Platforms, AI and Concentration

Why the Cybersecurity Business Is Entering Its Most Demanding Phase

Cybersecurity has always been driven by urgency. What is different now is that the industry's own economic and operating model is being redefined in real time. A series of high-signal transactions and operational events over the past 21 months point to the same structural outcome: security is consolidating into platforms, AI is becoming an operating lever rather than a feature and risk is concentrating accordingly.

The first signal is platform consolidation. In March 2024, Cisco completed its acquisition of Splunk for approximately $28 billion in equity value, positioning security analytics, visibility and response as a core enterprise platform capability, not a standalone tool.[1] One year later, the hyperscalers reinforced this direction. In March 2025, Google announced an agreement to acquire Wiz for $32 billion, explicitly pulling cloud security closer to the cloud control plane and embedding it more deeply into hyperscaler economics and distribution.[2]

In parallel, the deployment of AI has shifted from incremental enhancement to operating leverage. In December 2025, 7AI announced a $130 million Series A, positioning autonomous security agents as a way to materially change the cost, speed and scalability of security operations rather than simply improve detection quality.[3]

Then concentration risk moved from abstract discussion to observable impact. In July 2024, a faulty update from CrowdStrike caused widespread global disruption. Microsoft estimated that 8.5 million Windows devices were affected.[4] Parametrix estimated $5.4 billion in direct losses for Fortune 500 companies (excluding Microsoft), while estimated insured losses in the range of $540 million to over $1 billion.[5]

Viewed individually, these developments could be dismissed as normal market evolution. Taken together, they reveal a consistent pattern: buyers and partners are converging on fewer security platforms; AI is being embedded to materially change cost structures and execution speed; and operational failures now spread faster and further because dependencies are increasingly concentrated.

The result is a new reality: Cybersecurity is now a platform business, shaped by hyperscalers, powered by AI-driven operating leverage and exposed to concentration risk that can directly impact enterprise continuity and vendor reputation at scale.

What This Means for Cybersecurity Companies

1) Security platform companies

- **Higher and larger expectations become reality for platforms:** Deals like Cisco and Splunk ($28B) and Google and Wiz ($32B) reinforce that integrated visibility and cloud security are core.
- **Zero Trust becomes the commercial baseline:** Zero Trust has moved from a technical buzzword to a buyer-side decision framework, shaping how security investments are evaluated and setting baseline expectations for integrated identity, consistent access control and enforcement across environments. This accelerates platform consolidation because fragmented portfolios create inconsistent outcomes.
- **Operational maturity becomes a go-to-market asset:** Due to headline-making platform scale outages, customers and partners are increasingly demanding visibility into vendors' approaches to disciplined and tested releases, predictable change control and operating practices.

2) Cloud security and AI native challengers

- **Hyperscaler adjacency is both an opportunity and a threat:** Google's $32B Wiz deal signals that large cloud players can internalize best-in-class capabilities, reshaping exit paths, partnerships and competitive dynamics.
- **The expectations are now enterprise-ready:** Buyers want proof that a challenger can scale support, delivery and economics at the enterprise level.
- Efficiency becomes valuation protection: With tighter macro conditions and higher scrutiny on profitability, challengers must show repeatable go-to-market motions and controlled unit economics.

3) Service providers (Managed Security Service and Managed Detection and Response)

- **Services must standardize on fewer platform stacks:** Platform consolidation pressures providers to reduce tool diversity and build repeatable service "products" aligned to dominant ecosystems.
- **AI changes the labor model:** If AI compresses manual triage and routine work (as the 7AI raise suggests the market expects), service operators must redesign pricing, staffing and delivery to protect margins rather than simply adding tools.
- **Concentration risk becomes part of the SLA promise:** Customers will increasingly expect providers to have operational playbooks for vendor disruptions and dependency failures and to provide transparency when outages occur.

Where Winners Will Focus

The next phase of the cybersecurity business will not be won by "more innovation" alone. It will be won by companies that realize value, in revenue quality, margin and scalability, while operating reliably in a concentrated ecosystem.

1) Simplify to fit platform economics

- **Security platform companies:** Reduce SKU sprawl by packaging around outcomes rather than features, improving cross sell efficiency, retention and platform economics.
- **Cloud security & AI native challengers:** Clearly define the company's role in a platform-centric market to align product and GTM decisions.
- **Service providers:** Standardize on a smaller set of platforms and productize services to reduce bespoke delivery, protect margins and scale efficiently.
- **Monitoring companies:** Re-imagine products to include learning loops, where every incident improves the system. Create monitoring systems that **act**, not just alert.

