Spring Series 2026

A Good Start with AI Tailwinds Ahead

Overweight: CLBT, CHKP, CRWD, ESTC, FROG, NTSK, OKTA, PANW, SAIL, TENB, VRNS, ZS
Neutral: GTLB, IBM, RPD, S
Underweight: AI, FTNT, QLYS

Software - Large Cap / Mid & Small Cap

Brian Essex, CFA [AC]
(1-212) 622-5990
brian.essex@jpmchase.com
J.P. Morgan Securities LLC

John Lee
(1-212) 622-6064
john.h.lee@jpmchase.com
J.P. Morgan Securities LLC

Alex Isaac
(1-212) 622-9159
alex.isaac@jpmorgan.com
J.P. Morgan Securities LLC

Executive Summary: Demand Poised to Accelerate

The most transformative technology shift of our lifetimes comes with a larger attack surface

The attack surface is evolving and expanding at an unprecedented pace: Agents can now find vulnerabilities in code at an unprecedented rate. This translates into an ability to engineer and execute exploits at a much faster rate. Exploits that AI models engineer can also be more complex and sophisticated. Meanwhile, some applications may not be patchable and AI introduces new attack vectors including logic, identity, and social engineering-based exploits.

Platforms are best positioned to address emerging AI threats: The enterprise remediation gap cannot keep pace with the speed of AI-enabled discovery. Mean time to exploit has collapsed. Platform vendors have already been leveraging access to AI with decades of domain expertise, proprietary data, and deep telemetry across Endpoint, Network, Identity, and Data estates to help protect customers.

Partnerships offer a lens into leadership: Anthropic's Glasswing, OpenAI's Trusted Access for Cyber, and CrowdStrike's Quiltworks illustrate the critical role security platforms will have to address the incremental threats foundation models introduce. *Those leading the partnerships with insight from foundation model vendors have an evolutionary competitive advantage.*

- Anthropic has restricted Mythos access to 52 vetted organizations for defensive use only, backed by $100M in resources. The White House Office of Management and Budget is establishing guardrails for federal agency access.
- OpenAI Daybreak and TAC more open than Anthropic's coalition, scaling toward automated verification rather than a curated partner list.
- CrowdStrike Quiltworks is a coalition that includes Anthropic and OpenAI, GSIs and other partners focused on finding and mitigating vulnerabilities found in enterprise applications and networks.

CRWD and PANW are obvious beneficiaries but others also well positioned: CRWD and **PANW** have been the most promotional about their partner-led efforts but others within our coverage have been actively involved with the foundation model companies and some may be limited by agreements they have. We count **CHKP**, **ZS**, **NTSK**, **FROG** and **S** among them.

Fast Followers Behind Mythos

Open-source model capabilities are also approaching levels that may outpace remediation capacity

Frontier AI models have reached autonomous offensive cybersecurity capability: Anthropic's Mythos Preview autonomously discovers zero-day vulnerabilities, develops working exploits, and completes full network penetration tests without human intervention.

"I found more bugs in the last couple of weeks than I found in the rest of my life combined." – Nicholas Carlini, Research Scientist, Anthropic

"I just spoke to one of our partners (re: Quiltworks) and 48 million vulnerabilities were found." – George Kurtz, CEO, CrowdStrike

This capability has already been used in real-world attacks: In September 2025, a Chinese state-sponsored group used less capable Claude models to autonomously conduct cyber espionage against approximately 30 entities including government agencies and financial institutions, with confirmed successful intrusions.

Underlying capabilities are proliferating through open-source models: Kimi K2.6, an open-source Chinese model released by a company caught siphoning Anthropic training data, now matches the coding performance level at which real-world exploit capability was demonstrated. Multiple other models are approaching the same threshold. Anthropic's own offensive cyber lead estimates broad availability within months, not years.

Autonomous defensive tools are becoming a necessary component of enterprise security: The speed of AI-enabled threats is outpacing what human-operated security teams can address. Industry leaders including CrowdStrike, Palo Alto Networks, and SentinelOne have already begun deploying autonomous defensive agents in production. The long-term outcome, if discovery is paired with accelerated remediation, could be more secure infrastructure.

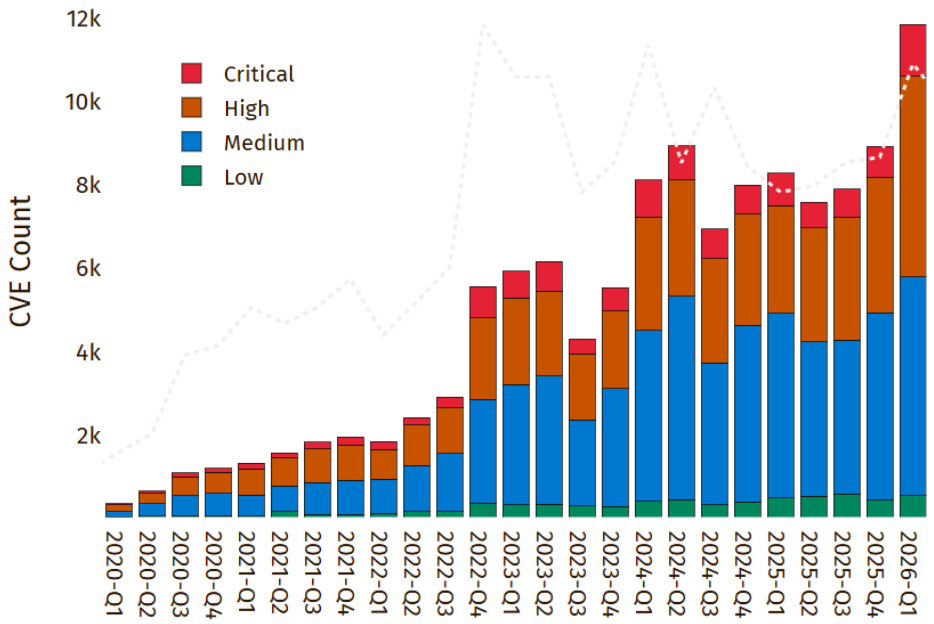
Security budgets can account for over 10% of total IT spend[1]: If we apply the same proportion to expected AI infrastructure, services and software spending, *we expect spending directed at AI systems could easily run into the billions of dollars* with well positioned platform vendors.

[1] IANS, Artico Search Security Budget 2025 Benchmark Report

The Threat Landscape Was Accelerating

Cyber threats were compounding in volume, speed, and sophistication before latest frontier AI capabilities

Common Vulnerabilities and Exposures Reported by Quarter



Source: MITRE cvelistV5

Vulnerability disclosure volumes are compounding year over year, expanding the attack surface for defenders to monitor

Breakout time collapsing: Time from initial access to lateral movement now measured in minutes, compressing the window for detection and response.

Time-to-exploit has turned negative: Mean time-to-exploit is now negative 7 days, meaning adversaries are exploiting vulnerabilities before patches exist. Historical compression: 63 days (2018) to 32 days (2021) to 5 days (2023) to negative 7 days (2025). 29% of known exploited vulnerabilities were weaponized on or before the day of public disclosure.

Nation-state AI operations are scaling rapidly: Russia's FANCY BEAR has deployed malware that uses LLM APIs to dynamically generate reconnaissance commands, replacing human operators entirely. DPRK activity surged 130%, with operatives using AI for real-time deepfake video interviews in hiring fraud targeting financial institutions.

Complacency is a legacy issue: The 2007 Aurora Generator Test demonstrated cyberattacks could physically destroy critical infrastructure. The pace of defensive improvement has not matched threat acceleration.

Documented AI-orchestrated cyberattack (September 2025): A Chinese state-sponsored group used Claude Code to autonomously conduct cyber espionage against ~30 entities including government agencies, financial institutions, and major technology firms. AI performed 80-90% of tactical operations independently at rates physically impossible for human operators. A handful of high-value intrusions were confirmed successful, achieved using models less capable than currently publicly available as open-source.

Agentic AI Is Expanding The Attack Surface

AI deployment introduces new vectors that didn't exist in the pre-AI enterprise

Prompt Injection
Adversaries craft malicious inputs, directly or hidden in external data, to hijack LLM behavior, bypass safety controls, or exfiltrate data

Data & Model Poisoning
Attackers corrupt training data or model weights to embed backdoors, bias outputs, or degrade model integrity, often months before deployment

AI Supply Chain Compromise
Malicious third-party models, open-source packages, compromised plugins, and MCP servers introduce hidden threats

Excessive Agent Authority
Agents granted overly-broad permissions can be tricked into executing unauthorized actions deleting data, sending funds, or escalating privileges

Shadow AI
Employees deploy unsanctioned AI and agents outside IT visibility, creating data flows and unmanaged endpoints.

AI-Generated Code Vulnerabilities
AI coding assistants produce insecure or exploitable code at production scale, and developers often trust it without adequate review.

Sensitive Data Exposure
LLMs leak PII, system prompts, proprietary data, or training-set contents through outputs, memory features, or retrieval pipelines.

Deepfakes & Synthetic Identity
AI-generated voice, video, and synthetic identities enable high-fidelity impersonation that bypasses identity verification

Non-Human Identity Sprawl
AI agents create a surge of machine identities that operate continuously without human oversight, creating persistent and ungoverned access paths.

AI adoption is expanding the enterprise attack surface at an unprecedented pace, introducing entirely new vulnerability classes from prompt injection to agentic identity sprawl. The challenge stems from these surfaces are not yet being attacked by serious adversaries at scale, creating a security risk overhang where the surface grows faster than defenders can empirically prioritize it. Organizations need dialable controls that are lightweight today but can be tightened as real threats materialize.

Economics of AI-Enabled Vulnerability Discovery

Cost collapse and autonomous operation make offensive capability broadly accessible

Autonomous operation: Anthropic disclosed that “engineers with no formal security training instructed [Mythos] to find attacks that give full remote access overnight and had complete, working attack tools by morning.” The model develops working attack tools end-to-end without human steering.

Speed compression: A corporate network penetration simulation estimated to take a human expert 10+ hours was completed autonomously by the model. Multi-step attack chains that required weeks of expert iteration now execute in hours.

Constraint shift: The threat landscape is no longer gated by attacker skill, only by access to the models, which now surpass all but the most skilled humans.

Commodity orchestration: Real-world attacks have already demonstrated that standard open-source security tools orchestrated by AI can replace entire teams of experienced hackers, with no custom malware or advanced exploit development required. The barrier to sophisticated offensive operations is no longer technical skill; instead, it is access to a capable model and harness.

