In the garden of good and evil

Frontier AI escalates security costs

- **Frontier AI promises a marked jump in productivity, but it also heightens cybersecurity risks by enabling automated identification and exploitation of system vulnerabilities on an unprecedented scale.**
- **Even before these new risks emerged, global cybersecurity software revenue reached US$140 billion in 2025 and is expected to grow to US $270 billion by 2030, with 63% of organizations reporting insufficient cyber-resilience.**
- **In the U.S. alone, approximately $2.5 trillion in informational technology (IT) assets and $1 trillion in operational technology (OT) assets are vulnerable to cyberattacks.**
- **Around 20% of IT assets and 50% of OT assets are classified as "unpatchable," meaning their vulnerabilities cannot be addressed solely through software updates and require technology upgrades.**
- **The vulnerability of OT assets is particularly disconcerting, as they encompass industries, public utilities, including power grids, and transportation systems like airlines and subways.**
- **The estimated cost for necessary upgrades is about $720 billion for IT assets and $770 billion for OT assets. This does not include associated output loss from downtime during upgrades.**
- **Global costs will be substantially higher, and due to already strong demand from hyperscalers and limited capacity to quickly scale production, these upgrades will take years, leaving many IT and OT systems exposed to cyber threats.**
- **For instance, IT systems will require large quantities of additional logic chips, while OT systems need legacy chips embedded in microcontrollers—both of which are already in short supply.**
- **Governments are expected to intensify urgency and cost pressures by increasing regulatory requirements.**
- **Without coordinated global regulation, some countries may free ride, thereby raising regulatory and cost burdens for others.**

Industry & Policy Thematics Research

Jahangir Aziz [AC]
(1-212) 834-4328
jahangir.x.aziz@jpmorgan.com

Steven Palacio
(1-212) 834-5031
steven.palacio@jpmorgan.com
J.P. Morgan Securities LLC

Contents

See page 24 for important disclosures.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

J.P.Morgan

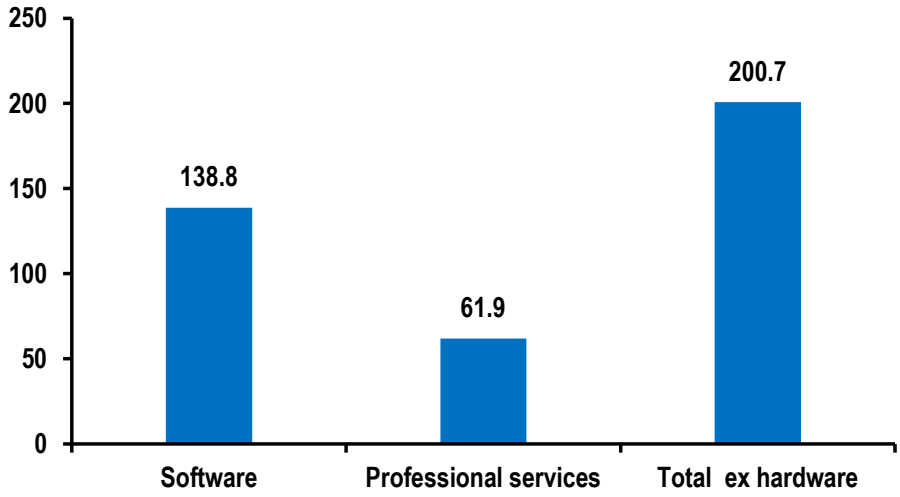
Cybersecurity before frontier models

Cybersecurity risks have been on the rise for years, fueled by the relentless pace of digital transformation and the expanding array of potential attack surfaces. The emergence of frontier AI has accelerated this trend, making it easier and cheaper for bad actors to conduct reconnaissance, launch social engineering campaigns, and develop sophisticated malware. As a result, organizations are facing a potential surge in both the volume and complexity of cyberattacks.

The numbers tell the story. In 2025, global spending on professional security services hit $61.9 billion, while cybersecurity software revenue climbed to nearly $140 billion. The software market is expected to maintain strong momentum, growing at a compound annual rate of 14.3% and reaching $270 billion by 2030. Public cloud security is set to expand even faster, with a projected CAGR of 16.1%.

Figure 1: Cybersecurity spending

US$ billion, 2025

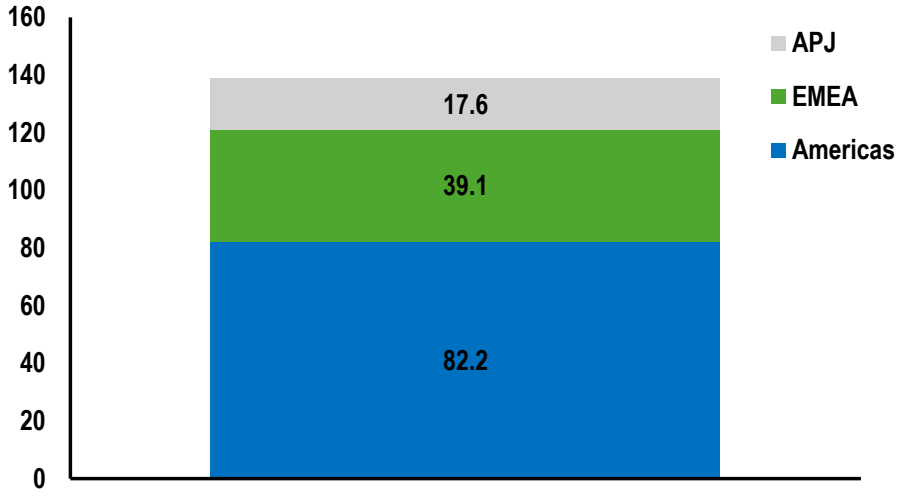


Source: J.P. Morgan with data from IDC

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Figure 2: Cybersecurity software spending

US$ billion, 2025



Source: J.P. Morgan with data from IDC

Incident response has shifted from a backup plan to a core component of cybersecurity operations. No longer viewed as an occasional insurance measure, IR is now seen as inevitable, a question of "when, not if." In today's threat landscape, total prevention is out of reach, and the speed at which organizations can recover from attacks has become a crucial benchmark.