2) Treat AI as an operating leverage program

- **Security platform companies:** Apply AI to reduce customer complexity and internal cost (fewer alerts, faster decisions and lower support and operations burden).
- **Cloud security & AI native challengers:** Demonstrate AI-driven ROI in onboarding and day to day operations to shorten ramp time, protect renewals and support expansion.
- **Service providers:** Redesign delivery so AI reduces labor intensity, improves consistency and lowers cost-to-serve without proportional headcount growth.
- **Monitoring companies:** Greater automation for tier 1 and tier 2 alert handling, with AI conducting initial triages, signal correlation and proposed remediation.

3) Manage concentration deliberately

- **Put guardrails around concentration:** Establish clear commercial and operational controls to manage unavoidable platform dependency, including partner terms, customer communication protocols, continuity planning and disciplined change management.
- **Intentional management:** Avoid the "one brain" problem by leveraging distributed AI agents instead of one monolithic model and tiered autonomy, with low-risk actions fully automated and higher-risk actions requiring human approval or quorum.
- **Treat reliability as a growth lever:** In a platform centric market, trust compounds faster than features, while failures cascade quickly when dependencies are concentrated.
- **Centralize intelligence, not raw data:** More data helps AI, but centralizing everything creates massive risk. Federate learning across customers without pooling sensitive data. Share Indicators of Compromise (IOCs) but never raw logs or identities.

4) Align growth to execution capacity

- **Higher quality Annual Rate of Return (ARR):** Shift focus from headline growth to durable retention and expansion, ensuring ARR is resilient, predictable and supported by clear customer value realization.
- **Margin discipline:** Enforce cost-to-serve and cloud spend control as usage scales, recognizing that margin performance will increasingly separate winners from growth at any cost models.
- **Integration speed:** Prioritize rapid integration for acquisitive platforms and rollups so synergies, cost efficiencies and cross-sale opportunities are captured early rather than diluted over time.
- **Repeatable operating models:** Design operating models that scale consistently across customers, products and geographies without introducing incremental complexity or execution risk.
- **Design for scrutiny:** Anticipate that AI-driven security decisions will be regulated. Every AI decision should be logged with explanations and customer audit trails should be logged. These allow regulators and customers to replay decisions when required.

At the end of the day, the bottom line is this: AI naturally concentrates power, data and decisions. **Winning cybersecurity companies will deliberately design against that gravity while still capturing scale benefits.**

Endnotes

[1] Splunk, "Cisco Completes Acquisition of Splunk," Press Release (Mar. 18, 2024), https://www.splunk.com/en_us/newsroom/press-releases/2024/cisco-completes-acquisition-of-splunk.html; see also, McColl, Bill, "Cisco Systems Completes Its $28 Billion Purchase of Splunk," Investopedia (Mar. 18, 2024), https://www.investopedia.com/cisco-systems-completes-its-usd28-billion-purchase-of-splunk-8610584.

[2] Google, "Google announces agreement to acquire Wiz," Company News (Mar. 18, 2025), https://blog.google/company-news/inside-google/company-announcements/google-agreement-acquire-wiz/.

[3] Burke, Nate, "Citing the 'Agentic Security Inflection Point,' 7AI Raises Largest Cybersecurity A Round in History to Bring AI Security Agents to Enterprises," 7AI Blog (Dec. 4, 2025), https://blog.7ai.com/citing-the-agentic-security-inflection-point-7ai-raises-largest-cybersecurity-a-round-in-history-to-bring-ai-security-agents-to-enterprises.

[4] Cybersecurity and Infrastructure Security Agency, Alert: Widespread IT Outage Due to CrowdStrike Update (Aug. 6, 2024), https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update; see also Weston, David, "Helping our customers through the CrowdStrike outage," Official Microsoft Blog (Jul. 20, 2024), https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

[5] "Fortune 500 firms to see $5.4 bln in CrowdStrike losses, says insurer Parametrix," Reuters (July 24, 2024), https://www.reuters.com/technology/fortune-500-firms-see-54-bln-crowdstrike-losses-says-insurer-parametrix-2024-07-24/; see also, Parametrix Impact Analysis, "CrowdStrike's Impact on the Fortune 500," https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500

YI SUN
Managing Director
yi.sun@fticonsulting.com

JENIFER VISEK
Managing Director
jenifer.visek@fticonsulting.com