## 2021 Analyst Day | Webcast Replays

Click the links below to immediately launch a replay of the specific segment

<table>
<thead>
<tr>
<th>Presenter</th>
<th>Video replay link</th>
<th>Slide</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nikesh Arora, CEO &amp; Chairman</strong></td>
<td>Where We Are &amp; Looking Ahead</td>
<td>4</td>
</tr>
<tr>
<td><strong>Lee Klarich, Chief Product Officer</strong></td>
<td>Market Needs &amp; Our Platforms</td>
<td>15</td>
</tr>
<tr>
<td>Anand Oswal, SVP Products</td>
<td>Network Security (starts @ 6:26)</td>
<td>21</td>
</tr>
<tr>
<td>Ankur Shah, SVP Products</td>
<td>Cloud Security (starts @ 16:07)</td>
<td>34</td>
</tr>
<tr>
<td>Lee Klarich, Chief Product Officer &amp; Tim Junio, SVP Products</td>
<td>Security Operations (starts @ 24:31)</td>
<td>45</td>
</tr>
<tr>
<td><strong>Nir Zuk, Founder and Chief Technology Officer</strong></td>
<td>What does Zero Trust Really Mean?</td>
<td>57</td>
</tr>
<tr>
<td><strong>BJ Jenkins, President</strong></td>
<td>Driving Sustainable Growth &amp; Securing Our Customers</td>
<td>66</td>
</tr>
<tr>
<td><strong>Liane Hornsey, Chief People Officer</strong></td>
<td>Drivers of Change - Our People. ESG for Palo Alto Networks.</td>
<td>74</td>
</tr>
<tr>
<td><strong>Dipak Golechha, Chief Financial Officer</strong></td>
<td>Managing for Scale and Efficiency &amp; Bringing it All Together</td>
<td>81</td>
</tr>
</tbody>
</table>
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 that are based on our management’s beliefs and assumptions and on information currently available to management, including statements regarding our expectations regarding our strategic plans, growth drivers for fiscal 2022 and beyond, our product and service offerings, our financial guidance for the first quarter of fiscal 2022 and fiscal year 2022, and our financial targets for fiscal year 2024. Many of these assumptions relate to matters that are beyond our control and changing rapidly, including, but not limited to, the impact of COVID-19 on our customers’ purchasing decisions and the length of our sales cycles, particularly for customers in certain industries or geographies highly affected by COVID-19.

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; the duration and global impact of COVID-19; risks associated with managing our growth; the risks associated with new products and subscription and support offerings, including the discovery of software bugs; our ability to attract and retain new customers; delays in the development or release of new subscription offerings; our competition; rapidly evolving technological developments in the market for network security products and subscription and support offerings; our ability as an organization to acquire and integrate other companies, products or technologies in a successful manner; length of sales cycles; our ability to obtain adequate supply of our products from our third-party manufacturing partners; 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 Annual Report on Form 10-K filed for the fiscal year ended July 31, 2021, 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 our current beliefs and on information available to us 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 or to update the reasons why actual results could differ materially from those anticipated in the forward-looking statements, even if new information becomes available in the future.

All information in this presentation is as of September 13, 2021. This presentation contains non-GAAP financial measures and key metrics relating to the company's past and expected future performance. The presentation of these non-GAAP financial measures and key metrics are not meant to be considered in isolation or as a substitute for comparable GAAP financial measures and should be read only in conjunction with the company's consolidated financial statements prepared in accordance with GAAP. A reconciliation of the company's historical non-GAAP financial measures to their most directly comparable GAAP measures has been provided in the Appendix. We have not reconciled certain non-GAAP financial measures because we do not provide guidance on the comparable GAAP financial measures and would not be able to present the various reconciling items between GAAP and non-GAAP financial measures without unreasonable effort.
Three years ago...

We were known for the strength and scale of our NGFW business but not yet for our cutting-edge security innovation.

We set an ambition to become the cybersecurity partner of choice, to innovate and to stay ahead of the curve.
We identified several trends

**Shift to cloud going mainstream:** Enterprises needed to increasingly operate with hybrid, multi-cloud estates

**Accelerating digital transformation:** Enterprises needed to secure users working anywhere, anytime and across any devices and apps

**AI/ML and automation gaining traction:** Enterprises needed better security outcomes but also to reduce need for scarce SecOps talent

**Intensifying security landscape:** Proliferation of attacks drove need for better threat intel and for trusted partners familiar with client architecture
We delivered on our three big bets...

**Transform Network Security**
- Extended our winning hardware to Software and aaS
- Scaled our best of breed cloud-delivered security stack
- Developed simplified ‘Single Pane of Glass’ experience

**Deliver Comprehensive Cloud Native Security**
- United compliance, container, & micro-segmentation capabilities
- Launched comprehensive cloud security platform
- Integrated cutting-edge Shift Left security

**Revolutionize Security Operations**
- Established the XDR category with cutting edge technology
- Delivered world-class automation and remediation
- Broadened visibility across the attack surface
...which was made possible by becoming an innovation leader

Major Product Releases

<table>
<thead>
<tr>
<th></th>
<th>FY19</th>
<th>FY20</th>
<th>FY21</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>13</td>
<td>22</td>
<td>29</td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

>2X Major product releases in FY21 vs. FY19

Groundbreaking Product Innovation

**Network Security**
- DNS Security
- Prisma Access 1.0
- First ML powered NGFW
- Acquired CloudGenix SD-WAN
- NFGW IoT, DLP, SD-WAN subs
- CN-series for 5G infrastructure
- Access 2.0 with DEM²
- Refreshed NGFW hardware
- NGFW as a Service

**Cloud Security**
- Acquired Redlock, Twistlock
- Prisma Cloud 1.0
- Container Cloud Security
- Serverless Cloud Security
- Acquired AperoTo
- IAM Security
- Data Protection
- Microsegmentation
- Web App & API Security
- Acquired Bridgecrew

**SOC Security**
- Cortex XDR 1.0
- Acquired Demisto for XSOAR
- Cortex XDR 2.0 with MTH²
- Cortex XSOAR with TIM²
- XDR Host Insights
- Acquired Xpanse for ASM²
- Cortex XSOAR Marketplace
- XDR 3.0 with cloud / ID analytics

1. Major product release is defined as full or dot release with significant new capability, new or add-on modules, or subscription services, new software or hardware appliance models, significant PAN-OS, acquired capabilities and significant new platform support. Fiscal year ending on July 3, 2021.
2. Digital Experience Management
3. Managed Threat Hunting
4. Attack Surface Management
5. Threat Intel Management

© 2021 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.
We now have three best-of-breed platforms

Network Security  
**STRATA | PRISMA SASE**  
Best-in-class Firewall Platform across hardware, software and aaS

Cloud Security  
**PRISMA CLOUD**  
Comprehensive platform to secure everything that runs in the cloud

SOC Security  
**CORTEX**  
A new approach to SOC with data, analytics and automation

Zero Trust security
We built out our speedboat Go-To-Market model to help us scale

<table>
<thead>
<tr>
<th>3 Years Ago</th>
<th>Today</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 2.5k+ <strong>Core Sales</strong> Team</td>
<td>• 3.2k+ <strong>Core Sales</strong> Team</td>
</tr>
<tr>
<td>• Limited Specialist Sellers</td>
<td>• 850+ <strong>Speedboat Specialists</strong></td>
</tr>
</tbody>
</table>

Note: 3 years ago refers to FY19; today refers to FY21
We have exceeded growth targets from our prior analyst day

**FY’22 Targets (From Analyst Day 2019)**

<table>
<thead>
<tr>
<th>Total Revenue</th>
<th>Total Billings</th>
<th>NGS Billings</th>
<th>Non-GAAP Operating Margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5,000M</td>
<td></td>
<td>$1,750M</td>
<td>21.5%</td>
</tr>
</tbody>
</table>

**FY’22 Guidance**

<table>
<thead>
<tr>
<th>Total Revenue</th>
<th>Total Billings</th>
<th>NGS Billings</th>
<th>Non-GAAP Operating Margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5,300M</td>
<td></td>
<td>$1,530M</td>
<td>18.5 - 19%</td>
</tr>
</tbody>
</table>

1 Represents midpoint of FY’22 Guidance.
2 Total billings is a key financial metric calculated as total revenue plus change in total deferred revenue, net of total acquired deferred revenue.
3 Next-Gen Security (NGS) billings is a key financial and operating metric. Prior to Q2’21, NGS billings was defined as the total amount invoiced and billed during the period stated for Prisma and Cortex offerings inclusive of the VM-Series and related services. For Q2’21 and afterwards, NGS billings is defined as total revenue plus change in total deferred revenue, net of total acquired deferred revenue for Prisma and Cortex offerings inclusive of the VM-Series and related services.
4 Guidance for NGS Billings in FY’22 not provided.

