FORTINET: OPTIMIZING BUSINESS OUTCOMES THROUGH NETWORK AND SECURITY CONVERGENCE

EXECUTIVE SUMMARY

Traditionally, networking and security have functioned in isolation. However, today's highly distributed hybrid work environments demand a different approach. Siloed operations, although suitable for fixed network perimeters and predictable traffic flow of the past, no longer meet the demands of modern IT applications and workloads.

Instead, what is needed is a unified technology stack, one that seamlessly integrates best-in-class networking and security that can be deployed at scale and across multiple domains, including on-premises, in the cloud, and at network edges. The era of bolt-on security solutions is a consideration of the past, given the value that convergence brings in simplified management, elimination of blind spots, and dramatically improved efficacy.

Ultimately, consolidation will lead to improved business outcomes for organizations of all sizes through higher operational efficiency and lower operational expenditures. It also allows IT professionals to focus on business innovation rather than network break-fix and reactive security triage. However, to realize these benefits, any modern network strategy must also comprehend the security process and deployment lifecycle.

Moor Insights & Strategy believes Fortinet is well positioned to deliver robust networking and security at scale cross-domain as a market innovator and leader. The combination of Fortinet's FortiOS, next-generation firewalls (NGFWs), network access points (APs), and switches, all of which can be managed through a single fabric and management console with robust security features, is compelling. Furthermore, the company's custom application-specific integrated circuit (ASIC) capabilities and continued investment in research and development serve as a foundation for continued innovation.

THE VALUE OF CONVERGING NETWORKING AND SECURITY

The value of converging networking and security cannot be overstated. With cyber threats ever increasing and growing in complexity, tighter collaboration between NetOps and SecOps teams will improve network resilience and security postures. Additionally, the proliferation of security point solutions that layer on top of networks, often reaching tens to hundreds of instances, depending on an organization's size, is becoming untenable to manage.

The disaggregated nature of modern infrastructure and hybrid work also presents unique challenges. Supporting people, places, and the Internet of Things continues to expand an overall threat surface, creating opportunities for bad actors to exploit gaps and vulnerabilities. Tight integration of networks and security promises to mitigate and eliminate breaches with proactive threat detection and advanced security analytics. Through real-time network traffic monitoring, integrated security protocols can neutralize threats, often before materializing into full-scale attacks that require reactive, time-consuming efforts to resolve.

With all of this in mind, the convergence of networking and security promises to simplify management, ensure consistent application access and performance, safeguard organizational "crown jewels," protect confidential data, meet critical compliance objectives, and, most importantly, optimize business outcomes for internal stakeholders through streamlined operational efficiency. Through tight security feature integration that is comprehended within the network infrastructure product development process, designs can be optimized and tested to ensure the highest levels of reliability, performance, and resilience. This starkly contrasts security point solutions that are layered into network infrastructure via application programming interface (API) calls that are vulnerable to misconfiguration, often resulting in swivel chair management through a proliferation of individual management consoles.

FORTIOS

Fortinet delivers a converged networking and security fabric through FortiOS. FortiOS provides a foundation for a single source of truth by aggregating all network functions (LAN, WLAN, SD-WAN, and WAN backhaul) in a single platform. It leverages a single codebase to support secure networking, zero-trust access, and onboard network access control (NAC) services, facilitating the consolidation of network and security operations.

Furthermore, onboard NAC services are continually fed and expanded by security services, facilitating onboarding of wired and wireless devices automatically, placing each in the appropriate security context when connected to Fortinet access points and switches. This closed-loop architecture can also be deployed across various network edges, operating as a single system that enables consistent connectivity and security policy enforcement. As a result, data, devices, workflows, and applications can traverse today's dynamic networking landscape efficiently and securely, allowing organizations to track, optimize, and protect the underlying data, applications, devices, and workflows end-to-end. Consequently, advanced services and automation can be seamlessly integrated into the FortiOS platform and extended to network edges, thus preventing threats at scale.

Fortinet Security and Networking Platforms

To augment its network and security fabric, Fortinet offers NGFWs as well as a broad portfolio of Wi-Fi APs and network switches; all managed through FortiOS. The company claims its FortiGate is the only NGFW delivering unified management for hybrid mesh network environments. Furthermore, FortiOS traverses multiple domains, providing secure wired and wireless LAN access for traditional branch offices, remote locations, and campus environments. Fortinet's FortiAP lineup is complete and features Wi-Fi 6, Wi-Fi6E, and Wi-Fi 7 indoor and outdoor form factors. At the same time, the company's FortiSwitch portfolio of 1GE to 100 GE switches is designed to deliver the necessary performance and port density to support any organization's connectivity needs, including ruggedized form factors.

Custom Silicon Anchored by Deep Research and Development

Fortinet is also investing considerable resources in its custom silicon, designed to accelerate networking performance and harden security. These ASICs are designed to speed network processing and increase management scalability, resulting in the improvement of network performance within modern branch and campus environments.

Developing custom silicon is a high bar, as many networking and security infrastructure providers leverage merchant silicon. An example of Fortinet's custom silicon depth lies in its latest ASIC design, the FortiSP5. FortiSP5 is designed to enhance the security and network functions of the company's FortiGate firewall portfolio. Based on a cutting-edge seven-nanometer package, Fortinet claims that the FortiSP5 delivers an astounding 17x improvement in firewall performance and 32x faster encryption, all at an

88% reduction in power compared to standard CPUs. Fortinet's security processing units (SPUs) can also tailor the quality of service levels to steer application performance for latency-intensive applications such as video conferencing.

Fortinet's intellectual property portfolio is also worth highlighting. Although patent counting is not necessarily a barometer of innovation, the company's accomplishments are significant. Fortinet boasts over 1,500 patents pending and issued that span Ethernet, wireless LAN, NAC, SD-WAN, SASE, ZTNA, endpoint protection, and more. Investment in research and development is a long-term strategy designed to provide differentiation and customer value. It is not a trivial undertaking, especially in recent times marked by inflation and operational expense reduction among many IT and OT infrastructure providers.

Call to Action

Given the nature of today's modern, hybrid work, organizations demand integrated network and security solutions. It is becoming increasingly difficult to manage security point solution tool sprawl, and a bolt-on approach creates vulnerabilities that bad actors can exploit. A unified technology stack that provides embedded security within networking infrastructure is the optimal choice. The resulting benefits are compelling, reducing complexity and improving operational efficiency while freeing IT professionals to provide more value-added services to the lines of business supported.

Moor Insights & Strategy believes that Fortinet is not simply a value leader with respect to its networking and security portfolio. Rather, it is a leader given a broad and deep portfolio that can be managed through a single policy construct for network and security deployment and ongoing management. Ultimately, Fortinet can optimize business outcomes for organizations through network and security convergence at scale.

CONTRIBUTOR

Will Townsend, Vice President & Principal Analyst, Networking & Security Practices at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Chief Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES

This paper was commissioned by Fortinet. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.