# Complexity Is the Moat:
# How AI Expansion Is Widening Cybersecurity's Opportunity

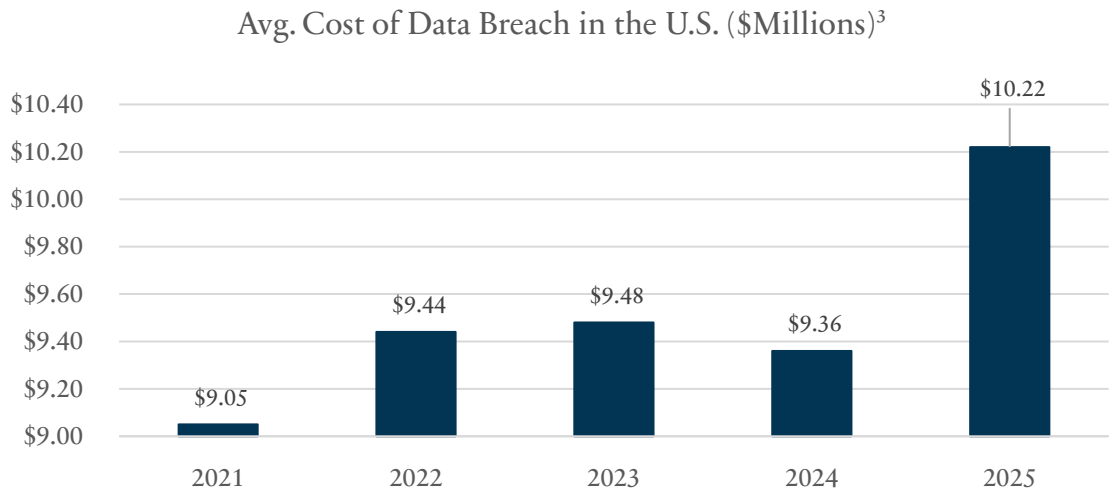
**Sonu Chawla, CFA**
*Portfolio Manager & Research Analyst*
Software and Technology Services

***"The same force disrupting every other software category is writing the growth story for cybersecurity."***

Generative AI has resulted in broad based sell-off in software stocks and cybersecurity stocks haven't been immune either. However, the broad-based sell-off in cyber names seems misplaced. After Anthropic rolled out Project Glasswing and Claude Mythos Preview, OpenAI quickly followed with GPT-5.4-Cyber, a targeted model for defensive use-cases being deployed in a limited way to approved security vendors/organizations. OpenAI's rollout to vetted cyber vendors including Palo Alto Networks (Nasdaq: PANW) and CrowdStrike Holdings (Nasdaq: CRWD), coming right on the heels of Anthropic's, reinforces the same core point; rather than declaring war on cyber vendors, these labs are doing close to the opposite by explicitly bringing key cyber vendors into the tent as launch partners. These labs explicitly recognize that their models require enterprise-grade security frameworks to function safely within complex corporate environments, reinforcing the value of established cybersecurity platforms rather than seeking to disrupt them.

The advancement of AI creates a more dangerous landscape where threat actors can exploit new technologies just as effectively as defenders. The proliferation of machine-speed traffic and ephemeral non-human identities has drastically expanded the attack surface, making zero-trust processes more critical than ever. While AI may commoditize repetitive tasks such as basic code hygiene and patch suggestions, the overall security environment is becoming increasingly chaotic. This complexity shifts the true value upward toward orchestration, governance, and incident response. More AI-generated code, more agentic traffic, more ephemeral non-human identities, more open source dependencies, and more autonomous experimentation all widen the attack surface. As AI-generated code and autonomous experimentation increase, the resulting messiness underscores the need for sophisticated enforcement and telemetry that only leading cybersecurity platforms can provide.

The urgency is driven by a rapidly accelerating threat landscape. Recent data from Microsoft suggests that 80% to 90%[1] of all phishing cyberattacks now leverage AI in some capacity, making them more sophisticated and harder to detect. The speed of these attacks has reached a breaking point; Palo Alto Networks recently noted that hackers can now break in and steal data in under an hour.[2] That is four times faster than just a year ago. This isn't just a technical headache; it's a massive financial liability. The average cost of a data breach in the U.S. now exceeds $10 million.[3] The cost of "getting it wrong" has never been higher.




Crucially, the rise of powerful AI models actually increases the need for independent security providers. Companies are unlikely to trust an AI developer to grade their own homework when it comes to safety. Instead, they are layering specialized security controls around their AI workloads to prevent employees from leaking sensitive data and to block autonomous bots from being weaponized by bad actors. This creates a "redundancy by design" that favors incumbent security vendors with established relationships within the enterprise.

## How is TimesSquare positioned for this secular change?

At the time this piece was written, we maintain an active overweight to the cybersecurity space, expressed through a select number of positions across our small- and mid-cap portfolios. Importantly, we believe we are still in the early innings of AI-driven cybersecurity challenges, which we expect to drive sustained demand for innovative solutions. One such investment held across both strategies is **JFrog Ltd** (**Nasdaq: FROG**). JFrog is a software development company that provides a comprehensive software supply chain platform, offering end-to-end visibility, security, and control to automate the delivery of trusted software releases.

---

[1] KnowBe4, Inc. (2025, March 20). *New KnowBe4 report reveals a spike in ransomware payloads and AI-powered polymorphic phishing campaigns*.
[2] Palo Alto Networks, Inc. (2026, February 17). Fiscal second quarter 2026 earnings call transcript.
[3] IBM Security. (2025). *Cost of a data breach report 2025: The AI oversight gap*. Ponemon Institute.