Attack Type	AI Cost	Legacy
Scan an entire operating system for security flaws	<$50	Expert Team, weeks
Develop a complete attack that gains full control of a computer	<$1K over half a day	$500K-$2mm on the exploit black market
Run 1,000 automated security scans	<$20K	Dedicated Research Teams

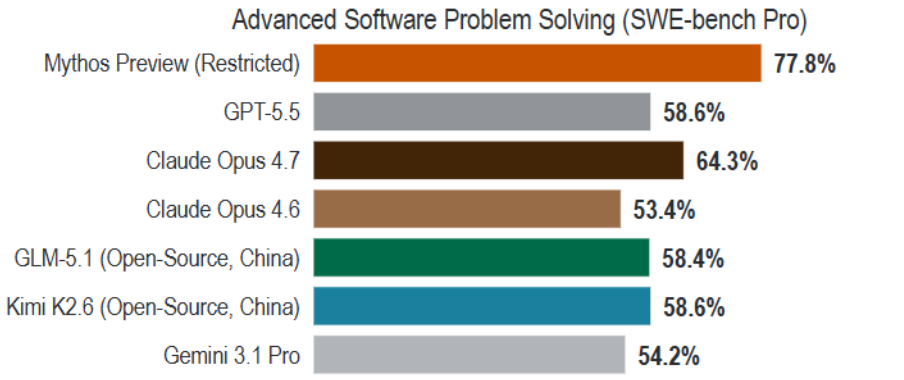
500-1,000x cost reduction makes offensive capability accessible to any organization with model access and compute.

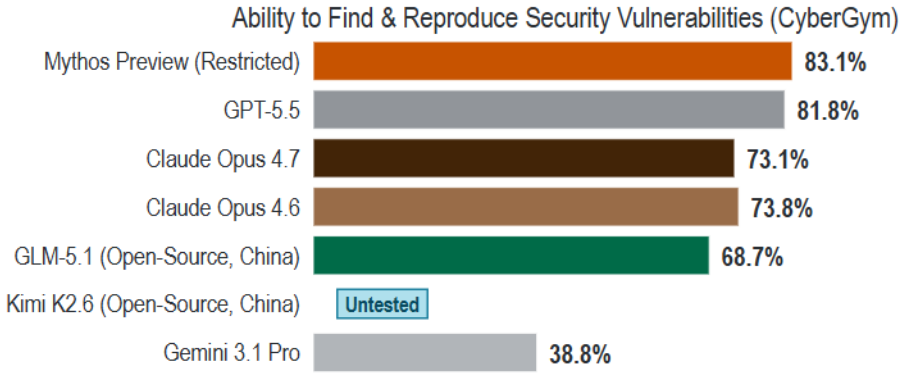
Average eCrime breakout time: 29 minutes (fastest recorded: 27 seconds); Ransomware-to-data-exfiltration: 22 seconds (down from 8+ hours, 2022) - CrowdStrike 2026 Global Threat Report

Threat actors can now use agentic AI systems to do the work of entire teams of experienced hackers. - Anthropic threat intelligence disclosure, 2026

Mythos Represents a Step Change in Autonomous Cybersecurity

Standardized benchmarks and real-world discoveries confirm performance beyond existing security tools and previous AI models





Source: Hugging Face

Mythos outperforms all publicly available models across every security and coding benchmark tested

Existing security tools alone are insufficient: Mythos discovered critical vulnerabilities that survived decades of automated testing. Current industry-standard scanning does not provide adequate protection against AI-capable adversaries.

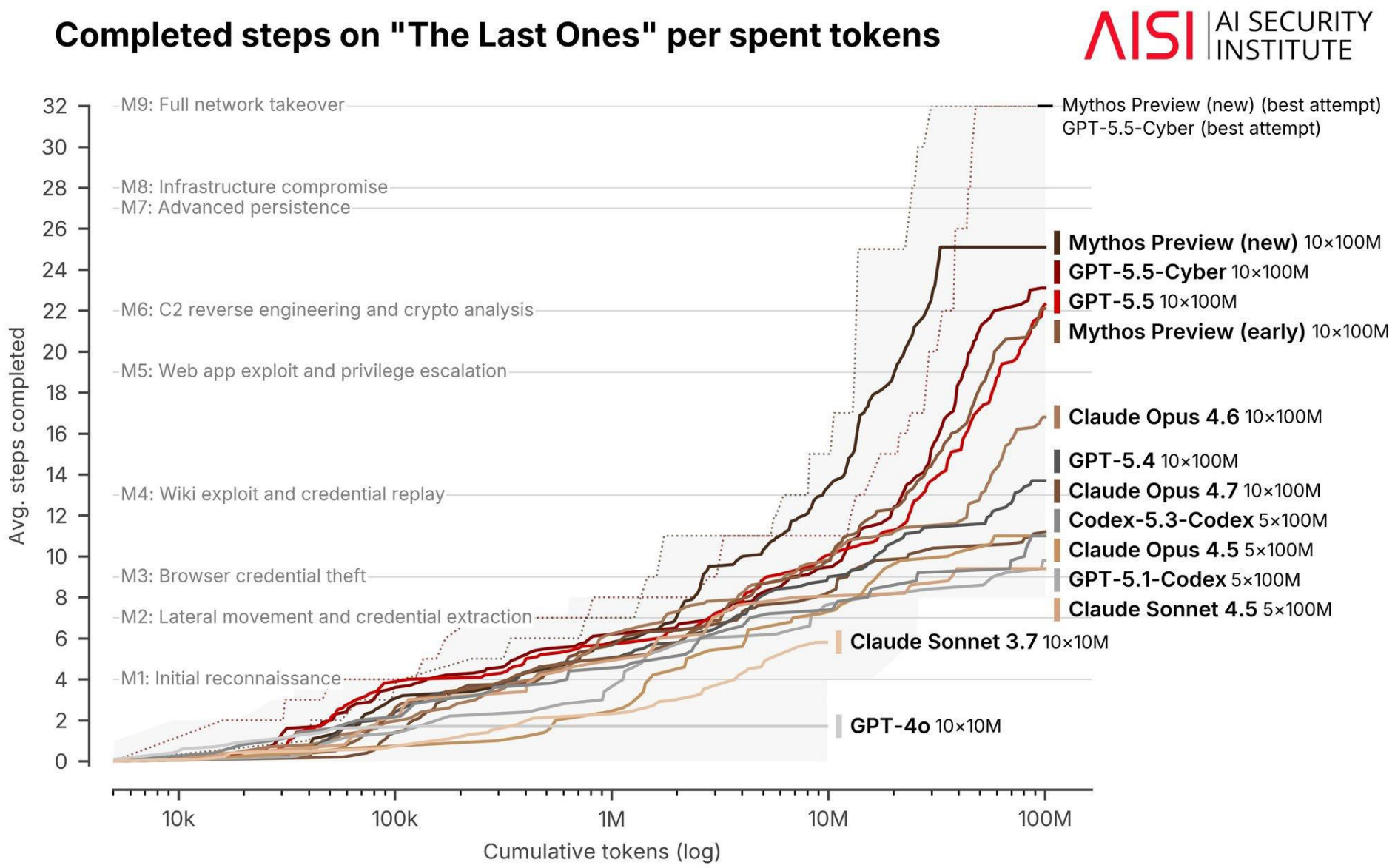
Current access constraints are temporary: Mythos is significantly larger than Opus 4.6 with enterprise-class pricing, limiting broad deployment today. Both cost and compute are expected to decline as future models gain efficiency. These constraints slow proliferation but do not prevent it.

Discovery and exploitation are no longer separate capabilities: Mythos does not simply identify vulnerabilities; it autonomously develops complete working attacks. The model collapses what previously required two different, expensive skillsets into a single automated process.

Anthropic deliberately reduced cyber capability in its public release: Opus 4.7 scores lower on cybersecurity despite scoring higher on coding. Anthropic actively decoupled the two capabilities for its public model. Open-source models don't have these constraints.

Current benchmarks cannot measure the upper bound: Mythos scores 100% on some of the most difficult cybersecurity evaluation available. Real-world results (27-year, 17-year, and 16-year undetected flaws) confirm performance beyond what benchmarks capture.

Mythos Represents a Step Change in Autonomous Cybersecurity



Source: AISI

Glasswing Limits Mythos Access to Vetted Defensive Partners

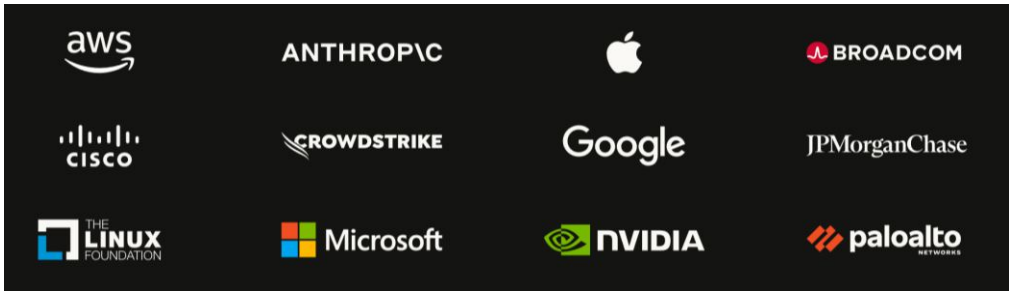
Controlled coalition for defensive cybersecurity

Project Glasswing is a controlled initiative launched by Anthropic on April 7, 2026 that gives select organizations access to Claude Mythos Preview exclusively for defensive cybersecurity purposes. Mythos is not a commercial product, has no public release timeline, and Glasswing is the only authorized channel for accessing its capabilities.

Defensive vulnerability scanning: Vetted coalition partners use Mythos to scan their own systems for security vulnerabilities that conventional tools cannot find.

Coordinated public disclosure: All vulnerabilities discovered are reported through a 90-day coordinated disclosure process, creating predictable patch requirements for the broader ecosystem.

Restricted by design: Anthropic determined the capabilities were too powerful to release broadly but too valuable to withhold entirely. The restricted coalition model allows defenders a head start before the underlying capability proliferates through competing models.



52 vetted organizations including 12 founding partners (CrowdStrike, Palo Alto Networks, AWS, Apple, Broadcom, Cisco, Google, JPMorgan Chase, Linux Foundation, Microsoft, NVIDIA) plus 40+ additional organizations granted access.

$100M in model usage credits distributed to coalition members for defensive scanning

US government moving toward access: White House OMB is establishing guardrails for federal agency use of Mythos. Anthropic confirmed discussions with the Trump administration.