Fiscal year ending on July 31.
LOOKING AHEAD...
In the next 3 years we see accelerating change in cybersecurity

<table>
<thead>
<tr>
<th>Our beliefs</th>
<th>In the next 3 Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad actors are innovating faster and attacks are becoming more sophisticated</td>
<td>Innovation in security will accelerate to keep pace and will be a key differentiator</td>
</tr>
<tr>
<td>Point solutions are gradually being deprecated</td>
<td>Customers will standardize on a platform approach</td>
</tr>
<tr>
<td>Non-AI or data driven security is becoming obsolete</td>
<td>Embedded AI / ML and automation will be the norm across the security stack</td>
</tr>
<tr>
<td>Smaller vendors are finding it harder to capture customer mindshare</td>
<td>Trusted scale players will capture a larger ‘piece of the pie’</td>
</tr>
<tr>
<td>Vendors are being asked for ‘security with an opinion’</td>
<td>Winning vendors will shift from being product providers to trusted partners</td>
</tr>
</tbody>
</table>
Our convictions drive our strategy

**Keep driving innovation**
- Maintain our accelerated pace of product innovation and releases
- Continue to scan the security vendor landscape for emerging technologies

**Bet on our platforms**
- Continue to innovate in Network Security transformation and lead the transition to SASE andaaS Security
- Deliver comprehensive Cloud Native Security that is fully integrated across the application lifecycle
- Revolutionize Security Operations by providing complete visibility, advanced analytics and end-to-end automation

**Embed AI / ML everywhere**
- Infuse ML / AI across our entire platform portfolio
- Design solutions with automation in mind, so resolving security issues is easier and faster

**Leverage our scale**
- Leverage our 4k+ person sales force and deep ecosystem relationships to reach new customers
- Drive more of our 85k+ customers to become multi-platform

**Become a trusted partner**
- Leverage our brand and reach to become a trusted advisor at the highest levels
- Build a portfolio that supports customers through every step of their security journey
Our path to get there...

Agenda

Market Needs and Our Platforms

Securing our Customers

Drivers of Change - Our People

Bringing it All Together... for Total Shareholder Return

Lee Klarich & Nir Zuk
Chief Product Officer & Chief Technology Officer

BJ Jenkins
President

Liane Hornsey
Chief People Officer

Dipak Golechha
Chief Financial Officer
Market Needs & Our Platforms

Lee Klarich
The pandemic has accelerated three core technology trends, increasing the enterprise attack surface:

- **Hybrid work is here to stay**
  Users working from anywhere, anytime and across any devices and apps

- **Shift to cloud is accelerating**
  Increasingly operating in hybrid, multi-cloud estates

- **AI/ML enabling enterprise digitization**
  Integrating and normalizing data at scale to enable advanced analytics
Attackers are taking advantage of this larger attack surface

Rise of Nation State Attacks

10+

Publicly attributed cyber attacks per month

In 2021

100%

Increase in Nation State cyber incidents

Since 2019

<table>
<thead>
<tr>
<th>Significant cyber incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan Olympics data breach</td>
</tr>
<tr>
<td>Verizon and Microsoft hacks</td>
</tr>
<tr>
<td>Southeast Asia APT</td>
</tr>
<tr>
<td>South Africa port and freight halted</td>
</tr>
<tr>
<td>Kaseya hack</td>
</tr>
<tr>
<td>1,500 SMB ransomed</td>
</tr>
</tbody>
</table>

Sources: CSIS Significant Cyber Incidents; Nation States, Sep 2021; Cyberconflict and the web of Profit, by Dr Michael McGuire, Apr 2021
This is accelerating our TAM for Network Security, Cloud Security, and Security Operations

Total Addressable Market (TAM)
14% CAGR (CY21-CY24)

Our strategic bets in the past three years position us well to win in this market

**Network Security**
- STRATA | PRISMA SASE
- Best-in-class platform across hardware, software and SASE

**Cloud Security**
- PRISMA CLOUD
- Cloud-native platform to secure everything that runs in the cloud

**Security Operations**
- CORTEX
- A new approach to SOC with full data integration, analytics and automation
The market recognizes our leadership across several categories

### 3 Years Ago
**Leadership in 1 category**

1. **NGFW**
   - **Leader** in Gartner Magic Quadrant Network Firewalls

### Now a Leader
**in 7 categories**

1. **NGFW**
   - **Leader** in Gartner Magic Quadrant Network Firewalls
2. **Zero Trust**
   - **Leader** in Forrester Zero Trust eXtended Ecosystem Platform Providers Wave
3. **SD-WAN**
   - **Leader** in Gartner Magic Quadrant WAN Edge Infrastructure
4. **SOAR**
   - **Leader** in KuppingerCole Security Orchestration Automation & Response Leadership Compass
5. **XDR**
   - **Leader** in Forrester Endpoint Security Software As A Service Wave
6. **Vulnerability Management**
   - **Outperformer Leader** in GigaOm’s Vulnerability Management Radar
7. **ZTNA**
   - **Leader** in Forrester Zero Trust Network Access New Wave

---

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner content described herein (the “Gartner Content”) represents(s) research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. (“Gartner”), and are not representations of fact. Gartner Content speaks as of its original publication date (and not as of the date of this analyst day), and the opinions expressed in the Gartner Content are subject to change without notice.
Network Security
Network security evolution: First, network security was centralized with a firewall
Network security evolution: Expanding security needs quickly resulted in the proliferation of point products
Network security evolution: As apps moved to the cloud and users became mobile, traffic was backhauled to keep security centralized.
Today: Network security is now delivered in multiple form factors, with differing technologies.
Our solution: A network security platform delivering best-in-class security across the entire enterprise

- Consistent security for all users and applications
- Best-in-class security services across hardware, software and SASE
- Best possible end-user experience at all locations
- Unified security operations
**Next-Gen Firewalls: Extending our leadership position with continued innovation**

- 9 times leader in Gartner Magic Quadrant for Network Firewalls
- Introduced ML-Powered 4th generation appliances: industry-leading price-performance
- Largest software firewall player in the market, offering consistent protection of virtual / container workloads, 5G infrastructure

---

### Network Security Platform

<table>
<thead>
<tr>
<th>Security Services</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TP</td>
<td>WP</td>
<td>GP</td>
<td>SD-WAN</td>
<td>DNS</td>
<td>ADV</td>
<td>URL</td>
<td>DLP</td>
</tr>
<tr>
<td>PA-Series Hardware Firewalls</td>
<td>VM-Series</td>
<td>CN-Series Software Firewalls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PA-Series Hardware Firewalls</td>
<td>VM-Series</td>
<td>CN-Series Software Firewalls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

SASE
Prisma SASE: The industry’s most complete SASE solution

- Full set of best-of-breed capabilities
  - Firewall as a Service (FWaaS)
  - Secure Web Gateway (SWG)
  - Cloud Access Security Broker (CASB)
  - Zero Trust Network Access (ZTNA)
  - Software-defined WAN (SD-WAN)

- Industry-first innovations:
  - Autonomous digital experience management (ADEM)
  - Next-Gen CASB*
  - Integrated 5G SD-WAN*
  - Okyo Garde

