

Dear Stockholders:

May 21, 2020

While our usual cadence for stockholder letters is in the fall, given the unique circumstances of the time we find ourselves in, I thought it would be appropriate to extend additional communication. As I write, over 5 million cases of COVID-19 have been diagnosed globally, impacting virtually every country, company and person in the world. Amid the pain and uncertainty, people are adapting to a new reality – finding new ways to work and developing new social norms. Palo Alto Networks has long been a company at the forefront of change and innovation. In many ways, that spirit of innovation has better prepared us to weather such a crisis. The work that we have been doing over the past few years to move security to the cloud, expand online customer support resources, and offer virtual training to our customers and employees now serves as a strong foundation while the crisis catalyses us to accelerate our efforts.

The current conversation around the world is centered on the health crisis, and it will continue to evolve as science and policy eventually overcome the COVID challenge. In the early months of the pandemic, I have tried to focus our attention internally to how this affects life for Palo Alto Networks and our customers in the near to midterm, and also the potential lasting impacts to our business. A clear understanding of those factors will allow us to leverage our advantages and come through this unprecedented event stronger and more resilient than before. In this letter, I wish to provide insight into how Palo Alto Networks is addressing this new normal and what we expect and are planning for the near future.

Global Outlook: Long-Term Trends

I speak with leaders across many industries daily to discuss not just their cybersecurity needs and plans but also how they are reacting to the current circumstances. There are several short-term impacts that they are all dealing with: declining revenue, employees working from home and uncertainty around how long this will last. It is clear that not one company out there is exempt from the phenomenon we are dealing with. Everyone's situation is definitely unique, but from my conversations, I have gleaned some insights that inform our view into how this may unfold, for both Palo Alto Networks and the world at large.

Global Economy: Just a few short weeks ago, the world economy was firing on all cylinders, and we now face large parts of the world being shut down, disrupting supply chains, and impacting consumer behavior and consumer confidence. Until this confidence is restored, likely by a vaccine, treatment and widespread testing, we will have a slow build back to former levels. We at Palo Alto Networks are planning for a 12-18 month time frame for recovery on the consumer end and its flow through impact to our enterprise-level customers. As we see it, consumer spending is ~70% of GDP, so until the consumer recovers, enterprises will definitely share the impact, oftentimes with a delay compared with the consumer impact.

How Does the Workplace Change: There are some aspects that may be permanently affected, specifically the paradigm of employees reporting to the office every day. We believe it is highly likely that various permutations of work from home become the new normal, with not every employee reporting to the office every day and a much broader degree of choice bestowed on individuals to decide where they want to work. To this end, we are striving to address this proactively.

Announcing FLEXWORK: We do not believe the right answer for us all is to stay home forever, nor is it for all of us to rush to work as things open up. We have established a new program at Palo Alto Networks we are calling FLEXWORK, a new way of working for Palo Alto Networks and perhaps for all of us. Initially *valid till the end of the year*, we will monitor the adoption and behaviors of the workforce to see how we can adapt it for the future. We just published a post on the Palo Alto Networks blog with more details on FLEXWORK¹.

We will continue to open offices around the world as local regulations allow, prioritizing the well-being of our employees as we do so. The significant longer term change we envisage is that our employees must be given the choice regarding how to be most effective in their work. With FLEXWORK, a few essential employees will be

¹ <https://blog.paloaltonetworks.com/2020/05/flexwork/>

encouraged to come in to work, while others will choose how many days they wish to spend in our offices. For employees choosing to work in the office, we will ensure social distancing and all local safety regulations. Over this calendar year, we'll follow how our teams experience and utilize this new policy, and take the opportunity to rethink our workspaces. We're conscious that the gyms, cafes and micro-kitchens that have become the norm in many companies now provide reasons for our employees to be cautious. Some or many of these perks may have to be rethought for the future. Finally, we will help employees enhance their home workspaces, making resources available for key items such as office chairs, external monitors and the like.

We are a company that is guided by our employees, and we will continue to listen to them as we navigate this time together.

