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

paloalto NETWORKS

# 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.

# 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**

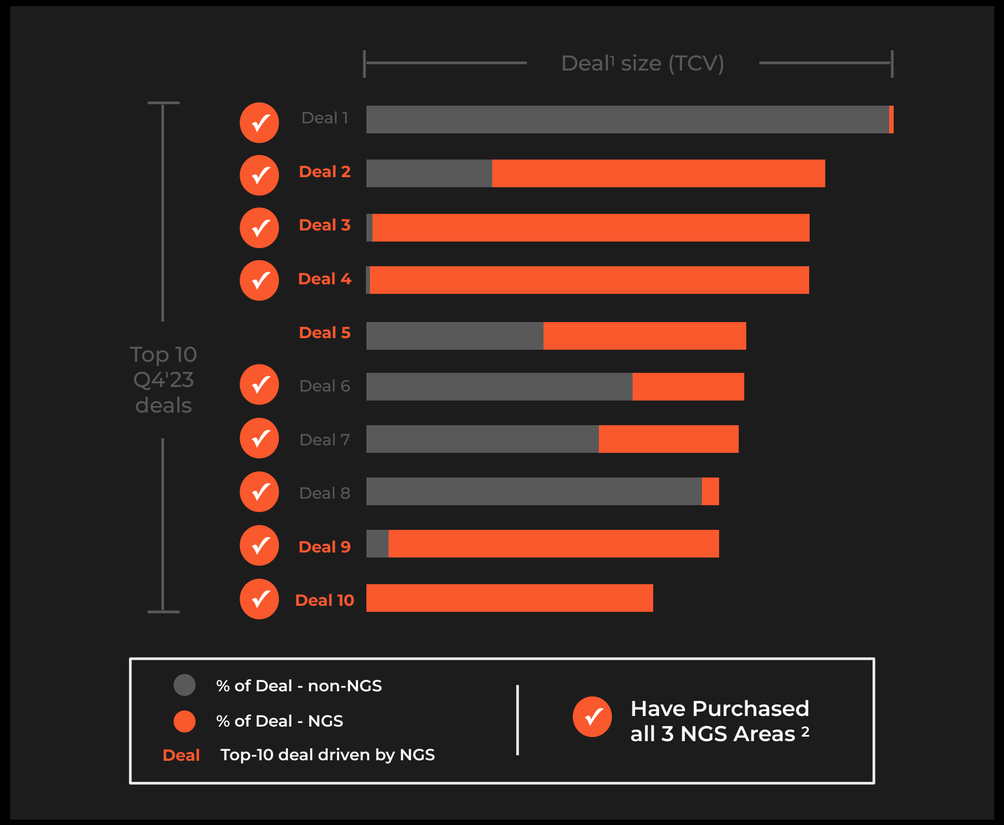
**Largest Net New ARR** in PANW history

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

[1] ARR = Annualized Recurring Revenue. Next-Gen Security ARR is annualized allocated revenue of all active contracts as of the final day of the reporting period for Prisma and Cortex offerings inclusive of the VM-Series and related services, and certain cloud-delivered security services.
[2] Prisma Cloud ARR represents Annual Recurring Revenue for Prisma Cloud, VM-Series for Public Cloud, and CN-Series.
[3] Largest publicly disclosed Net New ARR of any pure-play cybersecurity company.
Fiscal year ending on July 31.

# Platformization continues to drive large deal momentum

## Six out of top-10 deals were Driven by NGS




## 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.

CORTEX

# XSIAM traction amplifying Cortex trajectory

XSIAM

**>$200M**

XSIAM Bookings within first year of release

XSIAM Transactions are Large and Strategic

| 3-5 Year | >$1M | Driving MTTR [2] from days to hours / minutes |
|---|---|---|
| customer commitments | Average ACV [1] | |

Cortex Active Customers

**>5K**

+28% y/y

Q4'23 Average Cortex Deal Size

**+50%**

y/y

Driven by XDR customer adds and market-leading XSOAR

[1] Average ACV = Average Annual Contract Value for deals signed in Q4'23.
[2] MTTR = Median Time To Resolve (time from incident creation to incident resolution). Fiscal year ending on July 31.

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

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

SASE

# 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

**BREAKING NEWS**

Gartner

## Single Vendor SASE Magic Quadrant

*Published: August 16th, 2023*

## Marquee deals in Q4

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

**$[illegible]**
Expansion with a US Technology Company

**$[illegible]M**
Expansion with a European Food and Beverages company

**$11M**
Expansion with a US Financial Services Company

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

PRISMA® CLOUD

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

**Growth in Q4'23 Prisma Cloud Credit Consumption**

**+45%** y/y

**Growth in multi-module adoption customers [2]**

| +31% y/y | +57% y/y | +179% y/y |
|---|---|---|
| 2+ modules | 3+ modules | 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

[1] Prisma Cloud ARR represents Annual Recurring Revenue for Prisma Cloud, VM-Series for Public Cloud, and CN-Series.
[2] Multi-module adoption customers is based on customers with module adoption over the 90 day period ending 7/31/2023, and excludes any Prisma Cloud Compute only self-hosted customers.

# FY23: Successful execution through a tough macro environment

Platformization

Go to market transformation

Strong product innovation

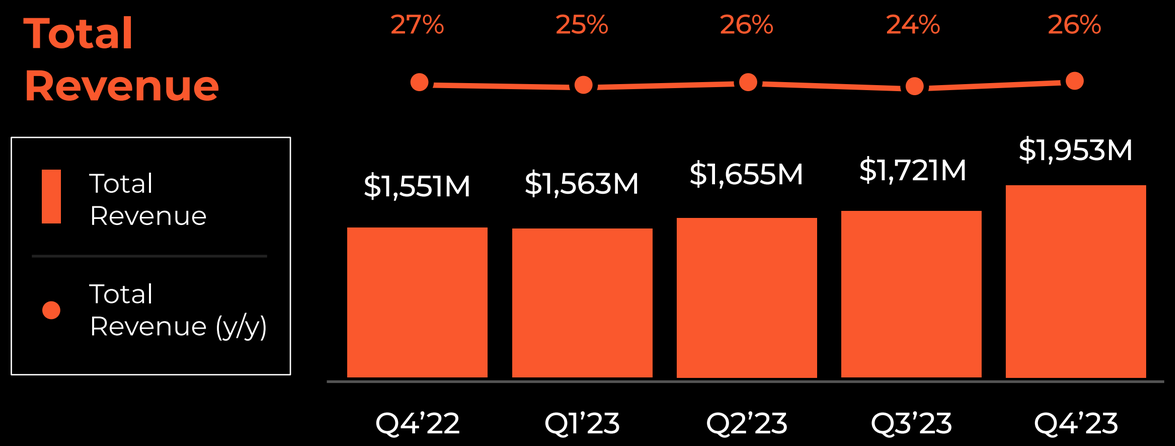
Driving efficiency and leverage

# Dipak Golechha

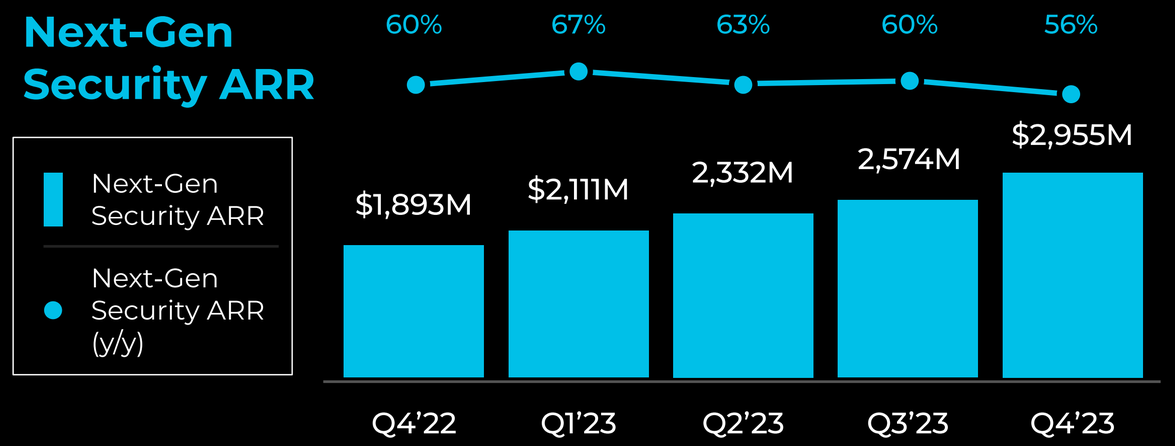
Chief Financial Officer

# Strong top-line growth at industry leading scale

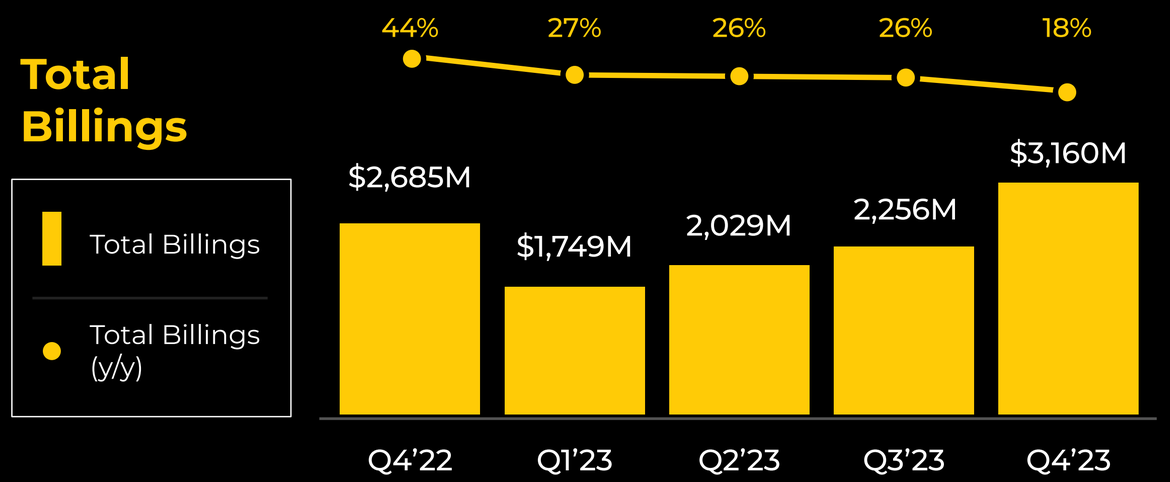
## Total Revenue



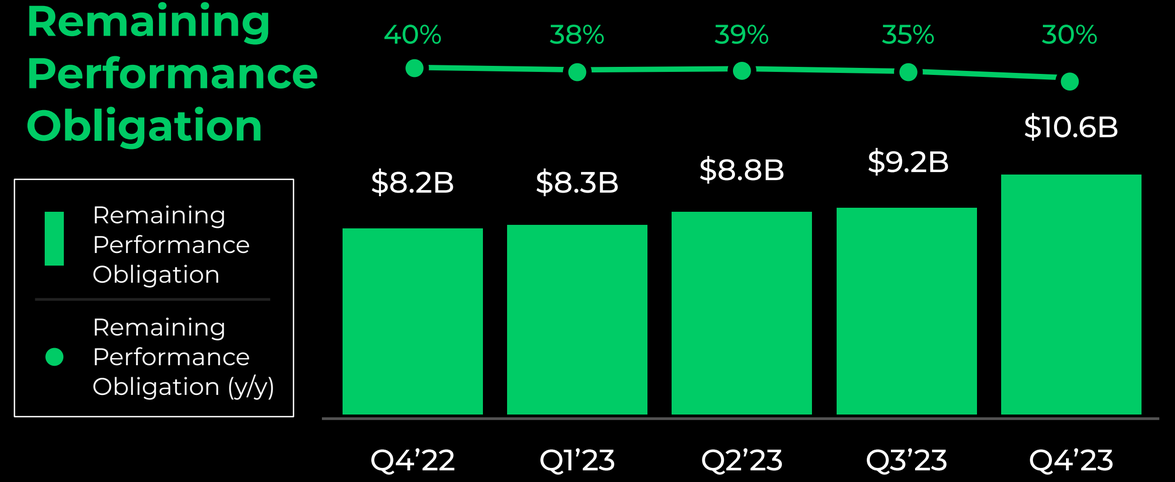

## Next-Gen Security ARR




## Total Billings



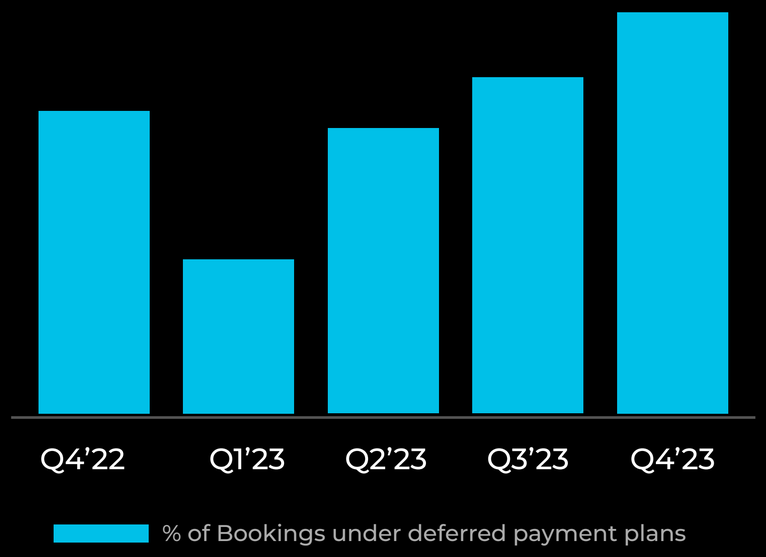

## Remaining Performance Obligation



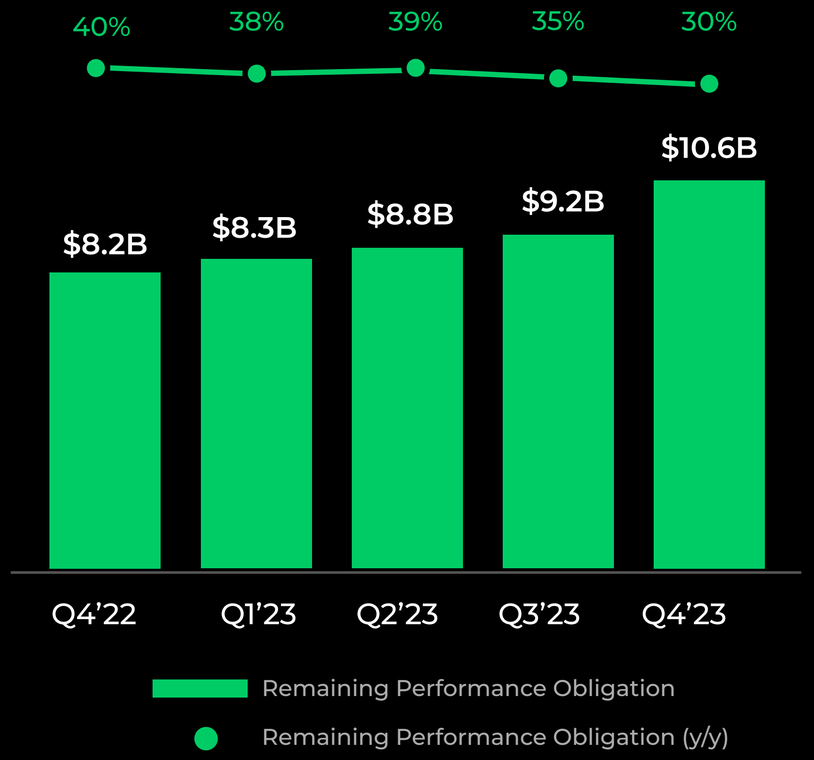

Fiscal year ending on July 31.

# Managing through the impact of the rising cost of money

## % of Bookings under Deferred Payment Plans [1]

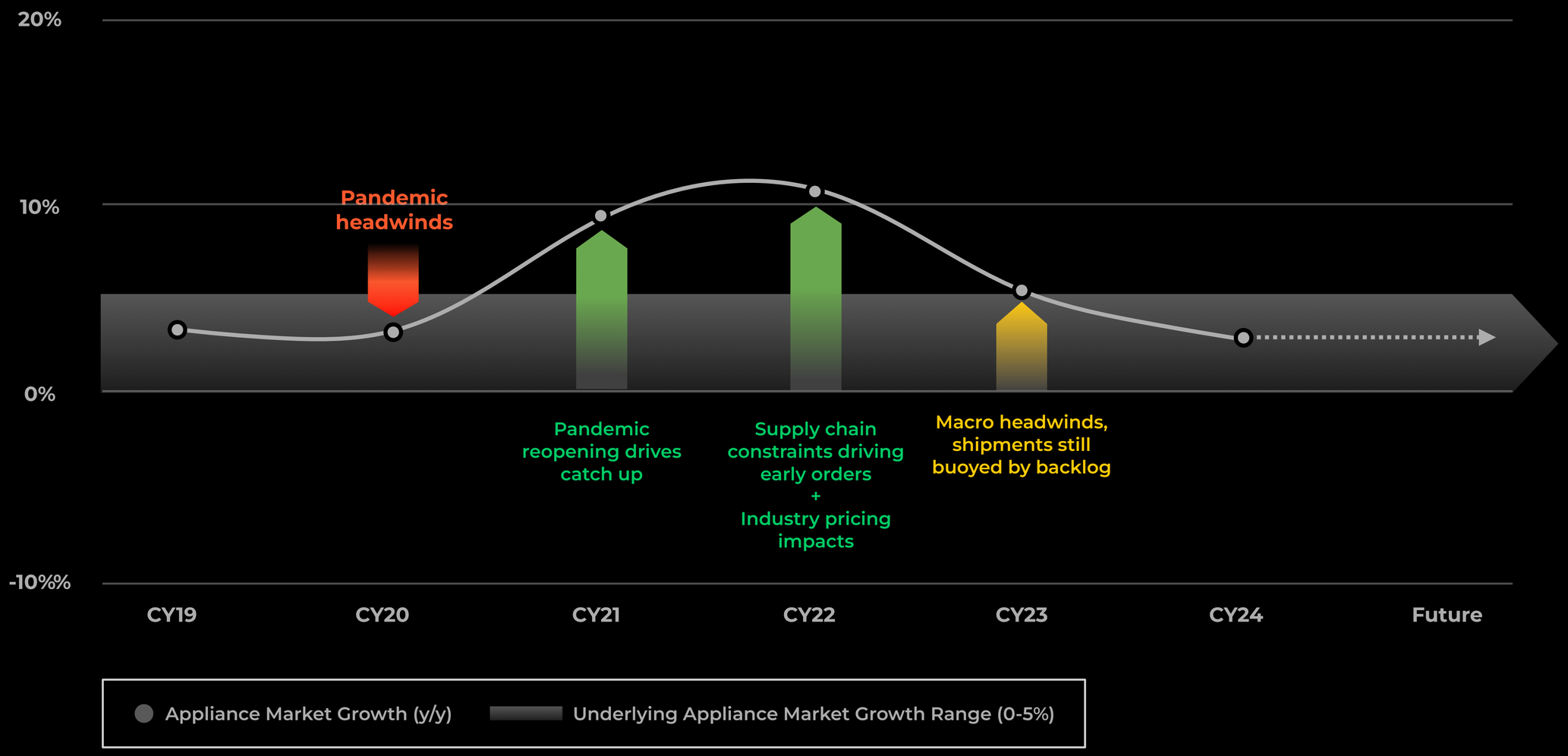



## Remaining Performance Obligation




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

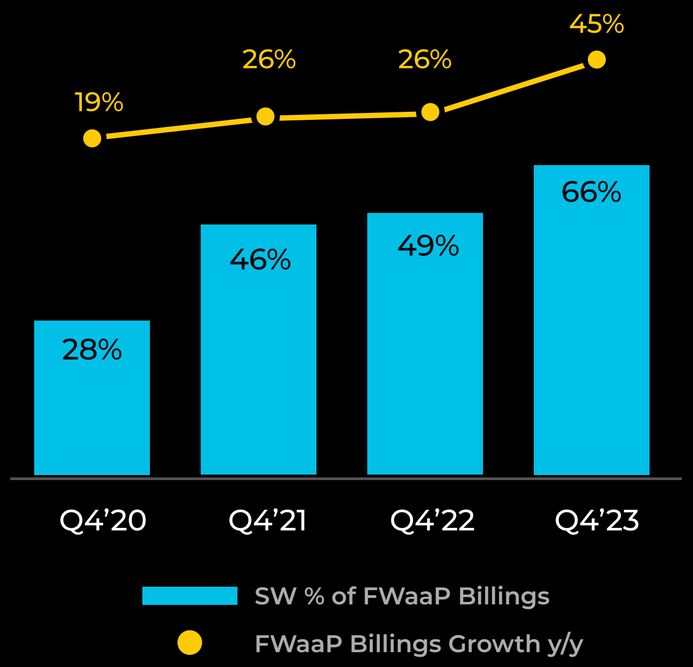
# Industry hardware growth trend is returning to expected baseline level



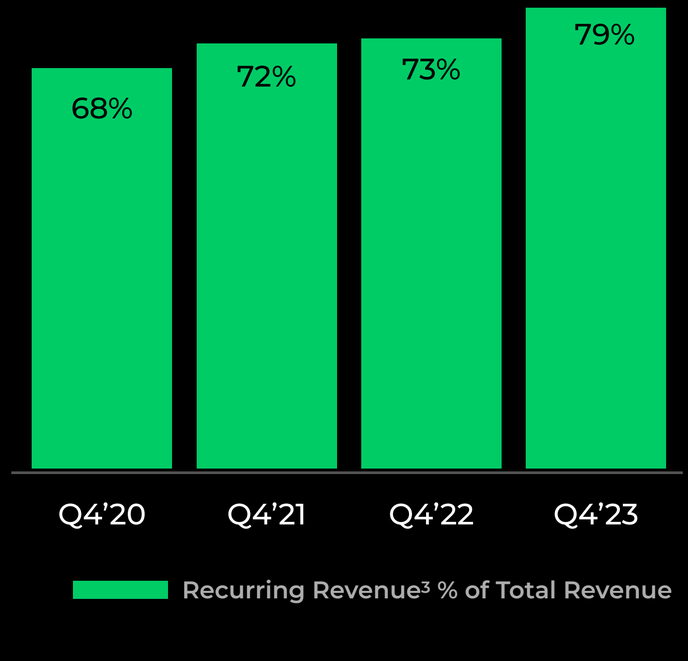

**Source:** Appliance growth rates from Omdia, Dell'Oro and Palo Alto Networks internal estimates. All data based on calendar year.