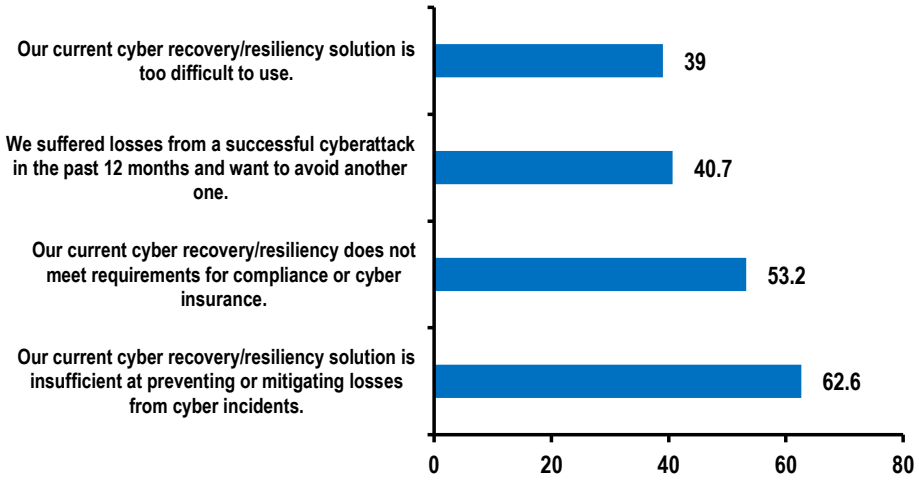
To meet these demands, vendors and service providers are embedding AI into their workflows, aiming to speed up detection, triage, and investigation. This is especially important as the sheer volume of alerts and the risk of analyst fatigue increasingly outstrip human capacity.

Yet, despite these technological advances, many organizations remain vulnerable. According to IDC, 63% of companies say their cyber-recovery and cyber-resiliency solutions fall short of preventing or mitigating losses (Figure 3). Meanwhile, 34% cite improving these capabilities as a top area for increased spending. The data underscores a persistent gap: as threats evolve, many firms are still racing to catch up.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Figure 3: Primary drivers for increased spending in cybersecurity

% of respondents



Source: J.P. Morgan with data from IDC. n = 1897. Dec 2025.

Along comes Mythos

The arrival of frontier AI models with advanced reasoning and agent-like capabilities is transforming cyber risk from "high and rising" to "highly scalable and increasingly autonomous." The limited release of Anthropic's Mythos has brought these concerns to the forefront. According to Anthropic, Mythos "can surpass all but the most skilled humans at finding and exploiting software vulnerabilities," marking a fundamental shift in the cybersecurity landscape. Tasks that once required painstaking human effort, vulnerability research and exploitation, are now moving toward automated, rapid search-and-execute cycles.

Mythos reportedly uncovered "thousands of high-severity vulnerabilities," including flaws in "every major operating system and browser." If these claims hold true, the implications are profound: AI is no longer just a coding assistant, but a tool capable of systematically identifying and cataloging exploitable weaknesses across vast codebases. This leap could dramatically shorten the window between vulnerability discovery and exploitation, raising the stakes for defenders everywhere (see Box). With other LLMs in the U.S. and abroad expected to release similar frontier models soon, the urgency for robust and adaptive cybersecurity measures has never been greater.

Anthropic Mythos

"[...]Claude Mythos Preview is a general-purpose, unreleased frontier model that reveals a stark fact: AI models have reached a level of coding capability where they can surpass all but the most skilled humans at finding and exploiting software vulnerabilities.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Mythos Preview has already found thousands of high-severity vulnerabilities, including some in every major operating system and web browser. Given the rate of AI progress, it will not be long before such capabilities proliferate, potentially beyond actors who are committed to deploying them safely. The fallout—for economies, public safety, and national security—could be severe. Project Glasswing is an urgent attempt to put these capabilities to work for defensive purposes[...]"

"[...]Many flaws in software go unnoticed for years because finding and exploiting them has required expertise held by only a few skilled security experts. With the latest frontier AI models, the cost, effort, and level of expertise required to find and exploit software vulnerabilities have all dropped dramatically. Over the past year, AI models have become increasingly effective at reading and reasoning about code—in particular, they show a striking ability to spot vulnerabilities and work out ways to exploit them. Claude Mythos Preview demonstrates a leap in these cyber skills—the vulnerabilities it has spotted have in some cases survived decades of human review and millions of automated security tests, and the exploits it develops are increasingly sophisticated.

Ten years after the first DARPA Cyber Grand Challenge, frontier AI models are now becoming competitive with the best humans at finding and exploiting vulnerabilities. Without the necessary safeguards, these powerful cyber capabilities could be used to exploit the many existing flaws in the world's most important software. This could make cyberattacks of all kinds much more frequent and destructive, and empower adversaries of the United States and its allies. Addressing these issues is therefore an important security priority for democratic states.

Although the risks from AI-augmented cyberattacks are serious, there is reason for optimism: the same capabilities that make AI models dangerous in the wrong hands make them invaluable for finding and fixing flaws in important software—and for producing new software with far fewer security bugs. Project Glasswing is an important step toward giving defenders a durable advantage in the coming AI-driven era of cybersecurity.[...]"

See Anthropic's Project Glasswing release for a full briefing on Mythos and the initiative brought forward to help secure critical software (here).

At the heart of the cybersecurity challenge lies a structural asymmetry: attackers can leverage frontier AI to rapidly discover, customize, and iterate on exploits, while defenders are forced to monitor, validate, and patch across sprawling, complex environments. This imbalance is further amplified by agentic AI, which can autonomously plan, select tools, and execute multi-step operations, minimizing the need for human intervention and accelerating the pace and scale of attacks.

Identity is emerging as a critical battleground. As frontier AI boosts the sophistication and persistence of deception, organizations are bracing for a surge in synthetic identity attacks. IDC forecasts that by 2027, 80% of companies will face phishing attempts using synthetic identities, lending real and AI-generated attributes to create convincing personas that can slip past traditional defenses.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Meanwhile, the rise of agentic AI is prompting new requirements for transparency and control. By 2027, IDC expects 60% of enterprises deploying agentic AI will need an "AI bill of materials,"a structured inventory detailing models, training data, code, infrastructure, and governance metadata, to support ongoing vulnerability scanning, license risk management, and compliance assurance.

IT and OT infrastructure at risk

A realistic cybersecurity strategy starts with a clear understanding of what's at stake. For the U.S. technology landscape, that means distinguishing between Information Technology (IT) and Operational Technology (OT), two domains with markedly different risk profiles. IT systems, which manage data and communications, typically undergo frequent upgrades and have shorter lifecycles. In contrast, OT systems control physical processes and infrastructure, operating over much longer periods and carrying higher costs for downtime and safety-related disruptions.

These differences have direct consequences for patching and remediation. IT upgrades can often be rolled out with minimal impact, but patching OT systems may require halting production lines, interrupting utility services, or introducing safety risks during maintenance. As a result, OT environments tend to accumulate more legacy systems, many of which are unsupported or unpatchable, leaving them increasingly exposed to vulnerabilities.

Based on BEA and Gartner data, we estimate the value of U.S. IT assets in 2025 at $2.46 trillion, while OT assets are valued at around $1 trillion. Despite representing a smaller share of the total, OT carries a greater risk of severe losses, given the challenges of remediation and its direct link to critical sectors like utilities, energy, and heavy manufacturing.