* coming soon
**Prisma SASE: Extending our enterprise offering to secure our customers’ home networks**

<table>
<thead>
<tr>
<th>Security Services</th>
<th>TP</th>
<th>WP</th>
<th>GP</th>
<th>SD-WAN</th>
<th>DNS</th>
<th>ADV URL</th>
<th>DLP</th>
<th>CASB</th>
<th>IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Firewalls</td>
<td>PA-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Firewalls</td>
<td></td>
<td>VM-</td>
<td>CN-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Homes have become an extension of the enterprise network
- More devices than ever before are connected to the home network

---

**Enterprise-grade security with consumer simplicity for work from home employees and small businesses**
Security Services: Expanding our offering, available on all form factors

- Expanded from 4 to 9 services: higher attach to our platform and consolidation of point products
- Consistently available across all form factors: hardware, software and SASE
- ML-powered and real-time: protecting against zero-day threats and increasing value of security services
Industry recognition: Recognized by industry analysts as a leader in network security
Our TAM: Our platform approach addresses a large and growing network security market

Three drivers of growth

1. **36% CAGR**\(^1\) for SASE driven by hybrid work and cloud adoption

2. **13% CAGR**\(^1\) for Software firewalls driven by multi-cloud transition

3. Introduction of new security services (IoT, DLP, NG-CASB)

Form factor transition is favorable - SASE adoption drives 2:1 hardware replacement value

Note: Strata Core TAM includes DNS as part of product offerings; \(^1\) FY’19-FY’24 CAGR


---

**Network Security TAM**

CY21 - CY24 CAGR = 9%

<table>
<thead>
<tr>
<th>Year</th>
<th>Network Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>$27B</td>
</tr>
<tr>
<td>2020</td>
<td>$31B</td>
</tr>
<tr>
<td>2021</td>
<td>$35B</td>
</tr>
<tr>
<td>2022</td>
<td>$37B</td>
</tr>
<tr>
<td>2023</td>
<td>$41B</td>
</tr>
<tr>
<td>2024</td>
<td>$45B</td>
</tr>
</tbody>
</table>
Network Security: The largest network security business, successfully executing on our transformation

<table>
<thead>
<tr>
<th>77% of Global 2000&lt;sup&gt;1&lt;/sup&gt; companies secured</th>
<th>224B Threats blocked per day</th>
<th>4.3M Updates per day</th>
</tr>
</thead>
</table>

**Firewalls**

85,000+

Customers<sup>2</sup> in 150+ Countries

90%

Avg. CSAT score

**SASE**

154%

CAGR

Prisma SASE billings

**Security services**

66%

Customers have 3+ services (out of 9)

>90%

SASE customers have 4+ services

---

<sup>1</sup>G2000 is the Forbes Global 2000 Companies

<sup>2</sup>Customers represent all customers acquired since inception. A customer is defined as an account that has purchased products and services excluding not-for-resale services.
Cloud Security
Demystifying **Cloud Security**

**Securing access to the cloud**

- Internet
- Private Cloud/DC
- Public Cloud
- SaaS Applications
- HQ, Branches, Remote

**Securing the cloud**

- Private Cloud
- Public Cloud
- Multi-cloud
- Hybrid Cloud

*$152B*

**Public Cloud** spend

Cloud Applications: Organizations started their cloud-first journey with “Lift and Shift”
Cloud Applications: They then started building and deploying cloud-native applications.
Cloud Applications: And are now deploying applications across multi-cloud and hybrid cloud environments
Cloud Security: Customers need a growing number of capabilities to secure their cloud environments

Visibility, Compliance, Governance
- Misconfigurations
- Compliance
- Advanced threats (Cryptomining, Account Compromise)

Workload Security
- Vulnerabilities - Host, Container, Serverless
- Runtime Threats
- Web Application & API Protection

Network Security
- Cloud-native network segmentation
- Network Threat Prevention

Identity Security
- Identity and access misconfiguration
- Over-Privileged access

Application Lifecycle Security
- Code vulnerabilities, CI / CD pipeline vulnerabilities

Lift and shift apps in Public Cloud

Cloud-native Apps in Public Clouds

Cloud-native apps in Private Cloud / Datacenter
Typical industry approach requires 12-15 point products
Prisma Cloud: A cloud platform to secure the “full cloud stack”

Cloud Security Posture Management
- Visibility, Compliance, Governance
- Threat Detection
- Data Security

Cloud Workload Protection
- Single agent - host, container, serverless, APIs
- Vulnerability management
- Runtime security

Cloud Network Security
- Cloud-native Microsegmentation
- Virtual Firewalls

Cloud Infrastructure Entitlement Management
- Visibility & Governance
- Least privileged access enforcement

DevSecOps
Secure applications across the lifecycle (build-deploy-run)
Our Vision: Expanding the platform to cover more use cases

- ENABLING VISIBILITY, COMPLIANCE, AND SECURING WORKLOADS
- SECURING NETWORKS AND IDENTITIES, AND ENFORCING PERMISSIONS
- EXTENDING APPLICATION LIFECYCLE SECURITY
- CONTINUED INNOVATIONS

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Cloud Workloads Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Security</td>
<td>Q4'20 0.9M</td>
</tr>
<tr>
<td>Posture Management</td>
<td>Q4'21 2.0M</td>
</tr>
<tr>
<td>Cloud Workload</td>
<td></td>
</tr>
<tr>
<td>Security Protection</td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Entitlement</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
</tr>
</tbody>
</table>

Cloud Workloads Protected

- 122% YoY
- Q4'20 0.9M
- Q4'21 2.0M

<table>
<thead>
<tr>
<th>Cloud Security Posture Management</th>
<th>Cloud Network Security</th>
<th>Cloud Infrastructure Entitlement Management</th>
<th>DevSecOps</th>
<th>Q4'20</th>
<th>Q4'21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Expansions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2021 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.
**Our TAM: A $10B Cloud Security market growing at 30% YoY**

- Public cloud spend\(^1\) expected to continue to grow at >25% YoY
- Cloud security spend expected to stabilize at 6-7% of public cloud spend\(^1\)
- Multi-cloud and hybrid-cloud will position us as security partner of choice
- Securing software supply chains will further expand the TAM

---


Source: Gartner: Public Cloud Services Forecast, 1Q21; Gartner: Information Security and Risk Management, Worldwide, 2019-2025, 2Q21 Update; 451 Group Custom Cloud Security Forecasts (Jan 21, Prisma Cloud Marketbook) expanded by PANW internal estimates for CIEM, cloud application security, services and integration.
Prisma Cloud: The largest cloud security solution in the industry

Our platform in numbers

- **3B+** Assets protected
- **2M+** Workloads protected
- **700B+** weekly cloud events processed

**INCREASING ADOPTION OF MODULES**

- **50+%** of customers are using 2 or more modules
- **20+%** are using 3 or more

**GROWING CUSTOMER BASE**

- **Total Prisma Cloud Customer Count**
  - Q4’20: 1,835
  - Q4’21: 2,703 (+47% Y/Y)

- **G2000 Prisma Cloud Customer Count**
  - Q4’20: 368
  - Q4’21: 512 (+39% Y/Y)

**ANALYST RECOGNITION**

- Gartner 2021 Hype Cycle: Prisma Cloud included in 7 market categories
- GigaOm Vulnerability Management Radar: Prisma Cloud a Leader and Outperformer
- Forrester Total Economic Impact Study: 276% ROI and $5.8M in NPV

---

1. G2000 is the Forbes Global 2000 Companies
2. Customers represent all customers acquired since inception. A customer is defined as an account that has purchased products and services excluding not-for-resale services.
Security Operations
Security Operations Center (SOC): Quick overview - the SOC’s goal is to detect and respond to ALL threats