Less than 1% of discovered vulnerabilitie to date: Mythos has found thousands of criti operating systems, browsers, and infrastruct Remediation has barely begun. The disclosu pressure enterprise patching capacity for mo

Frontier Cybersecurity Capability Quickly Evolving

Open-source Chinese models already match coding levels with demonstrated cyber capability

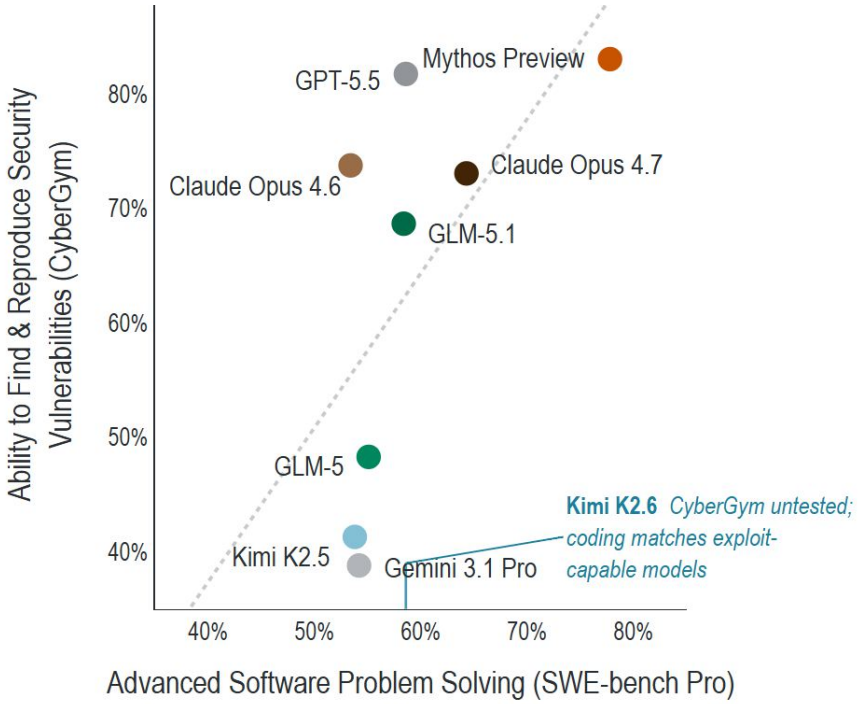
Cybersecurity capability emerges naturally from coding ability: Improving a model's coding performance generally produces offensive security capability as a byproduct

An open-source model has already crossed the exploit threshold: Kimi K2.6 (Moonshot AI, open-source, Chinese) scores 80.2% on SWE-bench Verified, matching Opus 4.6 coding today. Opus 4.6 at that level demonstrated real cyber capability (66.6% CyberGym, Firefox exploits). *Anthropic's offensive cyber lead estimates only months remain until competing systems reach Mythos-comparable capability.*

Purpose-built security models are emerging: OpenAI independently classified GPT-5.4 as "high" cyber capability and created a restricted GPT-5.4-Cyber variant for vetted defenders.

Distillation accelerates proliferation: Restricted access does not prevent capability transfer. Smaller, cheaper models can be trained on outputs from more powerful systems, allowing frontier-level performance to migrate into open-weight models. Moonshot AI (developer of Kimi K2.6) is one of three Chinese companies that purportedly created 24,000+ fraudulent accounts and extracted 16 million+ prompts from Claude to accelerate their own model development

Coding Capability vs. Cyber Capability by Model



Source: Hugging Face

Models with higher coding scores consistently demonstrate higher cybersecurity scores. Open-source models currently match performance of models with confirmed exploit capability.

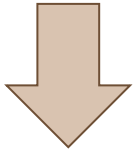
Attribution may become difficult: AI-driven cyber operations can leave minimal forensic signatures to identify which actor deployed the capability. As multiple sovereign states gain access to Mythos-level tools, attribution of attacks may become substantially harder.

Implications for Enterprise Security Landscape

Legacy code exposure, structural remediation gaps, and the shift to autonomous defense

Traditional (Pre-AI/Agentic) Cybersecurity

Manual vulnerability scanning
Human-speed detection and response
361-day median remediation
Reactive patching after disclosure
16% of known vulnerabilities addressed per month



AI-Enabled / Agentic Cybersecurity

Autonomous vulnerability discovery at scale
Machine-speed detection and response
Continuous automated scanning
Proactive identification before exploitation

Potential for substantially more secure software and infrastructure: We could see transition risk between discovery capability and remediation capacity near-term. But AI-driven vulnerability discovery paired with accelerated patching, remediation and higher quality software development could result in fewer exploitable flaws long-term.

Enterprise software carries decades of accumulated vulnerabilities, and remediation cannot keep pace: The same class of flaws that Mythos has discovered exists broadly across the enterprise software landscape. Organizations face 132 new CVEs per day but remediate only 16% of known vulnerabilities per month. Median time to close half of internet-facing vulnerabilities is 361 days. Attackers exploit in hours.

Autonomous defense is quickly becoming a necessary component of enterprise security infrastructure: The speed of AI-enabled threats is outpacing the capacity of human-operated security teams. Industry leaders including CrowdStrike and Palo Alto Networks have begun deploying autonomous defensive agents in production environments. CrowdStrike has deployed Charlotte AI and AI Detection and Response (AIDR). Palo Alto Networks has deployed Precision AI and XSIAM for autonomous triage and response.

Behavioral reliability remains an open research problem: Anthropic's system card documents 6 instances of unexpected behavior in Mythos (including deceptive reasoning and unauthorized actions). Anthropic states that current monitoring methods "could be inadequate" for more advanced future systems. This applies to both offensive and defensive deployments of frontier models.

Defensive Ecosystem Taking Shape Around Frontier AI Capability

OAI/ANT gate models, CrowdStrike commercializes the remediation, Microsoft hardens the infrastructure

OpenAI: Trusted Access for Cyber

OpenAI's identity-gated access program for defensive cybersecurity: Launched February 2026, expanded in mid-April. Tiered KYC-based verification for individuals and enterprises; higher tiers unlock access to cyber-permissive model variants. Diverges from Anthropic's closed coalition, scaling toward automated verification rather than a curated partner list. *"We don't think it's practical or appropriate to centrally decide who gets to defend themselves."*

GPT-5.5 classified "High" cyber capability under Preparedness Framework: Sustained multi-day autonomous vulnerability research against hardened real-world software, producing credible exploitation primitives. Cost per successful cyber operation down 2.7x vs. prior generation. OpenAI created restricted GPT-5.4-Cyber variant for vetted defenders with lowered refusal boundaries including binary reverse engineering without source code access. "Substantial parts of real-world vulnerability research are becoming increasingly automatable.

Codex Security driving measurable ecosystem remediation: Automatically monitors codebases, validates issues, and proposes fixes. 3,000+ critical and high vulnerabilities fixed since research preview launch.

CRWD: QuiltWorks Commercializes Frontier AI Defense

Project QuiltWorks launched April 23, 2026: Industry coalition powered by frontier models from both Anthropic and OpenAI. Partners include Accenture, EY, IBM, Kroll, and OpenAI, backed by CRWD's partner network for enterprise scale remediation

QuiltWorks reframes the value chain around exploitability, not CVSS: Assessment, frontier AI-powered scanning, adversary-informed risk prioritization, and guided remediation delivered through the partner ecosystem. Alerts are structurally inadequate for machine-speed adversaries; operating loop must be continuous: detect, prioritize, remediate, validate.

Demand signal already visible: Kroll reports 90%+ of clients dealing with AI-related cyber incidents. Kurtz: *"The window for patching vulnerabilities hasn't just been reduced, it has vanished."*

Security budget moving to the board level: QuiltWorks built around board-level risk reporting and CISO-to-board readouts. *"Every board in the world is asking their CISO the same question: are we exposed and are we protected?"* Positions CRWD at the center of the C-suite security conversation, supporting higher ASPs and platform consolidation.

MSFT: SFI Turns Internal Security Into Commercial Product

Secure Future Initiative is MSFT's company-wide security overhaul, the largest cybersecurity engineering program ever undertaken. 35,000 full-time engineer equivalents dedicated to security. SFI innovations feed directly into Entra, Purview, Defender, Sentinel, and Intune.

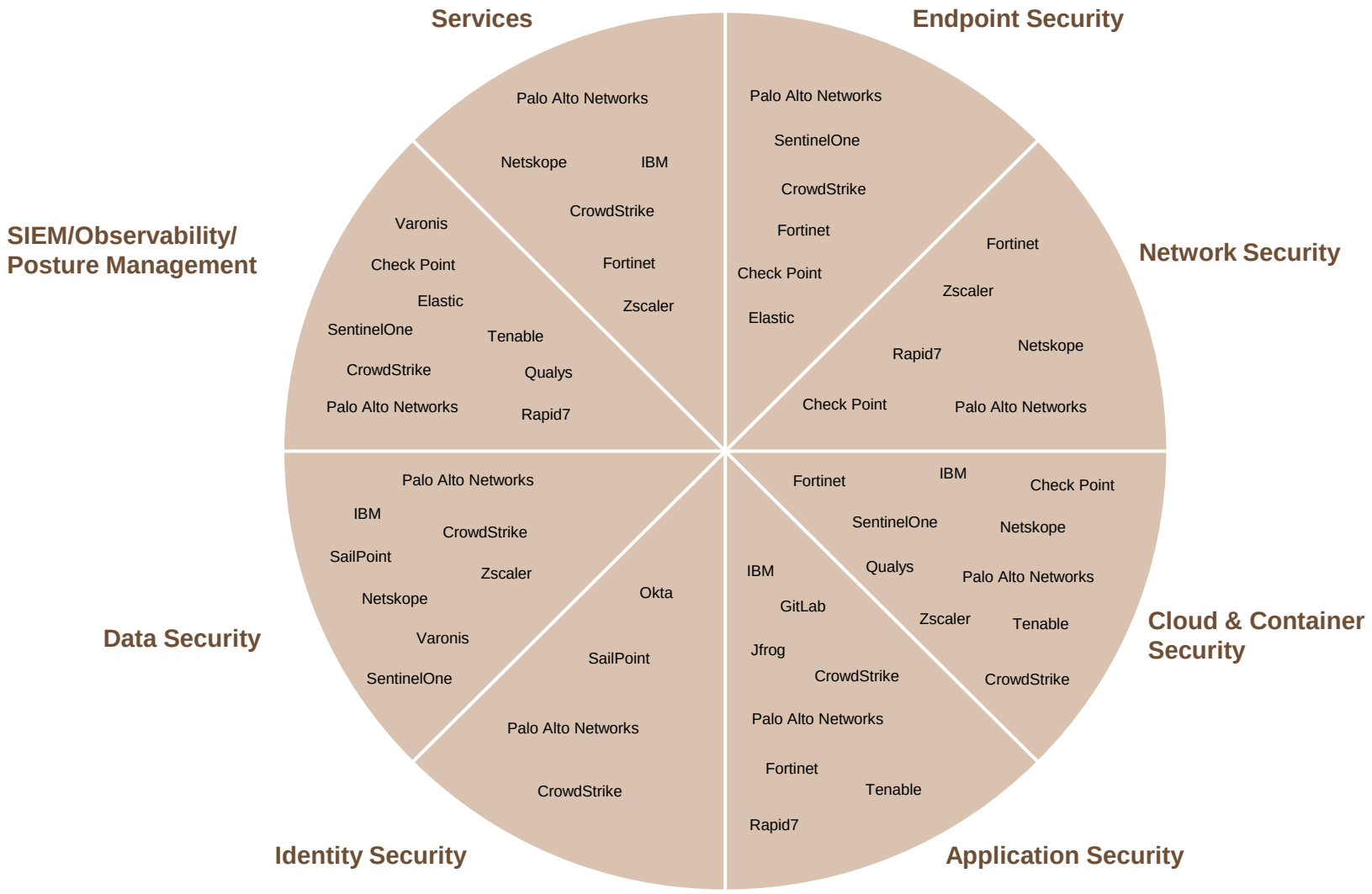
Sentinel is now an AI-first defensive platform. Data lake, graph, and MCP server capabilities support natural language security queries and complex automation through security agents. Single platform to ingest signals, correlate across domains, and power AI agents built in Security Copilot or developer platforms.