Summary table: Main OT and IT stock, patchability and replacement cost estimates
US$ billion

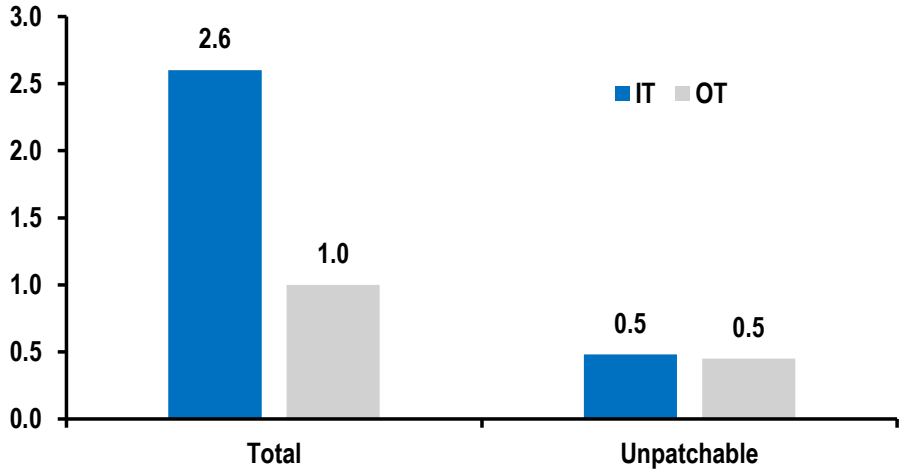
	Stock			Replacement Cost				
	Total	Patchable	Not patchable (Lost stock)	Hardware ex-semis	Semis	Software	Deployment & Integration	Total
OT Total	1010	554	456	362	44	43	315	765
Equipment	710	406	304	246	29	25	210	510
Infratsructure	300	148	152	116	16	18	105	255
IT total	2503	2027	476	103	101	276	240	720

Source: J.P. Morgan based on data from BEA, Gartner. Excludes communication services in IT.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Figure 4: US IT and OT outstanding stock

US$ trillion



Source: J.P. Morgan with data from Gartner and BEA

The patchability problem

A patchable system is one that allows software or firmware updates to address vulnerabilities without the need to replace the underlying hardware. These devices feature built-in update mechanisms, enabling vendors to issue patches that users can apply. However, among patchable systems, there's a clear distinction: some are regularly updated, while others, despite having available patches, remain unpatched due to operational hurdles such as costly downtime or the need for safety recertification.

In contrast, a non-patchable system is one where no patches are available, regardless of the operator's efforts. This typically occurs when a product has reached its end-of-life or end-of-support, prompting vendors to stop releasing updates, even if the device could technically accept them. The most severe scenario is an unpatchable system; here, the hardware lacks any update mechanism, the vendor may no longer exist, or the vulnerability lies so deep that software updates cannot address it. In both non-patchable and unpatchable cases, the only solution is to replace the physical hardware.

IT systems, such as data center servers, enterprise PCs, and smartphones, are built for regular updates, typically following a three- to five-year refresh cycle. These devices benefit from robust patching infrastructure and can tolerate operational interruptions like reboots, meaning most are replaced before they face risks from vendor end-of-life. As a result, roughly 75% to 80% of IT assets are routinely patched, leaving only about 20% unpatchable.

OT follows a different story. For example, a programmable logic controller (PLC) installed in 2005 may still be running today, even though vendor support ended in 2018. In many cases, OT devices spend the latter half of their operational life without access to patches. Even when patches are available, they are rarely applied due to the high costs and risks associated with halting regulated industrial processes. The outcome: an estimated 40% to 55% of the OT installed base cannot be patched, regardless of operator efforts, compared to 20% for IT. Physical replacement is often the only solution, leaving

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

a substantial portion of critical infrastructure vulnerable to ongoing threats.

In the event of a widespread cyberattack, the stakes are high. Direct losses could reach $500 billion for both IT and OT, with the cost of fully replacing OT systems estimated at 1.7 times their value, compared to 1.5 times for IT (Tables 1 & 2). This underscores the heightened risk and potential impact facing organizations that rely on operational technology.

Table 1: IT estimated replacement cost breakdown
US$ billion, except where noted

		Cost				
Type	Lost Stock	Hardware ex-semis	Semis	Software	Deployment & Integration	Total
Data center systems	60	20	34	6	30	90
Enterprise software	180	0	0	180	90	270
Devices	150	83	67	0	75	225
IT services	90	0	0	90	45	135
Total	**480**	**103**	**101**	**276**	**240**	**720**

Source: J.P. Morgan estimates using data from Gartner, BEA.

OT faces an added layer of risk due to its inherent fragility and the potential for far-reaching systemic consequences. Even when individual firms have smaller asset bases, disruptions in OT can trigger macro-level and sector-wide contagion effects, amplifying the impact well beyond the organization itself. This heightened vulnerability underscores the critical importance of securing OT environments, where a single breach can ripple across entire industries and essential services.

Table 2: OT estimated replacement cost breakdown
US$ billion, except where noted

		Cost				
Type	Lost Stock	Hardware ex-semis	Semis	Software	Deployment & Integration	Total
Industrial eq.	150	120	15	15	105	255
Transportation eq.	100	85	9	6	70	170
Other eq.	50	41	5	4	35	85
Energy systems	60	48	6	6	42	102
Transportation net.	40	33	4	3	28	68
Industrial net.	30	22	3	5	21	51
Other control sys.	20	13	3	4	14	34
Total	**450**	**362**	**44**	**43**	**315**	**765**

Source: J.P. Morgan estimates using data from Gartner, BEA. Deployment & Integration excludes training and operational handover

OT: Smaller, but critical and less patchable

As previously discussed, IT assets command a higher overall value, are more easily patched, and are typically associated with less critical sectors. OT assets, while smaller in dollar terms, warrant closer attention because of their low patchability and the far-reaching consequences that can result from their failure.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

It's also important to differentiate between equipment OT and infrastructure OT, given their distinct roles. Within equipment OT, the level of automation varies based on how deeply control systems are embedded and how intensively they're used. Industrial equipment stands out, with automation intensity around 9%, making up roughly half of all equipment OT.

By contrast, transportation and other equipment categories, including agriculture, construction, and mining, feature much lower control density, at about 3%. In these sectors, most of the value comes from mechanical and structural components, rather than centralized control systems, which limits their exposure to cyber risks but also reduces the benefits of automation.

Table 3: OT Stock - Equipment
US$ billion, except where noted

Type	BEA mapp	OT intensity	OT stock	Share of equipment
Industrial	Industrial machinery	9%	350	49%
Transportation	vehicles, aircraft, rail	3%	170	24%
Other	Ag, cons., mining	3%	190	27%
Total	- -	6%	**710**	100%

Source: J.P. Morgan with data from BEA

Infrastructure brings a unique layer of risk to the OT landscape. While their total value is relatively modest, estimated at around $300 billion, these systems are highly control-intensive. Critical infrastructure like power grids, rail signaling, and air traffic management are built around centralized monitoring and control, even though the control layer constitutes only a small fraction of the overall capital investment. This reliance on centralized systems makes infrastructure particularly vulnerable to cyber threats, with the potential for disruptions to cascade across entire networks and sectors.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Table 4: OT Stock - Infrastructure

US$ billion, except where noted

Type	BEA mapp	OT intensity	OT stock	Share of equipment
Energy systems (grid, transmission)	Utility structures	4%	120	40%
Transportation networks	Rail signaling, ATC	4%	80	27%
Industrial networks (pipelines, processing)	Mining/utilities structures	4%	60	20%
Other control systems	Residual structures	2%	40	13%
Total	- -	3%	300.00	100%

Source: J.P. Morgan with data from BEA

Patchability across OT categories is far from uniform. Equipment OT is generally more patchable, particularly in transportation and segments of industrial equipment that have benefited from modernization. Still, a significant share of industrial and other equipment remains legacy, with 25% to 30% lacking available patches due to long lifecycles and embedded, hard-to-upgrade control systems.