# Software transition and NGS growth is driving more recurring revenue

## FWaaP Billings Growth & SW as a % of FWaaP



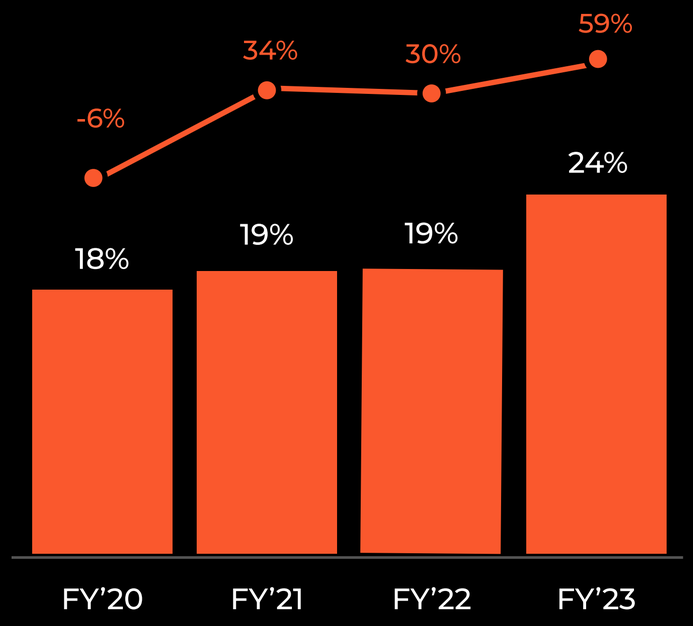

## Recurring Revenue as a % of Total Revenue



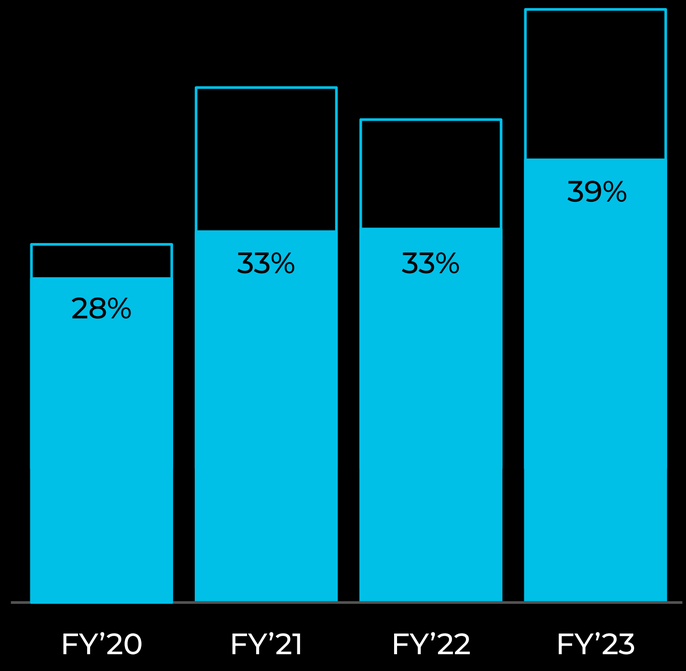

[1] Firewall as a Platform (FWaaP) billings is a key financial and operating metric defined as publicly reported product billings, together with the services billings for Prisma Access, VM-Series, and SD-WAN offerings, during the period stated.
[2] SW % of Total FWaaP billings is the billings for the 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

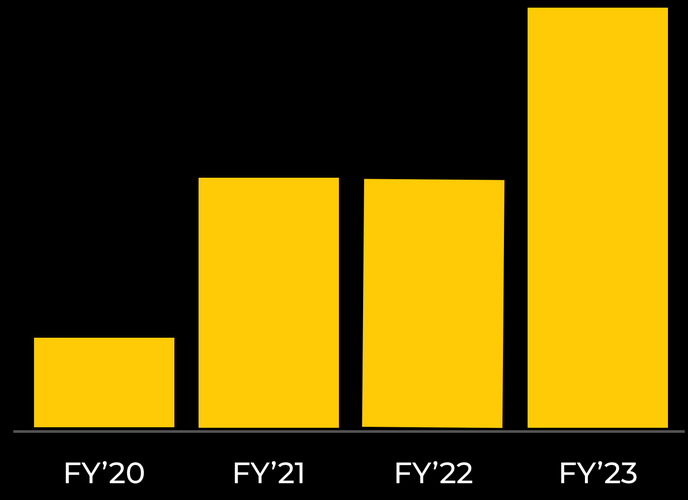
## Operating Income Growth & Margin (Non-GAAP)




## Fiscal Year Adjusted Non-GAAP Free Cash Flow Margin




## % of Bookings on Deferred Payment Plans[1]




[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** |

Reconciliations of historical non-GAAP measures can be found in the Appendix.
Fiscal year ending on July 31.

# Fiscal Year 2024 Guidance

| | FY 2023<br>Actuals | FY 2024<br>Guidance as of 8/18/23 |
|---|---|---|
| Total Billings | **$9.19B**<br>+23% yr/yr | **$10.9B - $11.0B**<br>+19%-20% yr/yr |
| Next-Gen Security ARR | **$2.95B**<br>+56% yr/yr | **$3.95B - $4.00B**<br>+34%-36% yr/yr |
| Total Revenue | **$6.89B**<br>+25% yr/yr | **$8.15B - $8.20B**<br>+18%-19% yr/yr |
| Op Margin (Non-GAAP) | **24.1%** | **25.0-25.5%** |
| EPS (Non-GAAP) | **$4.44**<br>+76% yr/yr | **$5.27 - $5.40**<br>+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<br>Guidance as of 8/18/23 |
|---|---|
| Total Billings | $2.05B - $2.08B<br>17%-19% yr/yr |
| Total Revenue | $1.82B - $1.85B<br>16%-18% yr/yr |
| EPS (Non-GAAP) | $1.15 - $1.17<br>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

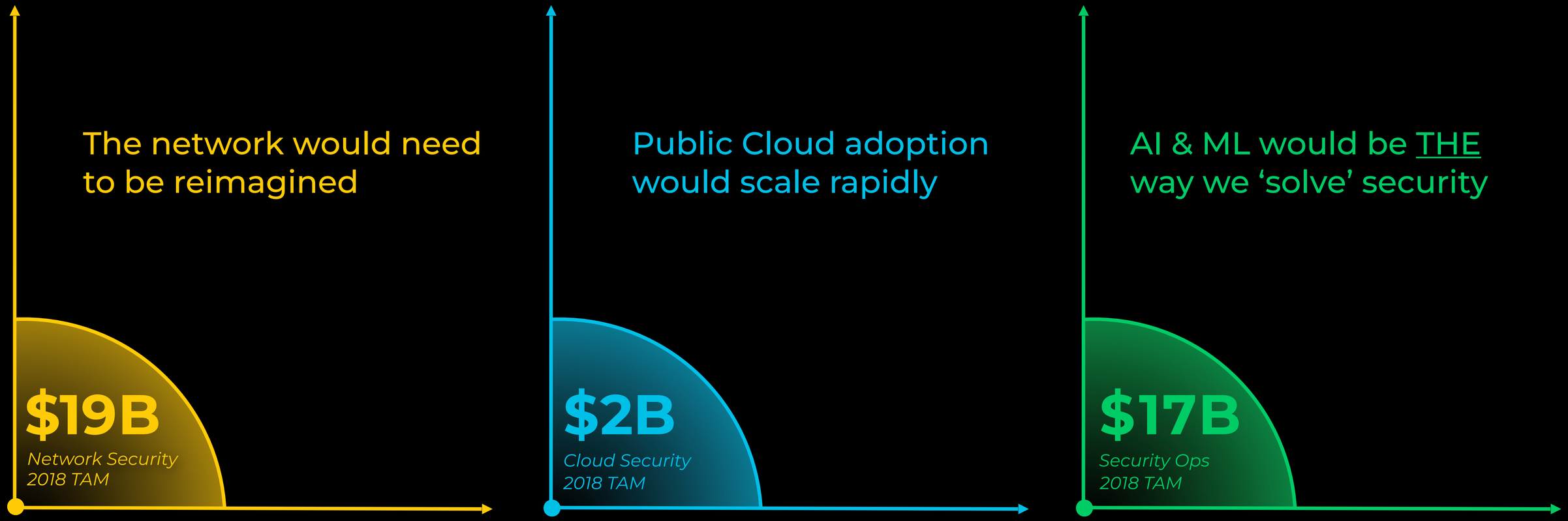
| TAM '23 ('18-'23 CAGR) | |
|---|---|
| **$29B** (35%) | **New segments**<br>SASE, Cloud Security, IoT Security |
| **$72B** (19%) | **Segments undergoing transformation**<br>Endpoint / XDR, SecOps (+SIEM), Network Security |
| **$31B** (13%) | **Largely steady segments**<br>Identity, App Security,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

**$213B**

**Note:** Communication services include Unified Communications, Mobile Network Services, Fixed Data, Fixed Voice ; Devices include Mobile Phones, Printers, Desktop, Laptops, and Tablets. Data Center includes Servers and external controller-based Storage. Application Software includes Enterprise Application Software and Vertical-Specific Software. Cybersecurity TAM excludes Integrated Risk Management.

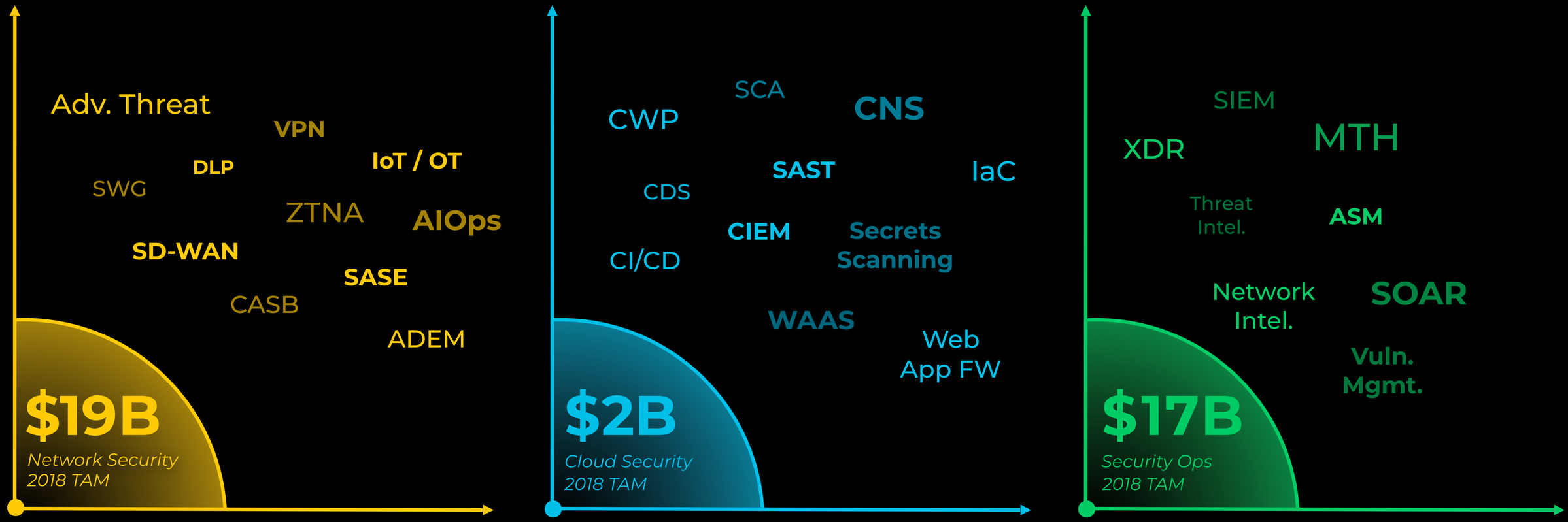
**All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.**

# Looking back, we envisioned three transformations



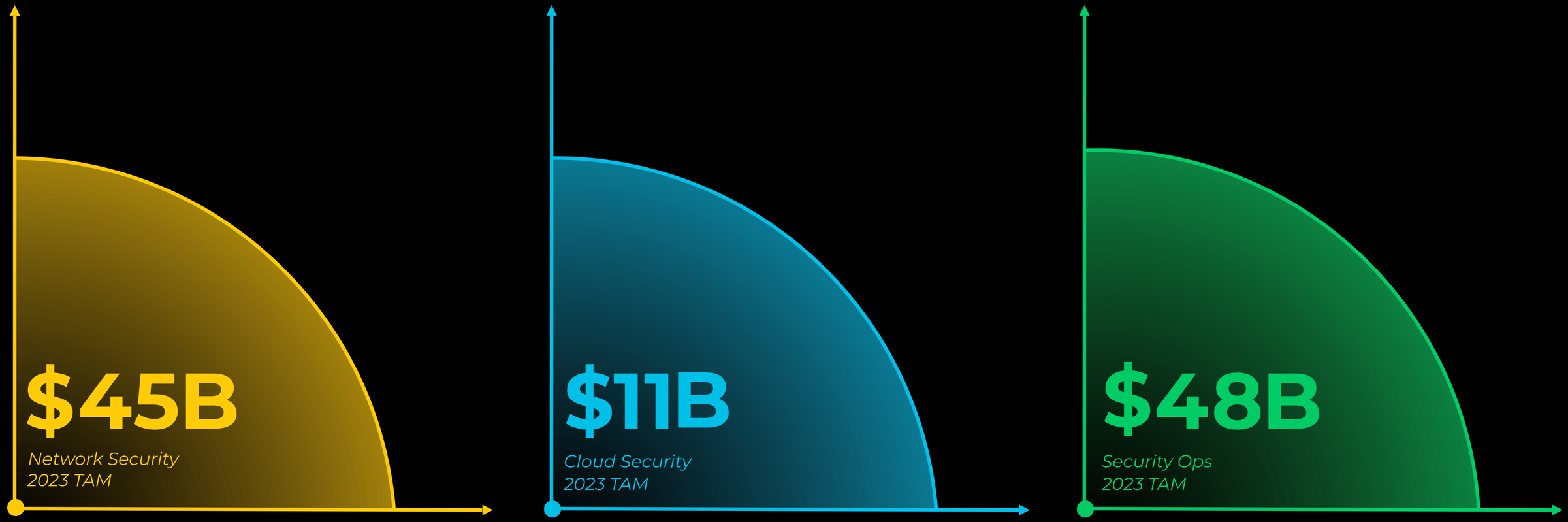

**Note:** the size of the bubbles in the chart is not adjusted to scale

# These transformations ended up driving rapid growth in cybersecurity




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

# These transformations ended up driving rapid growth in cybersecurity




**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

**20+** Industry Recognitions

Made **Innovation** the lifeblood of our multi-product business

**180+** major releases since FY19

Executed **“Build & Buy”** strategy to become the largest cyber player

**~3.5x** Market Cap growth[1]

[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


**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

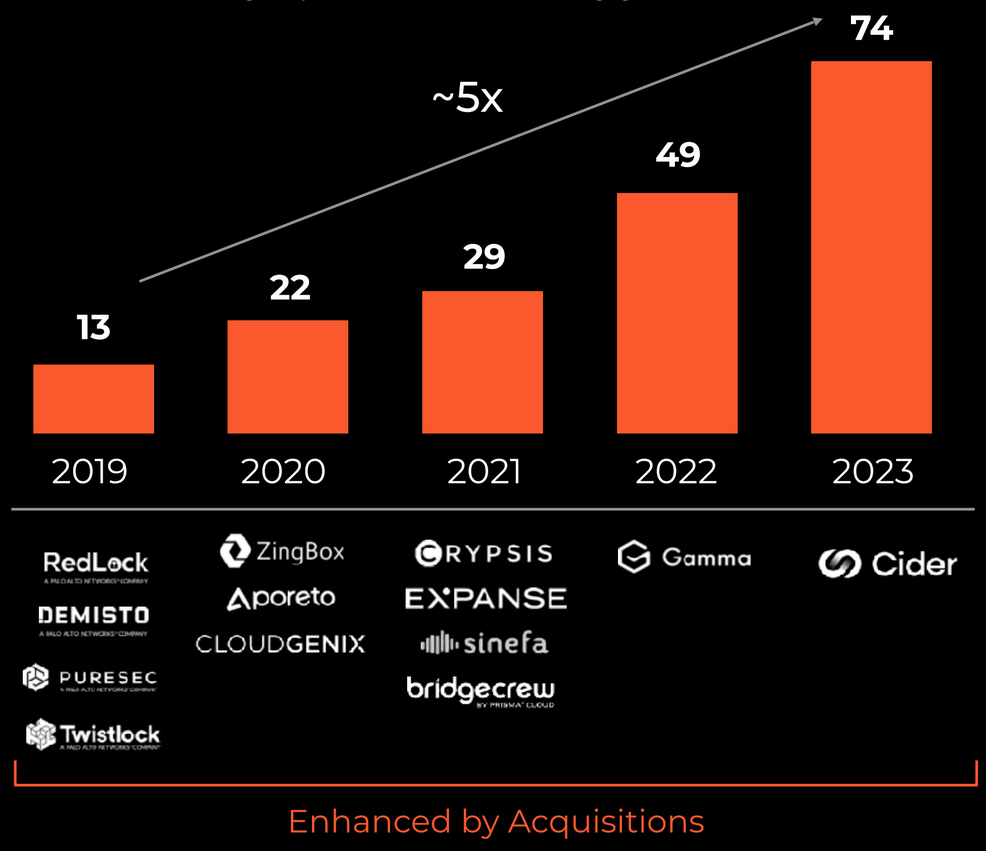
# Our strategy to win

- 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

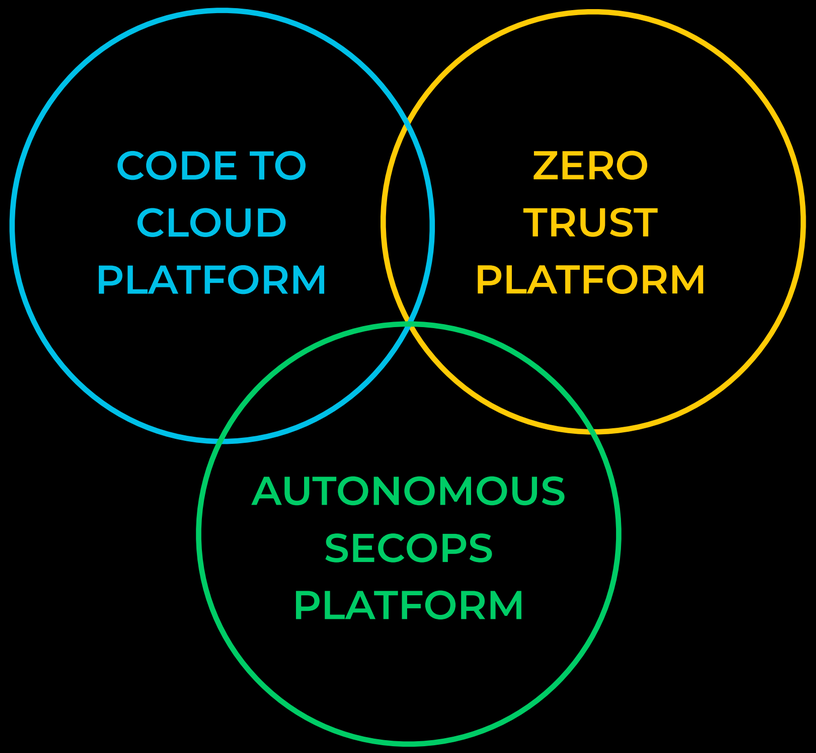



Enhanced by Acquisitions

## …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

# 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 [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

[1] Refers to active customers as of 08/07/2023

# 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

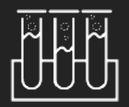
Relentless innovation across all 3 platforms

