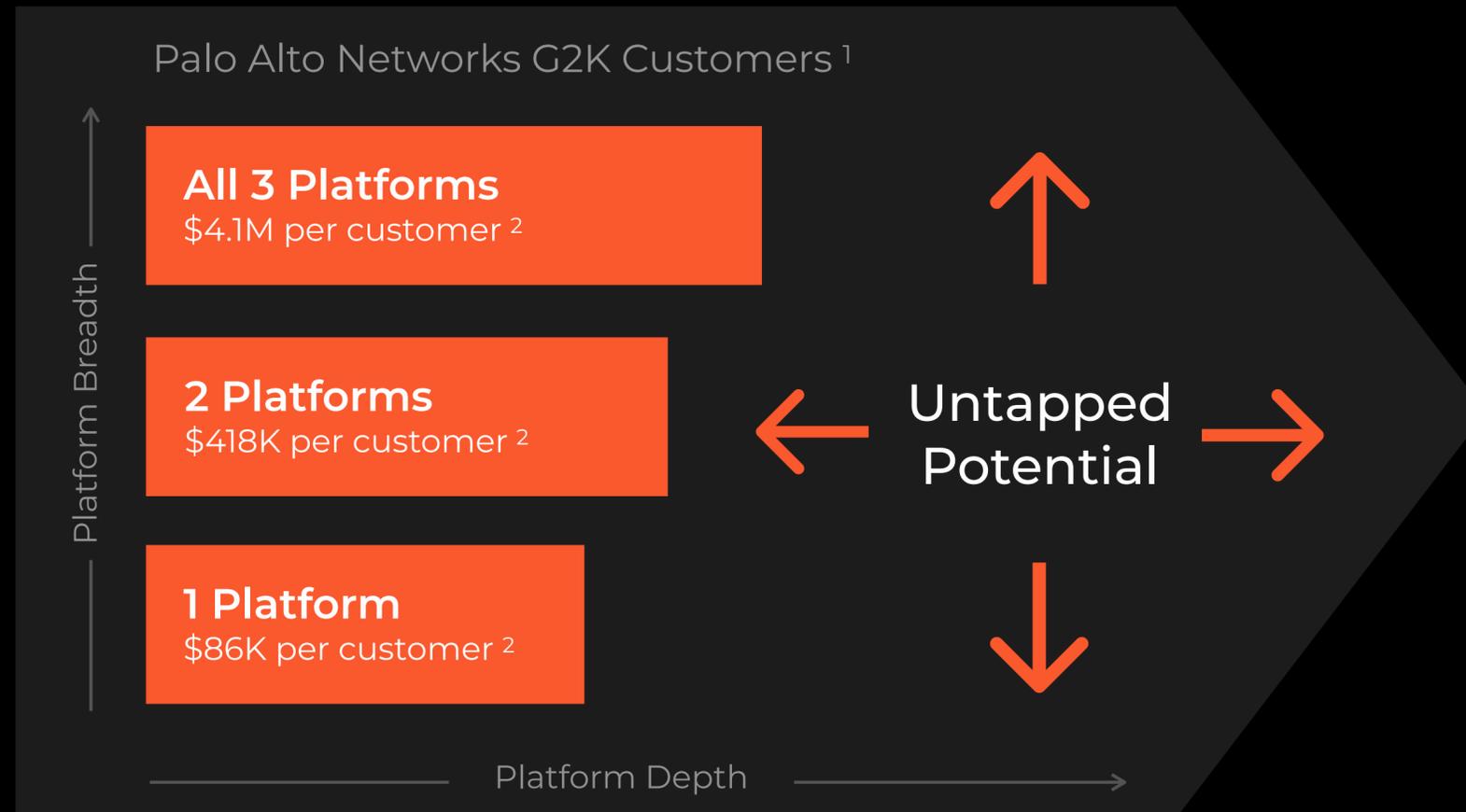
We have ample potential to expand the breadth & depth of our platforms…
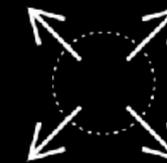
Breadth
Land every platform across our installed base
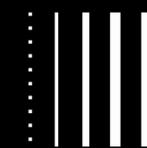
Depth
Increase penetration by covering full estate of every customer

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
[1] G2K refers to Forbes Global 2000 companies
[2] FY23 Sales per G2K customer who have purchased 1, 2, or all 3 platforms defined as Strata, Prisma, Cortex"

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 [1]