Enterprise Architecture

<table>
<thead>
<tr>
<th>Security Tools</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>![Network Alert]</td>
</tr>
<tr>
<td>Endpoint</td>
<td>![Endpoint Alert]</td>
</tr>
<tr>
<td>Identity</td>
<td>![Identity Alert]</td>
</tr>
<tr>
<td>Cloud</td>
<td>![Cloud Alert]</td>
</tr>
<tr>
<td>Other</td>
<td>![Other Alert]</td>
</tr>
</tbody>
</table>

Alert prioritization
Investigation & response
Threat hunting
Security operations: Increasing volume of alerts is overwhelming most SOCs

Security operations: “Single data source” products are not solving the problem

Our Approach: Provide the SOC with complete visibility, advanced AI/ML analytics and end-to-end automation

OUR GOALS

100% Of attack surface is visible and analyzed

100% Of attacks identified and stopped

Minutes To respond to threats, not days

Cortex XPANSE
Cortex XDR
Cortex XSOAR
Cortex XDR: The central product for a next-gen SOC; it integrates & normalizes all data, drives AI/ML analytics
Cortex XPANSE: Full visibility of all internet assets; when integrated with XDR, it provides a complete enterprise view

Cortex XPANSE

- Discovers and reduces the entire attack surface
- Cross-correlates internal view of assets with outside-in mapping
- Understands exposure to new attacks and how attacks have unfolded (including supply chain exposures and Nation State vulnerabilities)

Cortex XDR

- Endpoint Analytics
- Network Analytics
- Cloud Analytics
- Identity Analytics
- Continued Innovation

Data Sources

- Endpoints
- Network
- Cloud
- Identity
- Additional sources

All Data Stitched & Normalized
Cortex XSOAR: End-to-end workflow automation for security operations; it enables the SOC to focus on critical alerts

Cortex XPANSE
- DisCOVERs and reduces the entire attack surface
- Cross-correlates internal view of assets with outside-in mapping
- Understands exposure to new attacks and how attacks have unfolded (including supply chain exposures and Nation State vulnerabilities)

Cortex XDR
- Endpoint Analytics
- Network Analytics
- Cloud Analytics
- Identity Analytics
- Continued Innovation

Cortex XSOAR
- Scales and accelerates security operations with automation
- Provides playbook-driven security process orchestration
- Discovers third party playbooks through an extensive SOAR marketplace

Data Sources:
- Endpoints
- Network
- Cloud
- Identity
- Additional sources

All Data Stitched & Normalized
Palo Alto Networks SOC: Eating our own dog food

Cortex XPANSE
outside-in attack surface management

248K Public Assets
(Internet Attack surface exposures discovered and remediated)

Cortex XDR

23 TB / Day of Data

- Deployed across 100% of our endpoints
- Ingesting all network security data
- Ingesting identity & cloud data
- Prevented SolarWinds attack

Cortex XSOAR
orchestration tool to respond to alerts

~90% Automation
(47 Playbooks, run 350 times per day)

SOC Analysts
free to focus on remaining few high-risk incidents

Comprehensive security

<table>
<thead>
<tr>
<th>Network</th>
<th>Endpoint</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prisma Access</td>
<td>Cortex XDR</td>
<td>Prisma SaaS</td>
</tr>
<tr>
<td>NGFWs, VMs, and Security Services</td>
<td></td>
<td>Prisma Cloud</td>
</tr>
<tr>
<td>10K Employees</td>
<td>Cortex XDR</td>
<td>Data Security</td>
</tr>
<tr>
<td>50K Endpoints</td>
<td></td>
<td>4.3 Million Cloud Assets</td>
</tr>
</tbody>
</table>

23 TB / Day of Data

High-risk alerts

248K Public Assets

(Internet Attack surface exposures discovered and remediated)

~90% Automation
(47 Playbooks, run 350 times per day)

High-risk alerts

23 TB / Day of Data

High-risk alerts
Palo Alto Networks SOC: Industry-leading 1 min response time

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC

16.6 B Events

- **Events**
- **Alerts / incidents**
  - 467 Alerts
    - 67 Incidents
- **Automated / manual analysis**
  - 58 Automated
    - 9 Manual
- **Major incidents**
  - 0

**Mean time to detect**
- **10 SECONDS** (High priority alerts)

**Mean time to respond**
- **1 MINUTE**
Security Operations expected to grow ~15% YoY, driven by need for ML analytics and automation

Endpoint protection market expected to sustain a 20% CAGR fueled by EDR to XDR transition

Vulnerability Assessment market expected to grow at 24% YoY fueled by increasing need to monitor the enterprise attack surface

Total Addressable Market
15% CAGR (CY21-CY24)


Source: 451 Group, Gartner, IDC, Omdia, and PANW internal estimates
Cortex: Gaining industry recognition and customer traction across our product portfolio

Cortex XPANSE
Outperformer Leader in GigaOm's Vulnerability Management Radar; recognized in first Gartner ASM report

Cortex XDR
Best combined prevention and detection in MITRE ATT&CK evaluation and a leader in Forrester ESS Wave

Cortex XOAR
Leader in KuppingerCole Security Orchestration Automation and Response Leadership Compass

74 of Fortune 100 Customers

---

1. Acquisition closed less than a year ago
2. Cortex XDR Pro customer count
Delivering the Zero Trust Enterprise

Nir Zuk
Zero Trust is now a US Presidential Priority

What is Zero Trust?

A strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.
Securing users with Zero Trust

- **Identity**: Validate users using strong authentication
- **Device/Workload**: Verify user’s device integrity
- **Access**: Enforce least-privilege user access to data and applications
- **Transaction**: Scan all content for malicious activity and data theft
Securing applications with Zero Trust

Identity
Validate developers, devops, and admins with strong authentication

Device/Workload
Verify workload integrity

Access
Enforce least-privilege access for workloads accessing other workloads

Transaction
Scan all content for malicious activity and data theft
Securing infrastructure with Zero Trust

**Identity**

Validate all users with access to the infrastructure

**Device/Workload**

Identify all devices including IoT

**Access**

Least-privilege access segmentation for native and third-party infrastructure

**Transaction**

Scan all content within the infrastructure for malicious activity and data theft
Zero Trust demands a holistic and consistent approach that is actionable across all key domains

<table>
<thead>
<tr>
<th>Identity</th>
<th>Device/Workload</th>
<th>Access</th>
<th>Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate users</td>
<td>Verify user device</td>
<td>Enforce least-privilege</td>
<td>Scan all content for</td>
</tr>
<tr>
<td>with strong</td>
<td>integrity</td>
<td>access to data and</td>
<td>malicious activity and</td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td>applications</td>
<td>data theft</td>
</tr>
<tr>
<td>Validate</td>
<td>Verify workload</td>
<td>Enforce least-privilege</td>
<td>Scan all content for</td>
</tr>
<tr>
<td>developers,</td>
<td>integrity</td>
<td>access for workloads</td>
<td>malicious activity and</td>
</tr>
<tr>
<td>devops, and admins</td>
<td></td>
<td>accessing other</td>
<td>data theft</td>
</tr>
<tr>
<td>with strong</td>
<td></td>
<td>workloads</td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td>Validate all users</td>
<td>Least-privilege access</td>
<td>Scan all content within</td>
</tr>
<tr>
<td></td>
<td>with access to the</td>
<td>segmentation for</td>
<td>the infrastructure for</td>
</tr>
<tr>
<td></td>
<td>infrastructure</td>
<td>native and third-party</td>
<td>malicious activity and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>infrastructure</td>
<td>data theft</td>
</tr>
</tbody>
</table>

**Zero Trust for Users**

- Validate users with strong authentication
- Validate developers, devops, and admins with strong authentication
- Validate all users with access to the infrastructure

**Zero Trust for Applications**

- Validate users with strong authentication
- Validate developers, devops, and admins with strong authentication
- Validate all users with access to the infrastructure

**Zero Trust for Infrastructure**

- Validate users with strong authentication
- Validate developers, devops, and admins with strong authentication
- Validate all users with access to the infrastructure
While each of our three platforms are Zero Trust, deploying them together enables a strong foundation for a Zero Trust Enterprise
Our product portfolio is the foundation for sustained growth

**Revenue CAGR**

FY21–FY24

23%

**Billings CAGR**

FY21–FY24

22%

---

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 Represents midpoint of guidance.

