FORTINET

THE IMPORTANCE OF TRANSPARENCY IN CYBERSECURITY

SUMMARY

Broad industry efforts — including Secure by Design, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Joint Cyber Defense Collaborative within CISA, and widespread threat intelligence sharing — have bolstered cybersecurity defenses. Still, bad actors continue finding new ways to compromise security controls across infrastructure solution providers. It represents an unprecedented onslaught, further intensified by the rise of nation-state attacks buoyed by an ongoing and unstable geopolitical climate.

Modern generative and agentic AI tools have great promise for fortifying security posture and defense within cybersecurity platforms. However, cyber criminals are also leveraging the same technologies to improve the sophistication of attacks to disrupt operational efficiency and extort organizations via ransomware for ill-gained profit.

The sharing of threat intelligence goes far to help organizations stay one step ahead of bad actors. An example is Fortinet's recently published 2025 Global Threat Landscape Report highlighting malware campaigns and AI-powered techniques that bypass traditional detection methods. However, more is needed.

To allow defenders to stay ahead of cyberattacks, there is also a need for greater transparency from security infrastructure providers themselves. Security infrastructure providers must have the courage to be more forthcoming, rather than allowing the press to report incidents first. They must responsibly share the resulting learnings to bolster security resilience for the cybersecurity industry at large.

Moor Insights & Strategy believes that Fortinet is establishing itself as one of the leaders in providing cybersecurity transparency that is enabling improved security outcomes. Fortinet's CISA Secure by Design pledge, vulnerability identification and responsible disclosure approach, broad and deep consortia participation, and unique intellectual property distinguish it from competitors. Its proven history in identifying cyber threats early in the kill chain positions it as a wise choice. The company serves organizations seeking secure networking infrastructure that can scale across clouds, datacenters, campuses and branches, and network edges.

CYBERSECURITY TRANSPARENCY MATTERS

Responsible cybersecurity transparency matters. It encompasses the open sharing of processes, practices, and findings, including timely disclosures, that offer the broader industry the ability to minimize potential risk. Cybersecurity transparency also includes documented compliance with industry standards, auditability, and broader data management and protection provisions. However, these considerations should not come at the price of diminishing a vendor's reputation, expose architectural underpinnings or software code tied to intellectual property, or increase the risk of deeper infrastructure provider exploitation.

From an engineering standpoint, the introduction of the Secure By Design pledge by CISA last year underscores a broader effort that has existed for decades. It represents a fundamental shift in software development, one in which security considerations are integrated into a product instead of being addressed as an afterthought. This philosophy is accepted by many infrastructure providers in the cybersecurity industry as a best practice, yet it is not mandated, enforced broadly, or widely understood by customers. That must change, and when it does, the value realized through higher levels of trust and accountability, and continuous improvement of security controls and efficacy, will be significant. Today, nearly every security infrastructure provider is exposed. According to the NIST National Vulnerability Database, last year there were over 40,000 vulnerabilities tracked across 2,700 vendors.

The cybersecurity industry continues to grow and mature, and collaboration continues through ecosystem development, strategic partnerships and integrations, and the proactive sharing of threat intelligence. As a part of this process, the industry must also collectively raise the topic of the importance of proactive disclosure of vulnerabilities without stigma, given the need to protect organizations of all types and sizes against cyber adversaries.

WHY FORTINET

As one of the first CISA Secure by Design pledge members, Fortinet is committing to ensuring secure and responsible product development while balancing the need for proactive and responsible vulnerability disclosure. Through the company's adoption of CISA guidelines and international standards that are an integral part of its security policy construct, Fortinet is setting a high standard for other security infrastructure providers to follow. To ensure its success, Fortinet also tracks its own pledge progress

across ten internally defined principles while also ensuring its customers implement patches and upgrades.

To further its cybersecurity transparency endeavors, Fortinet diligently balances the commitment to customer security with a culture of transparency and ownership. This contrasts with other security solution providers that rely on independent researchers or other third parties to facilitate this capability in isolation. Through these efforts, Fortinet discovers the vast majority of security vulnerabilities internally, a rate that far exceeds what is typical in the industry. Its closed-loop process is powerful, and it provides a foundation for preemptive planning and breach mitigation with a responsible approach to disclosure and customer protection.

Finally, through Fortinet's consortia participation and its FortiGuard Labs efforts, it is making great strides in uncovering emerging AI-powered cybercrime and lurking threats. The company's work with Interpol, the World Economic Forum Cybercrime Atlas, the Cyber Threat Alliance, and the University of California, Berkeley's Center for Long-Term Cybersecurity is bringing impactful and needed change and resiliency to help defenders stay ahead of bad actors. These efforts complement the company's deep intellectual property portfolio, including its FortiOS converged networking and security fabric, and its purpose-built custom security silicon that increases the speed, scale, and efficiency of protection across its next-generation firewalls and other security appliances.

Call to Action

Modern AI tools represent a double-edged sword. On one hand, they are empowering defenders with runtime automation and security operations efficiencies. On the other, AI continues to be weaponized to empower and scale cyberattacks. Cybersecurity transparency is a powerful change agent to tip the scales to the benefit of defenders.

Moor Insights & Strategy believes that Fortinet is demonstrating an unwavering commitment to cybersecurity transparency with proactive vulnerability discovery and transparency through its CISA Secure by Design pledge, vulnerability identification and responsible disclosure, broad and deep consortia participation, unique intellectual property, and threat detection research efforts. The company's culture of proactive and responsible disclosure is a model for others in the cybersecurity industry to follow. Consequently, it is no surprise that Fortinet's efforts are validated by its inclusion in Forbes Most Trusted Companies list.

Important Information About This Paper

Contributor

Will Townsend, Vice President and Principal Analyst, Networking & Security Practices

Publisher

Patrick Moorhead, CEO, Founder, and 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

Fortinet commissioned this paper. 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.