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

# 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

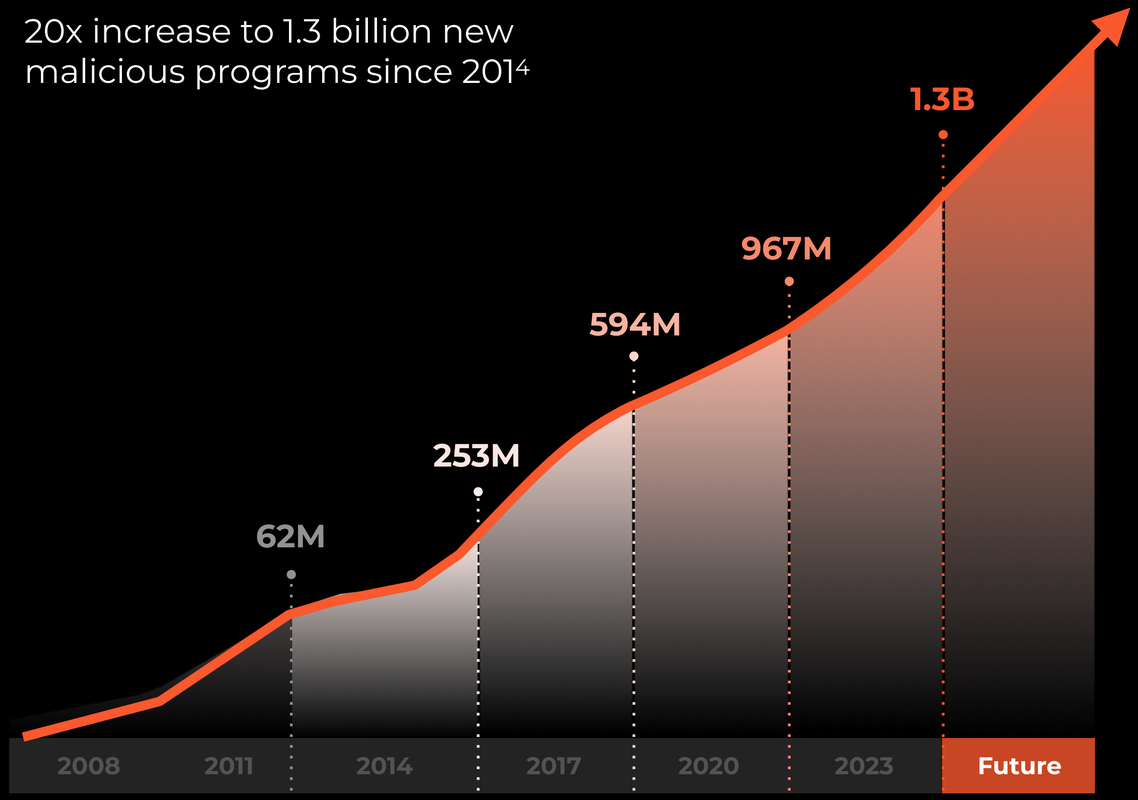
Automated attacks executed across regions within 1 hour of initial compromise [2]

>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

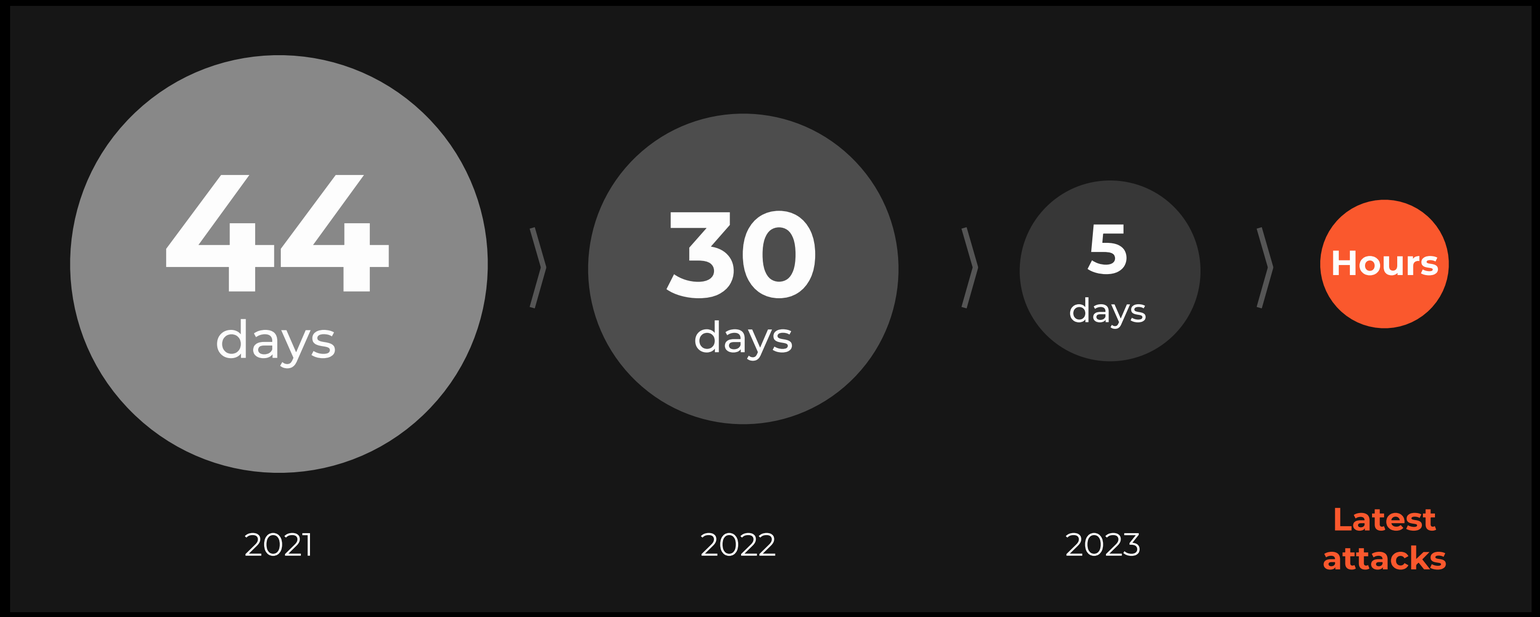
20x increase to 1.3 billion new malicious programs since 2014 [4]




**Sources:**
[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/;
[2] Unit 42 research: https://unit42.paloaltonetworks.com/purpleurchin-steals-cloud-resources/;
[3] https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf
[4] https://portal.av-atlas.org/malware.

# Attacks are happening faster than organizations can respond

## Average Days from “Compromise” to “Exfil” [1]




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”

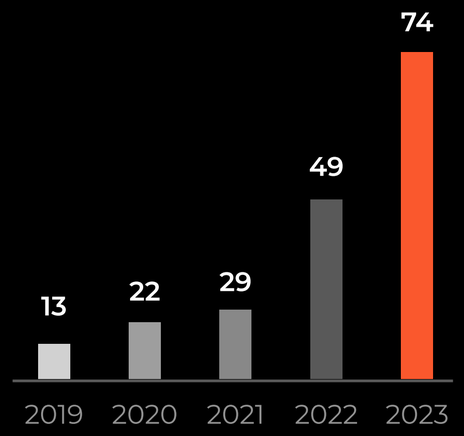
$10.5T[1] cybercrime “market” in 2025

**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




Major releases per fiscal year

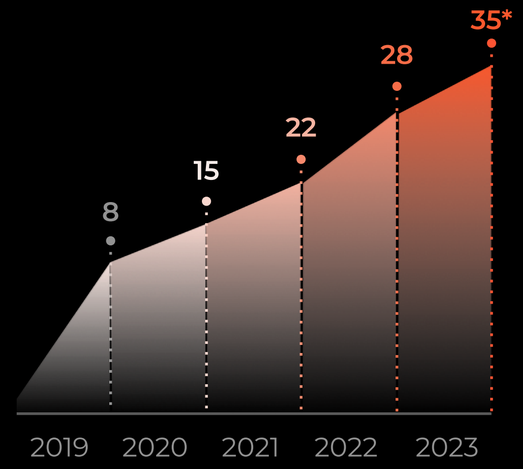
## While leveraging the broader market

Continuously identifying great tech
to include in our journey


Private cybersecurity companies
evaluated annually

## Embracing AI from the early days

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




Cumulative number of Palo Alto Networks
products that use AI

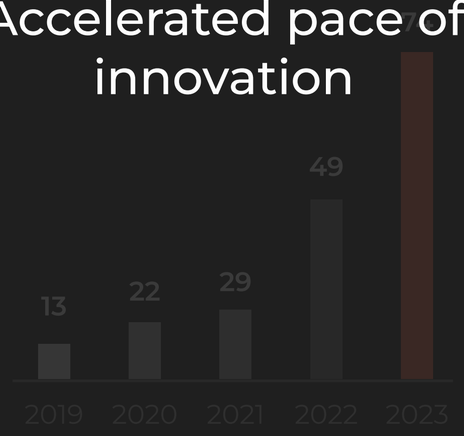
**Some still in development*

# 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

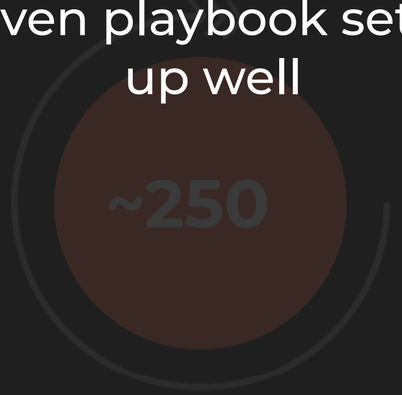



Major releases per fiscal year

## While leveraging the broader market

Continuously identifying great tech
to include in our journey

### Proven playbook sets us up well

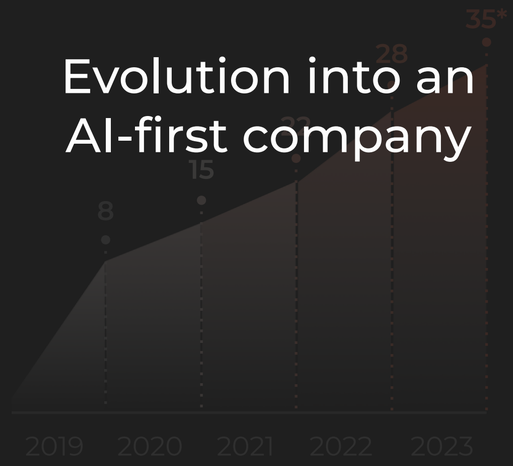



Private cybersecurity companies
evaluated annually

## Embracing AI from the early days

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

### Evolution into an AI-first company




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

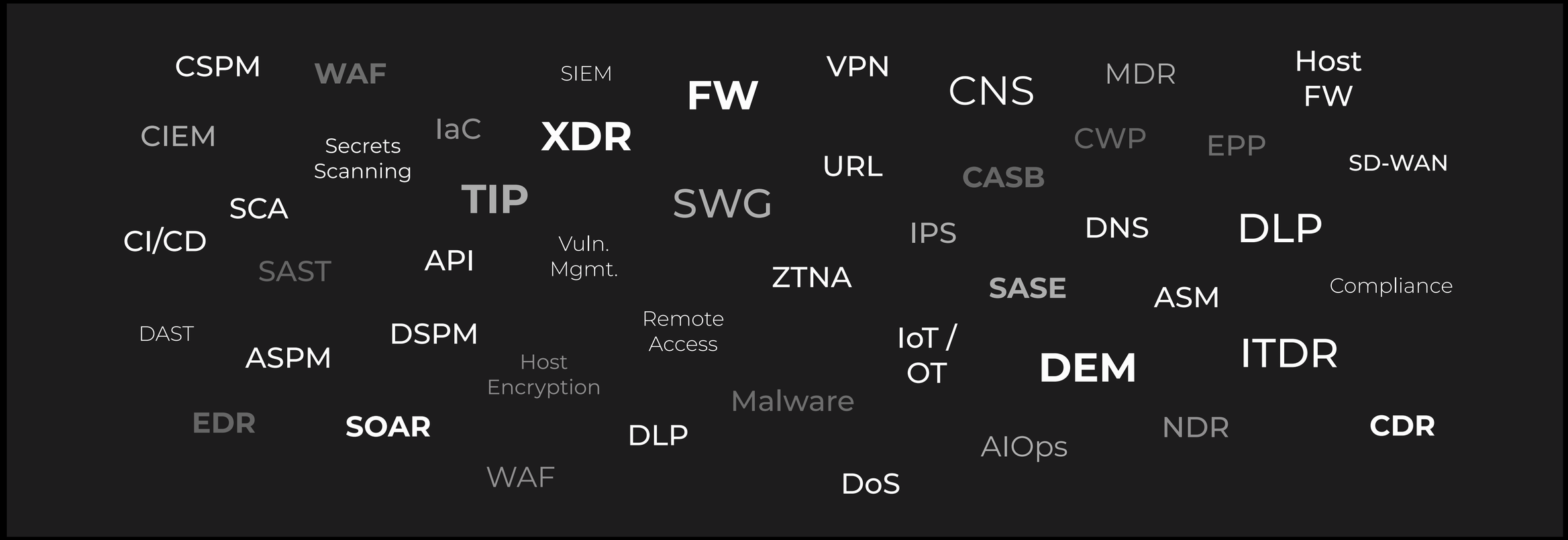
# The industry approach leads to point product proliferation

**~$210B**

to “solve” the problem

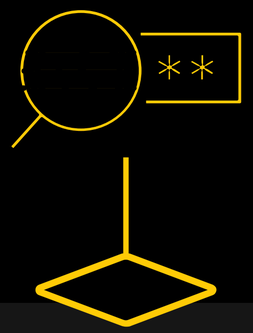
**Source:** All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.

# The industry approach leads to point product proliferation



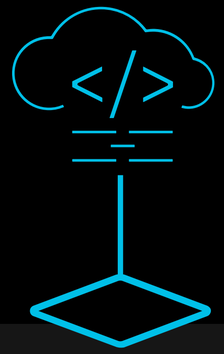

**Source:** All estimates and figures in this presentation related to total addressable markets or market sizes are based on Palo Alto Network estimates using third-party data. See Appendix for more information.

# Only a platform approach will work



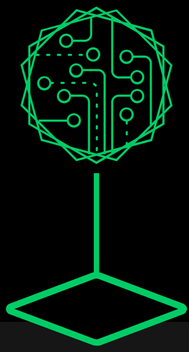
## Zero Trust Platform

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

# 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

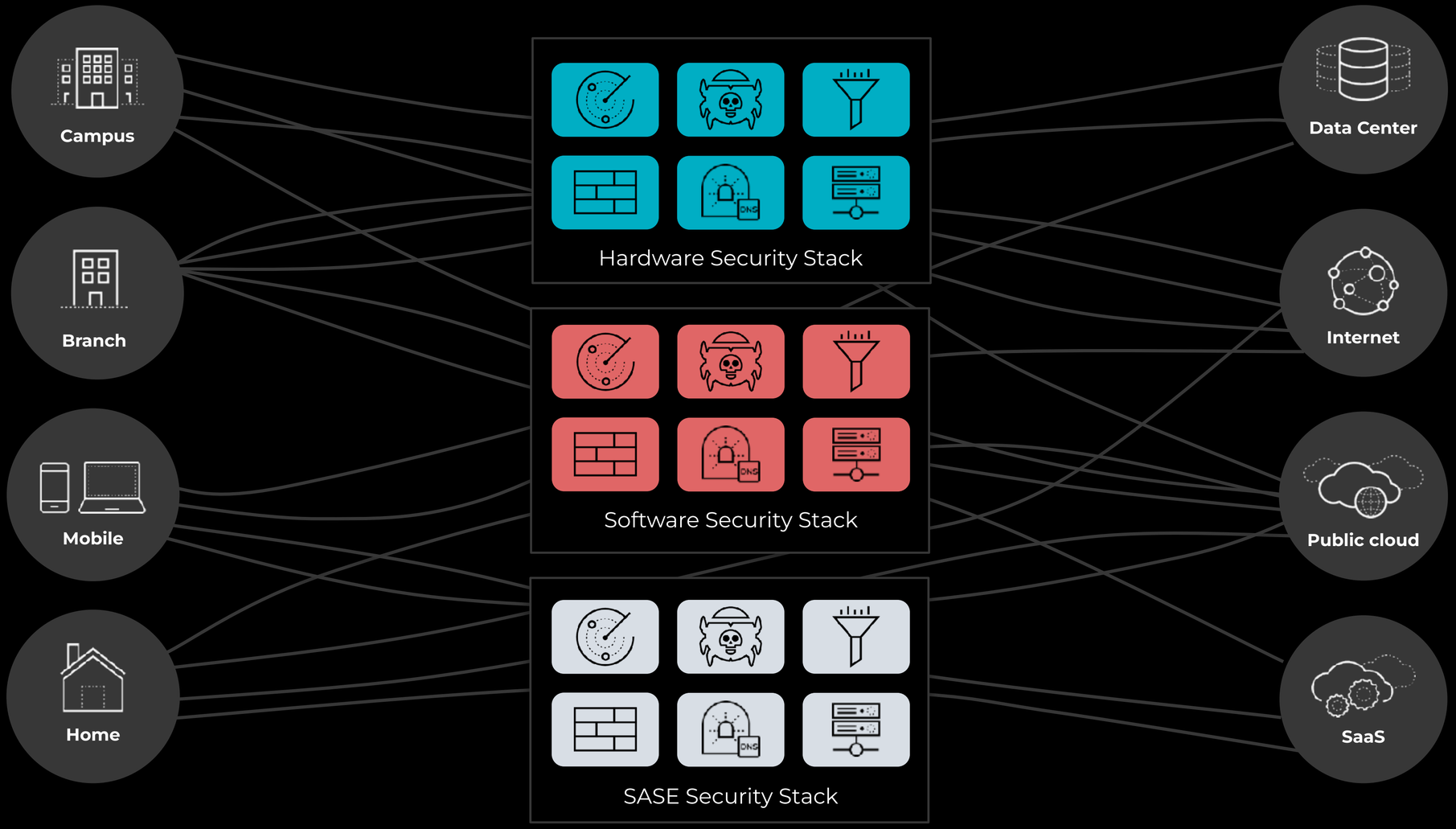
Great user experience across self-healing network