Fiscal year ending on July 31.
Securing Our Customers

BJ Jenkins
We have proven that our core + speedboat sales model works

Core sales

3.2K+ strong team

~5% systematic productivity gains annually

~50% of reps participated in 2 or more speedboats¹

Speedboat sales

850+ specialists

95%+ CAGR in speedboat product sales FY19-FY21

220+ accounts with > $1M in speedboat sales

¹Rep participation refers to FY21 closed deals across Prisma Cloud, Prisma SASE and Cortex
We have opportunity to drive scale and better execution

- **‘One team’ mindset**
  Aligned leadership with a common forecast and set of goals

- **Joint account plans**
  Singular account plans across Core and Speedboats

- **Shared incentives**
  Compensation structures that promote collaboration

- **World-class enablement**
  Investment in ensuring Core reps can sell full portfolio

Tighter coordination and collaboration to help secure our customers
Ecosystem transformation enables us to further leverage partnerships

Cybersecurity ecosystem adapting to Cloud & SaaS

- **Value-added resellers**: Transforming business models for Cloud & SaaS
- **System integrators**: Strengthening role on digital transformations
- **Service providers**: Driving network shift from MPLS to SASE
- **Cloud service providers**: Driving Cloud Native Security via marketplaces

Our portfolio breadth enables deeper partnerships

*Todays we have...*

- **8K+** NextWave Partners
- **~$1B** via SI & SP in FY21
- **$250M+** via AWS / GCP / Azure

---

1SI refers to System Integrators, SP refers to Service Providers
2FY21 sales through pay-as-you-go marketplaces and the private offer placement from via Amazon Web Services / Google Cloud Platform / Microsoft Azure only

© 2021 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.
We delivered stellar customer satisfaction while doubling our portfolio

- Professional services
- Customer success
- Customer support

2x number of offerings to support vs. FY19

63% Deflection rate

90% CSAT

7th consecutive TSIA & JD Power awards

1Based on unique use case and service offerings between FY'19 and FY'21
2Customer Satisfaction (CSAT) based on transactional surveys conducted at various points of the customer journey (e.g., once ticket is resolved for support)
Looking ahead...

Built a strong foundation over 3 Years

- Launched our three best-of-breed platforms
- Achieved product-market fit across our portfolio
- Stood up speedboat go-to-market motion with 850+ specialists
- Maintained customer satisfaction at 90%+ through all the change
- Landed at least two of our platforms with 70%+ of our G2000\(^1\) customers

Supercharge our model going forward

- Continue to innovate and make our platforms work better together
- Strengthen our brand & recognition
- Scale our reach across segments and geographies
- Develop a harmonized sales motion across Core and speedboats
- Land all three of our platforms at the majority of our largest customers

Palo Alto Networks - True multi-platform cybersecurity company set to win in three of the largest segments in the industry

\(^1\)G2000 is the Forbes Global 2000 Companies
Drivers of Change - Our People

Liane Hornsey
Our goal: Be the best company to work for
A clear plan to execute world-class environmental, social & governance strategies

ENVIRONMENT—Our Planet
We are committed to using 100% renewable energy and reducing emissions

SOCIAL—Our People & Our Communities
We are ensuring our employees are motivated and our communities are digitally secure

GOVERNANCE—Our Integrity
We do the right thing, always
<table>
<thead>
<tr>
<th><strong>FY19</strong></th>
<th><strong>FY20-21</strong></th>
<th><strong>FY22+</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A Legacy of Stewardship</strong></td>
<td><strong>Declare Carbon Neutral Goals</strong></td>
<td><strong>Execute at Scale &amp; Speed</strong></td>
</tr>
<tr>
<td>• Formed Green Teams to increase employee engagement and execute sustainability initiatives</td>
<td>• Achieved 85% LEED(^1) certification across real estate portfolio</td>
<td>• Engage supply chain in setting Science Based Targets</td>
</tr>
<tr>
<td>• Prioritized LEED(^1) certified workplaces</td>
<td>• Committed to 100% Renewable energy by 2030</td>
<td>• Secure CDP leadership rating</td>
</tr>
<tr>
<td></td>
<td>• Invested in high-quality carbon offset programs</td>
<td></td>
</tr>
</tbody>
</table>

---

"Green" for years

Reported to Carbon Disclosure Project (CDP)

Future reporting aligned to TCFD\(^2\) framework

---

\(^1\) LEED: Leadership in Energy and Environmental Design

\(^2\) TCFD: Task Force on Climate Related Financial Disclosures.
Social—Our People & Communities: Investing in the Future of Work

FY19 Employee-Driven Values and Learning
- Stood-up programmatic early in career development at scale
- Improved our URM and diversity percentages
- Helped youth stay safe online through Cybersecurity Education

FY20-21 People-centric, Inclusive & Diverse
- Achieved fair pay, promotion, and performance & mobility
- FLEXWORK Coalition; personalized location, benefits, and learning
- 81% of employees highly engaged—no diversity differential
- Raised ~$6M for COVID Relief, social injustice and racial inequity causes

FY22+ Targets
- Expand FLEXWORK initiatives and lead in the future of work
- Be the top cybersecurity company for diverse employees
- Grow Cybersecurity Education programs to reach 20M by 2025

Leadership hiring elevated; targeted top tech companies

~90% diverse slates & panels 25% women, 14.5% URM (U.S.)¹

100% leadership teams diverse² 40% women, 20% URM (U.S.)³

¹ As of August 30, 2021.
² By 2023.
³ By 2025.
Governance—Our Integrity: Underpinning Everything We Do

**FY19**
Corporate Behavior & Suppliers
- Ensured strong Code of Conduct and **compliance training**
- **Protected data** with cutting-edge Security Operations Center
- Deployed Global **Supplier Code of Conduct** across supply chain

**FY20-21**
Board Governance
- Amended NomGov Committee charter to include ESG
- Included ESG duties in Comp & People **Committee Charter**
- Launched a **Supplier Diversity** program

**FY22+**
Looking Ahead
- Tie FY22 executive **cash compensation** to ESG outcomes
- **Establish Security Committee** of our Board of Directors
- Increase **reporting transparency**, including ESG supplement

---

**Foundational structures in place**

**Board diversity up from 9% to 33%**

**Exec compensation tied to climate and diversity**

---

1 From FY18 to FY21
External stakeholders are recognizing our work

### Employer Branding Recognition

**InHerSight**
- **Support for Diversity**
- **Best Places to Work** #11 in July 2021

**Glassdoor Progression**
- **Overall rating:** 3.9 / 5.0 (an increase of 0.7)
- **CEO approval rating:** 87.4% (an increase of 30.4%)

**Overall Inclusion and Diversity score** (4.2 / 5.0)
- **Positive Business outlook:** 74.9% (an increase of 23.4%)

**Comparably**
- **Diversity Score:**
  - Palo Alto Networks currently ranks in the Top 10% of similarly sized companies on Comparably.
- **Gender Score:**
  - Palo Alto Networks currently ranks in the Top 15% of similarly sized companies on Comparably.

**WayUp**
- **Top 100 Internship Program**

### Inclusion & Diversity Recognition

- **Best Places to Work for Disability Inclusion**
- **DEI Equality Index**
- **Dun’s 100** The Standard of Achievement
- **CRN Women of the Channel 2021**

### Overall ESG Recognition

- **EcoVadis Gold Rating 2021**
- **Just Capital ESG Industry Top Rated**

---

1 Recognition as of July 31, 2021.
2 Increase occurred during the period of March 2020 to July 2021.
3 Recognition as of August 18, 2021.
4 Recognition as of 2021 reporting cycle for issuer.
All of our actions are driven by our 5 core values
Managing for Scale and Efficiency
Nikesh Arora
We are building three great businesses within a single company

**Strata / SASE**
- Top 1 in network security revenue ($3.7B)\(^1\) and adj. FCF ($1.6B)\(^1\)
- 55% - 60% software mix in FWaaP\(^3\) in FY24, leading the industry

**Cortex**
- >$400M in ARR\(^2\)
  - >80% growth
- #1 in network security revenue ($3.7B)\(^1\)
- >70% growth
- Leading the transformation of security operations

**Prisma Cloud**
- >$300M in ARR\(^2\)
  - >70% growth
- Top 3 in SASE growing billings faster than the leader, ARR\(^2\)
  - >90% growth
- 0 scaled competing cloud-native platforms
- Blue Ocean Opportunity, one-of-a-kind business

---

\(^1\) Revenue of $3.7B and $1.6B adjusted free cash flow is last 12 months (LTM) basis.

