BUSINESS INTELLIGENCE REPORT

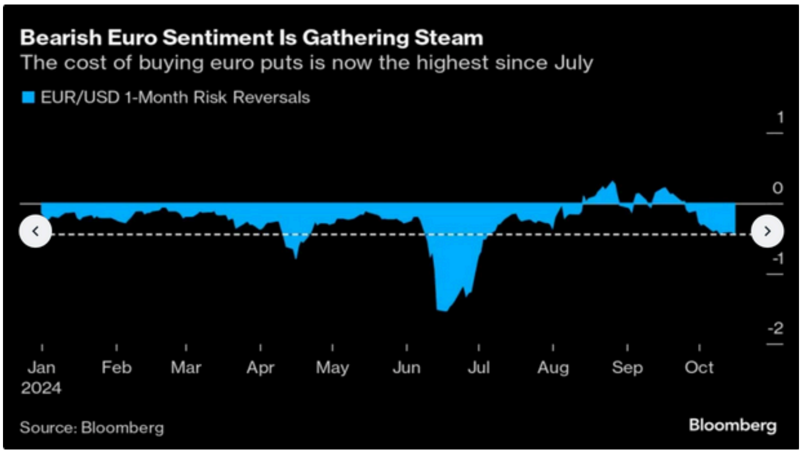
As we move toward the end of 2024, key financial sectors such as cybersecurity, private equity, venture capital, and family offices are experiencing dynamic shifts in response to the evolving global economy and technological innovation. This report dives into the most significant deals and trends from Q3 to the present, offering insights into the strategic decisions shaping these industries.

www.qwantiv.com

THE BUZZ

Euro Parity Threat Returns on Talk of Trump Tariffs and ECB Cuts

The risk of the euro sliding to parity with the dollar is mounting in financial markets after this week’s interest-rate cut and a stark reminder that a Donald Trump presidency could spark a global trade war. Read more **HERE**



The next big AI trade could be nuclear power: Morning Brief

Nuclear power is poised for a renaissance in the US, prompted by Big Tech’s seemingly insatiable need for electricity to power AI-generating data centres. Read more **HERE**

NHTSA probing Tesla's FSD software in 2.4 million vehicles over collisions

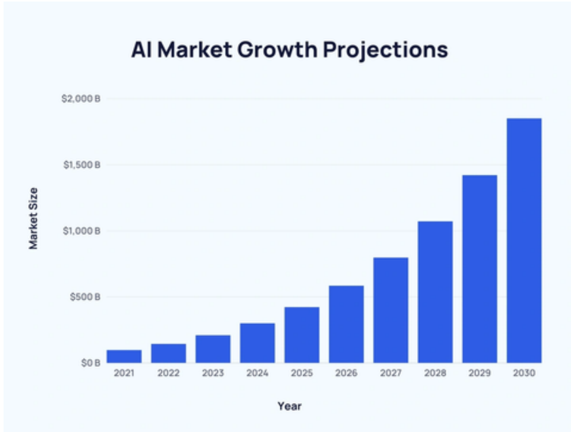
On Friday, the U.S. auto safety regulator said it opened an investigation into Tesla's Full Self-Driving software after reports of four collisions, including one fatal crash, involving its driver-assistance technology in low-visibility conditions.
Read more **HERE**

Saudi Tech Firm Ejada Taps Goldman for IPO at $1.5 Billion Value

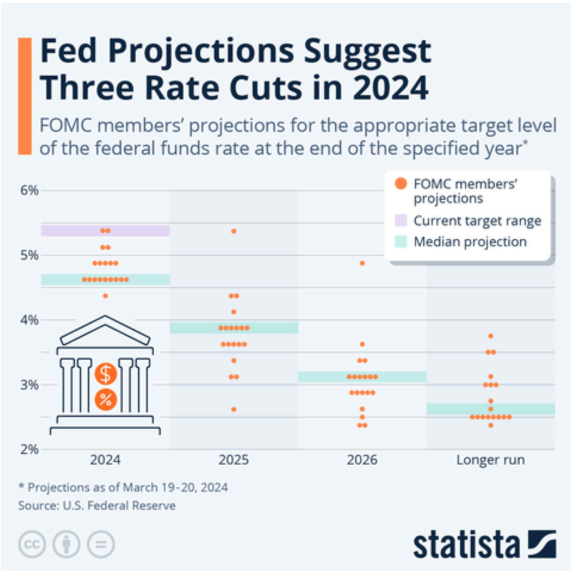
Ejada Systems Ltd. is considering an initial public offering in Riyadh at a valuation of as much as $1.5 billion, marking a rare listing by a technology services firm in Saudi Arabia.
Read more **HERE**