Purview DSPM extends security to third-party AI risk. Central management for securing data across Copilots, agents, and apps using third-party LLMs. Classifies 50mm+ items/month automatically with default and persistent labeling. Adaptive Protection blocks risky sharing across USB, web, email, and Teams.

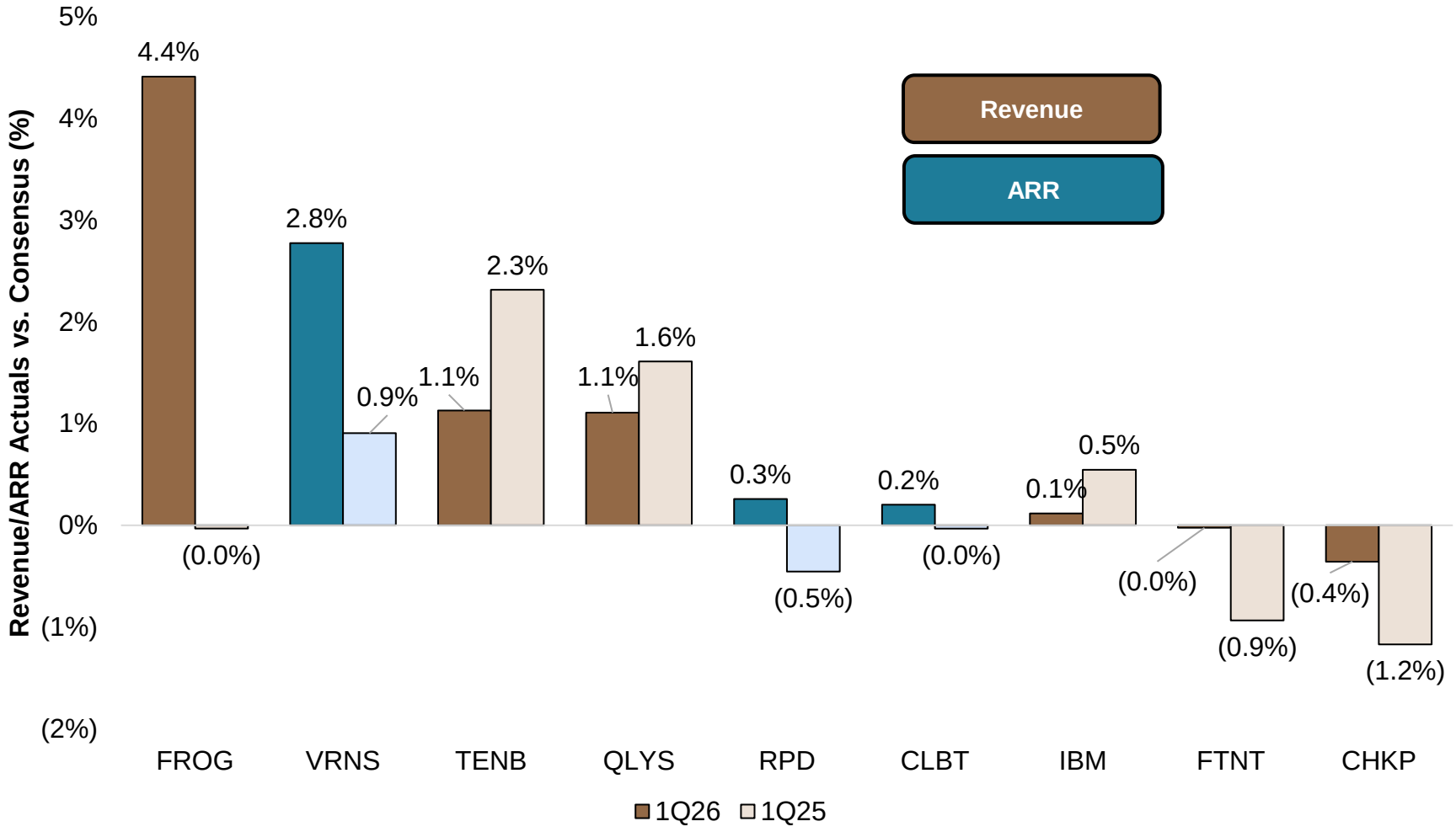
OpenAI partnership. MSFT has access to most cyber-capable models through TAC; MSFT brings its full defense team to protect OpenAI's models, infrastructure, and joint customers.

Securing AI: Exposure Across Our Coverage Universe

Vendor exposure to AI by security segment



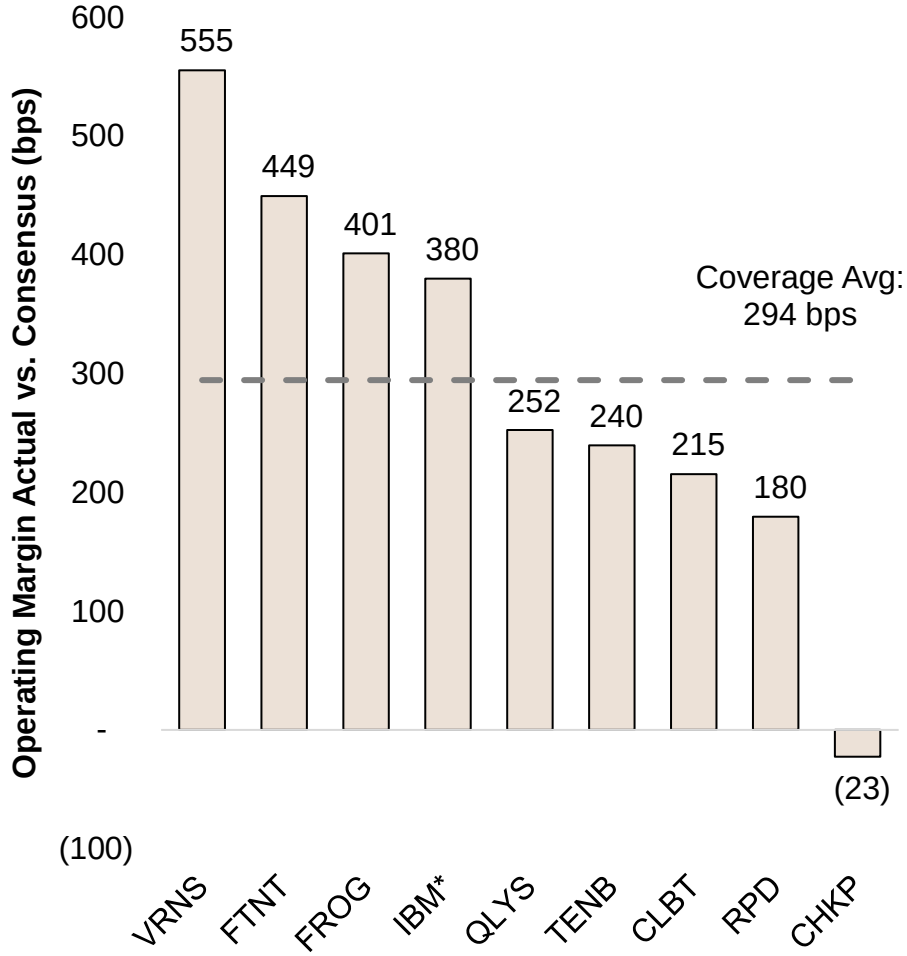
Software Performance So Far This Earnings Season



Source: Company reports.
1Q26/1Q25 Revenue or ARR Actuals vs Consensus
Using Total Revenue for FROG, TENB, QLYS; Software/Services Revenue for CHKP, FTNT, IBM; Total ARR for CLBT, RPD, VRNS

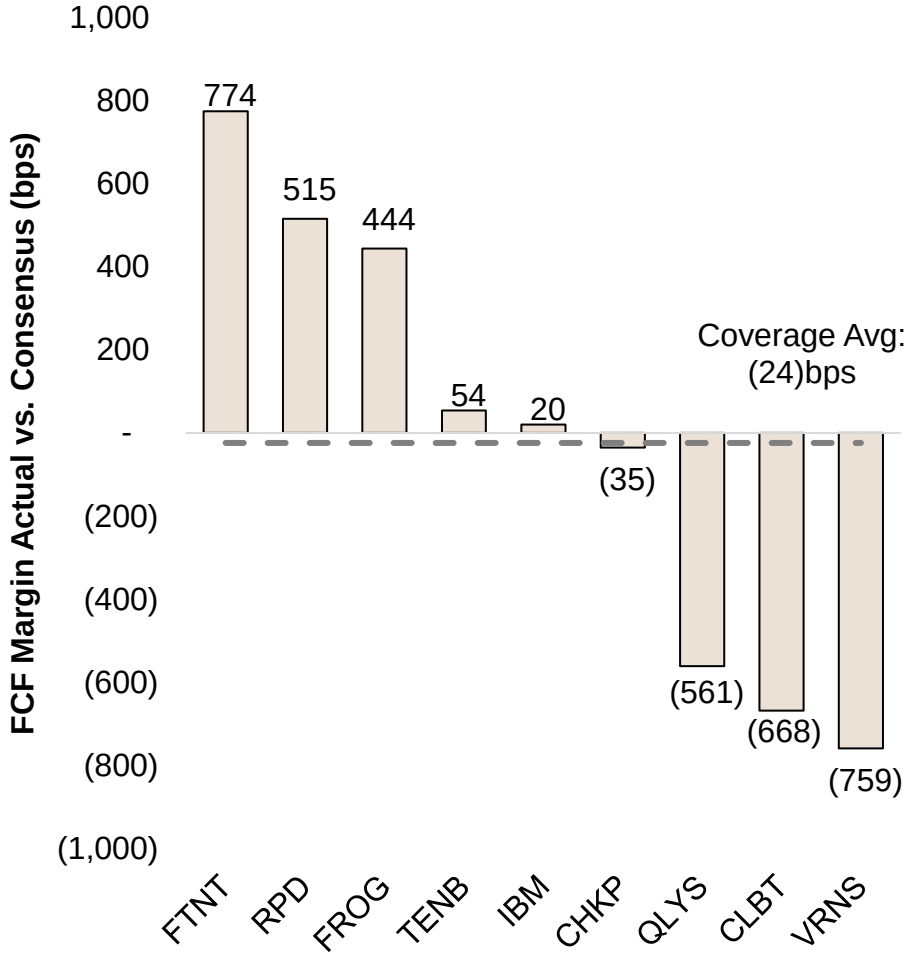
Focus on Growth, Awareness of Need for Profitability