\(^2\) ARR = Annualized Recurring Revenue, which is the annualized allocated revenue of all active contracts as of the final day of the reporting period, which is FY21. Prisma Cloud ARR includes VM-series (public cloud) and CN-series.

\(^3\) Represented by Software % of Firewall as a Platform (FWaaP) Billings. SW % of Total FWaaP billings is the total amount invoiced and billed for the Prisma Access offering, and the ratable portion of VM-Series and CloudGenix offerings, during the period stated, as a percentage of total Firewall as a Platform billings.
Bringing It All Together

Dipak Golechha
We are focusing on all-encompassing value creation

COMPONENTS OF TOTAL SHAREHOLDER RETURN

- Revenue growth
- Profitability
- Cash conversion
- Capital structure
Strong growth in key top-line metrics

**Revenue growth**

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Total Revenue</th>
<th>Total Revenue (Y/Y)</th>
<th>Total Billings</th>
<th>Total Billings (Y/Y)</th>
<th>Remaining Performance Obligation</th>
<th>Remaining Performance Obligation (Y/Y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q420</td>
<td>$950M</td>
<td>18%</td>
<td>$1,390M</td>
<td>32%</td>
<td>$4.3B</td>
<td>41%</td>
</tr>
<tr>
<td>Q121</td>
<td>$946M</td>
<td>23%</td>
<td>$1,083M</td>
<td>21%</td>
<td>$4.4B</td>
<td>40%</td>
</tr>
<tr>
<td>Q221</td>
<td>$1,074M</td>
<td>25%</td>
<td>$1,215M</td>
<td>22%</td>
<td>$4.6B</td>
<td>41%</td>
</tr>
<tr>
<td>Q321</td>
<td>$1,074M</td>
<td>24%</td>
<td>$1,286M</td>
<td>27%</td>
<td>$4.9B</td>
<td>38%</td>
</tr>
<tr>
<td>Q421</td>
<td>$1,219M</td>
<td>28%</td>
<td>$1,868M</td>
<td>34%</td>
<td>$5.9B</td>
<td>36%</td>
</tr>
</tbody>
</table>

1 Total billings is a key financial metric calculated as total revenue plus change in total deferred revenue, net of total acquired deferred revenue. Fiscal year ending on July 31.
RPO trends provide better revenue visibility

### Revenue growth

#### Current RPO Acceleration

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>Current RPO</th>
<th>Non-Current RPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY19 Ending/FY20 Beginning</td>
<td>$1.4B</td>
<td>$1.7B</td>
</tr>
<tr>
<td>FY20 Ending/FY21 Beginning</td>
<td>$2.1B</td>
<td>$2.2B</td>
</tr>
<tr>
<td>FY21 Ending/FY22 Beginning</td>
<td>$3.1B</td>
<td>$2.8B</td>
</tr>
<tr>
<td>FY20</td>
<td>$1.7B</td>
<td>$3.408M</td>
</tr>
<tr>
<td>FY21</td>
<td>$2.3B</td>
<td>$4.256M</td>
</tr>
<tr>
<td>FY22 E1</td>
<td>$3.1B</td>
<td>$5.300M</td>
</tr>
</tbody>
</table>

#### Current RPO a Growing Proportion of Revenue & Guidance

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>Current RPO from prior year ending</th>
<th>Total revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY20</td>
<td>$1.7B</td>
<td>$3,408M</td>
</tr>
<tr>
<td>FY21</td>
<td>$2.2B</td>
<td>$4,256M</td>
</tr>
<tr>
<td>FY22 E1</td>
<td>$3.1B</td>
<td>$5,300M</td>
</tr>
</tbody>
</table>

1 Represents the guidance midpoint for revenue in FY’22. Fiscal year ending on July 31.
We are building a large business in cybersecurity’s fastest-growing markets while transitioning to software

Revenue growth

Next-gen Security ARR\(^1\)

<table>
<thead>
<tr>
<th>Q420</th>
<th>Q121</th>
<th>Q221</th>
<th>Q321</th>
<th>Q421</th>
<th>FY22 E(^2)</th>
<th>FY24 T</th>
</tr>
</thead>
<tbody>
<tr>
<td>$651M</td>
<td>$719M</td>
<td>$840M</td>
<td>$973M</td>
<td>$1,180M</td>
<td>$3,250M</td>
<td></td>
</tr>
</tbody>
</table>

40% CAGR

Continued Transition to Software in Firewall as a Platform\(^3\)

<table>
<thead>
<tr>
<th>FY19</th>
<th>FY20</th>
<th>FY21</th>
<th>FY22 E(^4)</th>
<th>FY24 T</th>
</tr>
</thead>
<tbody>
<tr>
<td>11%</td>
<td>22%</td>
<td>39%</td>
<td>40-45%</td>
<td>55-60%</td>
</tr>
</tbody>
</table>

Mid single-digit product revenue growth CAGR, through FY24

---

\(^1\) ARR = Annualized Recurring Revenue. Next-Gen Security ARR is the 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.

\(^2\) Represents midpoint of FY22 guidance.

\(^3\) Firewall as a Platform (FWaaS) billings is a key financial and operating metric defined as publicly reported product billings, together with total amount invoiced and billed for Prisma Access offering, and the ratable portion of VM-Series and CloudGenix offerings, during the period stated.

\(^4\) Software % of Firewall as a Platform Billings is the total amount invoiced and billed for the Prisma Access offering, and the ratable portion of VM-Series and CloudGenix offerings, during the period stated, as a percentage of total Firewall as a Platform billings.

Fiscal year ending on July 31.
Sustaining gross margin as we drive NGS momentum

**Profitability**

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>NGS Billings % of Total Billings</th>
<th>Non-GAAP Gross Margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY19</td>
<td>13%</td>
<td>~75%</td>
</tr>
<tr>
<td>FY20</td>
<td>22%</td>
<td>~75%</td>
</tr>
<tr>
<td>FY21</td>
<td>28%</td>
<td>~75%</td>
</tr>
<tr>
<td>FY24 T</td>
<td>~75%</td>
<td>~75%</td>
</tr>
</tbody>
</table>

1. Next-Gen Security (NGS) billings is a key financial and operating metric. Prior to Q2’21, NGS billings was defined as the total amount invoiced and billed during the period stated for Prisma and Cortex offerings inclusive of the VM-Series and related services; for Q2’21 and afterwards, NGS billings is defined as total revenue plus change in total deferred revenue, net of total acquired deferred revenue for Prisma and Cortex offerings inclusive of the VM-Series and related services.

2. Total billings is a key financial metric calculated as total revenue plus change in total deferred revenue, net of total acquired deferred revenue.

Fiscal year ending on July 31.

- Increasing NGS mix, balancing gross margin
- Core margins stable
- In FY22, we expect total company gross margin to be a balance of these two forces
Coordinated execution is enabling leverage from sales and marketing

Sales rep productivity, post FY'19 speedboat investments

- Overlay (speedboat) model implemented in FY20
- Core productivity has improved throughout
- In FY22-24, we expect improvements in productivity across our go-to-market organization

Fiscal year ending on July 31.