Single pane of glass for network and security

**Our opportunity as TAM grows to ~$80B by 2028[1]**

**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

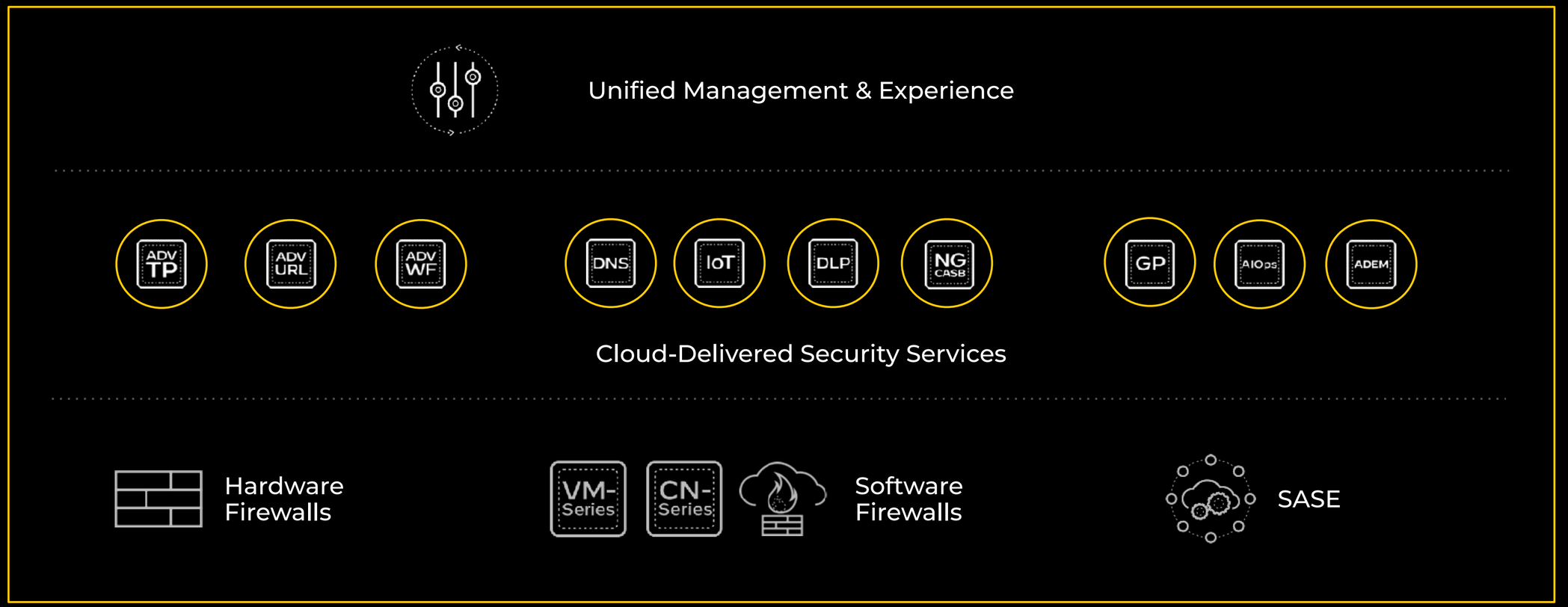


# What if we could take a radically new approach?


**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



# Best-in-class form factors — Hardware, Software and 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**

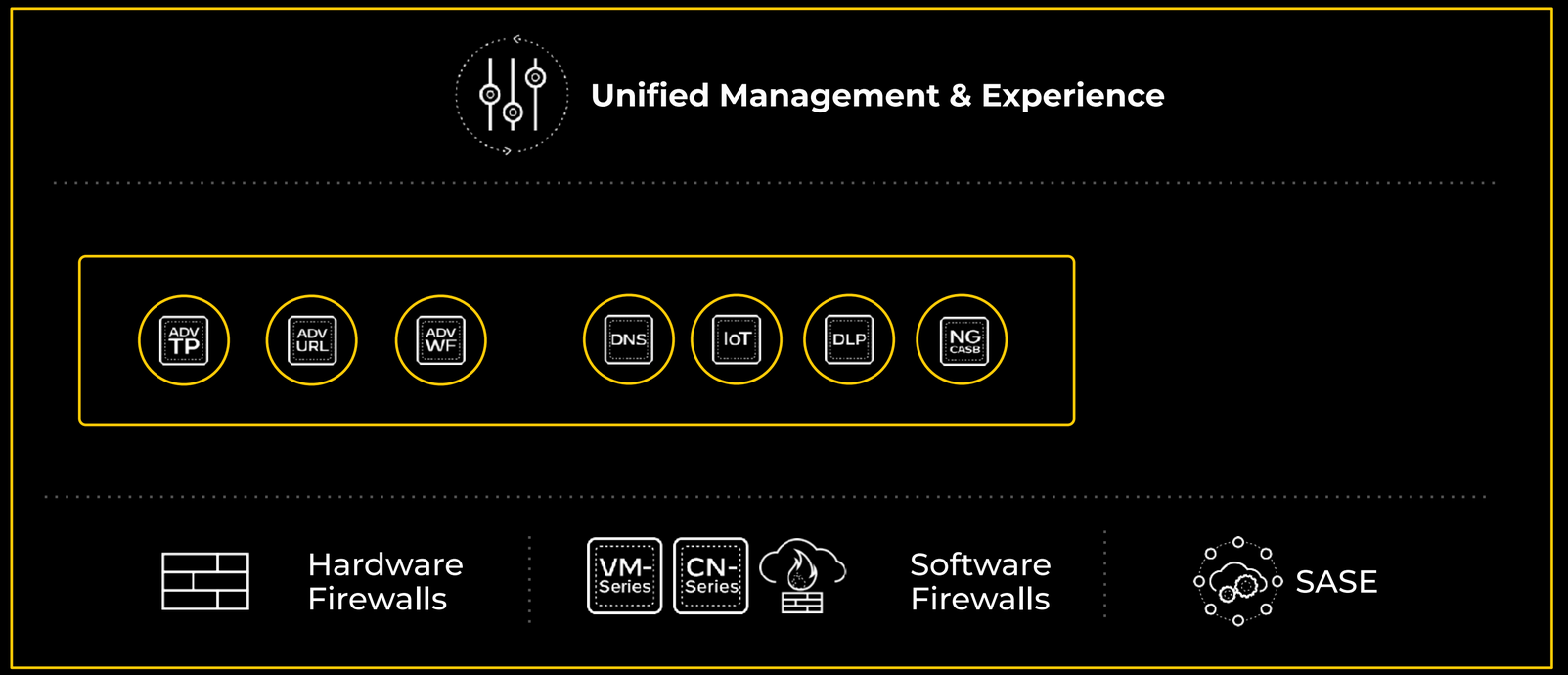
A **Leader** in Gartner Magic Quadrant WAN Edge Infrastructure [4]

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.

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




**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

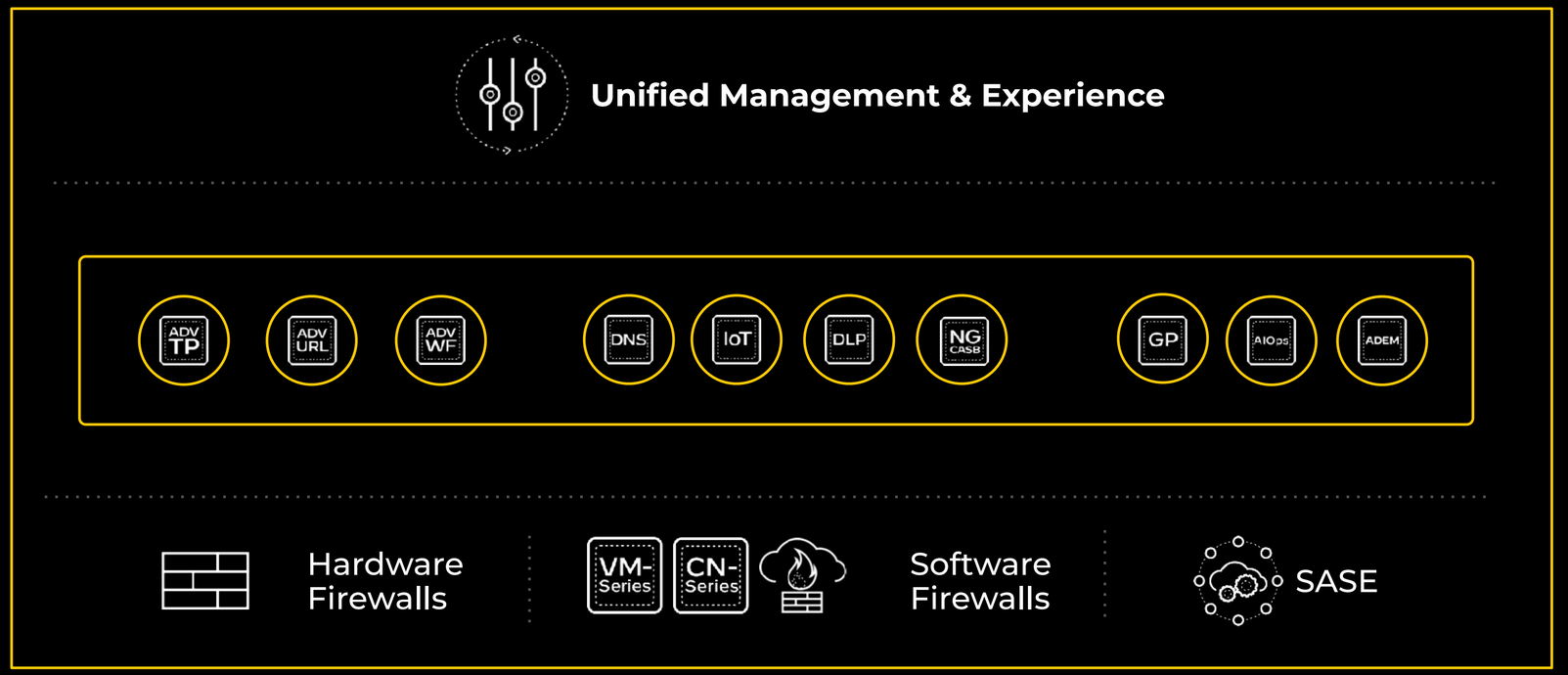
**IOT**

**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




**GlobalProtect**

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

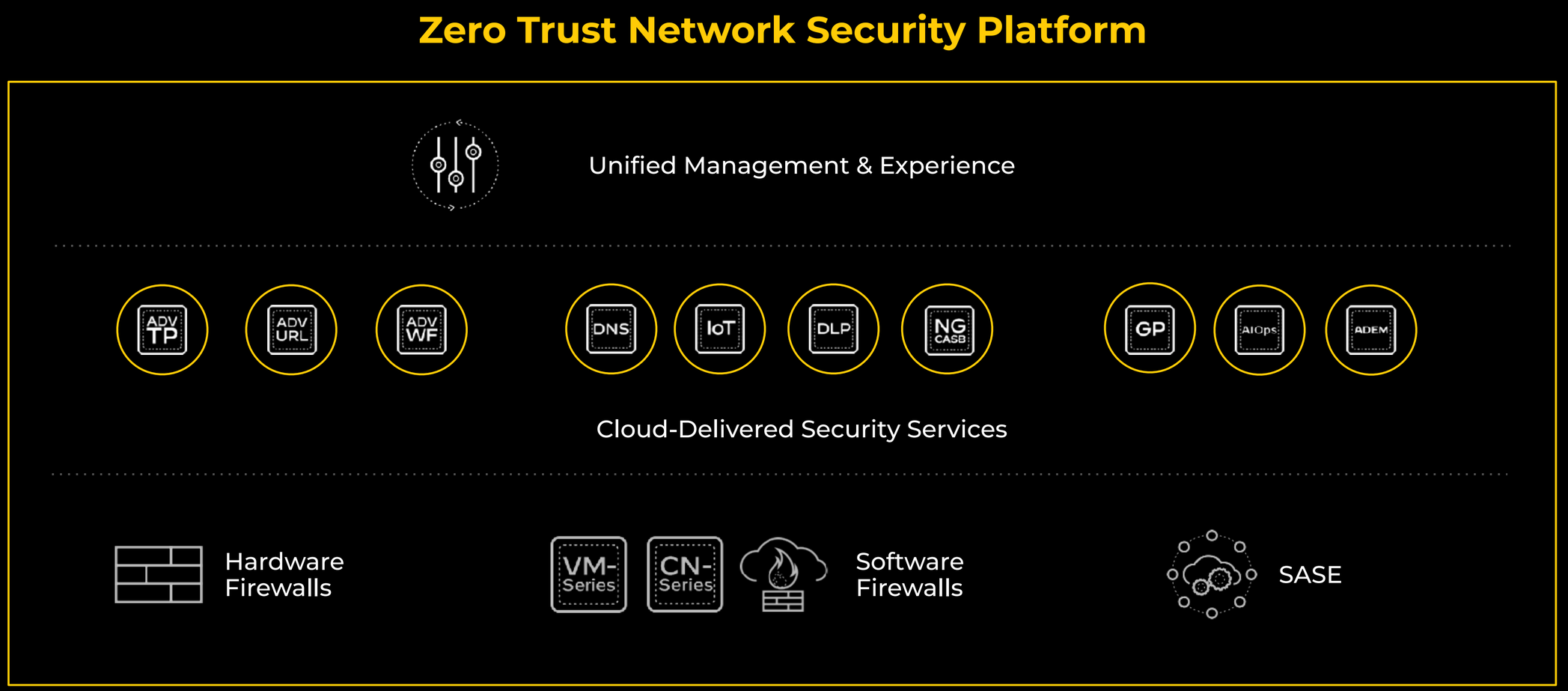
**AIOps**

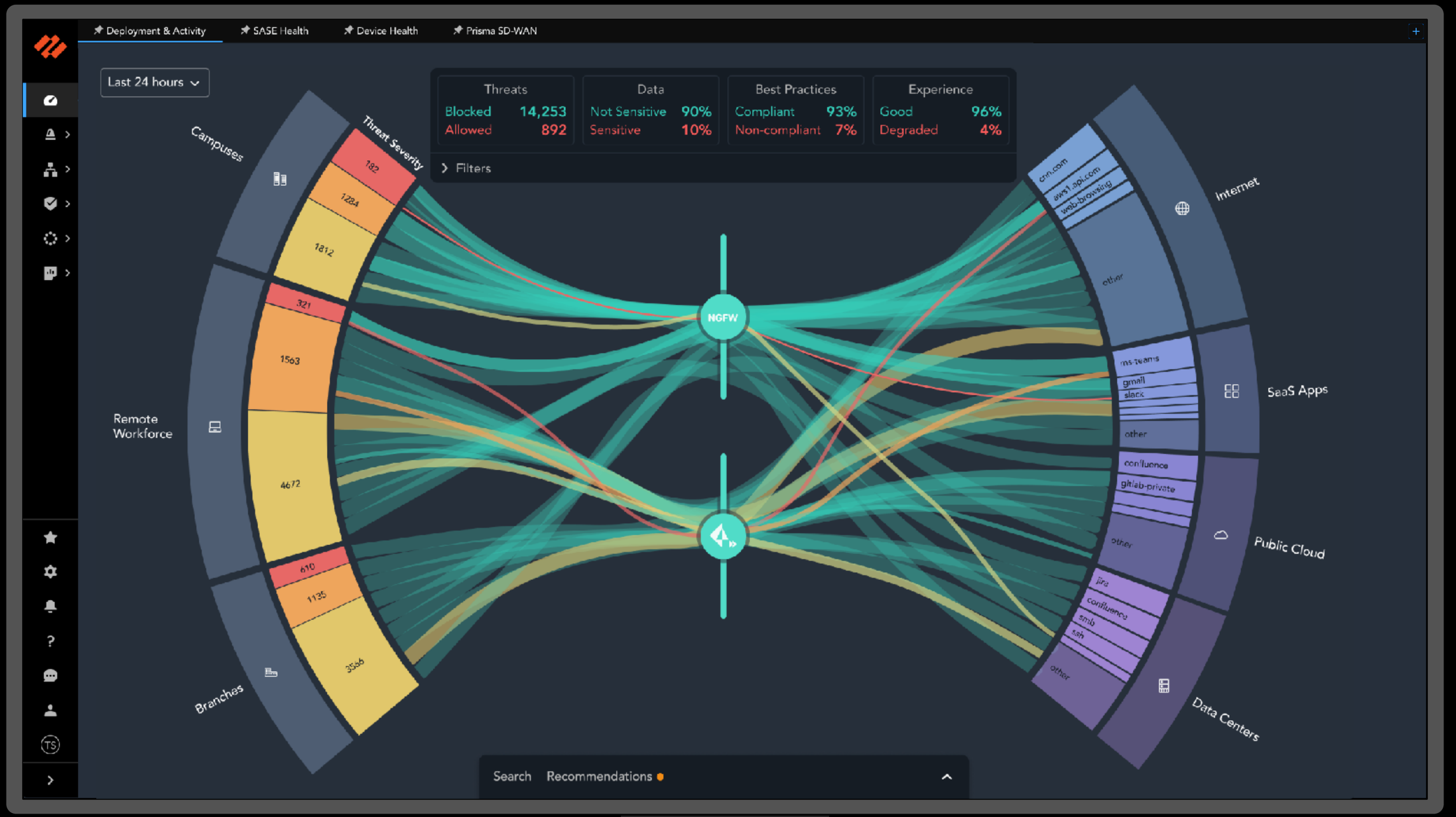
Predict **51%** of network disruptions before any customer impact