Business Impact: The global economy will be substantially impacted by the shutdowns imposed by governments to slow the spread of COVID-19. GDP estimates for 2020 have been universally reduced, and it's highly likely the impact will persist at least through the end of next year, if not beyond. Certain industries such as travel and hospitality will see the largest contraction, and even high performers like technology will not be immune. It is crucial to note the importance of the consumer and also small businesses to the overall health of the economy. Many businesses that rely on consumer strength are likely to be impacted and will follow their own path to recovery, in some cases, pivoting their business more to online. We will need the consumer to return to the marketplace with confidence before global growth can truly resume. There will also be some industries and companies that are poised to benefit. We will likely see their plans and investments accelerate rapidly; we will also see new businesses emerge that we have not yet envisioned.

Technology: On the technology front, we expect businesses to accelerate their technology investments in digital transformation and all the underlying infrastructure and processes to support it. Automation, cloud adoption and remote work will all be prioritized with this focus. These trends will result in a change in networking architectures, which have long been built around security mostly within the context of the data center and users working from secured office premises. In this new architecture, security will become more multifactorial, ubiquitous and standardized.

Businesses that have relied on physical presence – and lots of labor – will need to focus on automation and accelerate their digital transformations across multiple areas, including logistics, pricing and many others. These transitions will be harder to execute until we establish this new rhythm around flexible working. In the new world, digital transformations can be accelerated by cloud transformations, and therefore we anticipate increased activity around our customers moving to the cloud. Remote work infrastructures will need to become more robust and necessary across most organizations; this is not a passing trend. Additionally, we expect a concurrent change in networking architectures to support cloud transformations. *We see this as an opportunity for us to invest, not to be cautious.*

We also expect a renewed interest in homes being secured. As many of us split our time and work from home, enterprises are keen to ensure that employees are secured at home and not just in the office.

Business Practices: A final note on the overall business landscape: We may experience a contraction in the number of players in the cybersecurity ecosystem, specifically in the number of smaller providers. In these risk-averse times, we believe customers will prefer to work with larger, financially stable partners, who can be on call and help when things go wrong, which they invariably do. Given the uniquely fragmented nature of our industry, we are likely to see more demand by CTOs for reduction of security vendors in the IT stack and potential consolidation as a result. While we believe we are uniquely positioned in this environment, it will become important for the larger players in the industry to innovate.

Outlook for Cybersecurity

Cloud Security: With the acceleration away from physical infrastructure to the cloud, and the broad shift from physical workplaces to remote working, come changes to the attack surface and bad actors. Novel attack vectors will be developed specifically for the cloud. We may see employees rely more on non-corporate-approved IT applications for video, messaging and file sharing, along with the cybercriminals following those pathways seeking

opportunities. And to make things harder, cybersecurity has yet to catch up with many of the emergency changes that organizations have rushed to implement. We believe the pace of major data breaches of cloud-delivered services will accelerate, as many InfoSec and DevOps organizations have not yet brought their cloud security posture to the level of their traditional data centers. This will prompt increased investment in cloud security, especially in technologies that secure multi-cloud and hybrid environments.

Artificial Intelligence, Machine Learning and Automation: Traditionally, information security organizations have been accustomed to operating with a high degree of control, as network architectures were clearly defined and slow to change. There has, however, been a substantial amount of integration needed on the customer end. Security has required large SOCs as well as a lot of manual intervention. This will have to change faster. The move to the cloud has introduced uncertainty, with new constituents like DevOps and a new set of vendors, namely the public cloud providers. While businesses accelerate their move away from physical infrastructure to the cloud, and from physical offices to remote work, cybersecurity will need to rely more on technologies that enable InfoSec organizations to operate under uncertainty, namely AI/ML and automation.

Working from Branches and Homes: Moving away from relying primarily on physical offices and physical data centers to emphasizing remote work and the cloud is also accelerating the redesign of wide area networks (WANs). This provides an opportunity to finally realize the long-held vision of networking and network security coming together, as detailed recently by Gartner in their new SASE, or secure access service edge, framework.

Looking Forward: The massive changes that are needed to fit cybersecurity to our new reality provide an opportunity for organizations to pay the technical debt they have accumulated over the last two decades. We believe they will take the opportunity to:

- 1) Significantly reduce the number of cybersecurity solutions and vendors they have by moving to platforms.
- 2) Implement consistent security across the entire infrastructure - physical, virtual, and cloud-delivered as well as across network, endpoint, and cloud.
- 3) Move security from being physical to being delivered in the form of SaaS.
- 4) Secure the cloud with a single platform.
- 5) Automate their security operations.
- 6) Do more for their customers, who will expect more from their security partners, and rightfully so.