$38B — 2018 TAM
$104B — 2023 TAM
$163B — 2026 TAM

- 🟢 Cortex TAM
- 🔵 Prisma Cloud Security TAM
- 🟡 Network Security TAM
- 🟢 PANW share of Cortex TAM
- 🔵 PANW share of Cloud TAM
- 🟤 PANW share of NetSec TAM

Market share leaders [2] in other IT categories

Category	Share
ITOM	36%
Sales CRM	34%
Database Mgmt Systems	25%
ERP SW	17%
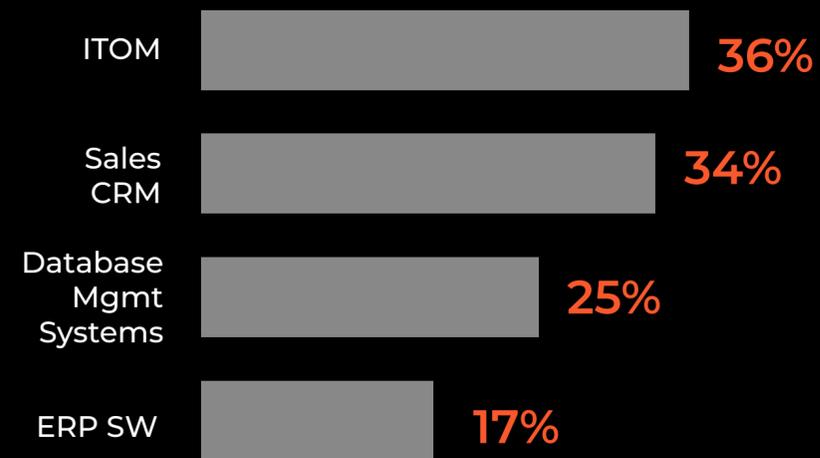
Our ~7% share of TAM remains well below that of leaders in other markets

Our platform leadership and innovation will fuel our growth and key metrics

Zero Trust

Code-to-Cloud

Autonomous SecOps

FWaaP growth

Market share gains

Credit consumption
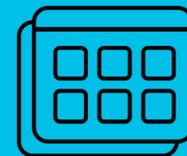
New Module Adoption

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)

15 — FY19
32 — FY20
42 — FY21
67 — FY22
110 — FY23

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

~2/3rds
Proportion of revenue from prior year cRPO
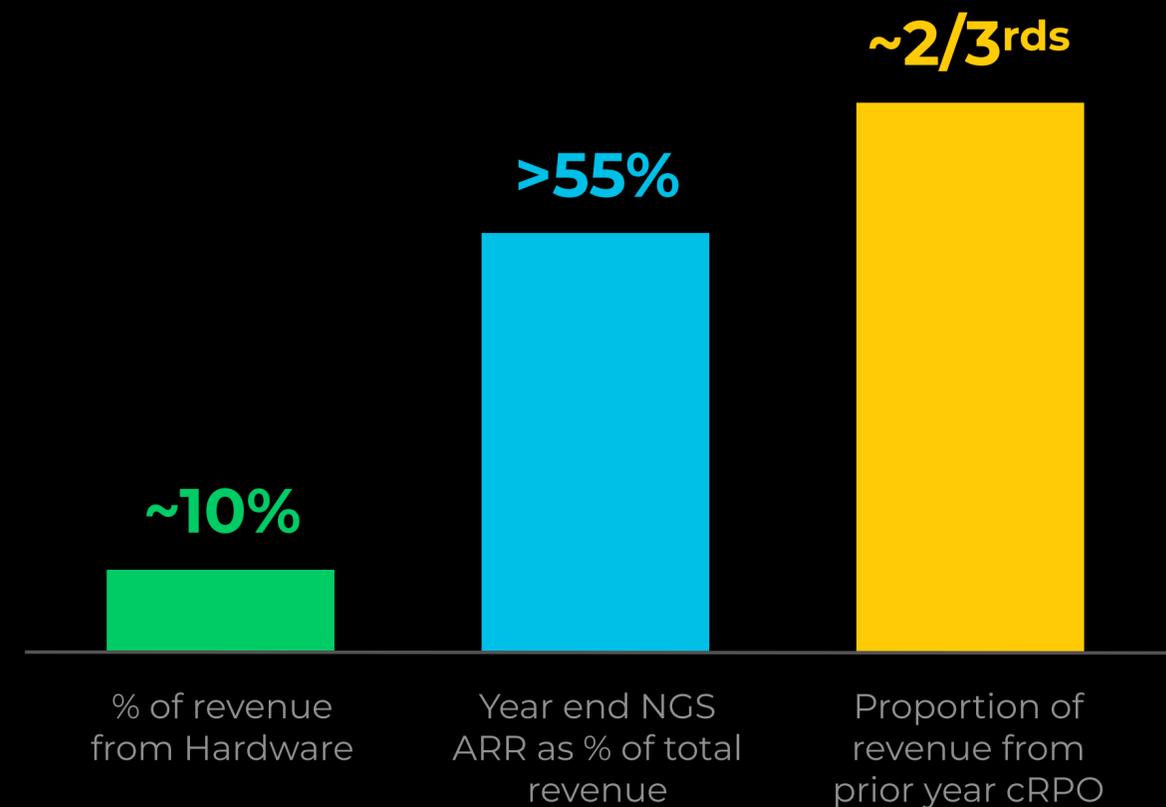
We can deliver steady gross margin while investing in cloud