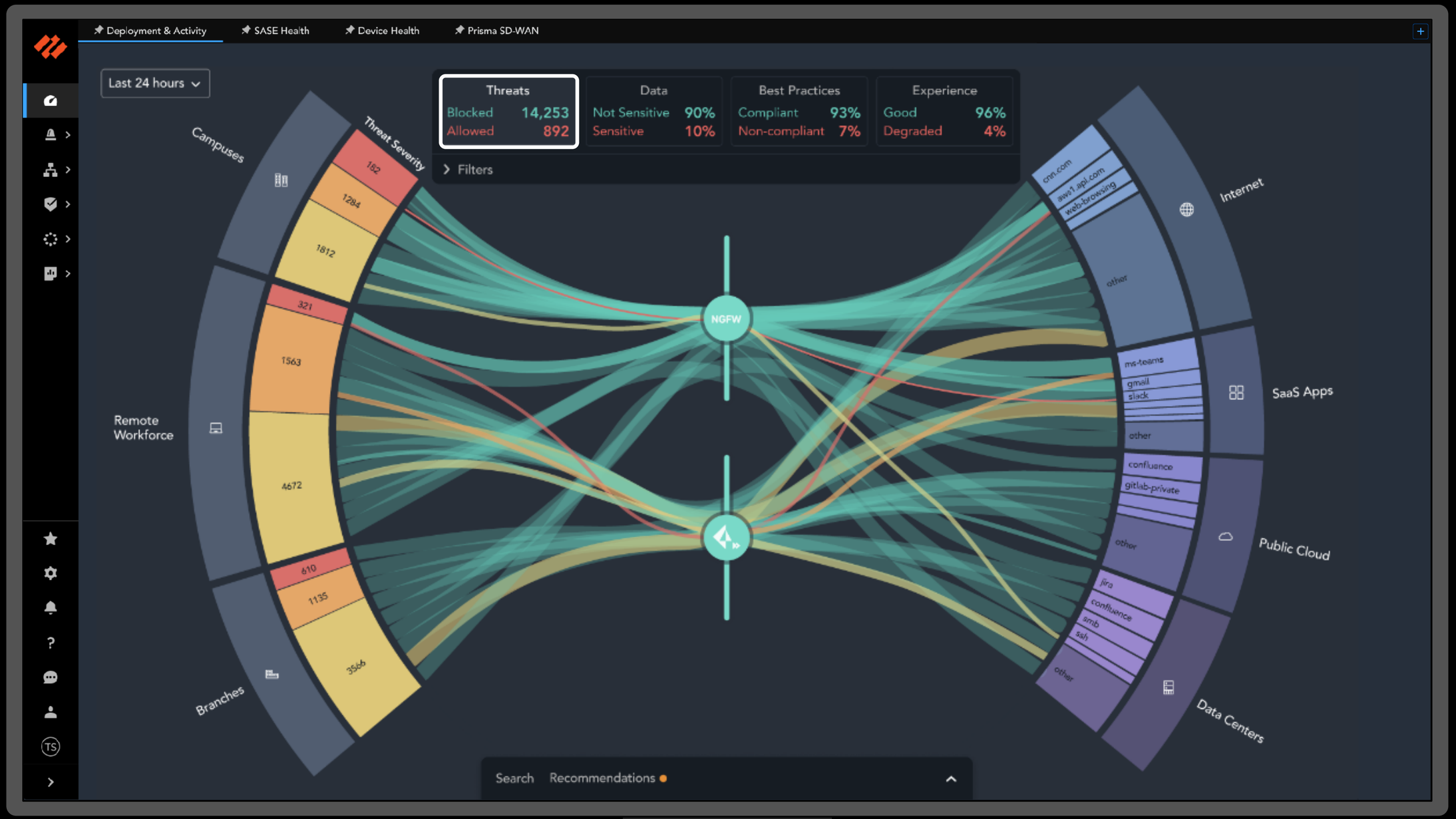
**ADEM**

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

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

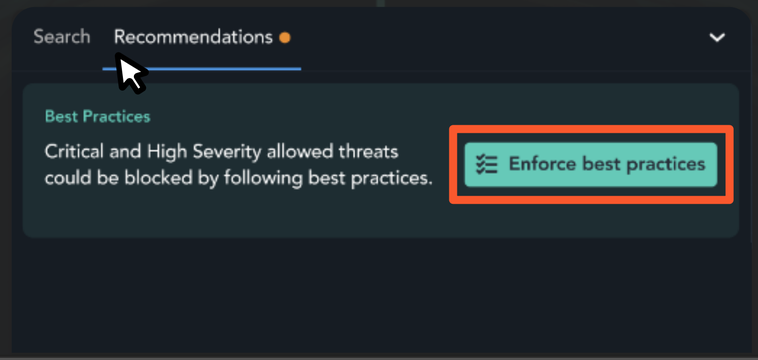




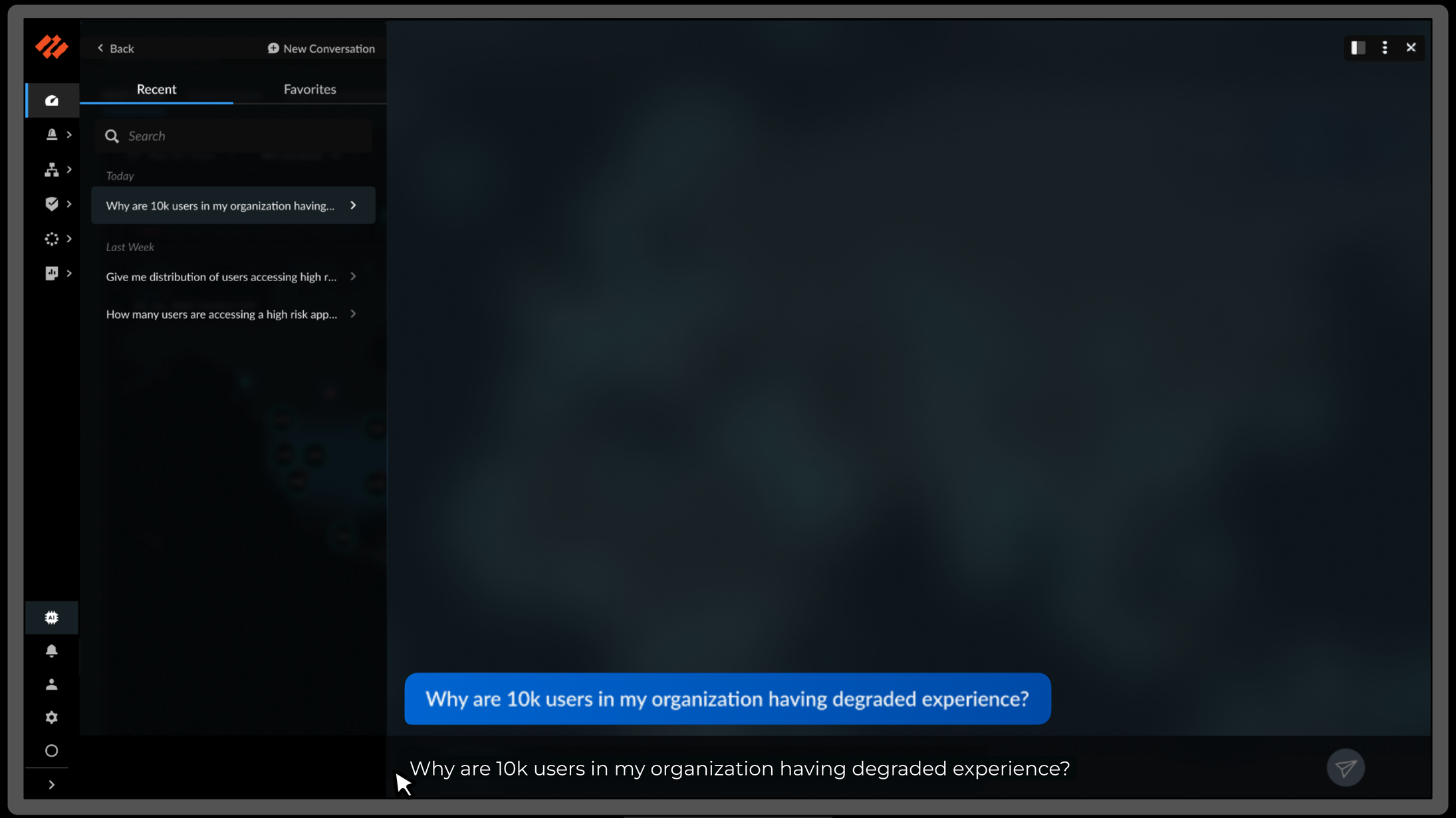


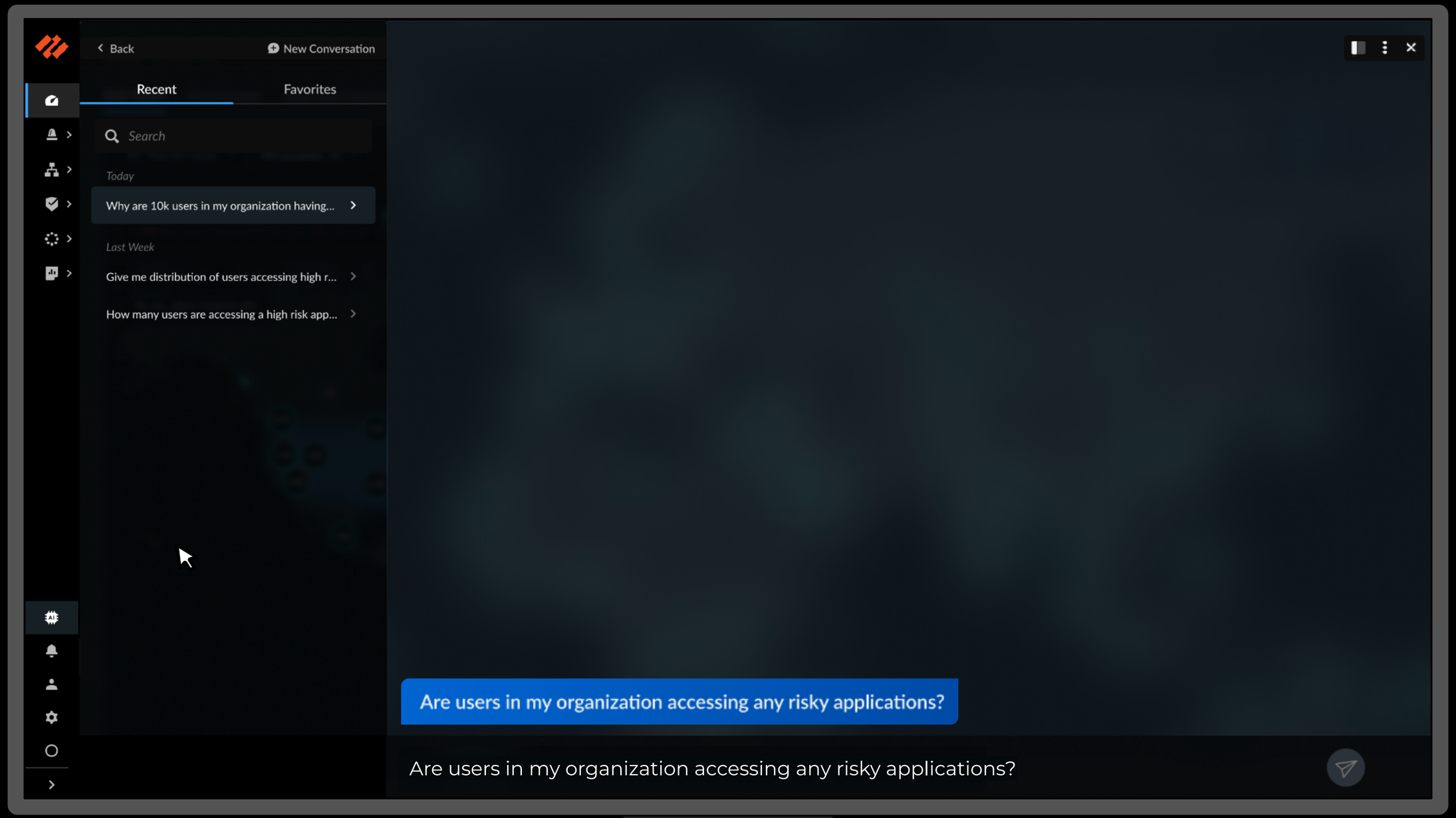
Is my environment impacted by
**CVE-2022-31706?**

# Guided remediation to secure against threats with “one click”



# Network Security Copilot





Back | New Conversation

Recent | Favorites

Search

Today

Are users in my organization accessing any ris...

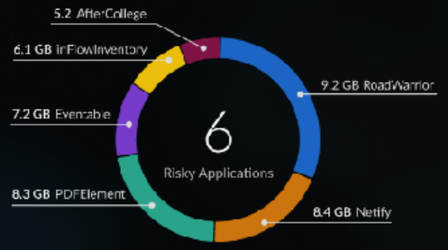
Why are 10k users in my organization having...

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 |

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?

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 |

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?

Type your question here

Back | New Conversation

Recent | Favorites

Search

Today

Are users in my organization accessing any ris...

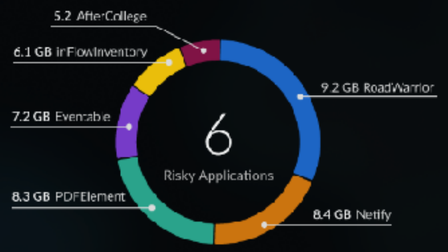
Why are 10k users in my organization having...

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 |

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.

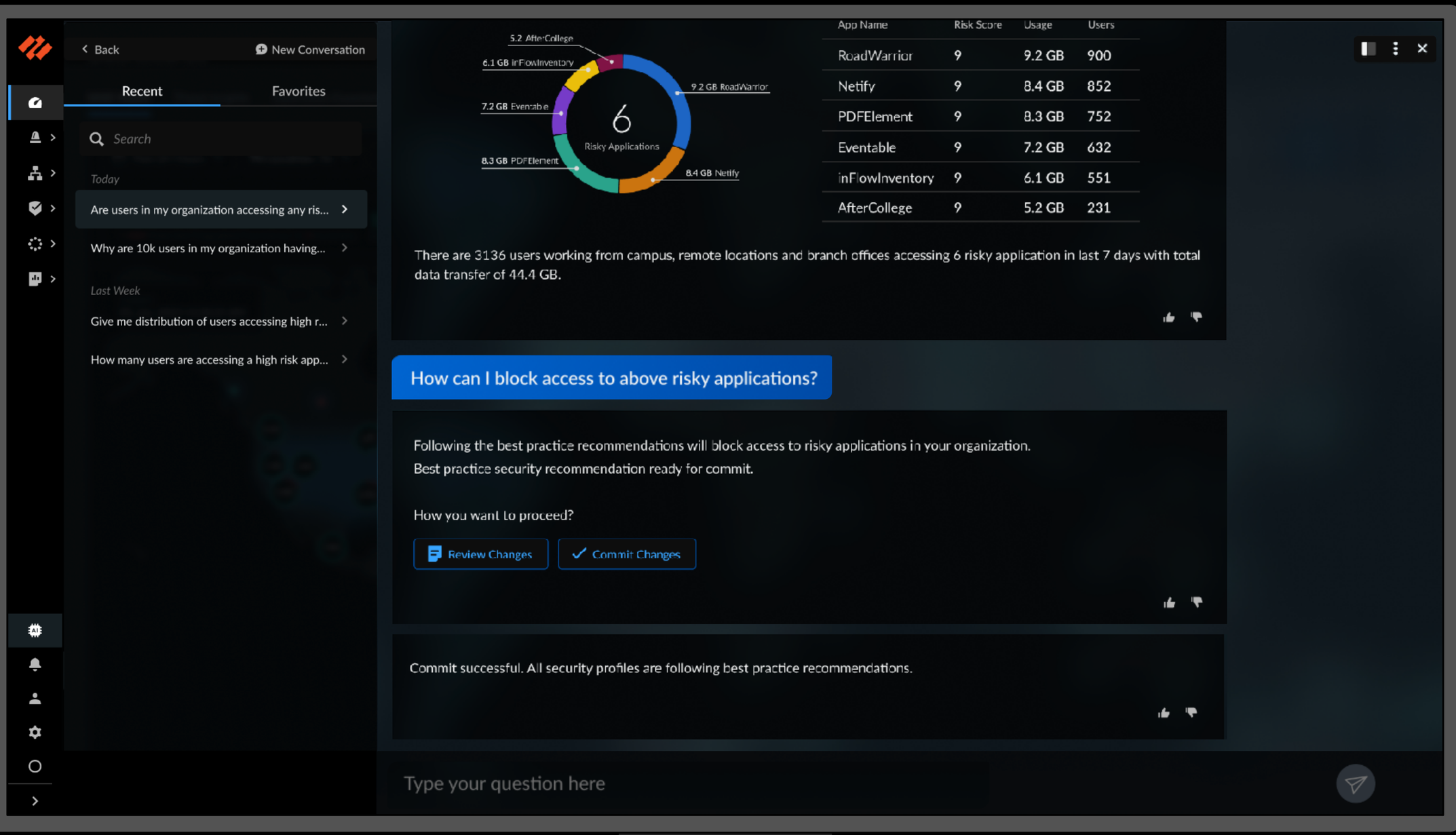
## How can I block access to above risky applications?

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

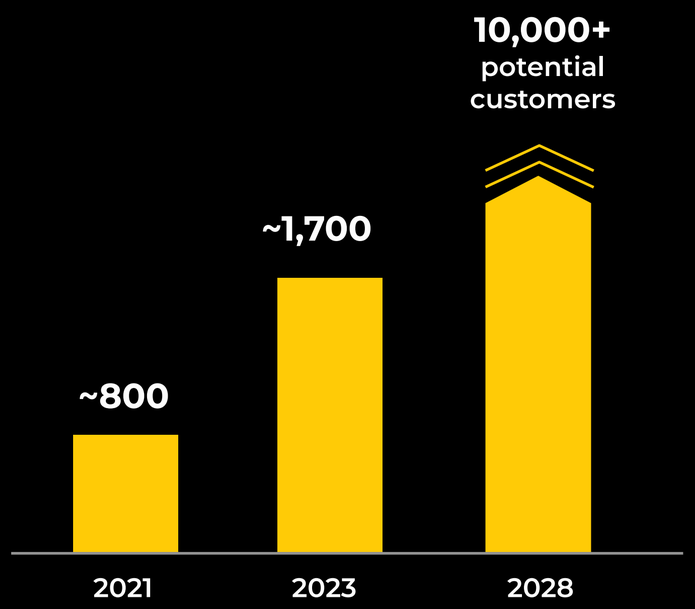
How you want to proceed?