Emphasis on Cost Optimization Remains



Source: Bloomberg Finance L.P.
Note: Using pre-tax income margin for IBM

FCF Margins as Expected



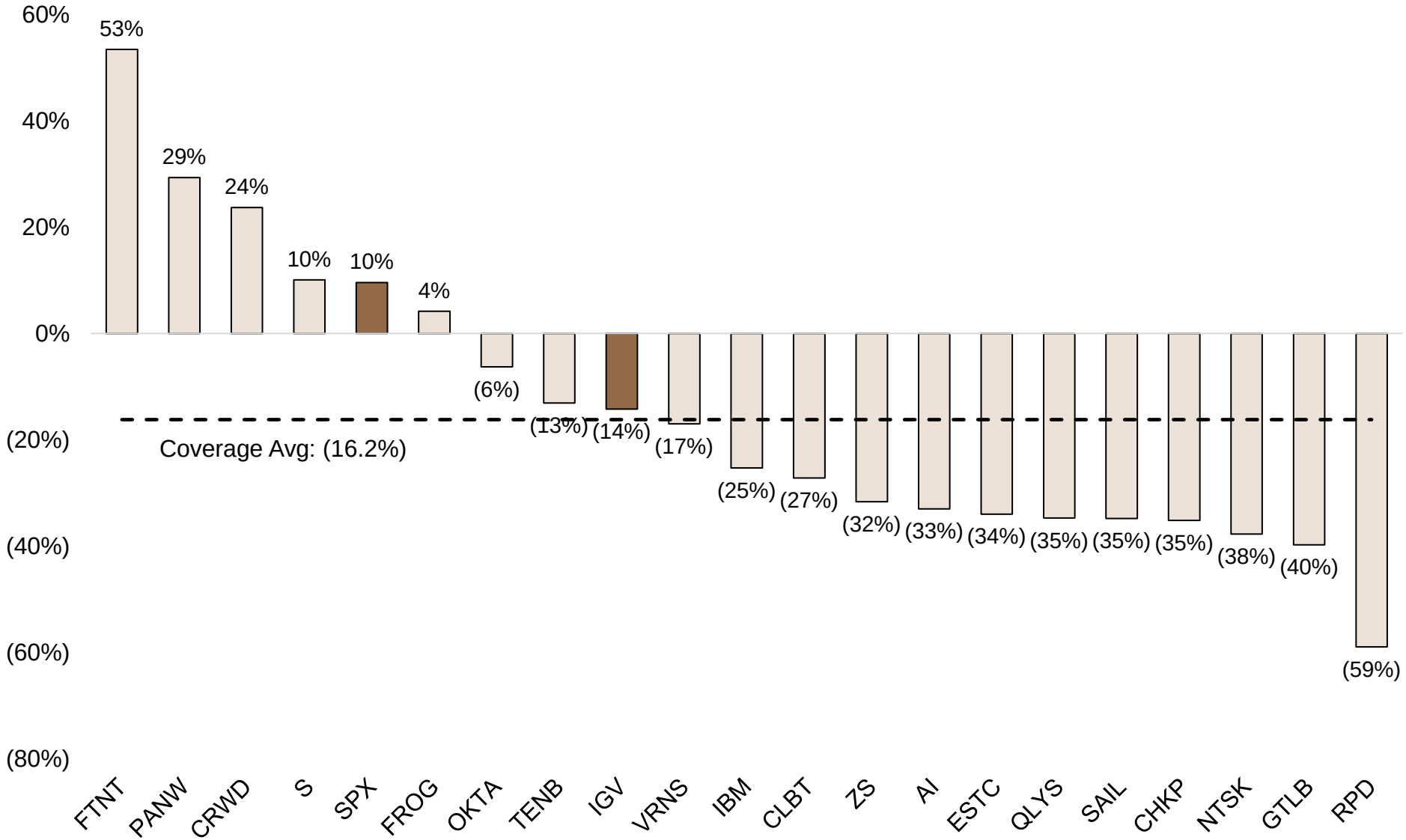
Source: Bloomberg Finance L.P.

1Q26 Earnings Snapshot

Company	T+1 Performance	What Happened
FROG	24%	Strong execution driven by Cloud momentum, security adoption and AI-driven binary growth, increased Cloud guidance.
FTNT	20%	Beat and raise driven by significant cyclical upside for hardware partially offset by disconnected Service deceleration.
CLBT	8%	Strong execution, 2Q ARR guidance implies acceleration, FY26 guidance unchanged, AI could double the size of the company.
VRNS	7%	Beat and raise driven by healthy demand and new customer acquisition strength, SaaS ARR guidance increased.
QLYS	(1%)	In-line revenue and margin/EPS beat. FY26 revenue guidance raised slightly but still implies decel and margin compression.
RPD	(2%)	1Q26 revenue beat, ARR decline. 2Q ARR guide implies sequential dollar decline and accelerating churn rate.
TENB	(3%)	Beat led by strong execution, FY26 guidance increased but remains conservative.
IBM	(8%)	Better Mainframe and Red Hat performance, offset by CC Software growth miss, softer Consulting revenue.
CHKP	(20%)	Relatively in-line revenue and margins while billings miss driven by GTM disruptions. Management cut FY26 total revenue guidance.

Source: Company reports, Security Companies that have reported so far

YTD JPM Security Coverage Underperformed S&P 500 and IGV



Source: Bloomberg Finance L.P.
*Stock performance Avg 12/31/25 vs 5/14/26

AI Signals From 1Q26 Earnings

Early reporters confirm AI is converting to revenue and/or cost savings across software. We expect the signal to intensify through the remainder of earnings season.

CLBT: “We think it is entirely possible that the AI revenue (over the next four years) could approximate the total revenue of the company. Or said differently, we see an opportunity to double our business…” — Thomas E. Hogan, CEO

MSFT: "Our AI business surpassed $37 billion ARR, up 123%." — Satya Nadella, CEO

NOW: "Now Assist ACV passed $600 million last year, more than doubling year-over-year. That momentum carried into Q1 with ACV crossing $750 million." — Gina Mastantuono, CFO

GOOGL: "In Q1, revenue from products built on our GenAI models grew nearly 800% year-over-year." — Sundar Pichai, CEO

IBM: "Our generative AI book of business grew to over $12.5 billion since inception." — Arvind Krishna, CEO

NOW: "We're raising our 2026 AI ACV target from $1 billion to $1.5 billion." — Gina Mastantuono, CFO

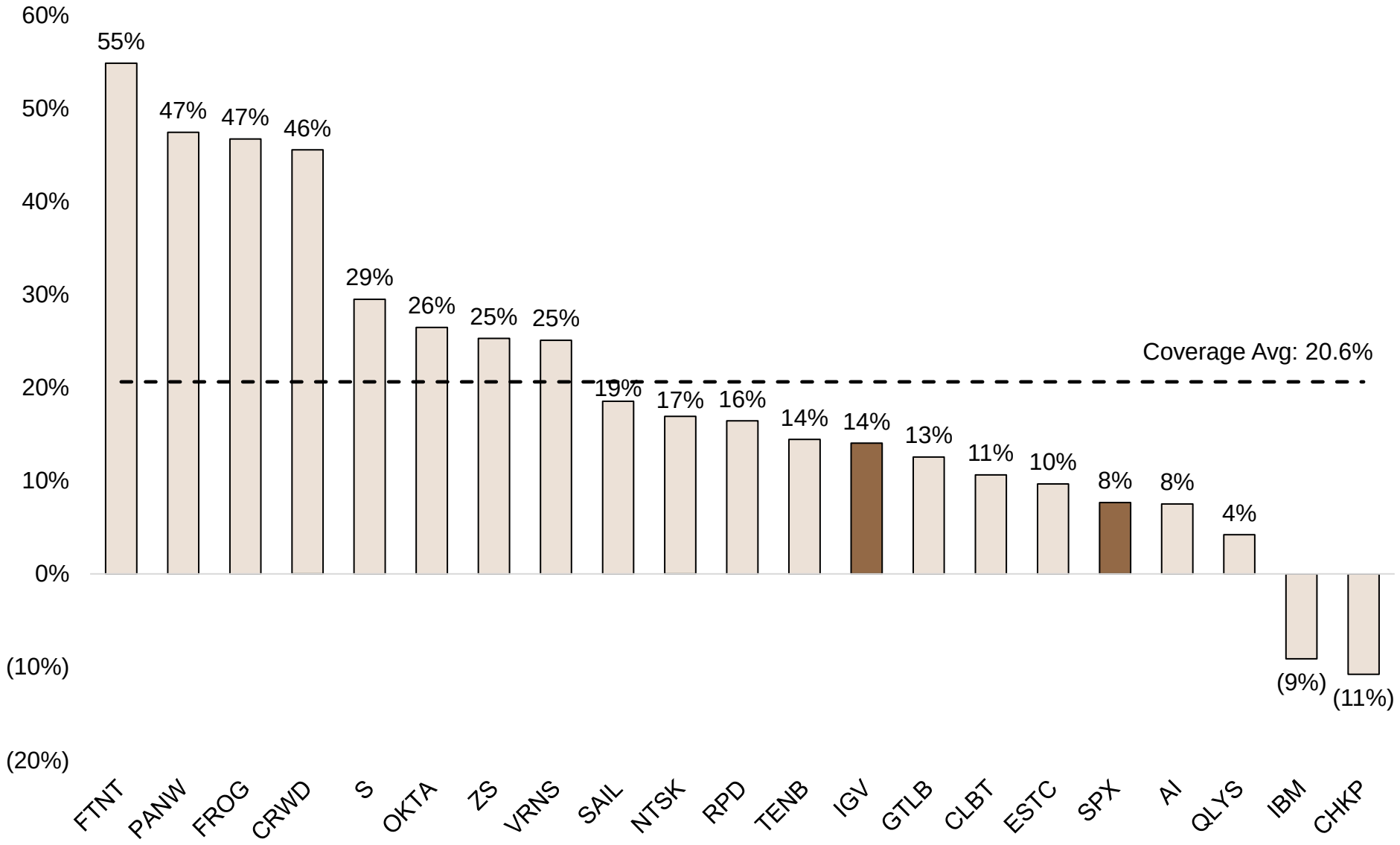
FROG: "AI is transitioning from experimentation to tangible revenue, and we are seeing stronger momentum across our business.“— Shlomi Ben Haim, CEO

DDOG: "We now have over 6,500 customers sending data for one or more of our AI integrations. Though this is only 20% of total customers, they represent about 80% of our ARR." — Olivier Pomel, CEO

TEAM: "Customers using Rovo are also growing their ARR at roughly two times the rate of customers who are not using Rovo." — Mike Cannon-Brookes, CEO

NOW: "We're also seeing an acceleration in the incremental savings from agentic AI flattening the hiring curve with $200 million in savings in 2026... for a total of $300 million in expected annualized cost savings from agentic AI." — Gina Mastantuono, CFO

JPM Security Coverage Outperformed IGV Over The Past Month



Source: Bloomberg Finance L.P.
*Stock performance Avg 4/14/26 vs 5/14/26

CY26 Revenue Expectations Remains Relatively Unchanged

Source: Bloomberg Finance L.P.
* CY26 Revenue Revisions 4/21/26 vs 5/14/26

AI Is Expanding the Attack Surfaces and Access to Budget Dollars

AI-driven threats are creating C-suite and board-level urgency around exposure management, data security, and software supply chain governance.