	FY'23 Drivers	FY'24 - FY'26 Net new drivers
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
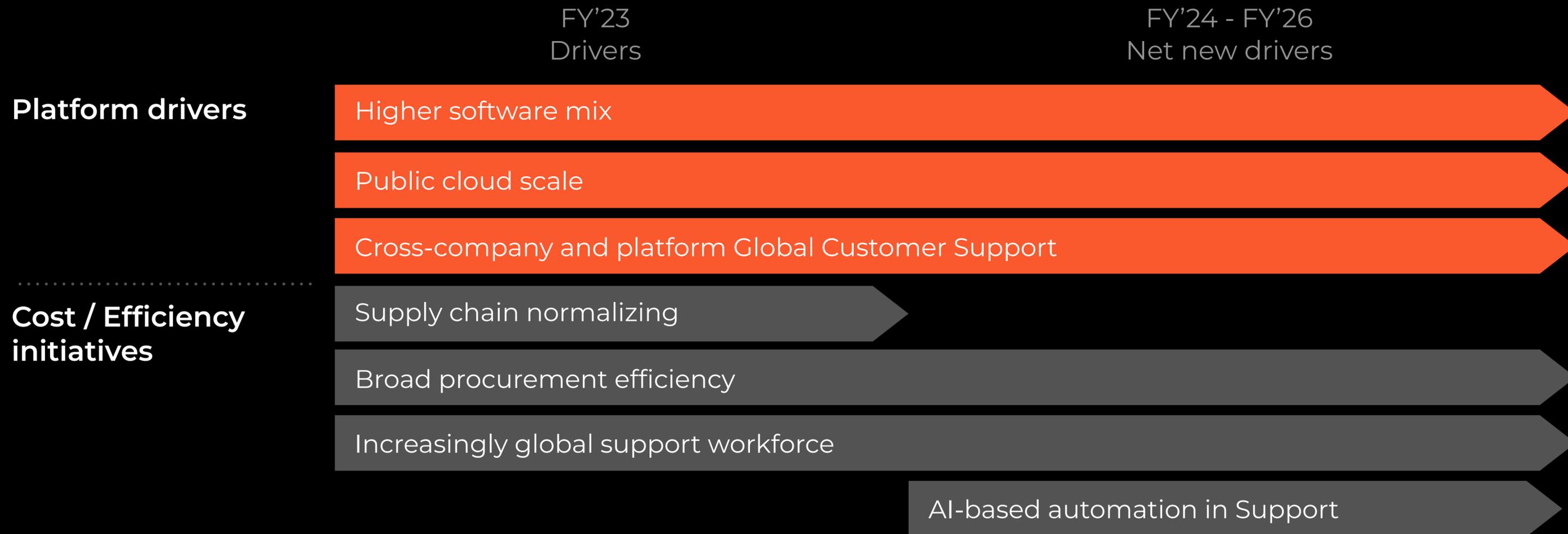
Steady gross margin as we drive core improvements and invest in new cloud-based offerings