Review Changes | Commit Changes

Type your question here

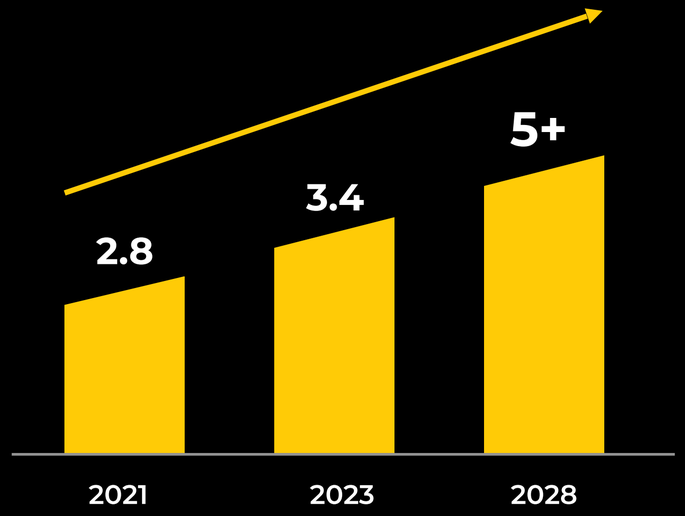


# The opportunity ahead




Customers with full network security platform

Uniquely positioned to deliver Enterprise wide Zero Trust




# 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

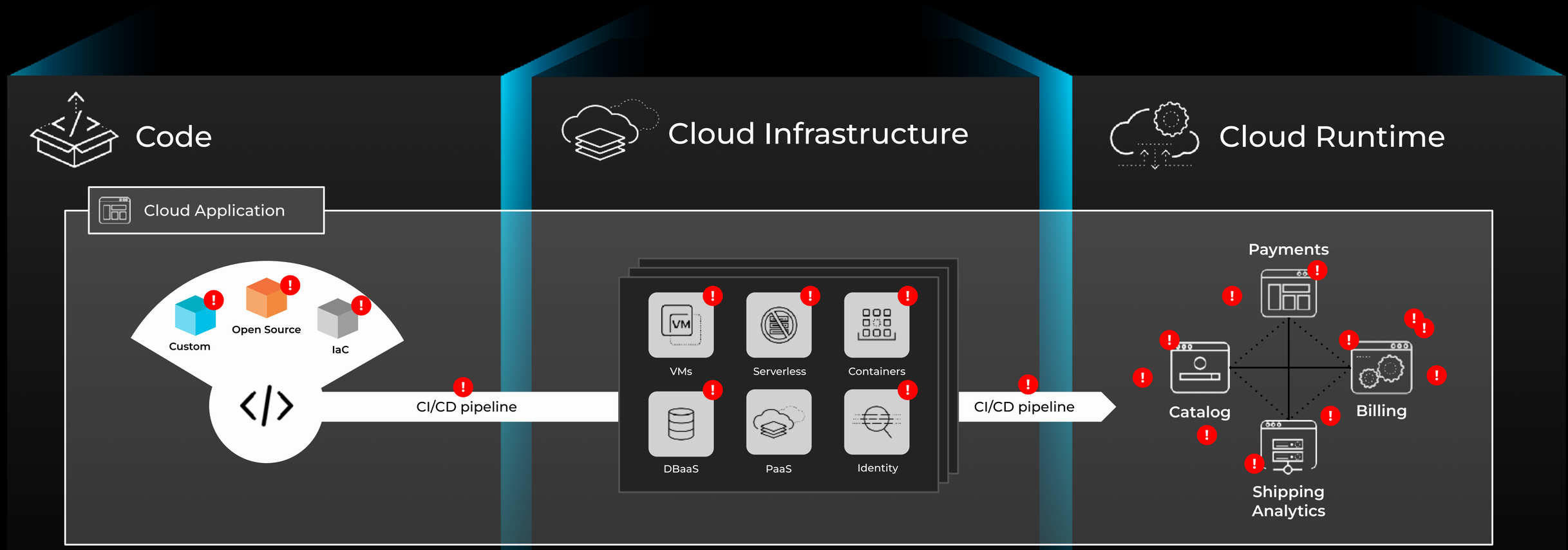
Preventing Breaches in Cloud and Fixing at the Source represents a ~$40B TAM in 2028

## Our opportunity: Deliver a AI-driven cloud security platform

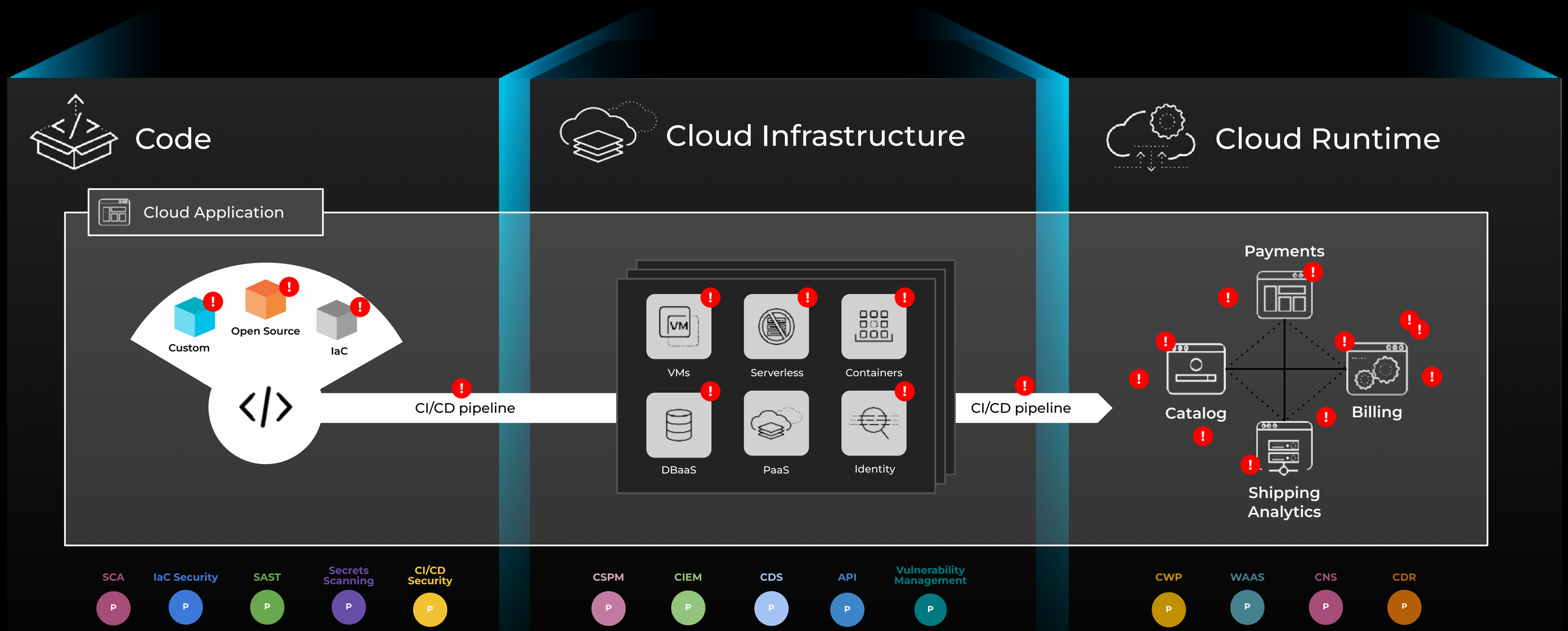
**Sources:**
[1] IDC FutureScape;
[2] State of the Developer Nation report, SlashData;
[3] ESG 2023 Technology Spending Intentions Survey of 742 enterprises; Worldwide IT Industry 2020 Predictions;
[4] Forrester, The Software Composition Analysis Landscape, Q1 2023.

# Cloud applications are assembled in multiple stages

# Security risks multiply across the application lifecycle

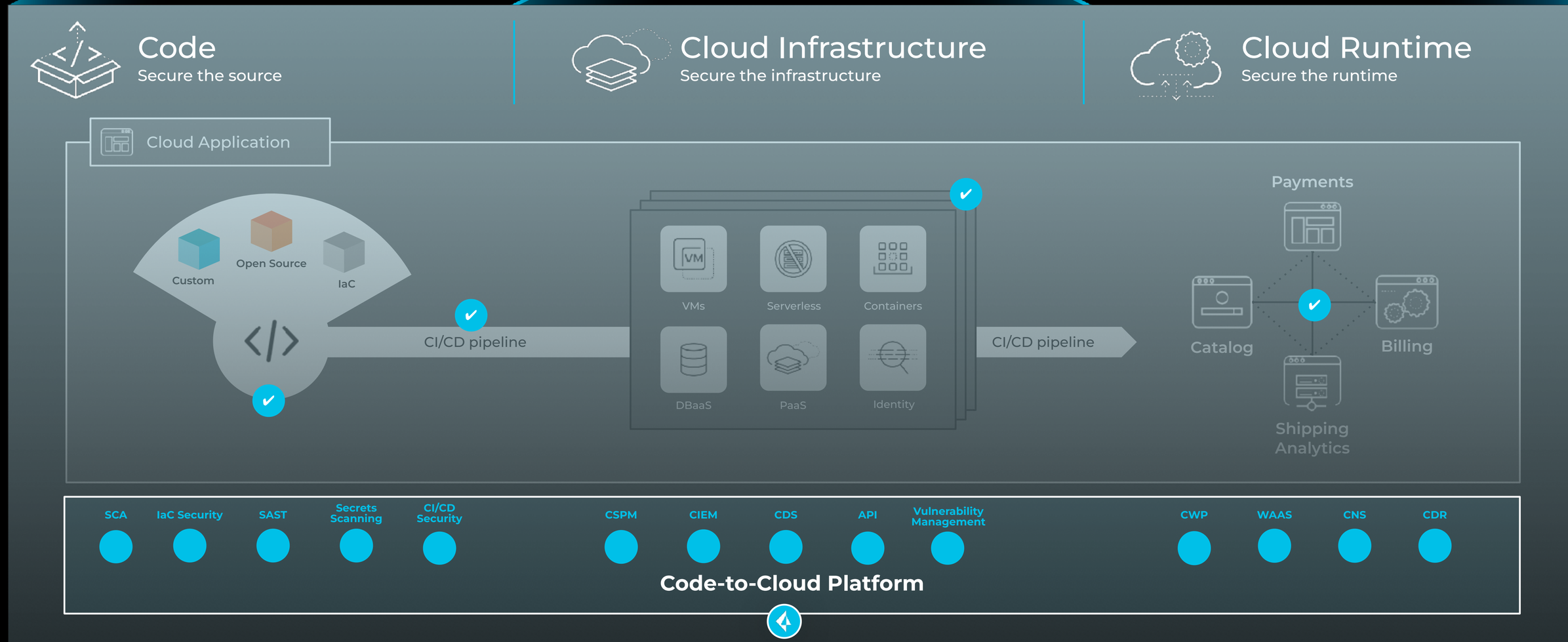


# Security risks go unaddressed as the industry delivers multiple point products



# 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

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**

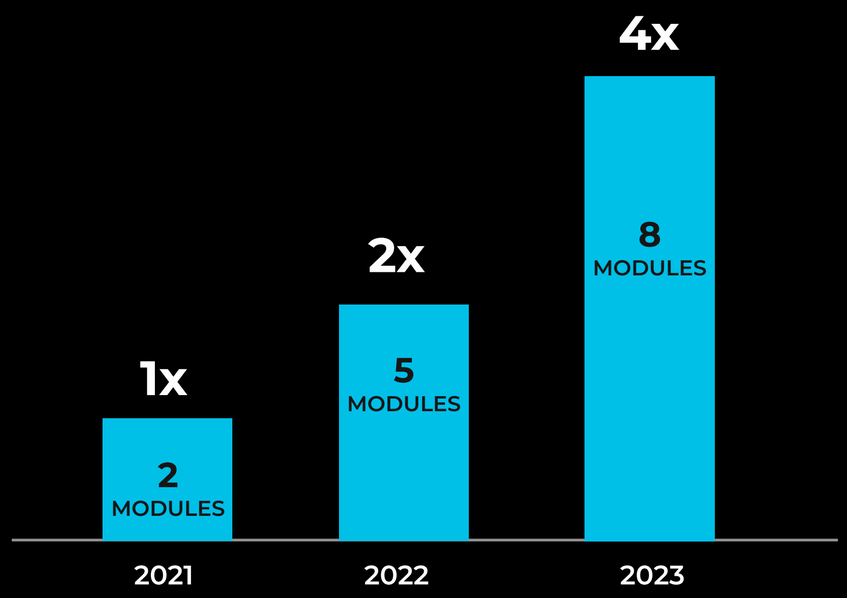
1,2,3 - Customers using at least one module within Code / Infrastructure / Runtime categories

4 - Customers using at least one module each of Code, Infrastructure, and Runtime categories

# Demo

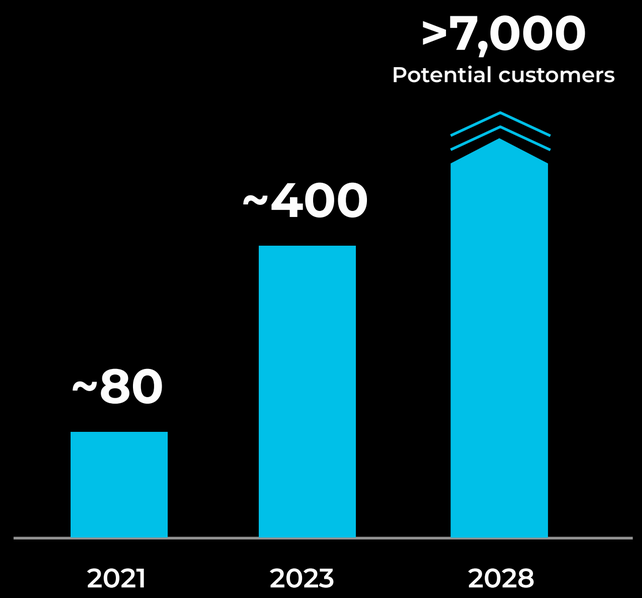
# The opportunity ahead

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




Credit consumption growth - evolution of current 8-module customers

Credit consumption grows with expansion across multiple modules




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

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


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 |

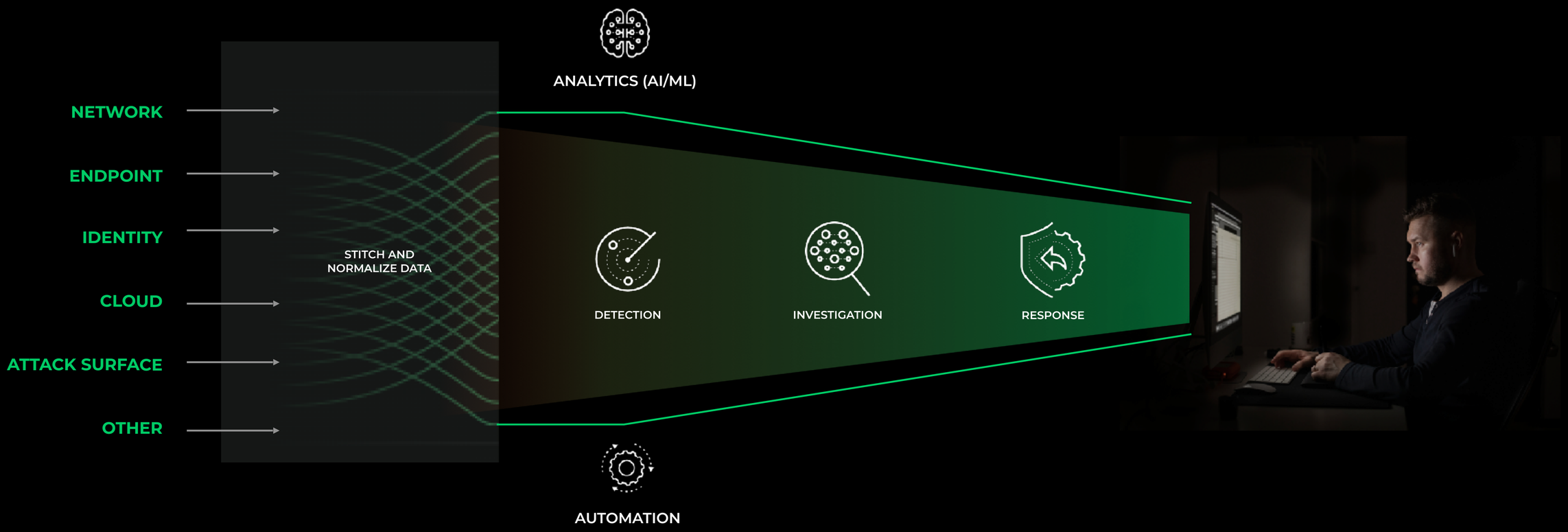
**Sources:**
[1] Forrester: The 2020 State of Security Operations
[2] IDC: In Cybersecurity Every Alert Matters, October 2021
[3] ESG: SOC Modernization and the Role of XDR, October 2022

# Real-time Security Operations requires a single data platform powered by AI and Automation

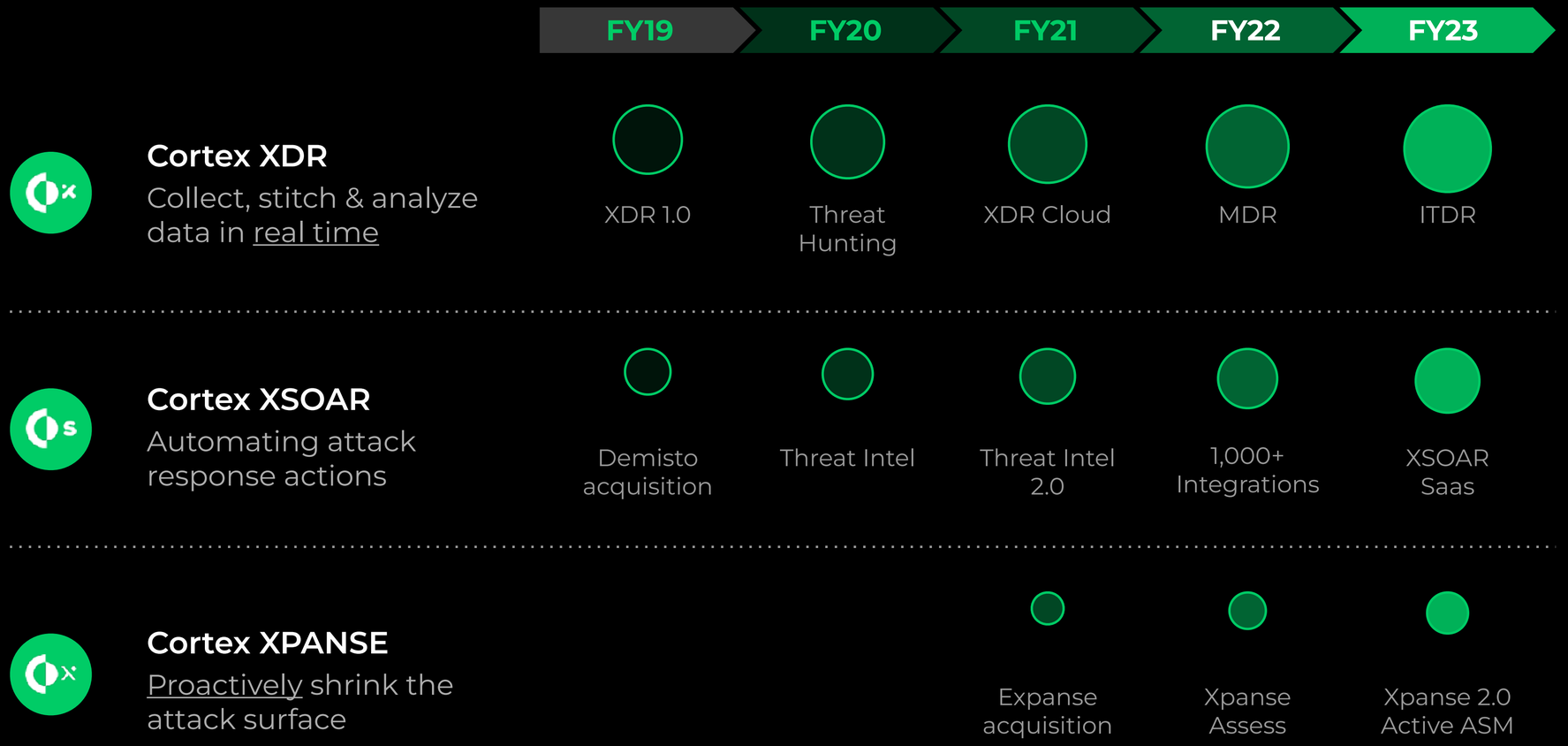
Massive data enhanced with stitching and correlation dramatically reduces the # of alerts

Machines automate detection, investigation, and response and make recommendations

Empowered analysts become more proactive



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




## 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]

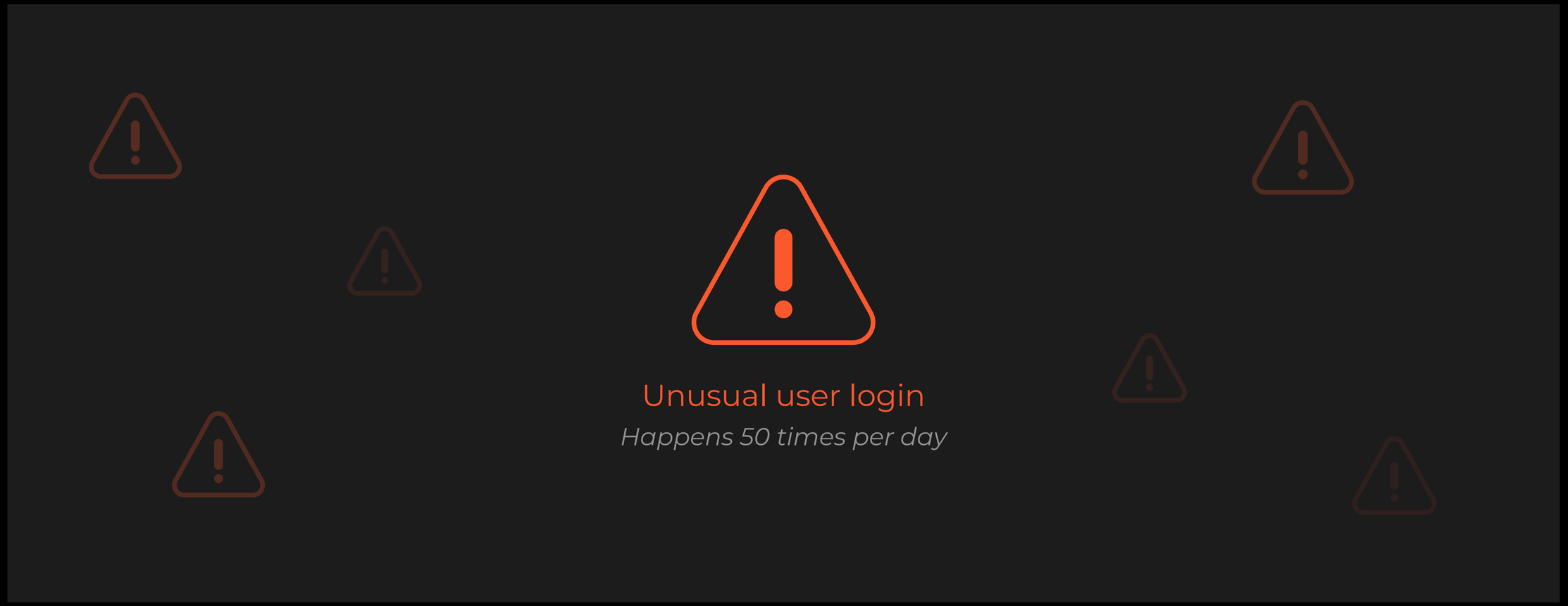
GIGAOM
Leader in GigaOm's Attack Surface Management Radar [3]

**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*

# Detecting attacks with siloed tools and data is impossible




Events in isolation can be suspicious...