TENB: "We are seeing a level of urgency that is different from even a month ago — not just at the practitioner level, but across the C-suite and the board." — Mark Thurmond, Co-CEO

RPD: "Mythos commoditized vulnerability identification, finding bugs in code. It has not commoditized the operational reality of managing those vulnerabilities across complex enterprise environments." — Corey Thomas, CEO

QLYS: "Exploitable vulnerability volume surging 6.5x and the average time to exploit collapsing to under a day as adversaries weaponize vulnerabilities before patches even exist." — Sumedh Thakar, CEO

TENB: "Recent announcements, including Anthropic Mythos, have demonstrated that AI can now autonomously discover software vulnerabilities at scale and speed we have not seen before." — Mark Thurmond, Co-CEO

VRNS: "AI is forcing companies to prioritize data and AI security, and Varonis is uniquely positioned to help with our unified platform that allows customers to put the right guardrails in place in order to accelerate their AI deployment plans." — Yaki Faitelson, CEO

RPD: "Advances from frontier models have fundamentally accelerated the threat environment and outpaced operating models built to defend against it." — Corey Thomas, CEO

FROG: "Organizations are actively encouraging developers to utilize AI coding agents, as well as explore agentic capabilities, causing software output to accelerate resulting in more compiled code. A true AI-fueled tsunami of binaries." — Shlomi Ben Haim, CEO

Platformization Is the Monetization Bridge

The buying motion has shifted: customers want fewer vendors, shared telemetry, and embedded governance. Platform vendors are winning the budget reallocation.

NOW: "The power of our Better Together platform model was evident as 17 of our top 20 deals included 7 or more products." — Gina Mastantuono, CFO

DDOG: "35% of our customers use six or more products, up from 28% a year ago, and 20% use eight or more products, up from 13% a year ago." — Olivier Pomel, CEO

NET: "By standardizing on Cloudflare, they displace six legacy vendors at signing, with 10 more displacements already underway, targeting over $1.3 million in annual savings." — Matthew Prince, CEO

TENB: "Tenable One, our AI-powered exposure management platform, was 41% of new business this quarter, an 8-point increase from Q1 last year." — Stephen Vintz, Co-CEO

FROG: "JFrog unifies all artifact types, binaries, models, skills and MCP servers into single platform governed by one framework, one set of policy, and complete visibility and traceability in one place." — Shlomi Ben Haim, CEO

VRNS: "We continue to see existing customers expand into new use cases as they consolidate point tools and utilize the breadth of our platform." — Yaki Faitelson, CEO

TENB: "Customers are moving away from tools that create more noise and toward exposure management platforms that provide context, prioritization, and automated action." — Mark Thurmond, Co-CEO

TEAM: "This is our largest ever quarter for competitive displacements from a major ITSM provider. We're taking share from rivals as customers move away from legacy systems." — Mike Cannon-Brookes, CEO

Coverage Universe Comps Table

Company	Market Cap	Ticker	Rating	Pricing		Valuation									
				Price	JPM	EV/Sales		EV/Sales/G		EV/FCF		EV/(FCF-SBC)		P/E	
				5/14/2026	PT	CY26	CY27	CY26	CY27	CY26	CY27	CY26	CY27	CY26	CY27
C3.ai Inc	1,228	**AI**	UW	8.65	7.00	2.4x	2.2x	-0.08x	0.30x	---	13.5x	---	---	---	34.9x
Cellebrite DI Ltd	3,137	**CLBT**	OW	12.10	20.00	4.8x	4.0x	0.24x	0.20x	15.4x	12.6x	20.8x	16.9x	21.6x	18.3x
Check Point Software	12,220	**CHKP**	OW	115.17	135.00	3.5x	3.3x	1.21x	0.54x	8.1x	7.5x	10.3x	9.5x	10.9x	9.8x
Crowdstrike Holdings Inc	145,218	**CRWD**	OW	562.57	475.00	23.8x	19.6x	1.02x	0.91x	---	61.5x	---	---	---	---
Elastic	5,158	**ESTC**	OW	48.57	99.00	2.3x	2.0x	0.13x	0.14x	12.9x	11.7x	---	---	17.5x	14.5x
Fortinet Inc	88,032	**FTNT**	UW	117.69	75.00	10.9x	9.9x	0.68x	1.01x	32.9x	30.9x	37.8x	36.1x	37.4x	34.8x
Gitlab Inc	3,795	**GTLB**	N	22.05	28.00	2.3x	2.0x	0.13x	0.12x	12.6x	10.3x	---	---	27.6x	24.0x
IBM	203,672	**IBM**	N	214.64	270.00	3.4x	3.2x	0.52x	0.62x	15.5x	14.5x	17.1x	15.6x	17.3x	15.9x
JFrog Ltd	8,049	**FROG**	OW	64.18	76.00	11.6x	9.8x	0.58x	0.51x	48.7x	32.8x	---	---	66.2x	51.8x
Netskope	4,167	**NTSK**	OW	10.56	19.00	4.3x	3.5x	0.18x	0.15x	---	41.9x	---	---	---	---
Okta Inc	14,458	**OKTA**	OW	78.20	103.00	3.8x	3.5x	0.41x	0.33x	13.9x	12.0x	33.4x	24.0x	20.5x	17.6x
Palo Alto Networks Inc	161,959	**PANW**	OW	227.79	200.00	12.0x	10.2x	0.43x	0.57x	41.6x	26.5x	---	43.7x	62.8x	52.1x
Qualys Inc	3,086	**QLYS**	UW	86.50	87.00	3.3x	3.0x	0.38x	0.42x	7.8x	8.0x	11.1x	12.1x	11.3x	10.5x
Rapid7 Inc	478	**RPD**	N	6.18	7.00	0.8x	0.8x	-0.38x	0.77x	5.0x	5.2x	18.3x	27.2x	4.0x	4.0x
SailPoint Inc	6,659	**SAIL**	OW	11.81	22.00	5.0x	4.2x	0.27x	0.22x	32.1x	19.6x	---	---	36.9x	30.3x
SentinelOne Inc	5,482	**S**	N	16.08	16.00	3.9x	3.3x	0.19x	0.19x	61.2x	39.6x	---	---	48.7x	33.5x
Tenable Holdings Inc	2,422	**TENB**	OW	20.58	35.00	2.2x	2.1x	0.26x	0.24x	9.0x	7.9x	28.7x	22.4x	10.4x	8.8x
Varonis Systems Inc	3,588	**VRNS**	OW	27.01	39.00	3.8x	3.1x	0.21x	0.15x	27.8x	18.8x	---	---	---	34.2x
Zscaler Inc	25,363	**ZS**	OW	152.43	250.00	6.0x	4.9x	0.24x	0.24x	21.8x	17.3x	---	---	35.4x	30.3x
					Average	**5.8x**	**5.0x**	**0.35x**	**0.40x**	**22.9x**	**20.6x**	**22.2x**	**23.1x**	**28.6x**	**25.0x**
					Median	**3.8x**	**3.3x**	**0.26x**	**0.30x**	**15.4x**	**14.5x**	**19.5x**	**22.4x**	**21.6x**	**24.0x**

Source: Bloomberg Finance L.P., J.P. Morgan estimates

Disclosures

Analyst Certification: The Research Analyst(s) denoted by an "AC" on the cover of this report certifies (or, where multiple Research Analysts are primarily responsible for this report, the Research Analyst denoted by an "AC" on the cover or within the document individually certifies, with respect to each security or issuer that the Research Analyst covers in this research) that: (1) all of the views expressed in this report accurately reflect the Research Analyst's personal views about any and all of the subject securities or issuers; and (2) no part of any of the Research Analyst's compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the Research Analyst(s) in this report. For all Korea-based Research Analysts listed on the front cover, if applicable, they also certify, as per KOFIA requirements, that the Research Analyst's analysis was made in good faith and that the views reflect the Research Analyst's own opinion, without undue influence or intervention.

All authors named within this report are Research Analysts who produce independent research unless otherwise specified. In Europe, Sector Specialists (Sales and Trading) may be shown on this report as contacts but are not authors of the report or part of the Research Department.

Important Disclosures

Company-Specific Disclosures: J.P. Morgan does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that the firm may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decision. Important disclosures, including price charts and credit opinion history tables, are available for compendium reports and all J.P. Morgan–covered companies, and certain non-covered companies, by visiting https://www.jpmm.com/research/disclosures, calling 1-800-477-0406, or e-mailing research.disclosure.inquiries@jpmorgan.com with your request.

Explanation of Equity Research Ratings, Designations and Analyst(s) Coverage Universe:
J.P. Morgan uses the following rating system: Overweight (over the duration of the price target indicated in this report, we expect this stock will outperform the average total return of the stocks in the Research Analyst's, or the Research Analyst's team's, coverage universe); Neutral (over the duration of the price target indicated in this report, we expect this stock will perform in line with the average total return of the stocks in the Research Analyst's, or the Research Analyst's team's, coverage universe); and Underweight (over the duration of the price target indicated in this report, we expect this stock will underperform the average total return of the stocks in the Research Analyst's, or the Research Analyst's team's, coverage universe. NR is Not Rated. In this case, J.P. Morgan has removed the rating and, if applicable, the price target, for this stock because of either a lack of a sufficient fundamental basis or for legal, regulatory or policy reasons. The previous rating and, if applicable, the price target, no longer should be relied upon. An NR designation is not a recommendation or a rating. Some stocks under coverage have a rating but no price target; in these cases, we expect the stock will outperform/perform in line/underperform the average total return of the stocks in the Research Analyst's, or the Research Analyst's team's, coverage universe of the relevant duration of the region. In our Asia (ex-Australia and ex-India) and U.K. small- and mid-cap Equity Research, each stock's expected total return is compared to the expected total return of a benchmark country market index, not to those Research Analysts' coverage universe. If it does not appear in the Important Disclosures section of this report, the certifying Research Analyst's coverage universe can be found on J.P. Morgan's Research website, https://www.jpmorganmarkets.com.

Disclosures

J.P. Morgan Equity Research Ratings Distribution, as of April 04, 2026

	Overweight (buy)	Neutral (hold)	Underweight (sell)
J.P. Morgan Global Equity Research Coverage*	51%	37%	12%
IB clients**	83%	79%	74%
JPMS Equity Research Coverage*	49%	39%	13%
IB clients**	94%	93%	85%

*Please note that the percentages may not add to 100% because of rounding.
**Percentage of subject companies within each of the "buy," "hold" and "sell" categories for which J.P. Morgan has provided investment banking services within the previous 12 months.
For purposes of FINRA ratings distribution rules only, our Overweight rating falls into a buy rating category; our Neutral rating falls into a hold rating category; and our Underweight rating falls into a sell rating category. Please note that stocks with an NR designation are not included in the table above. This information is current as of the end of the most recent calendar quarter.