Total Palo Alto Networks sales rep productivity (Bookings per sales rep)
Beyond operating leverage, cash conversion will drive free cash flow margin expansion

Cash conversion

Non-GAAP operating margin and adjusted free cash flow margin progression

- Driving to industry best in class working capital benchmarks
- Optimizing large transactions for long-term value and cash terms
- Use of public cloud as alternative to CAPEX
- Expecting 100–150bp of annual FCF margin expansion beyond FY22, through FY24

---

1. FY22 E represents the midpoint of guidance for adjusted free cash flow margin and non-GAAP operating margin. FY24 T represents the midpoint of the target for adjusted free cash flow margin and non-GAAP operating margin. Fiscal year ending on July 31.
Our cash conversion puts us at the top of our peer group

<table>
<thead>
<tr>
<th>Company Name (&gt;=$3B in revenue)</th>
<th>Latest FY Revenue</th>
<th>Forward Revenue Growth Rate</th>
<th>Latest FY FCF Margin</th>
<th>Revenue Growth + FCF Margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>$12.9 B</td>
<td>22%</td>
<td>41%</td>
<td>63%</td>
</tr>
<tr>
<td>ServiceNow</td>
<td>$4.5 B</td>
<td>29%</td>
<td>32%</td>
<td>61%</td>
</tr>
<tr>
<td>Palo Alto Networks</td>
<td><strong>$4.3 B</strong></td>
<td><strong>24% – 25%</strong></td>
<td><strong>33%</strong></td>
<td><strong>57% – 58%</strong></td>
</tr>
<tr>
<td>Autodesk</td>
<td>$3.8 B</td>
<td>15%</td>
<td>36%</td>
<td>51%</td>
</tr>
<tr>
<td>Intuit</td>
<td>$9.6 B</td>
<td>15%</td>
<td>33%</td>
<td>49%</td>
</tr>
<tr>
<td>Microsoft</td>
<td>$168.1 B</td>
<td>14%</td>
<td>33%</td>
<td>47%</td>
</tr>
<tr>
<td>VMware</td>
<td>$11.8 B</td>
<td>9%</td>
<td>35%</td>
<td>44%</td>
</tr>
<tr>
<td>Salesforce.com</td>
<td>$21.3 B</td>
<td>24%</td>
<td>19%</td>
<td>43%</td>
</tr>
<tr>
<td>Workday</td>
<td>$4.3 B</td>
<td>18%</td>
<td>24%</td>
<td>42%</td>
</tr>
<tr>
<td>Oracle</td>
<td>$40.5 B</td>
<td>4%</td>
<td>34%</td>
<td>38%</td>
</tr>
<tr>
<td>Citrix Systems</td>
<td>$3.2 B</td>
<td>0%</td>
<td>28%</td>
<td>27%</td>
</tr>
<tr>
<td>Open Text Corp</td>
<td>$3.4 B</td>
<td>2%</td>
<td>24%</td>
<td>26%</td>
</tr>
<tr>
<td>Akamai</td>
<td>$3.2 B</td>
<td>8%</td>
<td>15%</td>
<td>23%</td>
</tr>
<tr>
<td>SAP</td>
<td>$33.2 B</td>
<td>-3%</td>
<td>22%</td>
<td>19%</td>
</tr>
</tbody>
</table>

1. Palo Alto Networks Forward Revenue Growth Rate represents the guidance range for revenue growth for FY'22.
2. Latest FY Revenue is revenue for each company’s most recently completed fiscal year, as reported from FactSet on 9/8/2021.
3. Forward Revenue Growth Rate represents year over year growth % for next fiscal year revenue consensus, as reported from FactSet on 9/8/2021.
4. Latest FY FCF Margin is reported Free Cash Flow divided by Revenue for each company’s most recently completed fiscal year, as defined and reported from FactSet on 9/8/2021.

ASPIRE TO THE “RULE OF 60”
We expect to maintain a balanced capital allocation strategy

Capital structure

Focus areas of capital allocation strategy

Invest in organic growth

Return to holders

Optimize capital base

Acquisitions to accelerate strategy

FY2018 – FY2021

- Net debt proceeds of $2.7B\(^1\)
- Used $2.5B of cash in acquisitions\(^2\)
- Healthy buyback activity driven by cash generation

FY2022 – FY2024

- Adj. FCF Generation
- Use of Cash
  - Debt Repayment
  - M&A
  - Share Buybacks
- >$6.0B

---

\(^1\) Represents 2018 and 2020 new debt with $3.3B in proceeds, net of issuance and hedge costs, and 2019 debt maturity payment of $575M.

\(^2\) $2.5B is net of cash acquired. Total acquisition consideration, including equity for the FY18-21 period is $3.2B.

Fiscal year ending on July 31.
We are actively working down stock-based compensation while operating in a competitive environment.

### Stock-based compensation (SBC) Trends

<table>
<thead>
<tr>
<th>Year</th>
<th>M&amp;A SBC as a percentage of revenue</th>
<th>Underlying SBC per headcount ($k)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY18</td>
<td>0.6%</td>
<td>$93k</td>
</tr>
<tr>
<td>FY19</td>
<td>2.3%</td>
<td>$76k</td>
</tr>
<tr>
<td>FY20</td>
<td>4.0%</td>
<td>$68k</td>
</tr>
<tr>
<td>FY21</td>
<td>6.1%</td>
<td>$66k</td>
</tr>
<tr>
<td>FY22 E - FY24 T</td>
<td></td>
<td>Reduce SBC as % of revenue</td>
</tr>
</tbody>
</table>

- Historically we have used stock grants as part of acquisition currency for retention.
- We are focused on remaining competitive in our industry and geographies we operate.
- In FY22 and beyond, we expect SBC as % of revenue to decline.

1. Stock based compensation includes SBC expense and SBC capitalized for internally developed software.
2. Underlying SBC excludes any M&A SBC.
3. Fiscal year ending on July 31.
## Bringing it all together into an attractive financial profile

<table>
<thead>
<tr>
<th>Revenue</th>
<th>$8B in FY24 revenue, 23% CAGR from FY21</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$10B in FY24 billings, 22% CAGR from FY21</td>
</tr>
<tr>
<td></td>
<td>$3.25B in NGS ARR(^1), 40% CAGR from FY21</td>
</tr>
<tr>
<td></td>
<td>Mid single-digit product growth CAGR, through FY24</td>
</tr>
</tbody>
</table>

### Gross margin
Leverage from scaling products, offsetting mix shift

### Non-GAAP operating income
50–100bp margin expansion annually, beyond FY22, through FY24

### Adjusted free cash flow
100–150bp margin expansion annually, beyond FY22, through FY24

---

\(^1\) ARR = Annualized Recurring Revenue. Next-Gen Security ARR is the 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.

Fiscal year ending on July 31.
Wrap-Up

Nikesh Arora
THANK YOU
<table>
<thead>
<tr>
<th>Time</th>
<th>Section</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30-9:40am</td>
<td>Palo Alto Networks Vision</td>
<td>Nikesh</td>
</tr>
<tr>
<td>9:40-9:50am</td>
<td>Market Needs and Our Platforms</td>
<td>Lee</td>
</tr>
<tr>
<td>9:50-10:20am</td>
<td>Product Strategy - NetSec, Cloud and SOC</td>
<td>Various</td>
</tr>
<tr>
<td>10:20-10:35am</td>
<td>Delivering the Zero Trust Enterprise</td>
<td>Nir</td>
</tr>
<tr>
<td>10:35-10:40am</td>
<td>Driving Sustainable Growth</td>
<td>Nikesh</td>
</tr>
<tr>
<td>10:40-10:50am</td>
<td>Securing Our Customers</td>
<td>BJ</td>
</tr>
<tr>
<td>10:50-11:00am</td>
<td>Drivers of Change - Our People</td>
<td>Liane</td>
</tr>
<tr>
<td>11:00-11:05am</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>11:05-11:10am</td>
<td>Managing for Scale and Efficiency</td>
<td>Nikesh</td>
</tr>
<tr>
<td>11:10-11:35am</td>
<td>Bringing It All Together</td>
<td>Dipak</td>
</tr>
<tr>
<td>11:35-11:40pm</td>
<td>Wrap-up</td>
<td>Nikesh</td>
</tr>
<tr>
<td>11:40-12:30pm</td>
<td>Q&amp;A</td>
<td>All Presenters</td>
</tr>
</tbody>
</table>
# Calculation of Billings