# Detecting attacks with siloed tools and data is impossible


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

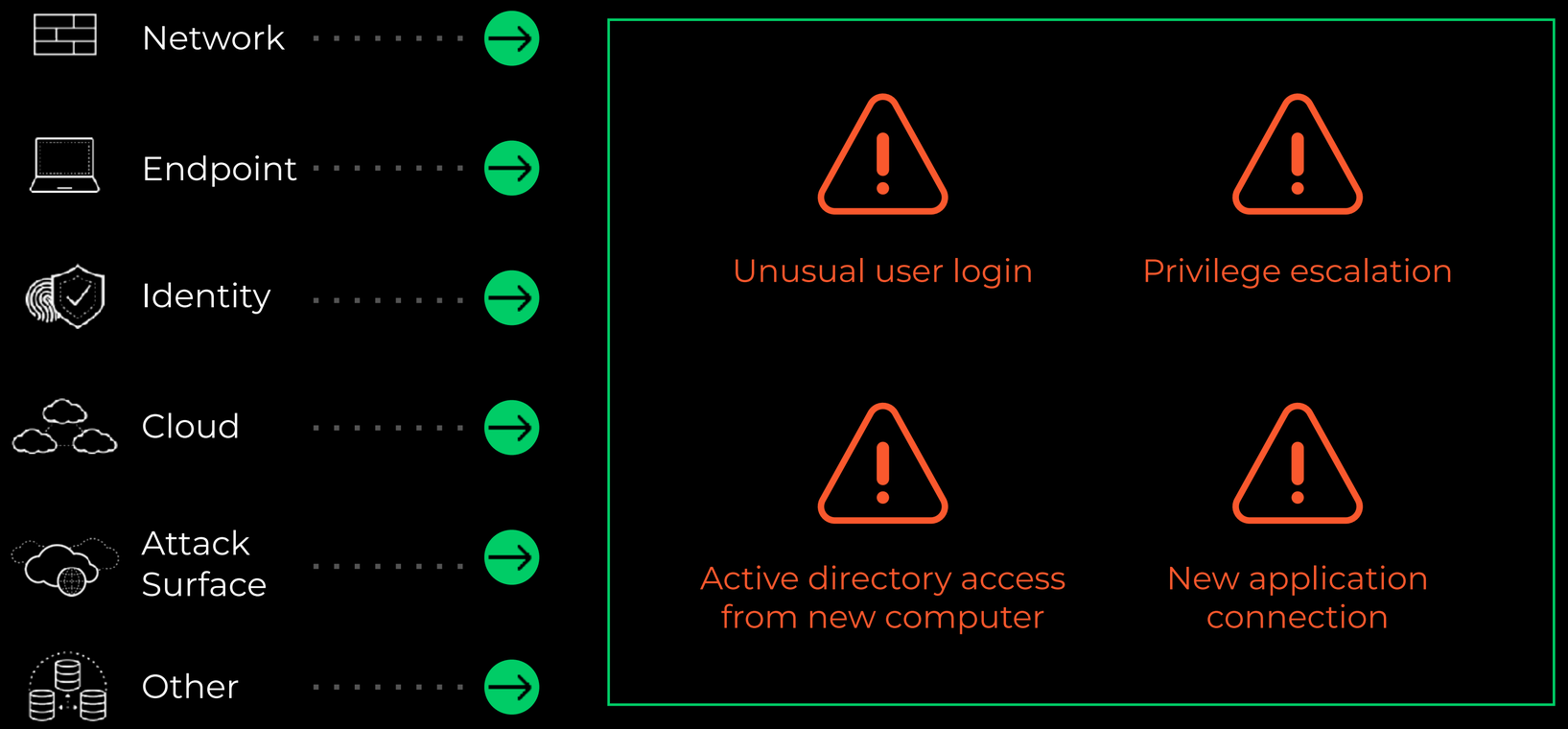
# Detecting attacks with siloed tools and data is impossible


This means attacks are missed...

# Detecting attacks with siloed tools and data is impossible

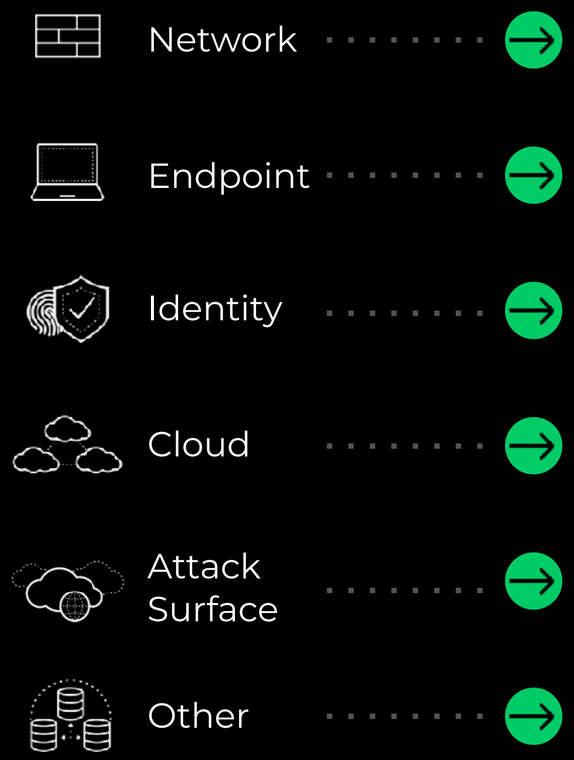

...because of a low confidence to act on any one alert.

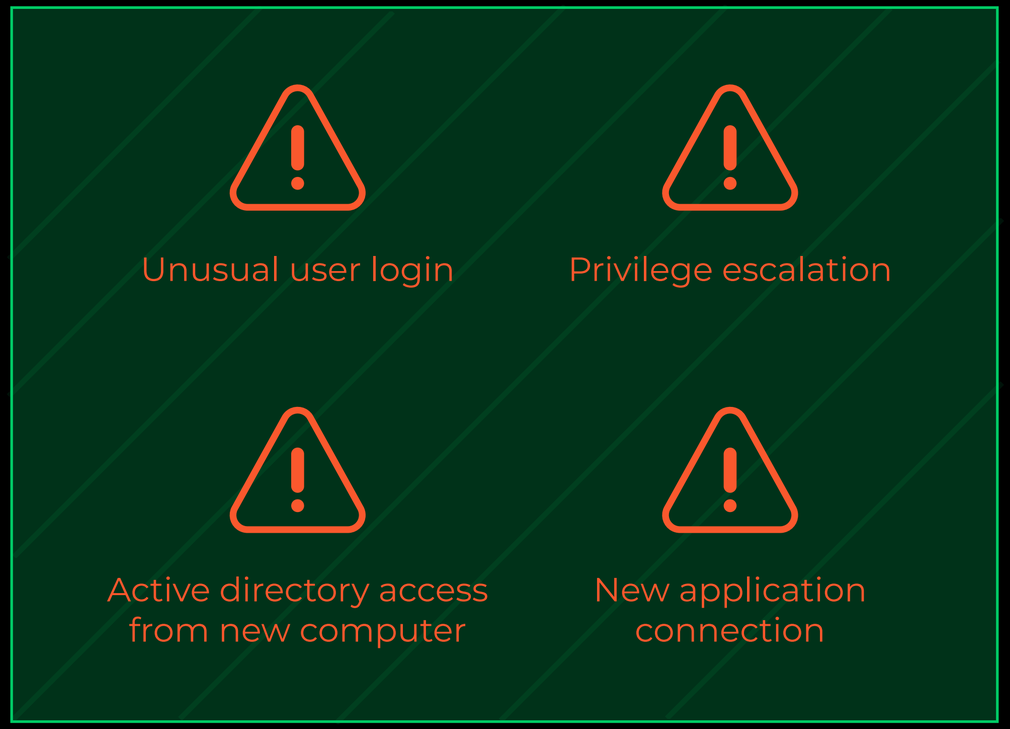
# Cortex XSIAM collects complete context and uses the power of AI to detect attacks that siloed tools miss




Stitching and normalizing alerts, augmented with contextual data...

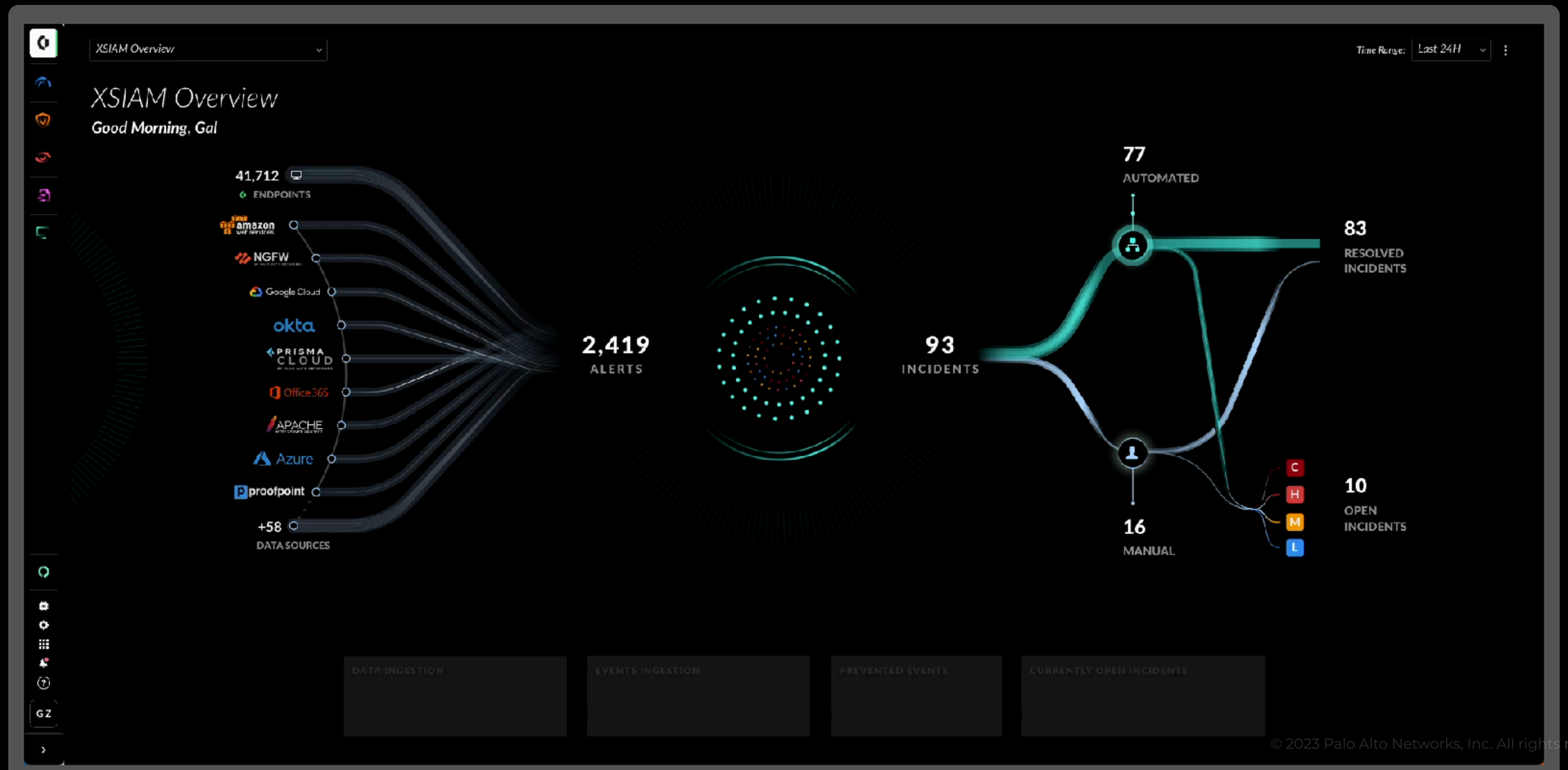
# Cortex XSIAM collects complete context and uses the power of AI to detect attacks that siloed tools miss



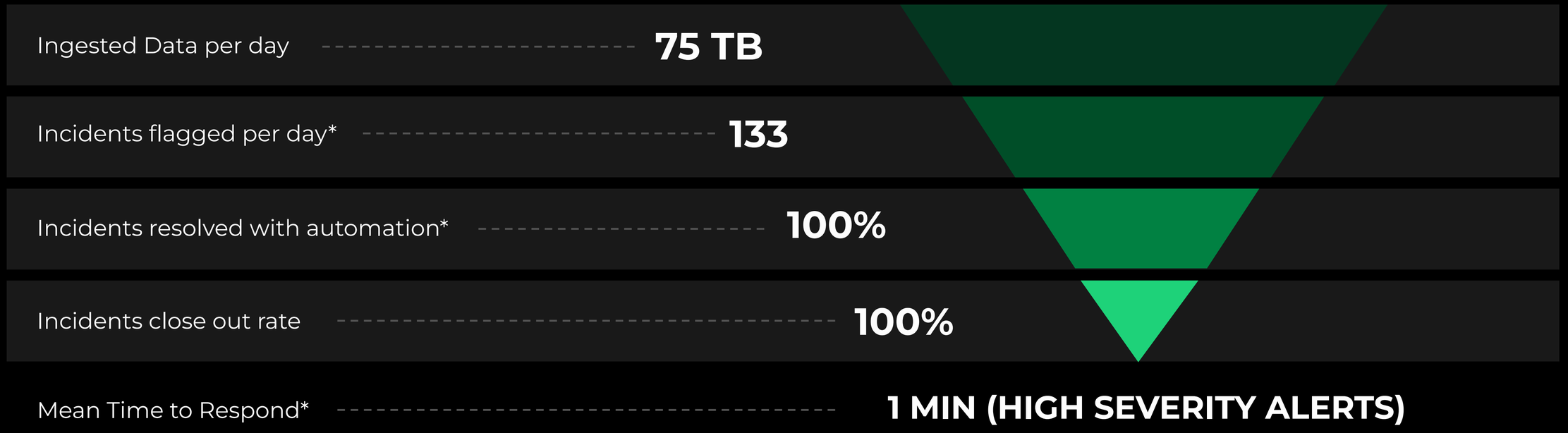

...enables us to automatically respond with high confidence.

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



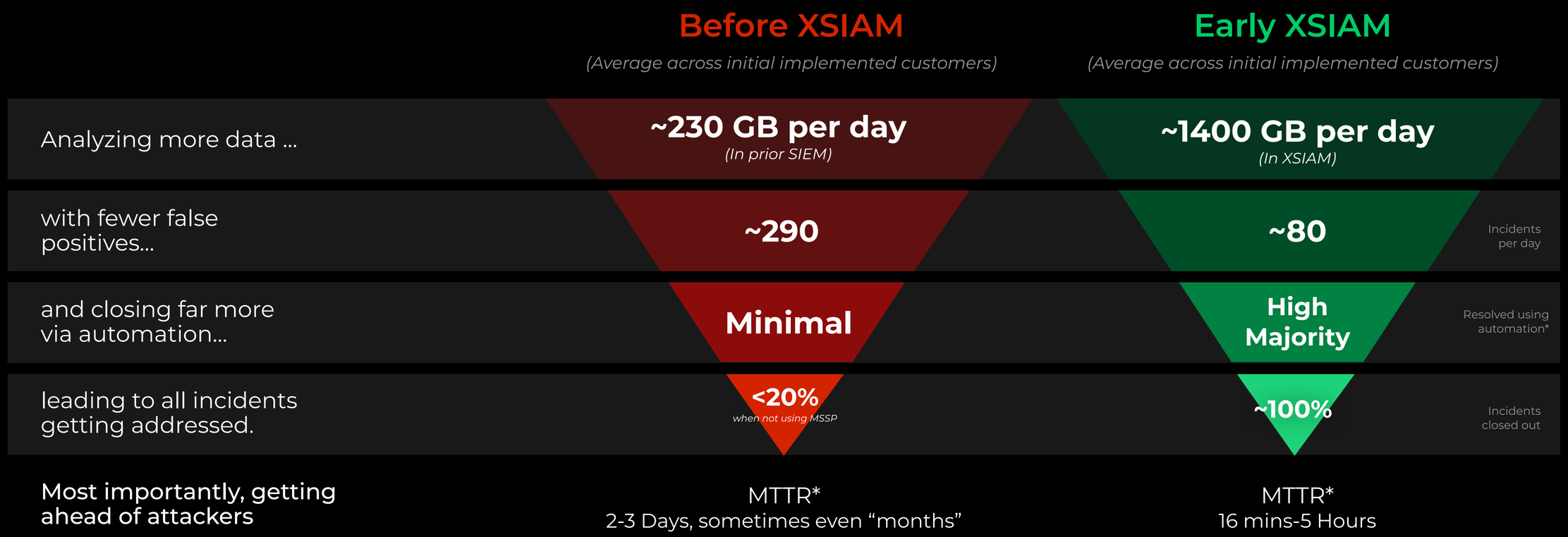
# XSIAM is driving incredible outcomes for the SOC at Palo Alto Networks

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




*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.