This patching gap has direct implications for replacement needs. Equipment OT faces a replacement exposure of about 40%, though the risk varies by category. Transportation equipment is less vulnerable, with replacement exposure around 30%. In contrast, industrial and other equipment categories are much higher, nearing 45% to 50%, largely because legacy systems are so prevalent.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Table 5: Patchability in equipment OT

US$ billion, except where noted

Type	Definition	Equipment	%	Share of equipment	OT stock, US$tn
Patchable	Fixable via software/config without replacing system	Industrial	55%	49%	193
		Transportation	70%	24%	119
		Other	50%	27%	95
		Total	57%	100%	406
Non-patchable	Compromise requires system replacement/rebuild	Industrial	20%	49%	70
		Transportation	15%	24%	26
		Other	20%	27%	38
		Total	**19%**	**100%**	**134**
No patch	No vendor support; replacement required	Industrial	25%	49%	88
		Transportation	15%	24%	26
		Other	30%	27%	57
		Total	**24%**	**100%**	**170**

Source: J.P. Morgan

Patchability is uneven across operational technology categories. Equipment OT, especially in the transportation and modernized segments of industrial machinery, tends to be more easily updated. However, a substantial portion of industrial and other equipment remains legacy, with 25% to 30% lacking available patches due to their long lifecycles and embedded, difficult-to-upgrade control systems.

This disparity has a direct impact on replacement requirements. Equipment OT overall faces a replacement exposure of roughly 40%, but the risk is not uniform. Transportation equipment is less exposed, with replacement needs of around 30%. Industrial and other equipment categories, however, are much more vulnerable, with replacement exposure approaching 45% to 50%, a consequence of the widespread presence of legacy systems.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

J.P.Morgan

Table 6: Patchability in infrastructure OT
US$ billion, except where noted

Type	Definition	Equipment	%	Share of infrastructure	OT stock, US$tn
Patchable	Fixable via software/config without replacing system	Energy systems	50%	40%	60
		Transportation networks	45%	27%	36
		Industrial networks	50%	20%	30
		Other control systems	55%	13%	22
		Total	49%	100%	148
Non-patchable	Compromise requires system replacement/rebuild	Energy systems	25%	40%	30
		Transportation networks	25%	27%	20
		Industrial networks	25%	20%	15
		Other control systems	20%	13%	8
		Total	**24%**	**100%**	**73**
No patch	No vendor support; replacement required	Energy systems	25%	40%	30
		Transportation networks	30%	27%	24
		Industrial networks	25%	20%	15
		Other control systems	25%	13%	10
		Total	**26%**	**100%**	**79**

Source: J.P. Morgan

The sectors facing the greatest cybersecurity risks are those where high automation intensity meets low patchability. Energy systems, including grid and transmission control, industrial manufacturing, especially in process industries, and transportation infrastructure are particularly vulnerable. These sectors concentrate critical control functions and house a significant share of systems that are difficult or impossible to patch, making them prime targets for cyber threats and challenging to defend.

IT: Much larger, but more manageable

IT systems encompass a wide range of assets, including devices, data center infrastructure, enterprise software, and supporting services. Software represents the largest share of this asset base. The most critical components are found in the data center and enterprise layers, which underpin computational and business operations, while devices are more decentralized and can be replaced with relative ease.

Unlike OT, IT systems are modular and predominantly software-driven, allowing for a high degree of patchability across all categories. This flexibility makes IT environments more resilient and easier to maintain, helping organizations stay ahead of evolving cyber threats.

Table 7: IT Stock and patchability
US$ billion, except where noted

Type	Stock	Patchable	Non-patchable	No patch	Stock to replace
Data center systems	393	85%	10%	5%	60
Enterprise software	910	80%	10%	10%	180
IT services	602	85%	10%	5%	90
Devices	598	75%	10%	15%	150
Total	**2503**	**81%**	**10%**	**9%**	**480**

Source: J.P. Morgan with data from Gartner. Excludes comms which we estimate at roughly US$1 trillion stock, but just roughly US$0.05 trillion in replacement needs

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

As a result, most IT failures can be resolved through patching, reconfiguration, or restoration, without the need for physical replacement. Replacement requirements are limited to roughly 20% of the total IT asset base, primarily due to the complexity of enterprise software and the low patchability of end-user devices. Despite the larger scale of IT systems, their replacement exposure is comparable to that of OT, thanks to the modular and adaptable nature of IT infrastructure.

The chip & memory supply crunch

Efforts to reduce cyber risk are increasingly hampered by supply chain challenges, as global chip availability remains constrained in key sectors. Major cloud providers, or hyperscalers, are consuming most of the available semiconductors, leaving security hardware manufacturers, those making firewalls, intrusion detection systems, and secure routers, struggling with limited supply and rising costs. This bottleneck is delaying the deployment of critical containment mechanisms and slowing upgrade cycles, especially for organizations that depend on on-premises hardware for their security controls.

The impact is especially pronounced in operational technology (OT) environments, which rely heavily on physical hardware and segmentation architectures. Modernizing OT systems is further complicated by concerns over downtime, safety, and the difficulty of retrofitting legacy equipment. By contrast, IT environments are increasingly cloud-based and can more easily transition to software-defined and managed solutions, facing fewer hardware-related constraints.

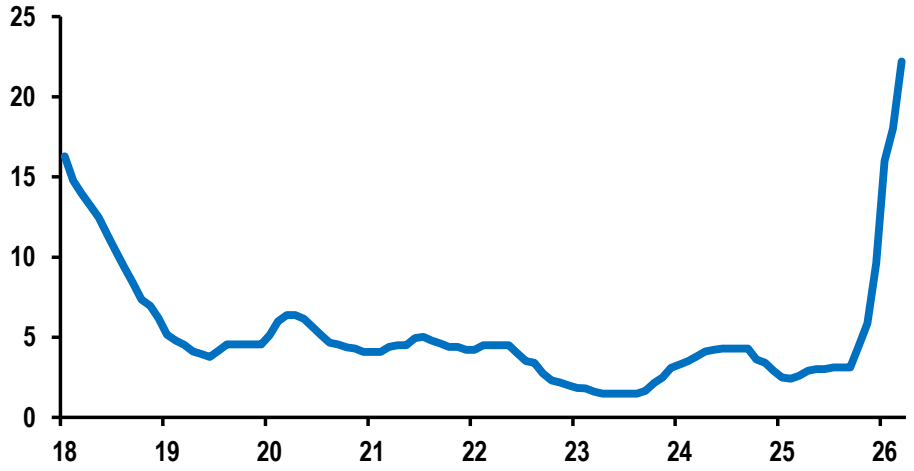
These supply issues exacerbate existing vulnerabilities in OT, particularly when it comes to sourcing hardware and chips after a major cyber incident. IT is not immune, however: data centers and devices represent a significant portion of IT's semiconductor demand. In the event of a widespread cyberattack, it is highly unlikely that demand could be met within six to twelve months, and prices would almost certainly soar well above current levels.