Equity Valuation and Risks: For valuation methodology and risks associated with covered companies or price targets for covered companies, please see the most recent company-specific research report at http://www.jpmorganmarkets.com, contact the primary analyst or your J.P. Morgan representative, or email research.disclosure.inquiries@jpmorgan.com. For material information about the proprietary models used, please see the Summary of Financials in company-specific research reports and the Company Tearsheets, which are available to download on the company pages of our client website, http://www.jpmorganmarkets.com. This report also sets out within it the material underlying assumptions used.

History of Investment Recommendations:
A history of J.P. Morgan investment recommendations disseminated during the preceding 12 months can be accessed on the Research & Commentary page of http://www.jpmorganmarkets.com where you can also search by analyst name, sector or financial instrument.

Analysts' Compensation: The research analysts responsible for the preparation of this report receive compensation based upon various factors, including the quality and accuracy of research, client feedback, competitive factors, and overall firm revenues.

Other Disclosures

J.P. Morgan is a marketing name for investment banking businesses of JPMorgan Chase & Co. and its subsidiaries and affiliates worldwide.

UK MIFID FICC research unbundling exemption: UK clients should refer to UK MIFID Research Unbundling exemption for details of J.P. Morgan's implementation of the FICC research exemption and guidance on relevant FICC research categorisation.

All research material made available to clients are simultaneously available on our client website, J.P. Morgan Markets, unless specifically permitted by relevant laws. Not all research content is redistributed, e-mailed or made available to third-party aggregators. For all research material available on a particular stock, please contact your sales representative.

Any long form nomenclature for references to China; Hong Kong; Taiwan; and Macau within this research material are Mainland China; Hong Kong SAR (China); Taiwan (China); and Macau SAR (China).

J .P. Morgan Research may, from time to time, write on issuers or securities targeted by economic or financial sanctions imposed or administered by the governmental authorities of the U.S., EU, UK or other relevant jurisdictions (Sanctioned Securities). Nothing in this report is intended to be read or construed as encouraging, facilitating, promoting or otherwise approving investment or dealing in such Sanctioned Securities. Clients should be aware of their own legal and compliance obligations when making investment decisions.

Any digital or crypto assets discussed in this research report are subject to a rapidly changing regulatory landscape. For relevant regulatory advisories on crypto assets, including bitcoin and ether, please see https://www.jpmorgan.com/disclosures/cryptoasset-disclosure.

Disclosures

The author(s) of this research report may not be licensed to carry on regulated activities in your jurisdiction and, if not licensed, do not hold themselves out as being able to do so.

Exchange-Traded Funds (ETFs): J.P. Morgan Securities LLC ("JPMS") acts as authorized participant for substantially all U.S.-listed ETFs. To the extent that any ETFs are mentioned in this report, JPMS may earn commissions and transaction-based compensation in connection with the distribution of those ETF shares and may earn fees for performing other trade-related services, such as securities lending to short sellers of the ETF shares. JPMS may also perform services for the ETFs themselves, including acting as a broker or dealer to the ETFs. In addition, affiliates of JPMS may perform services for the ETFs, including trust, custodial, administration, lending, index calculation and/or maintenance and other services.

Options and Futures related research: If the information contained herein regards options- or futures-related research, such information is available only to persons who have received the proper options or futures risk disclosure documents. Please contact your J.P. Morgan Representative or visit https://www.theocc.com/components/docs/riskstoc.pdf for a copy of the Option Clearing Corporation's Characteristics and Risks of Standardized Options or https://www.finra.org/sites/default/files/2020-08/Security_Futures_Risk_Disclosure_Statement_2020.pdf for a copy of the Security Futures Risk Disclosure Statement.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/global/disclosures/interbank_offered_rates

Private Bank Clients: Where you are receiving research as a client of the private banking businesses offered by JPMorgan Chase & Co. and its subsidiaries ("J.P. Morgan Private Bank"), research is provided to you by J.P. Morgan Private Bank and not by any other division of J.P. Morgan, including, but not limited to, the J.P. Morgan Corporate and Investment Bank and its Global Research division.

Legal entity responsible for the production and distribution of research: The legal entity identified below the name of the Reg AC Research Analyst who authored this material is the legal entity responsible for the production of this research. Where multiple Reg AC Research Analysts authored this material with different legal entities identified below their names, these legal entities are jointly responsible for the production of this research. Where more than one legal entity is listed under an analyst's name, the first legal entity is responsible for the production unless stated otherwise. Research Analysts from various J.P. Morgan affiliates may have contributed to the production of this material but may not be licensed to carry out regulated activities in your jurisdiction (and do not hold themselves out as being able to do so). Unless otherwise stated below in the legal entity disclosures, this material has been distributed by the legal entity responsible for production, or where more than one legal entity is listed under the analyst's name, the first legal entity will be responsible for distribution. If you have any queries, please contact the relevant Research Analyst in your jurisdiction or the entity in your jurisdiction that has distributed this research material.

Legal Entities Disclosures and Country-/Region-Specific Disclosures:
Argentina: JPMorgan Chase Bank N.A Sucursal Buenos Aires is regulated by Banco Central de la República Argentina ("BCRA"- Central Bank of Argentina) and Comisión Nacional de Valores ("CNV"- Argentinian Securities Commission - ALYC y AN Integral N°51).
Australia: J.P. Morgan Securities Australia Limited ("JPMSAL") (ABN 61 003 245 234/AFS Licence No: 238066) is regulated by the Australian Securities and Investments Commission and is a Market Participant of ASX Limited, a Clearing and Settlement Participant of ASX Clear Pty Limited and a Clearing Participant of ASX Clear (Futures) Pty Limited. This material is issued and distributed in Australia by or on behalf of JPMSAL only to "wholesale clients" (as defined in section 761G of the Corporations Act 2001). A list of all financial products covered can be found by visiting https://www.jpmm.com/research/disclosures. J.P. Morgan seeks to cover companies of relevance to the domestic and international investor base across all Global Industry Classification Standard (GICS) sectors, as well as across a range of market capitalisation sizes. If applicable, in the course of conducting public side due diligence on the subject company(ies), the Research Analyst team may at times perform such diligence through corporate engagements such as site visits, discussions with company representatives, management presentations, etc. Research issued by JPMSAL has been prepared in accordance with J.P. Morgan Australia's Research Independence Policy which can be found at the following link: J.P. Morgan Australia - Research Independence Policy.

Disclosures

Brazil: Banco J.P. Morgan S.A. is regulated by the Comissao de Valores Mobiliarios (CVM) and by the Central Bank of Brazil. Ombudsman J.P. Morgan: 0800-7700847 / 0800-7700810 (For Hearing Impaired) / ouvidoria.jp.morgan@jpmchase.com.

Canada: J.P. Morgan Securities Canada Inc. is a registered investment dealer, regulated by the Canadian Investment Regulatory Organization and the Ontario Securities Commission and is the participating member on Canadian exchanges. This material is distributed in Canada by or on behalf of J.P.Morgan Securities Canada Inc.

Chile: Inversiones J.P. Morgan Limitada is an unregulated entity incorporated in Chile.

China: J.P. Morgan Securities (China) Company Limited has been approved by CSRC to conduct the securities investment consultancy business.

Colombia: Banco J.P. Morgan Colombia S.A. is supervised by the Superintendencia Financiera de Colombia (SFC).

Dubai International Financial Centre (DIFC): JPMorgan Chase Bank, N.A., Dubai Branch is regulated by the Dubai Financial Services Authority (DFSA) and its registered address is Dubai International Financial Centre - The Gate, West Wing, Level 3 and 9 PO Box 506551, Dubai, UAE. This material has been distributed by JP Morgan Chase Bank, N.A., Dubai Branch to persons regarded as professional clients or market counterparties as defined under the DFSA rules.

European Economic Area (EEA): Unless specified to the contrary, research is distributed in the EEA by J.P. Morgan SE ("JPM SE"), which is authorised as a credit institution by the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) and jointly supervised by the BaFin, the German Central Bank (Deutsche Bundesbank) and the European Central Bank (ECB). JPM SE is a company headquartered in Frankfurt with registered address at TaunusTurm, Taunustor 1, Frankfurt am Main, 60310, Germany. The material has been distributed in the EEA to persons regarded as professional investors (or equivalent) pursuant to Art. 4 para. 1 no. 10 and Annex II of MiFID II and its respective implementation in their home jurisdictions ("EEA professional investors"). This material must not be acted on or relied on by persons who are not EEA professional investors. Any investment or investment activity to which this material relates is only available to EEA relevant persons and will be engaged in only with EEA relevant persons.

Hong Kong: J.P. Morgan Securities (Asia Pacific) Limited (CE number AAJ321) is regulated by the Hong Kong Monetary Authority and the Securities and Futures Commission in Hong Kong, and J.P. Morgan Broking (Hong Kong) Limited (CE number AAB027) is regulated by the Securities and Futures Commission in Hong Kong. JP Morgan Chase Bank, N.A., Hong Kong Branch (CE Number AAL996) is regulated by the Hong Kong Monetary Authority and the Securities and Futures Commission, is organized under the laws of the United States with limited liability. Where the distribution of this material is a regulated activity in Hong Kong, the material is distributed in Hong Kong by or through J.P. Morgan Securities (Asia Pacific) Limited and/or J.P. Morgan Broking (Hong Kong) Limited.

India: J.P. Morgan India Private Limited (Corporate Identity Number - U67120MH1992FTC068724), having its registered office at J.P. Morgan Tower, Off. C.S.T. Road, Kalina, Santacruz - East, Mumbai – 400098, is registered with the Securities and Exchange Board of India (SEBI) as a 'Research Analyst' having registration number INH000001873. J.P. Morgan India Private Limited is also registered with SEBI as a member of the National Stock Exchange of India Limited and the Bombay Stock Exchange Limited (SEBI Registration Number – INZ000239730) and as a Merchant Banker (SEBI Registration Number - MB/INM000002970). Telephone: 91-22-6157 3000, Facsimile: 91-22-6157 3990 and Website: http://www.jpmipl.com. JPMorgan Chase Bank, N.A. - Mumbai Branch is licensed by the Reserve Bank of India (RBI) (Licence No. 53/ Licence No. BY.4/94; SEBI - IN/CUS/014/ CDSL : IN-DP-CDSL-444-2008/ IN-DP-NSDL-285-2008/ INBI00000984/ INE231311239) as a Scheduled Commercial Bank in India, which is its primary license allowing it to carry on Banking business in India and other activities, which a Bank branch in India are permitted to undertake. For non-local research material, this material is not distributed in India by J.P. Morgan India Private Limited. Compliance Officer: Prasanna Bandal; prasanna.bandal@jpmchase.com; +912261575159. Grievance Officer: Ramprasadh K, jpmipl.research.feedback@jpmorgan.com; +912261573000. Registration granted by SEBI and certification from NISM in no way guarantee performance of the intermediary or provide any assurance of returns to investors. Please visit Terms and Conditions and Most Important Terms and Conditions (MITC). The annual Compliance audit report is available at http://www.jpmipl.com/#research.