$ in millions

<table>
<thead>
<tr>
<th>Billings:</th>
<th>Q420</th>
<th>Q121</th>
<th>Q221</th>
<th>Q321</th>
<th>Q421</th>
<th>FY'20</th>
<th>FY'21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total revenue</td>
<td>$950.4</td>
<td>$946.0</td>
<td>$1,016.9</td>
<td>$1,073.9</td>
<td>$1,219.3</td>
<td>$3,408.4</td>
<td>$4,256.1</td>
</tr>
<tr>
<td>Add: change in total deferred revenue, net of acquired deferred revenue</td>
<td>439.6</td>
<td>136.8</td>
<td>197.8</td>
<td>212.5</td>
<td>649.0</td>
<td>893.3</td>
<td>$1,196.1</td>
</tr>
<tr>
<td>Total billings</td>
<td>$1,390.0</td>
<td>$1,082.8</td>
<td>$1,214.7</td>
<td>$1,286.4</td>
<td>$1,868.3</td>
<td>$4,301.7</td>
<td>$5,452.2</td>
</tr>
</tbody>
</table>

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

$ in millions

<table>
<thead>
<tr>
<th>Non-GAAP gross profit and gross margin:</th>
<th>FY’19</th>
<th></th>
<th>FY’20</th>
<th></th>
<th>FY’21</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GAAP gross profit and gross margin</td>
<td>$2,091.2</td>
<td>72.1%</td>
<td>$2,408.9</td>
<td>70.7%</td>
<td>$2,981.2</td>
<td>70.0%</td>
</tr>
<tr>
<td>Share-based compensation-related charges</td>
<td>84.2</td>
<td>2.9%</td>
<td>93.9</td>
<td>2.8%</td>
<td>115.7</td>
<td>2.7%</td>
</tr>
<tr>
<td>Amortization expense of acquired intangible assets</td>
<td>40.4</td>
<td>1.4%</td>
<td>68.7</td>
<td>2.0%</td>
<td>97.4</td>
<td>2.3%</td>
</tr>
<tr>
<td>Litigation-related charges(^{(1)})</td>
<td>10.2</td>
<td>0.4%</td>
<td>3.6</td>
<td>0.1%</td>
<td>7.1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Non-GAAP total gross profit and gross margin</td>
<td>$2,226.0</td>
<td>76.8%</td>
<td>$2,575.1</td>
<td>75.6%</td>
<td>$3,201.4</td>
<td>75.2%</td>
</tr>
</tbody>
</table>

\(^{(1)}\) Consists of the amortization of intellectual property licenses and covenant not to sue. Fiscal year ends on July 31.
### GAAP to Non-GAAP Reconciliation - Operating Margin

$ In millions

<table>
<thead>
<tr>
<th>Non-GAAP Operating Income and Operating Margin:</th>
<th>FY'18</th>
<th>FY'19</th>
<th>FY'20</th>
<th>FY'21</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAAP operating loss</td>
<td>(5104.2)</td>
<td>-4.6%</td>
<td>(554.1)</td>
<td>-1.9%</td>
</tr>
<tr>
<td>Share-based compensation-related charges</td>
<td>516.4</td>
<td>22.7%</td>
<td>591.3</td>
<td>20.5%</td>
</tr>
<tr>
<td>Acquisition-related costs (1)</td>
<td>17.9</td>
<td>0.8%</td>
<td>29.8</td>
<td>1.0%</td>
</tr>
<tr>
<td>Amortization expense of acquired Intangible assets</td>
<td>15.6</td>
<td>0.7%</td>
<td>53.0</td>
<td>1.8%</td>
</tr>
<tr>
<td>Litigation-related charges (2)</td>
<td>12.3</td>
<td>0.5%</td>
<td>10.2</td>
<td>0.4%</td>
</tr>
<tr>
<td>(Gain) loss related to facility exit (3)</td>
<td>40.8</td>
<td>1.8%</td>
<td>7.0</td>
<td>0.2%</td>
</tr>
<tr>
<td>Non-GAAP operating income and operating margin</td>
<td>$488.8</td>
<td>21.9%</td>
<td>$637.2</td>
<td>22.0%</td>
</tr>
</tbody>
</table>

(1) Consists of acquisition transaction costs, share-based compensation related to the cash settlement of certain equity awards, and costs to terminate certain employment, operating lease, and other contracts of the acquired companies.
(2) Consists of the amortization of intellectual property licenses and covenant not to sue.
(3) Consists of charges related to the relocation of our corporate headquarters (cease-use loss of $39.2 million and accelerated depreciation in FY’18, cease-use loss of $70.0 million in FY’19 and gain of $3.1 million from the early termination of leases in FY’20) and charges related to the relocation of our research and development center in Israel (cease-use loss of $1.3 million and accelerated depreciation in FY’18).
Fiscal year ends on July 31.

© 2021 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.
### GAAP to Non-GAAP Reconciliation - Adjusted Free Cash Flow

$ In millions

<table>
<thead>
<tr>
<th>Net cash provided by operating activities</th>
<th>FY'18</th>
<th>FY'19</th>
<th>FY'20</th>
<th>FY'21</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$1,038.1</td>
<td>$1,055.6</td>
<td>$1,035.7</td>
<td>$1,503.0</td>
</tr>
<tr>
<td>Less: purchases of property, equipment, and other assets</td>
<td>112.0</td>
<td>131.2</td>
<td>214.4</td>
<td>116.0</td>
</tr>
<tr>
<td>Free cash flow (non-GAAP)</td>
<td>$926.1</td>
<td>$924.4</td>
<td>$821.3</td>
<td>$1,387.0</td>
</tr>
<tr>
<td>Add: capital expenditures for new headquarters(^{(a)})</td>
<td>11.2</td>
<td>28.4</td>
<td>94.3</td>
<td>-</td>
</tr>
<tr>
<td>Add: repayments of convertible senior notes attributable to debt discount</td>
<td>-</td>
<td>97.6</td>
<td>-</td>
<td>0.1</td>
</tr>
<tr>
<td>Add: litigation related payment(^{(b)})</td>
<td>-</td>
<td>-</td>
<td>50.0</td>
<td>-</td>
</tr>
<tr>
<td>Less: cash reimbursement (payments), net related to landlord lease amendment(^{(c)})</td>
<td>16.8</td>
<td>(14.8)</td>
<td>(2.0)</td>
<td>-</td>
</tr>
<tr>
<td>Adjusted free cash flow (non-GAAP)</td>
<td>$900.5</td>
<td>$1,065.2</td>
<td>$957.6</td>
<td>$1,387.1</td>
</tr>
</tbody>
</table>

Free cash flow margin (non-GAAP)

<table>
<thead>
<tr>
<th>FY'18</th>
<th>FY'19</th>
<th>FY'20</th>
<th>FY'21</th>
</tr>
</thead>
<tbody>
<tr>
<td>40.7 %</td>
<td>31.9 %</td>
<td>24.1 %</td>
<td>32.6 %</td>
</tr>
</tbody>
</table>

Adjusted free cash flow margin (non-GAAP)

<table>
<thead>
<tr>
<th>FY'18</th>
<th>FY'19</th>
<th>FY'20</th>
<th>FY'21</th>
</tr>
</thead>
<tbody>
<tr>
<td>40.5 %</td>
<td>36.7 %</td>
<td>28.4 %</td>
<td>32.6 %</td>
</tr>
</tbody>
</table>

\(^{(a)}\) Consists of capital expenditures for new headquarters including a land purchase of $51.7 million in FY’20.

\(^{(b)}\) Consists of a one-time payment in FY’20 related to covenant not to sue.

\(^{(c)}\) 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.