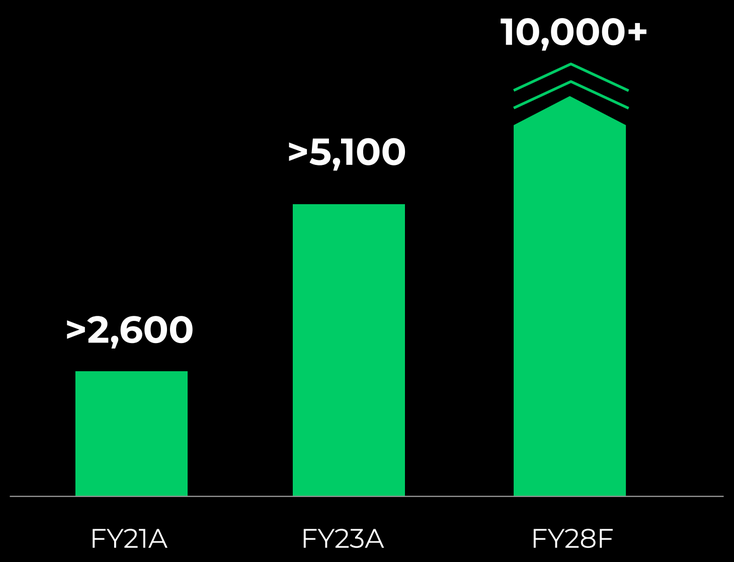
# And XSIAM is already driving amazing outcomes for our customers




> “ 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




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

**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**

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**

[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

| 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 | Evolving Motion across ~3,000 Sellers |
| --- | --- |
| Engaged by technical domain experts | Engaged by CxOs looking to transform |
| Pre-defined product requirements | Strategic discussions focused on security outcomes |
| Focus on price negotiation | ‘Seat at the table’ for architectural choices |
| Ends with a transactional product sale | 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]

[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+ today* [1]

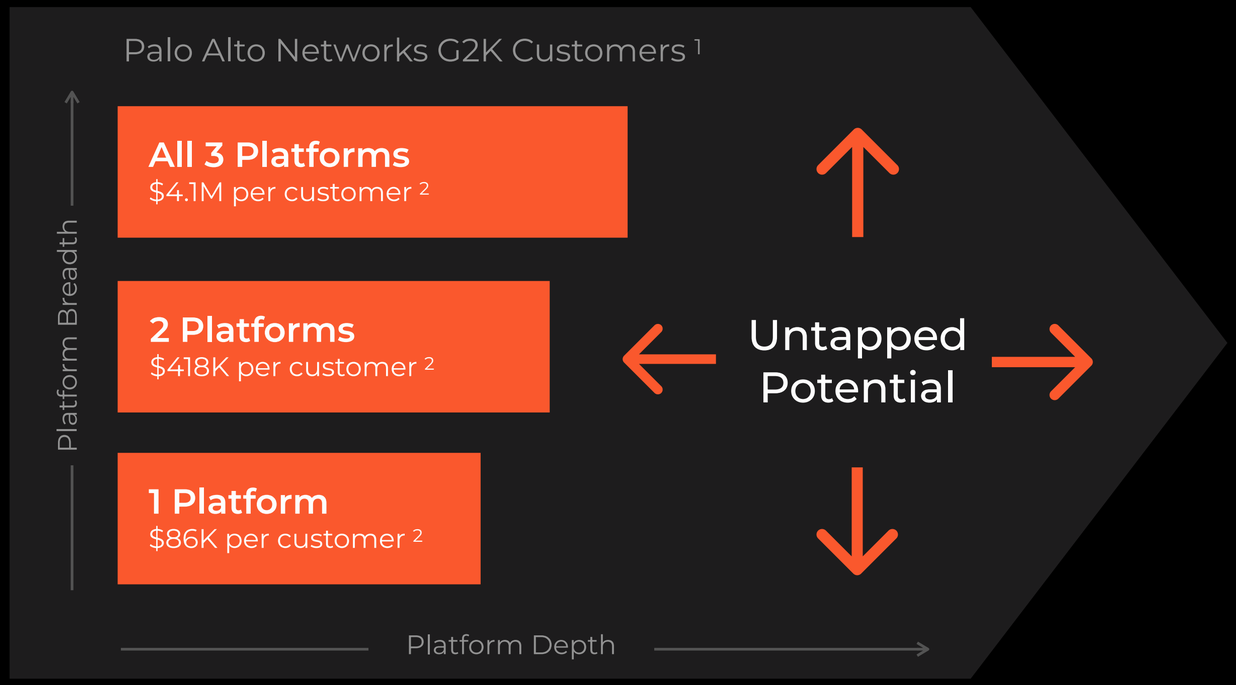
**Increased Adoption**

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...




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**

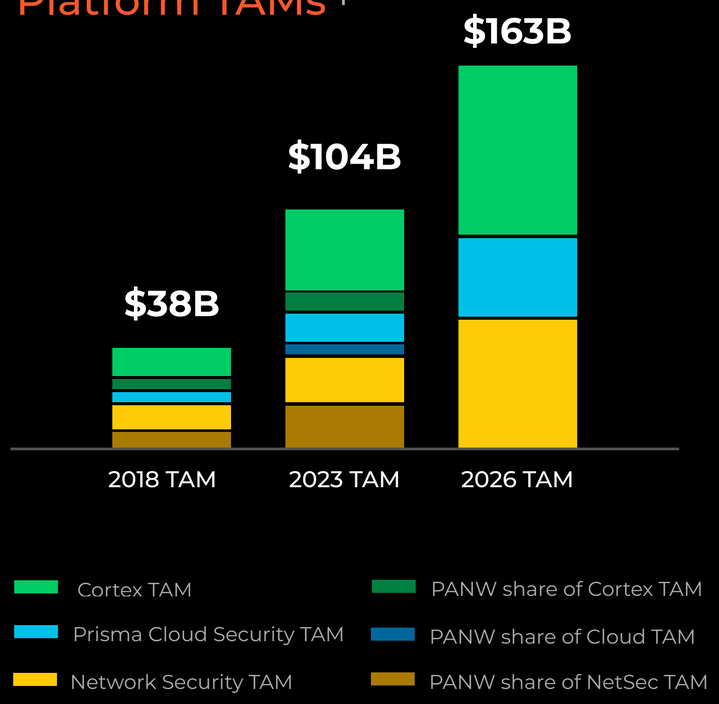
# Finance
Bringing it all Together

# Dipak Golechhha

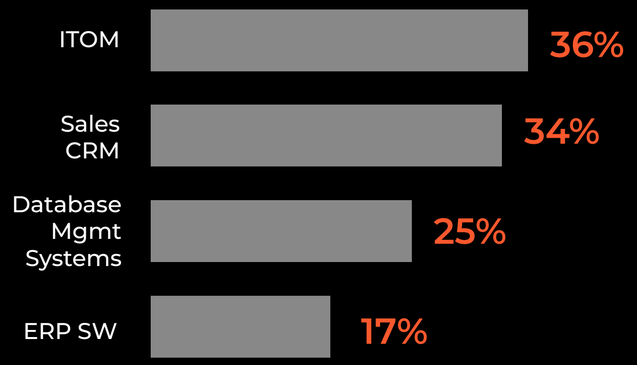
Chief Financial Officer

# We have shown we can capitalize on an expanding TAM

## Expanding Platform TAMs [1]




## Market share leaders [2] in other IT categories




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.
[2] Sources: Gartner Market Share Analysis: ITOM, Value Management Software, Worldwide, 2022; Gartner Customer Experience and Relationship Management, Worldwide, 2022; Gartner Market Share Analysis: Database Management Systems, Worldwide, 2022; Gartner Market Share Analysis: ERP Software, Worldwide, 2022.

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

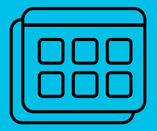
## Zero Trust

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)**


**Increasing core productivity and driving growth in new channels**

**>5%** core sales productivity improvement annually, over the last 3 years

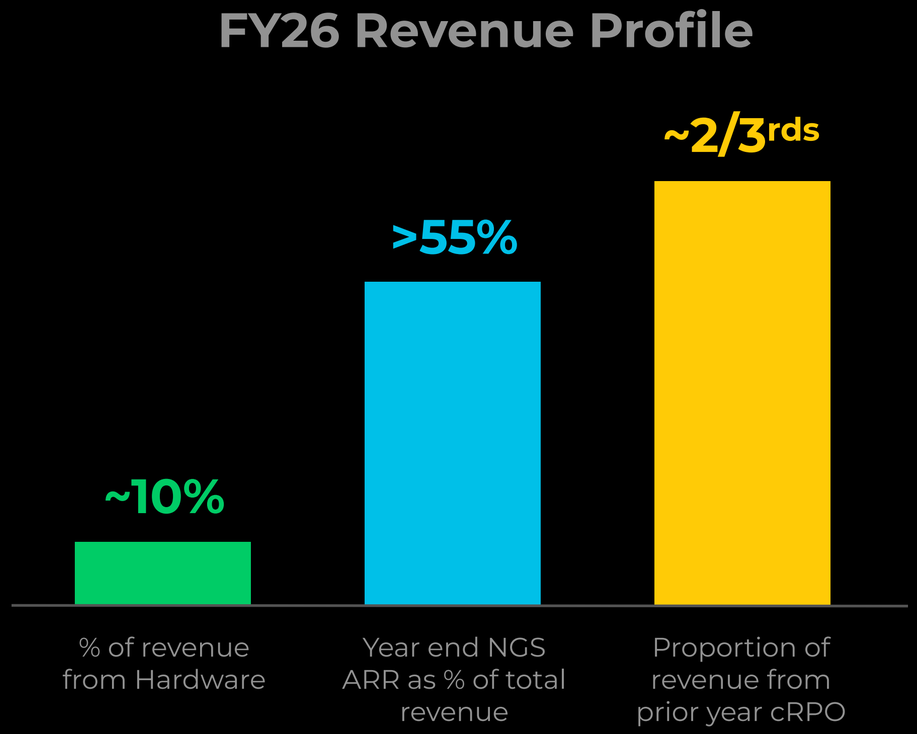
**~75%** growth in Cloud Service Provider (CSP) bookings in FY23

# Growing revenue ahead of our markets through FY26 while increasing predictability

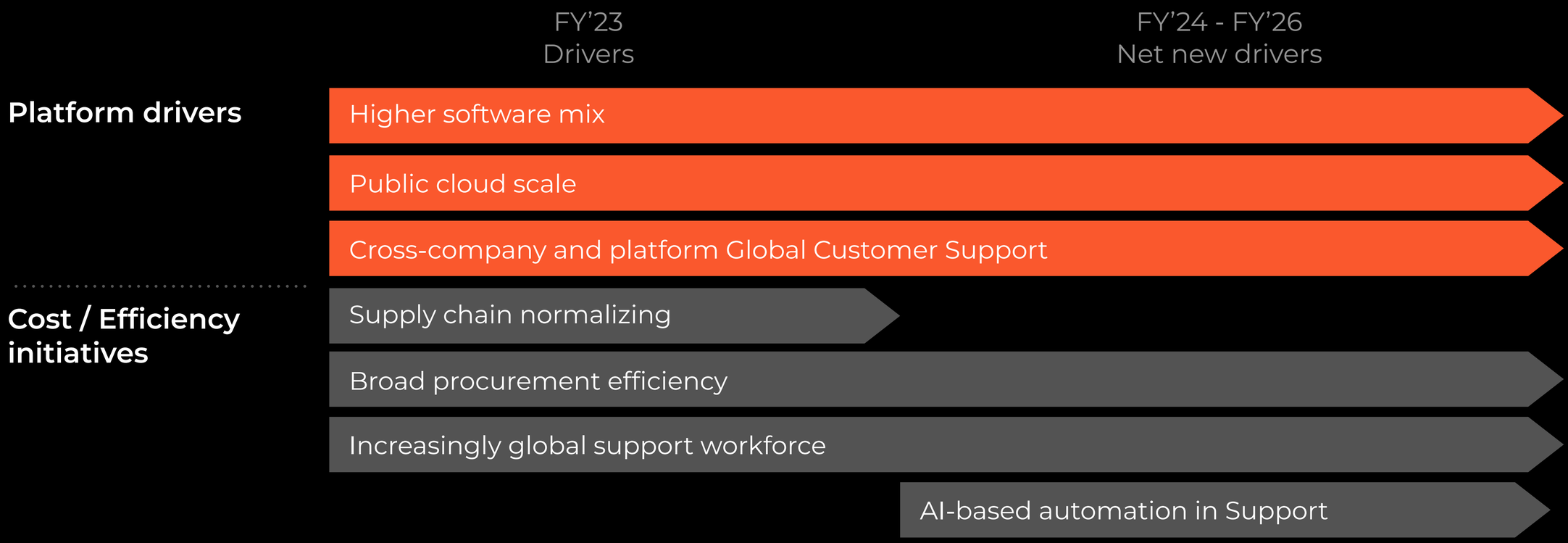
**17-19%** | 3-yr revenue and billings CAGR **FY23-26**

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

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

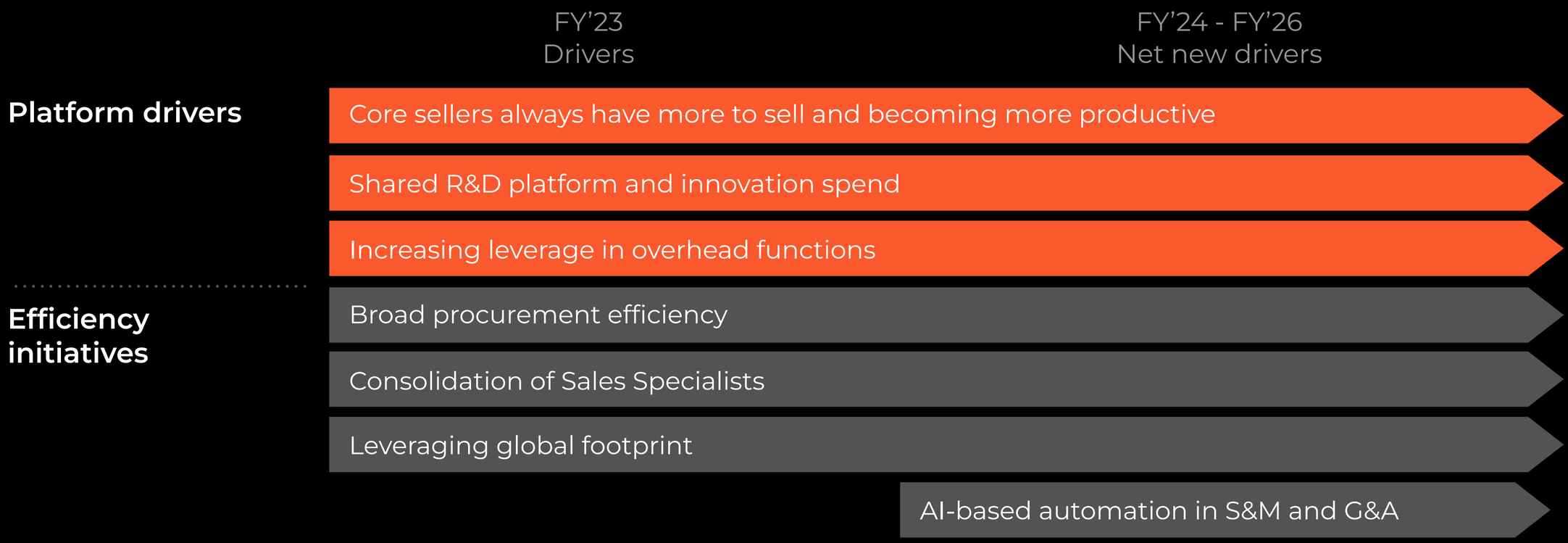


# We can deliver steady gross margin while investing in cloud




Steady gross margin as we drive core improvements and invest in new cloud-based offerings

# Platform and efficiency opportunities driving operating leverage




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**

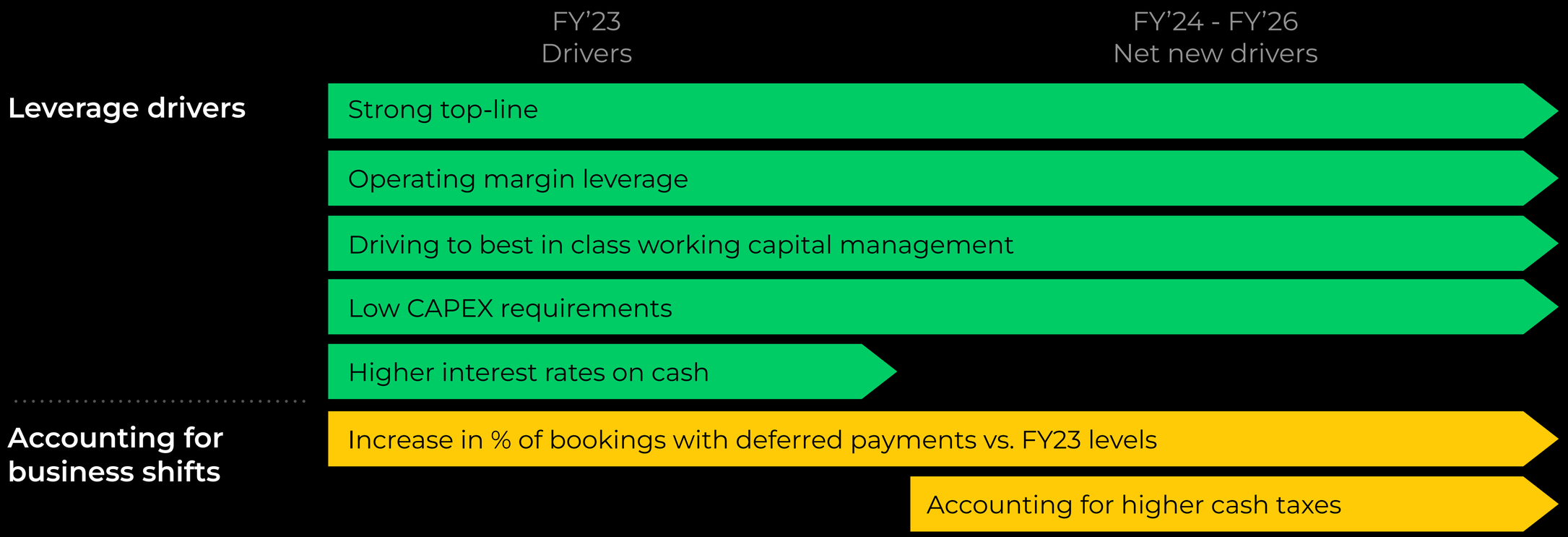
Long-term non-GAAP operating margin potential

**20%+**

non-GAAP EPS CAGR FY23-26

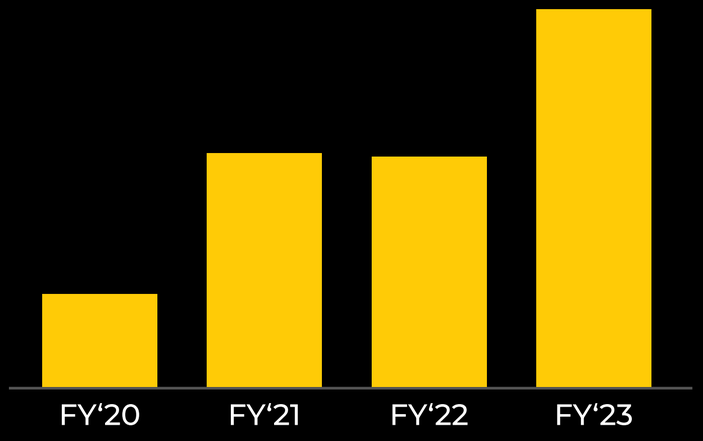
A reconciliation of forward-looking non-GAAP financial measures to the corresponding GAAP measures has not been provided as it is not available without unreasonable effort.
Fiscal year ending on July 31.

# Steady free cash flow margin with flexibility to navigate the environment



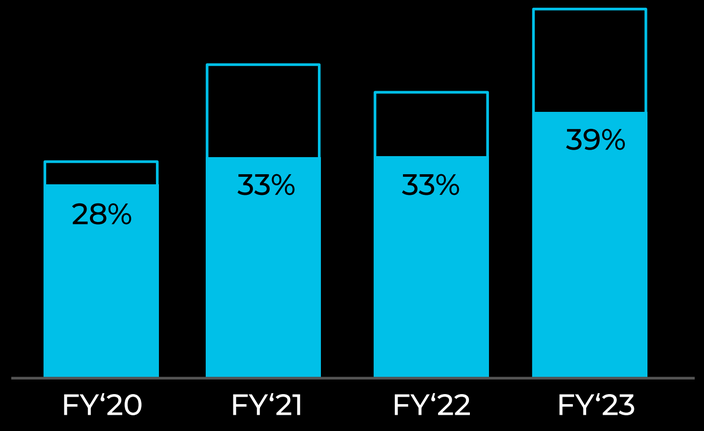
# We have already delivered strong cash flow while managing through an increase in deferred payments

Increased deals with Deferred Payments




Bookings $s for deals with Deferred Payment Plans

Robust Free Cash Flow Margins




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

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.

# 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

Planning to settle

**$2.0B**

FY25 convertible note with cash

Maintain capital structure that allows flexibility & minimizes dilution

**$3.9B**

In cash used for share repurchase over last 5 years

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

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.


paloalto
NETWORKS
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 |

Fiscal year ends on July 31.

# 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 |

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): | 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