We believe JFrog is well-positioned to benefit from AI-driven growth. As demand for enterprise applications, development tools, and security solutions increases, so too should platform usage and workloads. In addition, heightened cybersecurity risks and evolving compliance requirements are accelerating the adoption of its security and add-on offerings, creating incremental revenue opportunities.

In our view, JFrog is particularly well-positioned among software developer tools companies to capitalize on this trend. Its universal platform enables customers to manage growing volumes of AI models and binaries across multi-cloud environments without vendor lock-in. Combined with its integrated security capabilities and natural upsell opportunities, we believe JFrog has the potential to become a foundational "liquid software" backbone for continuous, automated software delivery in the AI era.

A second investment held in our Mid Cap Strategy is **Palo Alto Networks** (**Nasdaq: PANW**). Palo Alto is a leading cybersecurity platform helping enterprises secure increasingly complex environments across network, cloud, AI, and endpoint.

We see the company as a direct beneficiary of generative AI adoption. As enterprises deploy AI at scale, both network traffic and identity complexity are rising, driving incremental demand for security across SASE, firewalls, and identity layers. At the same time, AI is expanding the threat landscape, enabling more sophisticated attacks while increasing the risk of internal data leakage, further elevating cybersecurity as a mission-critical spend priority.

Palo Alto's inclusion in Anthropic's Glasswing initiative provides early access to advanced AI models, strengthening its competitive positioning versus smaller vendors. In parallel, the company is benefiting from a structural shift toward vendor consolidation, as customers move away from fragmented point solutions to integrated platforms.

With a large installed base of over 70,000 customers and only a small portion fully onboarded to its platform, we see a significant runway for expansion. Platform adoption typically leads to higher retention and increased spend per customer, reinforcing durable growth. Recent acquisitions, including Chronosphere and CyberArk, further enhance this opportunity, particularly in identity security, where the rapid growth of non-human identities is creating a new and underappreciated layer of demand.

We believe Palo Alto can sustain mid- to high-teens revenue growth while expanding margins, driving low-20% operating income growth over the next several years.

## Why This Matters for Long-Term Quality Growth Investors

Looking ahead, **we expect this tailwind to become increasingly visible in corporate earnings over the next 12 to 18 months**. As businesses move from "testing" AI to "deploying" it, they must first build the digital fences to keep it safe. For investors, the takeaway is clear: the complexity of the current threat environment creates significant barriers to entry for new competitors and a growing, addressable market for the leaders in the space.

Consistent with our approach, we seek to look beyond near-term volatility and identify underappreciated opportunities driven by secular change rather than market narratives. As AI adoption accelerates, cybersecurity is evolving from a defensive allocation into a core growth opportunity, one where long-term fundamentals may prove stronger than current expectations. Cybersecurity is no longer just about protecting value; it is about capturing it by positioning yourself on the right side of a multi-year structural trend.

---

Additional Source(s): Company commentary, industry conferences, and third-party research.

TimesSquare Capital Management LLC is a growth equity specialist that is registered as an investment adviser with the U.S. Securities and Exchange Commission and is majority owned by Affiliated Managers Group, Inc. With an experienced investment team and rigorous fundamental analysis, we identify high quality companies with strong management in inefficient market cap ranges. As a boutique, our highly collaborative process and integrated approach promote our commitment to meeting our clients' service needs. Importantly, employees share a common economic interest through equity participation aligning them with the success of our clients and the firm.

This material is for your private information and is provided for educational purposes only. The views expressed are the views of TimesSquare Capital Management, LLC only through the period ended April 2026 and are subject to change based on market and other conditions. The opinions expressed may differ from those with different investment philosophies. The information we provide does not constitute investment advice and it should not be relied on as such. It should not be considered an offer or solicitation to buy or an offer to sell a security. It does not consider any investor's particular investment objectives, strategies, tax status or investment horizon. We encourage you to consult your tax or financial advisor. All material has been obtained from sources believed to be reliable, but its accuracy is not guaranteed. There is no representation or warranty as to the current accuracy of, nor liability for, decisions based on such information. Specific investments described herein do not represent all investment decisions made by TimesSquare. No assumption should be made that investment decisions identified and discussed were or will be profitable. Specific investment advice references provided herein are for illustrative purposes only and are not necessarily representative of investments that will be made in the future.

Certain information contained herein has been obtained from third party sources and such information has not been independently verified by TSCM. No representation, warranty, or undertaking, expressed or implied, is given to the accuracy or completeness of such information by TSCM or any other person. While such sources are believed to be reliable, TimesSquare does not assume any responsibility for the accuracy or completeness of such information. It does not undertake any obligation to update the information contained herein as of any future date.

Certain information contained herein constitutes "forward-looking statements," which can be identified by the use of forward-looking terminology such as "may," "will," "should," "expect," "anticipate," "project," "estimate," "intend," "continue," or "believe," or the negatives thereof or other variations thereon or comparable terminology. Due to various risks and uncertainties, actual events, results or actual performance may differ materially from those reflected or contemplated in such forward-looking statements. Nothing contained herein may be relied upon as a guarantee, promise, assurance or a representation as to the future.

Past performance does not guarantee future results. There is risk that invested capital may be lost.

For the TimesSquare Glossary, please visit here.

For more information, please contact us at info@tscmllc.com.

TIMESSQUARE
CAPITAL MANAGEMENT, LLC

75 Rockefeller Plaza, 30th Floor, New York, NY 10019
Website: www.TSCMLLC.com