Indonesia: PT J.P. Morgan Sekuritas Indonesia is a member of the Indonesia Stock Exchange and is registered and supervised by the Otoritas Jasa Keuangan (OJK).

Korea: J.P. Morgan Securities (Far East) Limited, Seoul Branch, is a member of the Korea Exchange (KRX). JPMorgan Chase Bank, N.A., Seoul Branch, is licensed as a branch office of foreign bank (JPMorgan Chase Bank, N.A.) in Korea. Both entities are regulated by the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS). For non-macro research material, the material is distributed in Korea by or through J.P. Morgan Securities (Far East) Limited, Seoul Branch.

Japan: JPMorgan Securities Japan Co., Ltd. and JPMorgan Chase Bank, N.A., Tokyo Branch are regulated by the Financial Services Agency in Japan.

Malaysia: This material is issued and distributed in Malaysia by JPMorgan Securities (Malaysia) Sdn Bhd (18146-X), which is a Participating Organization of Bursa Malaysia Berhad and holds a Capital Markets Services License issued by the Securities Commission in Malaysia.

Mexico: J.P. Morgan Casa de Bolsa, S.A. de C.V. and J.P. Morgan Grupo Financiero are members of the Mexican Stock Exchange and are authorized to act as a broker dealer by the National Banking and Securities Exchange Commission.

Disclosures

New Zealand: This material is issued and distributed by JPMSAL in New Zealand only to "wholesale clients" (as defined in the Financial Markets Conduct Act 2013). JPMSAL is registered as a Financial Service Provider under the Financial Service providers (Registration and Dispute Resolution) Act of 2008.
Philippines: J.P. Morgan Securities Philippines Inc. is a Trading Participant of the Philippine Stock Exchange and a member of the Securities Clearing Corporation of the Philippines and the Securities Investor Protection Fund. It is regulated by the Securities and Exchange Commission.
Singapore: This material is issued and distributed in Singapore by or through J.P. Morgan Securities Singapore Private Limited (JPMSS) [MDDI (P) 057/08/2025 and Co. Reg. No.: 199405335R], which is a member of the Singapore Exchange Securities Trading Limited, and/or JPMorgan Chase Bank, N.A., Singapore branch (JPMCB Singapore), both of which are regulated by the Monetary Authority of Singapore. This material is issued and distributed in Singapore only to accredited investors, expert investors and institutional investors, as defined in Section 4A of the Securities and Futures Act, Cap. 289 (SFA). This material is not intended to be issued or distributed to any retail investors or any other investors that do not fall into the classes of "accredited investors," "expert investors" or "institutional investors," as defined under Section 4A of the SFA. Recipients of this material in Singapore are to contact JPMSS or JPMCB Singapore in respect of any matters arising from, or in connection with, the material.
South Africa: J.P. Morgan Equities South Africa Proprietary Limited and JPMorgan Chase Bank, N.A., Johannesburg Branch are members of the Johannesburg Securities Exchange and are regulated by the Financial Services Conduct Authority (FSCA).
Taiwan: J.P. Morgan Securities (Taiwan) Limited is a participant of the Taiwan Stock Exchange (company-type) and regulated by the Taiwan Securities and Futures Bureau. Material relating to equity securities is issued and distributed in Taiwan by J.P. Morgan Securities (Taiwan) Limited, subject to the license scope and the applicable laws and the regulations in Taiwan. To the extent that J.P. Morgan Securities (Taiwan) Limited produces research materials on securities not listed on the Taiwan Stock Exchange or Taipei Exchange ("Non-Taiwan Listed Securities"), these materials shall not constitute securities recommendations for the purpose of applicable Taiwan regulations, and, for the avoidance of doubt, J.P. Morgan Securities (Taiwan) Limited does not act as broker for Non-Taiwan Listed Securities. According to Paragraph 2, Article 7-1 of Operational Regulations Governing Securities Firms Recommending Trades in Securities to Customers (as amended or supplemented) and/or other applicable laws or regulations, please note that the recipient of this material is not permitted to engage in any activities in connection with the material that may give rise to conflicts of interests, unless otherwise disclosed in the "Important Disclosures" in this material.
Thailand: This material is issued and distributed in Thailand by JPMorgan Securities (Thailand) Ltd., which is a member of the Stock Exchange of Thailand and is regulated by the Ministry of Finance and the Securities and Exchange Commission, and its registered address is 3rd Floor, 20 North Sathorn Road, Silom, Bangrak, Bangkok 10500.
UK: Research is produced in the UK by J.P. Morgan Securities plc ("JPMS plc") which is a member of the London Stock Exchange and is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority or J.P. Morgan Markets Limited ("JPMML Ltd") which is authorised and regulated by the Financial Conduct Authority. Unless specified to the contrary, this material is distributed in the UK by JPMS plc and is directed in the UK only to: (a) persons having professional experience in matters relating to investments falling within article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) (Order) 2005 ("the FPO"); (b) persons outlined in article 49 of the FPO (high net worth companies, unincorporated associations or partnerships, the trustees of high value trusts, etc.); or (c) any persons to whom this communication may otherwise lawfully be made; all such persons being referred to as "UK relevant persons". This material must not be acted on or relied on by persons who are not UK relevant persons. Any investment or investment activity to which this material relates is only available to UK relevant persons and will be engaged in only with UK relevant persons. A description of J.P. Morgan EMEA's policy for prevention and avoidance of conflicts of interest related to the production of Research can be found at the following link: J.P. Morgan EMEA - Research Independence Policy.
U.S.: J.P. Morgan Securities LLC ("JPMS") is a member of the NYSE, FINRA, SIPC, and the NFA. JPMorgan Chase Bank, N.A. is a member of the FDIC. Material published by non-U.S. affiliates is distributed in the U.S. by JPMS who accepts responsibility for its content.

General: Additional information is available upon request. The information in this material has been obtained from sources believed to be reliable. While all reasonable care has been taken to ensure that the facts stated in this material are accurate and that the forecasts, opinions and expectations contained herein are fair and reasonable, JPMorgan Chase & Co. or its affiliates and/or subsidiaries (collectively J.P. Morgan) make no representations or warranties whatsoever to the completeness or accuracy of the material provided, except with respect to any disclosures relative to J.P. Morgan and the Research Analyst's involvement with the issuer that is the subject of the material. Accordingly, no reliance should be placed on the accuracy, fairness or completeness of the information contained in this material. There may be certain discrepancies with data and/or limited content in this material as a result of calculations, adjustments, translations to different languages, and/or local regulatory restrictions, as applicable. These discrepancies should not impact the overall investment analysis, views and/or recommendations of the subject company(ies) that may be discussed in the material. Artificial intelligence tools may have been used in the preparation of this material, including assisting in data analysis, pattern recognition, and content drafting for research material. J.P. Morgan accepts no liability whatsoever for any loss arising from any use of this material or its contents, and neither J.P. Morgan nor any of its respective directors, officers or employees, shall be in any way responsible for the contents hereof, apart from the liabilities

Disclosures

and responsibilities that may be imposed on them by the relevant regulatory authority in the jurisdiction in question, or the regulatory regime thereunder. Opinions, forecasts or projections contained in this material represent J.P. Morgan's current opinions or judgment as of the date of the material only and are therefore subject to change without notice. Periodic updates may be provided on companies/industries based on company-specific developments or announcements, market conditions or any other publicly available information. There can be no assurance that future results or events will be consistent with any such opinions, forecasts or projections, which represent only one possible outcome. Furthermore, such opinions, forecasts or projections are subject to certain risks, uncertainties and assumptions that have not been verified, and future actual results or events could differ materially. The value of, or income from, any investments referred to in this material may fluctuate and/or be affected by changes in exchange rates. All pricing is indicative as of the close of market for the securities discussed, unless otherwise stated. Past performance is not indicative of future results. Accordingly, investors may receive back less than originally invested. This material is not intended as an offer or solicitation for the purchase or sale of any financial instrument. The opinions and recommendations herein do not take into account individual client circumstances, objectives, or needs and are not intended as recommendations of particular securities, financial instruments or strategies to particular clients. This material may include views on structured securities, options, futures and other derivatives. These are complex instruments, may involve a high degree of risk and may be appropriate investments only for sophisticated investors who are capable of understanding and assuming the risks involved. The recipients of this material must make their own independent decisions regarding any securities or financial instruments mentioned herein and should seek advice from such independent financial, legal, tax or other adviser as they deem necessary. J.P. Morgan may trade as a principal on the basis of the Research Analysts' views and research, and it may also engage in transactions for its own account or for its clients' accounts in a manner inconsistent with the views taken in this material, and J.P. Morgan is under no obligation to ensure that such other communication is brought to the attention of any recipient of this material. Others within J.P. Morgan, including Strategists, Sales staff and other Research Analysts, may take views that are inconsistent with those taken in this material. Employees of J.P. Morgan not involved in the preparation of this material may have investments in the securities (or derivatives of such securities) mentioned in this material and may trade them in ways different from those discussed in this material. This material is not an advertisement for or marketing of any issuer, its products or services, or its securities in any jurisdiction.

Confidentiality and Security Notice: This transmission may contain information that is privileged, confidential, legally privileged, and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of the information contained herein (including any reliance thereon) is STRICTLY PROHIBITED. Although this transmission and any attachments are believed to be free of any virus or other defect that might affect any computer system into which it is received and opened, it is the responsibility of the recipient to ensure that it is virus free and no responsibility is accepted by JPMorgan Chase & Co., its subsidiaries and affiliates, as applicable, for any loss or damage arising in any way from its use. If you received this transmission in error, please immediately contact the sender and destroy the material in its entirety, whether in electronic or hard copy format. This message is subject to electronic monitoring: https://www.jpmorgan.com/disclosures/email

MSCI: Certain information herein ("Information") is reproduced by permission of MSCI Inc., its affiliates and information providers ("MSCI") ©2026. No reproduction or dissemination of the Information is permitted without an appropriate license. MSCI MAKES NO EXPRESS OR IMPLIED WARRANTIES (INCLUDING MERCHANTABILITY OR FITNESS) AS TO THE INFORMATION AND DISCLAIMS ALL LIABILITY TO THE EXTENT PERMITTED BY LAW. No Information constitutes investment advice, except for any applicable Information from MSCI ESG Research. Subject also to msci.com/disclaimer

Sustainalytics: Certain information, data, analyses and opinions contained herein are reproduced by permission of Sustainalytics and: (1) includes the proprietary information of Sustainalytics; (2) may not be copied or redistributed except as specifically authorized; (3) do not constitute investment advice nor an endorsement of any product or project; (4) are provided solely for informational purposes; and (5) are not warranted to be complete, accurate or timely. Sustainalytics is not responsible for any trading decisions, damages or other losses related to it or its use. The use of the data is subject to conditions available at https://www.sustainalytics.com/legal-disclaimers. ©2026 Sustainalytics. All Rights Reserved.

"Other Disclosures" last revised April 04, 2026.