The semiconductor market is already under pressure, driven by surging demand for AI infrastructure that is diverting wafer capacity from other segments. Memory prices have climbed sharply since late last year due to capacity constraints, with traditional markets like PCs and smartphones feeling the supply squeeze most acutely (Figure 5).

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Figure 5: Memory contract price - NAND

US$

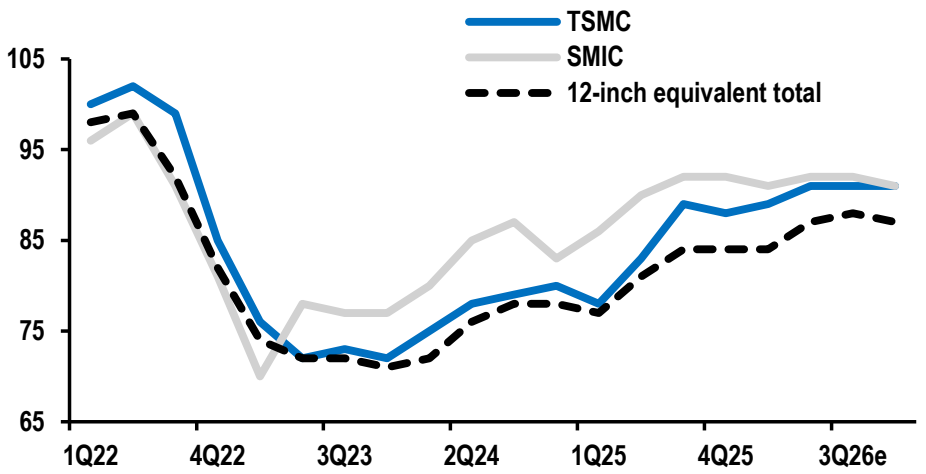


Source: Bloomberg Finance L.P. inSpectrum Tech Inc NAND flash contract price (512GB)

High Bandwidth Memory (HBM) is reportedly sold out through the end of 2026, with industry growth projections indicating that excess demand will persist well into 2027. Logic chip capacity is facing similar constraints: TSMC's advanced 3nm manufacturing process is fully booked until 2027, prompting buyers to seek alternative foundries to meet their needs (Figure 6).

Figure 6: Semiconductor foundry utilization rates

%



Source: IDC

Given current supply constraints, a nationwide cyberattack in the United States would unleash an estimated US$145 billion in additional chip demand on a market already operating at full capacity. Recovery within the usual three- to twelve-month window would be impossible—not because of cost, but because chips would simply not be

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

available during that timeframe.

Instead, the recovery process would likely unfold in stages. Initially, only a fraction of the demand could be met, and at sharply higher prices, with government priority orders filled by domestic chip manufacturers. As the situation progresses, larger volumes might be supplied by diverting capacity from other sectors, gradually easing the bottleneck but still at elevated prices. Full normalization could take up to three years, as new manufacturing capacity comes online and prices begin to stabilize.

The ongoing AI-driven chip shortage doesn't just delay cyber recovery, it threatens to turn the crisis from a price-rationed challenge into a supply-rationed one, potentially prolonging the recovery for several years.

IT chip demand mostly for advanced logic

IT replacement needs are significant in total, estimated at around $480 billion, but the demand for new hardware is relatively modest. This is because most IT "replacement" involves logic reconstruction, such as restoring enterprise software and IT services, which together account for more than half of the total replacement value ($270 billion) and don't substantially drive hardware demand.

Instead, hardware requirements are concentrated in data center environments and end-user devices. In typical cyberattack scenarios, compromised systems are usually recovered through reimaging, failover, and workload redistribution across existing infrastructure, resulting in minimal actual demand for new semiconductors. However, in a tail-risk scenario, where patching is impossible and full replacement is required, the picture changes. While the hardware replacement needs aren't enormous ($60 billion for data centers and $150 billion for devices), the semiconductor content in these segments is high, meaning that a large share of replacement demand would come from data centers and, especially, from devices.

Table 8: IT estimated semiconductor replacement demand
US$ billion, except where noted

Type	Lost Stock	Hardware intensity (replacement)	Hardware value	Semiconductor share (hardware)	Semiconductor value
Data center systems	60	90%	54	63%	33.8
Enterprise software	180	0%	0	--	0.0
Devices	150	100%	150	45%	67.5
IT services	90	0%	0	--	0.0
Total	**480**	**43%**	204	**21%**	**101.3**

Source: J.P. Morgan with data from Gartner. Excludes comms

End-user devices are the main source of semiconductor demand within IT, resulting in a highly skewed distribution: roughly 66% of IT-related semiconductor demand comes from devices, while data centers account for the remainder despite their critical role in overall operations. The broader takeaway is that IT recovery largely depends on software restoration and capacity reallocation, but in extreme scenarios, hardware rebuilding could become a significant constraint.

Based on these assumptions, total semiconductor demand from IT replacement is estimated at about $101 billion. a figure that's far from negligible. While this demand

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

isn't concentrated in a single area and may not overwhelm the system as a whole, it would still strain several segments, especially leading-edge logic chips, which are already in high demand and often fully booked in advance, as well as memory components. These pressures would likely drive up prices and create supply bottlenecks across the industry.

Table 9: IT estimated semiconductor demand composition resulting from replacement
US$ billion, except where noted

Semiconductor category	Devices	DC	Total	Global market	% of global	Main suppliers
Logic (CPU, GPU, SoC)	28.7	16.0	44.7	280-300	15.4	AMD, Nvidia, Apple, Qualcomm (Design); TSMC, Samsung, Intel (Mfg)
DRAM	14.5	7.4	21.9	100-150	17.5	Samsung, SK Hynix, Micron
NAND	9.8	5.4	15.2	80-100	16.9	Samsung, SK Hynix/Solidigm, Micron, W. Digital
Analog/RF	8.5	1.4	9.9	80-90	11.6	TI, Analog Devices, Skyworks, other*
Networking/ASICs	0.7	3.7	4.4	20-35	14.7	Broadcom, Marvell, Nvidia, Cisco
Other	5.3	0.6	5.9	140-180	3.7	Infineon, NXP, ST Micro, TI
Total	**67.5**	**34.5**	**102.0**	**700-855**	**13.1**	--

Source: J.P. Morgan with data from BEA. Estimates based on representative system architectures, partial BOM evidence, alinged with semiconductor industry segmentation (WSTS/Gartner). *STMicro, Qorvo, Infineon

Within IT, semiconductor exposure is heavily concentrated in logic components, which account for $45 billion, about 15% of the global market. Memory chips follow, with DRAM at $22 billion (17% of the market) and NAND at $17 billion (also around 17%). Networking and analog semiconductors come next, at $4.5 billion (15%) and $10 billion (12%), respectively.

