CYBERSECURITY
PARTNER OF CHOICE

Securing Your AI-Powered Network Transformation: A Guide for C-Suite Leaders

By Anand Oswal, SVP of Product, Network Security at Palo Alto Networks

Complexity is the bane of all network security teams, and they will attest that the more dashboards, screens, and manual integration which they must juggle, the slower their response time. It need not be complex, it need not be disjointed, nor does it need to require adroitness in the art of juggling.

Your network makes engagement with customers, suppliers, and your workforce possible and must include a comprehensive security solution with consistent experiences across the board. Your workforce may be in any location, be it in the office, on the road, or working from home. The network security solutions being used by far too many are unnecessarily complex.

The time for change was yesterday, the opportunity for transformation is today. Artificial intelligence (AI) and generative AI capabilities have advanced, and this means that today enterprises that embrace the transformation and adopt platformization can look across their infrastructure through a single pane of glass and deal with security incidents in near-real time to meet the challenges of today's environment.

Today, criminal entities are able to mount their exploits quicker than ever before. Their ability to have their exploits work at machine speed, means that network security must also be working at machine speed. This puts tremendous pressure across your network's security stack to identify, isolate and remediate incidents as they occur. Now we must measure resolution in minutes or seconds.

Threats have historically been analyzed in a siloed manner, where the exploit was taken into a protected environment (sandbox) and analyzed and a solution produced and distributed. Clearly not machine speed.

Clearly, there is a need for change, for leveraging the advances provided by AI which increases visibility, accelerates identification of threats. By sending user traffic through the network security infrastructure, the application of AI and Machine Learning (ML) on the traffic makes it possible to find the threats and to block them inline.

Platformization Leveraging AI

The unified security stack, platform approach, brings to the forefront the knowledge afforded by the Palo Alto Networks global footprint. This obviates the myopic vision that the industry has historically embraced, point solution products.

The opportunity which AI presents is amazing, our ability to understand the risks and threats increases as the information becomes a part of our corpus. This corpus permits us to implement generative AI in a powerful manner across the entire suite of our offerings. In doing so, the accuracy of identifying threats is not only increased, the ease of use and understanding follows, with a single pane of glass view.

With the natural language processing provided by the AI/ML the expected acceleration of risk identification and remediation is evidenced. Your information security team no longer must be solely versed in the unique cybersecurity nomenclature, but they are also able to ask questions such as along the lines of "what is the risk or threat being presented" or "what are the recommended paths to remediation" or "what processes may need adjusting" and have the answer provided. It is important to emphasize, with the unified security stack, the implementation is ordered once and implemented across the infrastructure, addressing all areas affected. The power of natural language engagement and generative AI implementation in the correct manner provides visibility into root cause and pathways to remediation, which is the desired destination.

Yet not all security platforms are created equal. The platform must be innovative, it must be comprehensive, it must be integrated, and it must be able to operate in real time. These four components are key to the platform approach embraced by Palo Alto Networks.

Innovated Transformation

In sum, the time for transformation is today, the advances in understanding the power of AI have arrived, the ability to bring speed, clarity and address threats known and unknown are in hand. The ability to segment incidents and problems is now possible resulting in the reduction of information technology team escalations.

Leaders do not eschew innovation; indeed, they embrace it as it provides competitive advantage and the opportunity to leapfrog and disrupt one's sector. Adversaries are also innovative and their reduction of time from compromise to exploitation from 44 days to hours provides us with sufficient evidence of their level of innovation. We are not, however, operating in a vacuum and we at Palo Alto Networks are blessed with visibility which enables us to employ AI strategically and comprehensively into our solution.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com