Platform and efficiency opportunities driving operating leverage

FY'23
Drivers

FY'24 - FY'26
Net new drivers

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

Steady free cash flow margin with flexibility to navigate the environment

	FY'23 Drivers	FY'24 - FY'26 Net new drivers

Leverage drivers

Strong top-line

Operating margin leverage

Driving to best in class working capital management

Low CAPEX requirements

Higher interest rates on cash

Accounting for business shifts

Increase in % of bookings with deferred payments vs. FY23 levels

Accounting for higher cash taxes
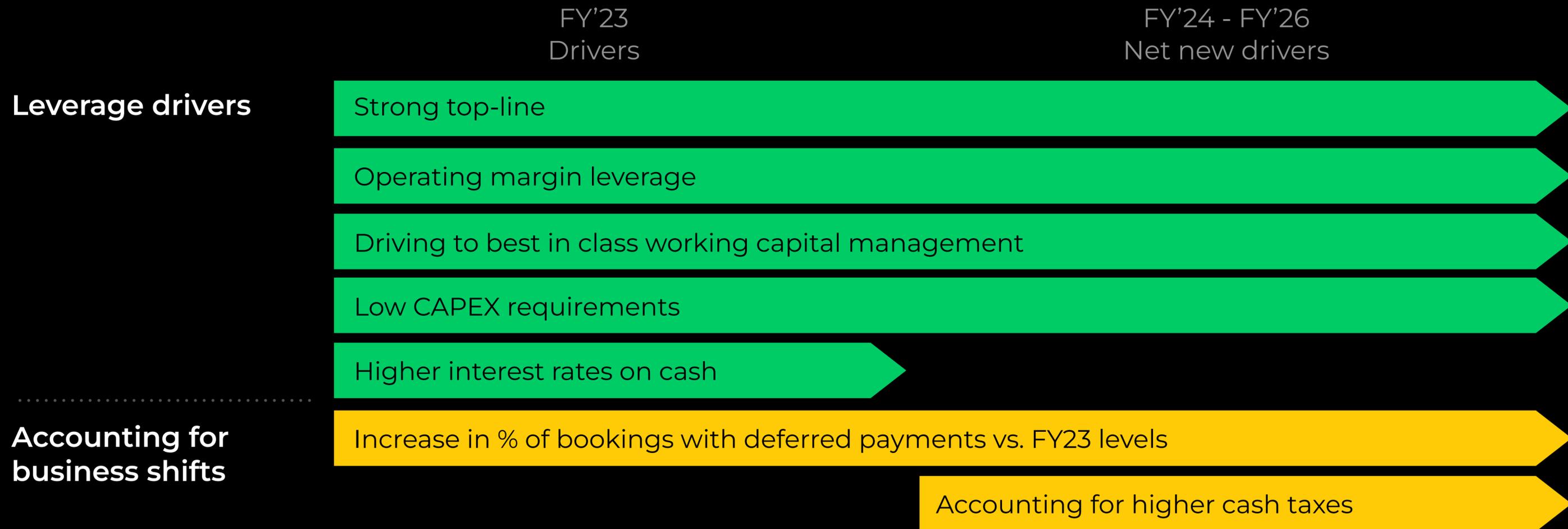
We have already delivered strong cash flow while managing through an increase in deferred payments

Increased deals with Deferred Payments

FY'20   FY'21   FY'22   FY'23

■ Bookings $s for deals with Deferred Payment Plans

Robust Free Cash Flow Margins

28%   33%   33%   39%

FY'20   FY'21   FY'22   FY'23
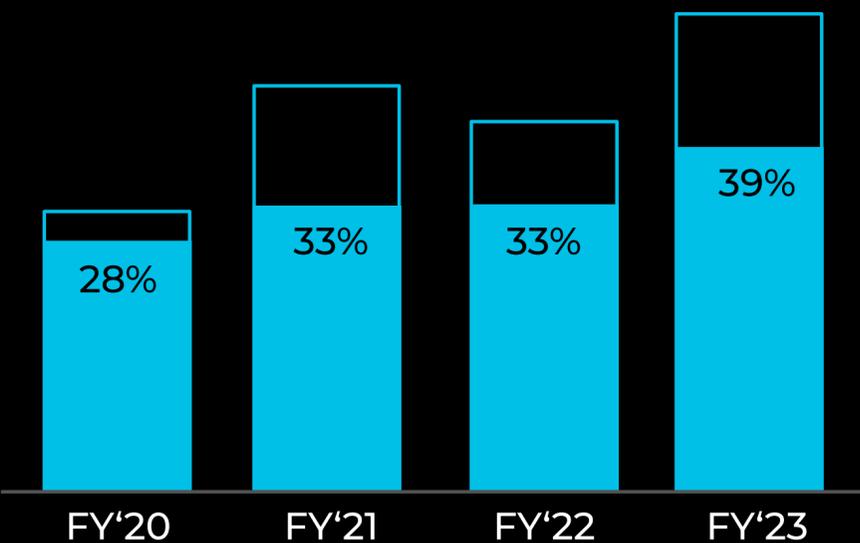
■ Adjusted Non-GAAP Free Cash Flow Margin
▢ Adjusted Non-GAAP Free Cash Flow Margin, without Deferred Payment Plans