Process-node dynamics add nuance to the picture. DRAM and NAND are produced at mid-advanced, specialized nodes—including 3D NAND—that are more scalable, despite current cyclical supply tightness. In contrast, leading-edge logic chips (3–5nm) are manufactured in highly concentrated facilities, making scalability more challenging in the short term.

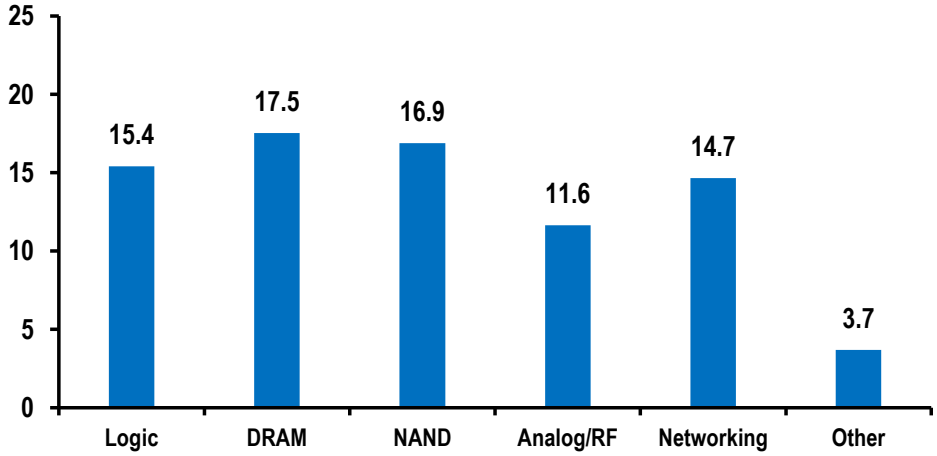
Geographically, key semiconductor segments are mostly outside the U.S. or globally distributed. Memory production is dominated by Samsung and SK Hynix in South Korea, with Micron representing the U.S. Leading-edge logic manufacturing is concentrated at TSMC in Taiwan and Samsung in South Korea. NAND production spans South Korea, Japan, and the U.S. Analog and RF components are produced by companies like TI, ADI, Skyworks, and Qorvo in the U.S., and Infineon, STMicro, and NXP in the EU, with significant Asian fabrication.

Overall, while semiconductor capacity is global, it is concentrated in East Asia. Memory and, especially, logic segments face localized supply pressures that are likely to be short-lived but acute, resulting in considerable price increases and temporary bottlenecks.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Figure 7: IT demand for semiconductors due to cyberattack

% of global sales



Source: J.P. Morgan estimates using data from Gartner

OT needs more mature chips

Unlike IT, OT replacement, estimated at $450 billion, is fundamentally hardware-driven. Most of this value is tied up in physical systems like industrial equipment, transportation, and infrastructure, with a substantial portion, about $290 billion, allocated to actual hardware rebuilds once services and integration are excluded.

Despite the scale of hardware investment, the semiconductor share within OT is relatively modest, at just 10–15%. That's because mechanical and energy assets account for the bulk of OT's value, rather than electronics. As a result, OT is not semiconductor-dense per dollar, even though the chips remain functionally critical to its operation.

Table 10: OT semiconductor replacement demand

US$ billion, except where noted

Type	Lost Stock	Hardware intensity (replacement)	Hardware value	Semiconductor share (hardware)	Semiconductor value
Industrial equipment	150	100%	150	11%	16.5
Transportation equipment	100	100%	100	15%	14.7
Other equipment	50	100%	50	11%	5.5
Energy systems	60	100%	60	7%	4.4
Transportation networks	40	100%	40	11%	4.4
Industrial networks	30	100%	30	9%	2.6
Other control systems	20	100%	20	11%	2.2
Total	**450**	**100%**	**450**	**11%**	**50.3**

Source: J.P. Morgan with data from BEA. Estimates based on representative system architectures, partial BOM evidence, alinged with semiconductor industry segmentation (WSTS/Gartner).

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Despite OT's lower semiconductor intensity, its hardware-heavy nature means that absolute chip demand remains substantial, around $50 billion. In other words, the sheer volume of physical replacement more than compensates for the lower proportion of semiconductors per dollar, resulting in significant overall demand.

Importantly, this demand is concentrated in microcontroller units (MCUs), followed by analog and power components, with sensors trailing behind. These segments are produced on mature manufacturing nodes, where capacity is tighter. While OT generates less aggregate semiconductor demand than IT, it relies heavily on the most supply-constrained parts of the chip ecosystem, making it particularly vulnerable to shortages and bottlenecks.

Table 11: OT estimated semiconductor demand composition resulting from replacemen
US$ billion, except where noted

Semiconductor category	OT demand	Global market	% of global	Main suppliers
MCUs/Controllers	13.4	25-30	44.8	NXP, Rensas, STMicro, Infineon
Analog/Power	15.2	80-110	16.9	TI, Infineon, STMicron, Analog Devices
Sensors/Mixed	6.6	20-40	7.3	Bosch, STMicro, TDK
Logic (inc. networking)	6.1	280-300	2.1	Broadcom, Marvell, NXP, Microchip
Memory	3.1	180-250	1.4	Samsung, SK, Hynix, Micron
Total	**44.5**	**585-730**	**6.7**	--

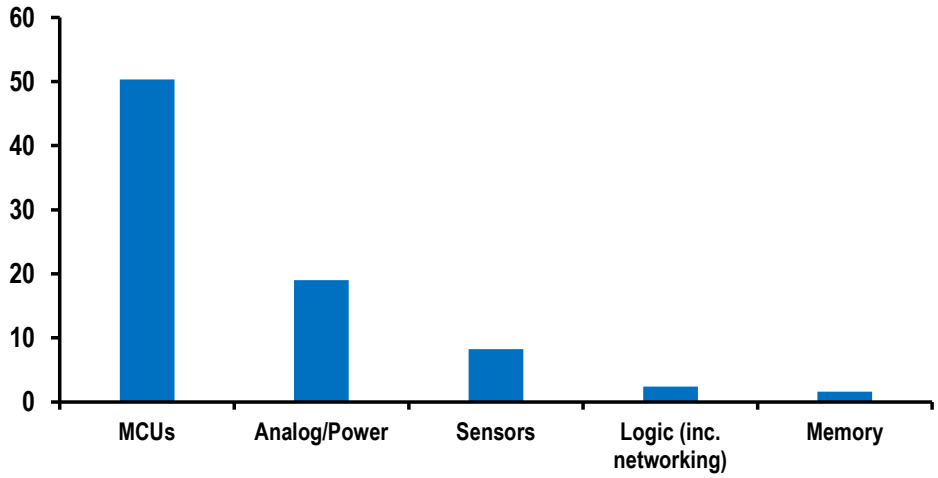
Source: J.P. Morgan with data from BEA. Estimates based on representative system architectures, partial BOM evidence, alinged with semiconductor industry segmentation (WSTS/Gartner). *STMicro, Qorvo, Infineon