Palo Alto Networks Strategy and Vision

Over the last two years, we have been working on our strategy to enable our customers to consolidate their cybersecurity deployments to achieve more optimal and efficient outcomes.

Strata: We've enhanced our network security platform, evolving our Next-Generation Firewall offering from the best Layer 7 security device to a robust platform with a broad set of services like sandboxing, Threat Prevention, Remote Access, URL Filtering, DNS Security, SD-WAN, DLP and soon-to-launch IoT Security. Each of these security services is best in class on its own, yet better when integrated together. These security services are then delivered across our hardware, software and cloud-delivered offerings, meeting customers' evolving architecture needs. This approach is working, and we continue to work hard to deliver the best network security platform.

Prisma SASE: Prisma Access, our cloud-delivered network security service, has been in the spotlight this past quarter, helping customers succeed in the new work-from-home environment. Prisma Access delivers our full set of network security services from the cloud and as a service. This has enabled customers to autoscale up to hundreds of thousands of remote workers and deploy over a weekend. Relatedly, the shift to the cloud is driving a change from backhaul network architectures to a direct-to-app architecture approach. By coupling Prisma Access with our recent acquisition of industry-leading SD-WAN provider CloudGenix, we will provide our customers with the best-in-class solution for securely connecting users to the applications they need, wherever they may be.

Prisma Cloud: We made a bet two years ago that the world would migrate to the cloud, and also that it would be a multi-cloud world, with most companies turning to multiple cloud providers as part of this migration. In the spirit of this vision, we set about acquiring the best businesses and products, and then rapidly integrated them with each other, creating the leading cloud security product in the marketplace and allowing us to get Prisma Cloud in the

hands of over 1,500 customers as well as over 40% of the Fortune 100. We aren't finished enhancing Prisma Cloud, with four new integrated modules soon to be added. We believe Prisma Cloud will continue to be the industry leader, with the broadest set of capabilities and the ability to provide cloud security to all customers who are making their journey to the cloud.

Cortex: Finally, our excitement continues to grow for our Cortex products. We looked at the traditional cybersecurity category of endpoint detection and response (EDR), and wanted to expand our ability to detect, respond to and *prevent* the most sophisticated attacks. So we built a new market category – a category where we apply next-generation AI security analytics across multiple data sources and vendors to deliver superior performance to our customers in their security operations center (SOC). We called it Cortex XDR, and the response from customers, analysts and even competitors has been highly complimentary. Additionally, it is our fundamental belief that we need to fight automated attacks with automation, not with more SOC analysts. This has led us to continue to enhance our Cortex XSOAR product with the expansion to Threat Intel Management. We are now able to automate another key function of the SOC. When combined with XDR, we believe this is the beginning of our opportunity to become the SOC solution of the future.

With this momentum in place driving our innovation engine, we believe we are well on our way to achieving our vision of offering the broadest and most tightly integrated set of cybersecurity products available from any company in the market today.

Conclusion

In closing, I believe that our transformation efforts have been prescient over the last two years, even as we face extreme uncertainty due to the global shock caused by the pandemic. To indirectly quote one of my friends and a legendary business leader, the path to stability will be like the waves caused by a tuning fork. The ongoing wave oscillations could, in our estimation, take 12-18 months before moderating, and the impact could be bumpy over the next nine months. We were early in our anticipation of the need to work from home for our employees, and we focused on settling them first. We continue to believe that our excellence depends on their health, safety and motivation, and we intend to leave no stone unturned to keep them in that state. We announced no COVID layoffs early, not just to keep our employees secure but also to ensure we are using this opportunity to invest.

We at Palo Alto Networks continue to work on our transformation, support our customers and build on our product strategies, which have been welcomed by the market. We think we will emerge from this pandemic even stronger, propelled by our efforts and strategic position.

We have a strong balance sheet, robust cash flow generation and have accelerated our profitability plans as evident in our results this quarter. We hope to continue to progress our strategies to achieve our goal of being the largest, most comprehensive, integrated and innovative cybersecurity company in the world.

I am honored to have the opportunity to be a part of the team at Palo Alto Networks.

A handwritten signature in black ink, appearing to read "Nikesh Arora", with a long horizontal flourish extending to the right.

Nikesh Arora
Chairman & CEO
Palo Alto Networks, Inc.