SPONSORED CONTENT | WHITE PAPER

AI at the foundation: A unified approach to enterprise network security

White paper

Many enterprises face a trio of costly security-related problems: fragmented data, limited visibility, and manual processes. The consequences include heightened risk of network downtime, increased fallout from undetected breaches, and snowballing human error. An integrated artificial intelligence (AI)–native security solution can boost network uptime, identify security threats, and dramatically reduce errors — shoring up security more efficiently than any alternatives to date.

CIO

SPONSORED BY JUNIPER NETWORKS

White paper

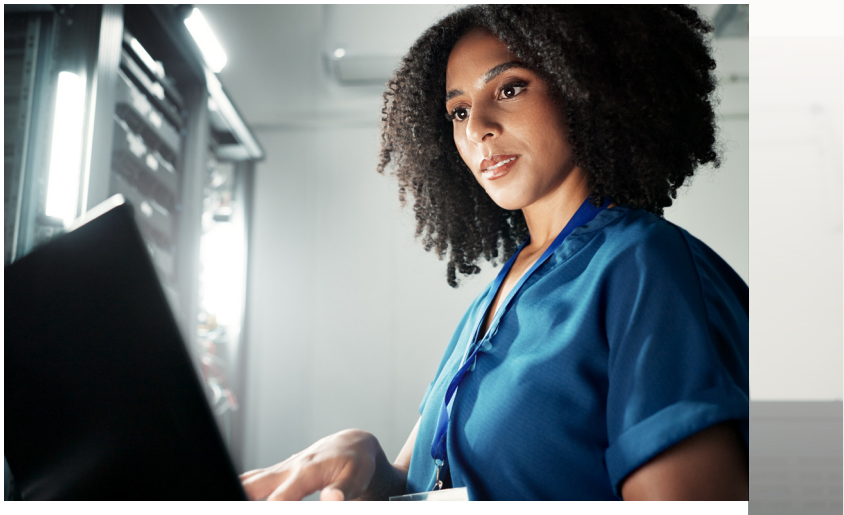
Enterprise security has emerged as the top priority for both IT and business leaders, driven by the increasing volume and complexity of threats and the expanding attack surface in today's digital environments. Those threats can result in nearly incalculable costs, with the future of the enterprise hanging in the balance.

Yet security and networking teams are often frustrated in their efforts to mitigate risks. Their systems are often siloed, and so are the teams themselves, with little to no communication between them. These disconnects limit visibility and efficiency, resulting in fragmented data, slower threat detection, and delays in addressing potential breaches.

There is a better way. Solutions that integrate security with WAN, wireless, wired, DC, and other networking technologies can provide comprehensive visibility across both domains. Solutions that are powered by AI can automate many aspects of threat detection and response, enabling ops teams to react faster and more accurately without impacting network performance. Juniper Networks offers the industry's first AI-powered solution for natively integrating networking and security management functions.

Integrating enterprise network security is no longer optional

Enterprise security systems are plagued with false positives. It is often challenging to differentiate between a network failure and a cyberthreat. This lack of clarity, compounded by the inability to easily collaborate, is frustrating for network and security teams alike. Without a coordinated approach, working out the origin of a problem is more time-consuming, delaying response and remediation



White paper

and potentially opening the door to additional risks — and even a small security issue can result in costly network downtime.

AI: The difference maker

One thing organizations don't have control over is when their systems will be attacked. What they can do is improve the likelihood of recognizing a threat and reducing its negative impact. An AI-native approach drastically reduces the potential for human error, by proactively analyzing network traffic data to detect anomalies and known threats. An AI-powered system will send security issues straight to the security team, relieving the networking team from having to figure out whether an incident is a cyberattack or something else.

AI offers visibility across all enterprise domains, even during off hours. An effective integrated system can manage firewalls, switches, Wi-Fi, and the like. It can isolate components if an anomaly is detected or even sever connections if the threat is definitive, increasing network reliability and uptime. An AI-native security solution can also shorten the time to innocence following an incident, freeing teams to focus on the origin of the problem — whether it was network-related, security-related, or both.

AI excels at documentation. It assists enterprises in achieving regulatory compliance by improving report accuracy and expediting security health assessments. It can compile comprehensive, detailed maps of an organization's entire networking and security infrastructure, identifying device types, connections, and paths.

By unifying disparate data, an AI-native solution amplifies data-driven decision-making. Real-time analytics can verify facts, make predictions, and deliver insights that encourage innovation. AI for IT operations (AIOps) speeds up decision-making and bolsters confidence in recommended

White paper

actions. For instance, when a security alert occurs, the investigation usually involves pulling logs, checking connection states, and hunting for evasive tactics. With AIOps, instead of manually investigating, teams can view a unified dashboard that shows network and security data, enabling them to quickly validate their assumptions and resolve issues faster.

The advantages of an AI-native system are not only more robust security and better network performance but also improved user experiences across the board. Staff members are much more productive, far less frustrated, and more likely to enjoy their job. With the ongoing shortage of skilled networking and cybersecurity professionals, an integrated AI-native network security solution can give an enterprise a decided edge.

Juniper's future-proofing approach to network security

Juniper Networks has developed the first industry solution to natively integrate networking and security functions. Trained with real-world network data, its AI models use natural-language processing and understanding to deliver accurate, relevant responses. Juniper employs an Agile development approach, constantly iterating and improving its models. Its cloud-native microservice architecture is updated, maintained, and optimized on an ongoing basis in real time.

AI can unify disparate data streams, rapidly identify security threats, and automate network problem resolution. Seamless integration of security and networking functions enhances real-time responses while minimizing disruptions for end users. By adopting Juniper's AI-native approach to network security, organizations can expect a more secure, reliable, productive network environment and be assured that any problems that do occur will be recognized and remediated quickly. Investing in AI-driven integrated network security management is fast becoming table stakes for enterprises seeking both enhanced security and optimal network performance.

Learn more | juniper.net