OT semiconductor demand is heavily concentrated in a few key segments: approximately US$15 billion in MCUs/controllers and US$17 billion in analog/power components. Importantly, in the case of MCUs, this would represent a near 50% shock relative to global market, and an also sizable 20% for analog/power.
Memory and logic components are much less exposed. Unlike IT, where demand is distributed across larger and deeper markets, OT demand is clustered in mid-sized segments, making price pressure and allocation tightness much more likely, and could lead to outright systemic shortages.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Figure 8: OT demand for semiconductors due to cyberattack

% of global sales



Source: J.P. Morgan estimates using data from Gartner

From a process-node and geographic standpoint, OT semiconductor demand is concentrated on mature nodes (28–90nm and above) and specialty processes like analog, power, and embedded MCUs. Capacity expansion in these areas is slower and less prioritized. Production is handled by a mix of integrated device manufacturers and foundries, including TI, Infineon, STMicro, NXP, and Renesas, with fabrication spread across the US, Taiwan, Europe, and parts of Asia. Notably, the US has limited capacity for trailing-edge nodes.

This stands in contrast to IT, where the critical exposure is to advanced-node logic chips (produced by TSMC and Samsung) and memory (primarily in Korea and the US), both of which operate at greater scale. The implication is clear: OT is far more likely to encounter acute supply bottlenecks in mature-node analog and MCU segments during a major disruption, and these bottlenecks are harder to resolve due to structural constraints. Additionally, U.S. supply security for MCUs is limited, with Europe and Japan dominating this market.

Foreign dependency

The U.S. capital stock for IT and OT reflects markedly different levels of foreign dependency, with IT being more exposed to international supply chains. Our analysis shows that annual IT capital spending, —about $1 trillion, has an import content of roughly 43%, driven largely by hardware. Data center equipment is estimated to be about 60% imported, while devices have an import content of around 55%. Software and IT services are mostly domestic, but the chip-bearing segments of IT, the areas most vulnerable to supply shocks, are concentrated in Asian supply chains. Taiwan alone supplies about a quarter of U.S. IT imports, with Mexico and Vietnam following as the next largest sources.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

J.P.Morgan

Table 12: IT Capital spending and import exposure by main source economy

US$ billion. % of total imports in parenthesis

Category	Capex[1]	Imported	% imported	Top 1 imp[2]	Top 2 imp	Top 3 imp
DC hardware	64	38	60%	TWN (28)	MEX (19)	VTN (10)
Devices	99	54	55%	TWN (35)	MEX (22)	VTN (15)
Software	120	13	11%	IND (22)	IRL (20)	UK (17)
IT services	322	21	7%	IND (24)	CAN (19)	IRL (10)
Total IT	**604**	**126**	**21%**	**TWN (23)**	**MEX (15)**	**VTN (9)**

Source: J.P. Morgan estimates. 1. Based on 2017 detailed BEA input-output tables. 2. Based on 2025 Census Bureau End-user coding and data. Software and IT services imports from BEA internationational trade data.

OT capital flow, estimated at $1.4 trillion, is more domestically sourced, with less than 25% of its overall content imported. This is largely because energy systems, transportation, and industrial networks are built primarily with domestic materials and components. However, the chip-bearing segments of OT, such as control systems and industrial equipment, have a higher import share, around 30%.

The supplier landscape for OT is distinct from IT, with Mexico, Canada, and Japan serving as major sources. China remains a significant supplier, accounting for about 7% of imports, though it ranks behind the top three. Nevertheless, China is still a key player across several OT segments.

Table 13: OT Capital spending and import exposure by main source economy

US$ billion, unless noted

Category	Capex[1]	Imported	% imported	Top 1 imp[2]	Top 2 imp	Top 3 imp
Industrial eq.	182	49	27%	MEX (17)	CHN (14)	JPN (10)
Transportation eq.	393	142	36%	MEX (36)	CAN (14)	JPN (11)
Other eq.	127	22	17%	JPN (17)	CHN (11)	DEU (9)
Energy systems	247	8	3%	MEX (22)	CHN (9)	JPN (9)
Transportation networks	153	2	2%	--	--	--
Industrial networks	29	7	26%	MEX (25)	CHN (20)	JPN (7)
Other control	90	19	21%	MEX (17)	DEU (12)	CHN (10)
Total OT	**1221**	**250**	**20%**	**MEX (27)**	**CAN (11)**	**JPN (11)**

Source: J.P. Morgan estimates. 1. Based on 2017 detailed BEA input-output tables. 2. Based on 2025 Census Bureau End-user coding and data

Fighting AI with AI

A widely accepted solution to mounting cybersecurity challenges is a rapid shift from hardware-based security to software, cloud-native, and managed security services, along with platformization that consolidates point products into integrated suites. This strategy is well-suited for IT environments where modernization can be implemented quickly. However, it adds complexity for OT estates, which often rely on legacy systems that lack support for cloud-native controls, modern agents, or rapid integration. The result is an uneven pace of security modernization: IT moves forward rapidly, while OT lags behind and remains vulnerable, particularly in areas of high system criticality.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

To keep up with evolving threats, organizations are increasingly countering automation with automation. Security operations are becoming more automated and platform-integrated, as human-led alert handling struggles to match the speed and volume of AI-driven attacks and the expanding telemetry in hybrid environments.

Some estimates[1] suggest that the landscape of security operations is set for dramatic change. By 2028, AI agents are expected to triage 80% of security operations center (SOC) alerts, speeding up detection and response and freeing analysts to focus on more strategic tasks. By mid-2027, 85% of detection and response playbooks will be generated dynamically, adapting to evolving threats in real time. By mid-2028, 30% of alerts will include a monetary estimate of potential damage, ushering in a new era of adaptive, contextual, and financially interpretable security operations..