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

$1.7B

FY23 convertible note repaid

Planning to settle

$2.0B

FY25 convertible note with cash

$3.9B

In cash used for share repurchase over last 5 years

Continue focus on acquiring emerging leaders and boosting with our GTM

Maintain capital structure that allows flexibility & minimizes dilution

Opportunistic buyback

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

Q&A

paloalto®
NETWORKS

Thank you for watching

Appendix

Calculation of Billings

$ In millions

Billings:	Q422	Q123	Q223	Q323	Q423	FY'22	FY'23
Total revenue	$1,550.5	$1,563.4	$1,655.1	$1,720.9	$1,953.3	$5,501.5	$6,892.7
Add: change in total deferred revenue, net of acquired deferred revenue	1,134.6	185.6	374.0	535.3	1,206.8	1,970.0	2,301.7
Total billings	$2,685.1	$1,749.0	$2,029.1	$2,256.2	$3,160.1	$7,471.5	$9,194.4

GAAP to Non-GAAP Reconciliations
Gross Margin

$ In millions

Non-GAAP gross profit and gross margin:			Q422		Q423	
%	$	%	$	%	$	%
GAAP gross profit and gross margin			$1,058.2	68.2%	$1,446.5	74.1%
Share-based compensation-related charges			36.0	2.3%	41.8	2.1%
Amortization expense of acquired intangible assets			25.8	1.7%	19.3	1.0%
Litigation-related charges[1]			1.7	0.1%	1.7	0.1%
Restructuring and other costs[2]			14.0	0.9%	-	0.0%
Non-GAAP total gross profit and gross margin			$1,135.7	73.2%	$1,509.3	77.3%

[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

Non-GAAP operating income and operating margin:	Q422		Q423	
	$	%	$	%
GAAP operating income and operating margin	$15.4	1.0%	$253.5	13.0%
Share-based compensation-related charges	251.3	16.1%	274.1	14.0%
Acquisition-related costs [1]	2.4	0.2%	-	0.0%
Amortization expense of acquired intangible assets	31.2	2.0%	24.7	1.3%
Litigation-related charges [2]	1.7	0.1%	1.7	0.1%
Restructuring and other costs [3]	21.2	1.4%	-	0.0%
Non-GAAP operating income and operating margin	$323.2	20.8%	$554.0	28.4%

[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

$ In millions

Non-GAAP operating income and operating margin:	FY'20		FY'21		FY'22		FY'23	
	$	%	$	%	$	%	$	%
GAAP operating income (loss) and operating margin	($179.0)	-5.3%	($304.1)	-7.1%	($188.8)	-3.4%	$387.3	5.6%
Share-based compensation-related charges	685.5	20.2%	936.5	22.0%	1,072.0	19.5%	1,145.1	16.6%
Acquisition-related costs [1]	15.7	0.5%	46.1	1.1%	5.5	0.1%	19.5	0.3%
Amortization expense of acquired intangible assets	76.4	2.2%	116.7	2.7%	125.8	2.3%	103.1	1.5%
Litigation-related charges [2]	3.6	0.1%	7.1	0.2%	7.1	0.1%	7.1	0.1%
Restructuring and other costs [3]	(3.1)	-0.1%	-	0.0%	21.2	0.4%	(2.2)	0.0%
Non-GAAP operating income and operating margin	$599.1	17.6%	$802.3	18.9%	$1,042.8	19.0%	$1,659.9	24.1%

[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

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

[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, 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] Consist 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

$ In millions

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

GAAP to Non-GAAP Reconciliations
Adjusted Free Cash Flow

$ In millions

Free cash flow and adjusted free cash flow (non-GAAP):	FY'20	FY'21	FY'22	FY'23
Net cash provided by operating activities	$1,035.7	$1,503.0	$1,984.7	$2,777.5
Less: purchases of property, equipment, and other assets	214.4	116.0	192.8	146.3
Free cash flow (non-GAAP)	$821.3	$1,387.0	$1,791.9	$2,631.2
Add: capital expenditures for headquarters [1]	94.3	-	38.9	-
Add: cash payment related to tax settlement	-	-	-	39.8
Add: repayments of convertible senior notes attributable to debt discount	-	0.1	-	-
Add: litigation related payment [2]	50.0	-	-	-
Less: cash payment related to landlord lease amendment [3]	(2.0)	-	-	-
Adjusted free cash flow (non-GAAP)	$967.6	$1,387.1	$1,830.8	$2,671.0
Adjusted free cash flow margin (non-GAAP)	28.4 %	32.6 %	33.3 %	38.8 %

[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 Q1'18, we received an upfront cash reimbursement of $38.2 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: Information Security and Risk Management, Worldwide, 2018-2024, Q420 Update (December 22, 2020)
- 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)
- Gartner, Forecast: IoT Market Opportunity by Technology Segment 2020-2025 (April 20, 2022)
- 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