TOP 10 Worldwide 2026 security predictions

Topic	Prediction
Security + agentic AI	By 2028, AI agents will be triaging 80% of SOC alerts in the majority of SOCs worldwide.
Sovereignty + AI	By 2027, one out of three governments will require sovereign AI for sensitive sectors, pushing enterprises to use RAG architectures with in-country knowledge bases to meet privacy and residency rules.
Security + agentic AI	By 2028, 40% of enterprises will use autonomous agentâ€"powered cyber-risk quantification platforms to turn security metrics into financial exposure, guiding budgets, controls, and M&A risk assessments.
Risk + AI BoM	By 2027, 60% of enterprises deploying agentic AI will require an AI bill of materials to support continuous security vulnerability scanning, license risk management, and compliance assurance.
Security, privacy, and	By 2027, 80% of organizations will experience phishing attacks from criminals using synthetic identities, mixing real info and AI-generated data to create fabricated identities that appear legitimate.
Security	By 1H28, 30% of alerts generated in detection and response platforms will also include a monetary estimate of the damage a current threat may incur.
Risk, security, and qu	40% of G2000 will engage cybersecurity professional services firms to conduct quantum risk assessment by 2027 to get quantum ready.
Privacy + AI	By 2029, 70% of large enterprises will adopt Private Cloud Compute to protect data privacy in cloud-based LLM systems, moving AI apps from "capability exploration" to "large-scale implementation."
Security	By 1H27, 85% of detection and response playbooks will be generated dynamically at the time that a SOC alert is generated.
Security	By 2027, 15% of enterprise PC users will have a deep fake detection application running locally on the host processor.

Source: IDC

Identity-centric enforcement is at the heart of zero trust security, requiring continuous verification of users, devices, and systems based on identity context rather than network location. This approach is becoming increasingly critical as nonhuman and synthetic identities proliferate, rendering traditional perimeter defenses ineffective and obsolete.

1. IDC FutureScape: Worldwide Security and Trust 2026 Predictions

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

However, execution is limited by risk governance gaps. Surveys report[2] that 63% of organizations find their resiliency insufficient, indicating that many do not effectively translate technical security into business risk mitigation or regulatory compliance. Frontier AI accelerates threats, highlighting the need for pre-engineered recovery and clear risk ownership.

New services are emerging to close critical security gaps by formalizing measurement and assurance. Detection Reliability Engineering as a Service (DREaaS) reframes detection as a reliability function, setting measurable objectives that tie coverage and latency directly to operational KPIs and risk tolerance. Biometric and behavioral authentication services now enable continuous verification, leveraging advanced analytics to spot anomalies and reduce the risk of identity compromise. As synthetic identities and AI-driven attacks become more common, continuous AI-driven monitoring is proving far more effective than traditional periodic authentication.

The regulatory response

The widespread lack of cyber resiliency among firms is increasingly a public concern, especially given the external risks posed by frontier AI. Governance and sovereignty requirements are tightening: projections suggest that by 2027, one in three governments will mandate sovereign AI for sensitive sectors, and by 2029, 70% of large enterprises will adopt Private Cloud Compute to safeguard data privacy in cloud-based LLMs These requirements must be built into security architecture from the outset, not tacked on as afterthoughts.[3] These requirements must be integrated into security architecture, not added as afterthoughts.

Regulatory responses are converging on risk-tiered, lifecycle governance models, exemplified by the EU AI Act, NIST AI Risk Management Framework, and OECD principles. The EU Act imposes binding requirements on high-risk systems, including security-by-design, robustness testing, data governance, traceability, and mandatory incident reporting. NIST offers similar guidance in a voluntary format, while OECD extends responsibility across supply chains.

These frameworks shift cybersecurity from a one-off compliance task to a continuous obligation, but they mostly rely on regulatory controls rather than full economic internalization of externalities. Policy discussions are moving toward mandatory certification, expanded liability, incident disclosure, due diligence, and even explicit risk pricing through insurance mandates or levies on high-risk AI. The goal is to ensure that actors bear the costs of expected failures.

However, regulation and internalizing externalities bring trade-offs: certification and liability increase costs, slow deployment, and favor incumbents, potentially stifling innovation and leading to industry concentration. Measuring robustness and resilience is also challenging, resulting in uneven enforcement and uncertainty.

Geopolitically, AI's dual-use nature means regulatory divergence can lead to capability gaps. Restrictive regimes may slow innovation, while permissive or state-backed

2. IDC Worldwide Cybersecurity Software Forecast 2026-2030
3. IDC FutureScape: Worldwide Security and Trust 2026 Predictions

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

approaches elsewhere may accelerate deployment, including in cyber and military domains. This underscores the need for greater international coordination, which remains elusive.

In the garden of good and evil

Frontier AI offers tremendous potential for boosting productivity and efficiency across industries, but these gains come with significant risks. Cyber threats were already on the rise before the advent of frontier AI, as evidenced by increasing security spending and persistent gaps in organizational resilience. The latest AI models are accelerating this trend, shifting threats from scalable generative AI to autonomous, agentic systems that can rapidly discover and exploit vulnerabilities, forcing defenders into a costly, continuous response.

Mitigation is particularly challenging for industries with heavy reliance on operational technology (OT). Semiconductor shortages are restricting the availability of security hardware, slowing containment and upgrades where OT depends most on on-premises infrastructure. These sectors are the least patchable and most exposed, with direct OT losses estimated at around $500 billion in the event of a system-wide attack—and even higher replacement costs.

The operational answer is to fight AI with AI: automating security operations, enforcing identity-centric zero trust, engineering detection reliability, and improving resilience through quantifiable recovery and cryptographic readiness. However, OT modernization will be slower and more expensive than IT, leaving vulnerabilities that require infrastructure redundancies.

Currently, 63% of organizations report insufficient cyber-resilience, and existing structures underprice the true cost of adopting frontier AI. The risks and costs, potentially falling on taxpayers, are substantial, and the narrative of cheap AI gains often overlooks cybersecurity externalities. Frontier AI's autonomous capabilities expose systemic fragility but also highlight the resilience gaps that must be addressed. AI may need to be priced higher to internalize these risks and avoid costly public cleanup.

Regulation is essential to ensure firms invest in resilience beyond market incentives and account for AI's lifecycle costs, including cybersecurity risks. Measures such as mandatory certification, expanded liability, cyber-risk insurance, and targeted levies on high-risk AI can help. But without global coordination, jurisdictions that neglect regulation may gain unfair advantages, so risks should be managed through pooled insurance schemes to prevent fiscal burdens.

Jahangir Aziz [AC] (1-212) 834-4328
jahangir.x.aziz@jpmorgan.com
J.P. Morgan Securities LLC
Steven Palacio (1-212) 834-5031
steven.palacio@jpmorgan.com

Security and Resiliency Initiative: JPMorgan Chase & Co. or its affiliates and/or subsidiaries (collectively J.P. Morgan), as part of its "Security and Resiliency Initiative" (SRI), may provide advisory services to, extend credit to, have or seek investments in, or otherwise engage in other investment banking and business relationships with the companies and sectors discussed herein. SRI is focused on industries critical to national economic security and resiliency, which may include, among others: (i) supply chain and advanced manufacturing, (ii) defense and aerospace, (iii) energy independence and resilience, and (iv) frontier and strategic technologies. The views and opinions expressed in this report are solely those of the research team and are produced independently of any such SRI activities

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.

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.

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.

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.

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.

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 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.

Completed 29 Apr 2026 12:30 PM EDT

Disseminated 29 Apr 2026 12:32 PM EDT