FINANCIAL TRENDS

AI and Stock Market Concentration:

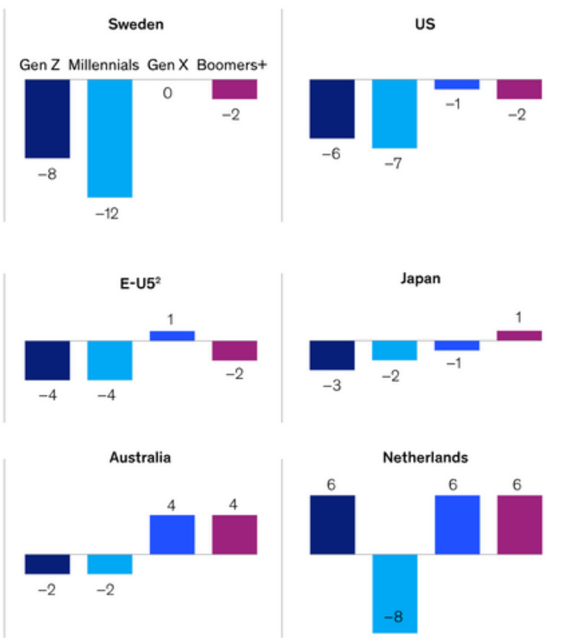


The market remains heavily influenced by the AI sector, especially companies like Nvidia and Microsoft, which have seen large growth. However, some experts now believe many AI stocks are overvalued, which may limit future returns for new investors. AI-driven investments are still a significant trend but could see more normalized growth rates moving forward
Read more **HERE**



Inflation Easing and Interest Rate Adjustments:

Inflation is gradually decreasing, and the Federal Reserve is expected to start cutting interest rates by 100 basis points by the end of 2024. This signals relief for both businesses and consumers, easing borrowing costs and stimulating economic growth
Read more **HERE**



Sustainability on the Backburner:

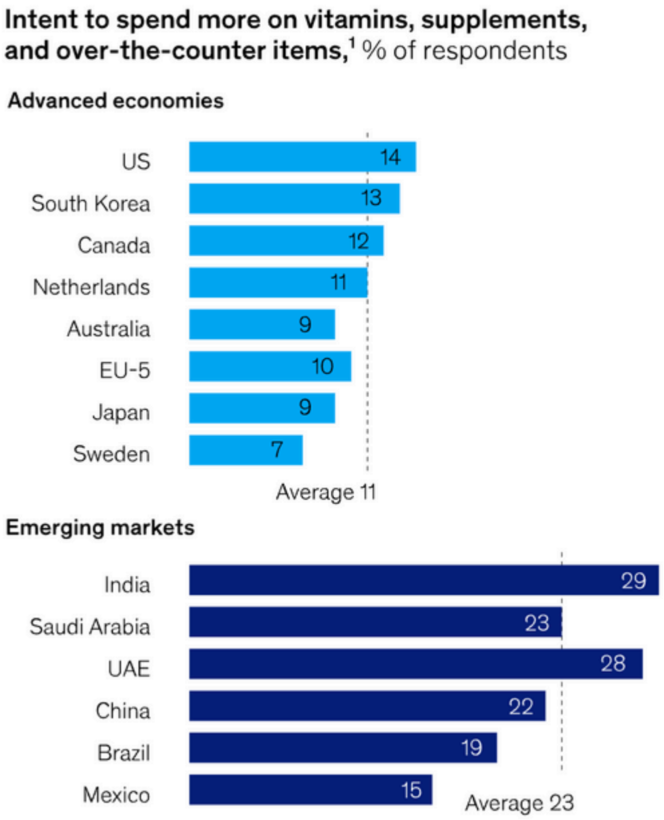
Due to economic uncertainty and inflation, consumers are less emphasising sustainability. Many, especially younger demographics, are no longer willing to pay premiums for eco-friendly products, opting for affordability instead. Read more **HERE**

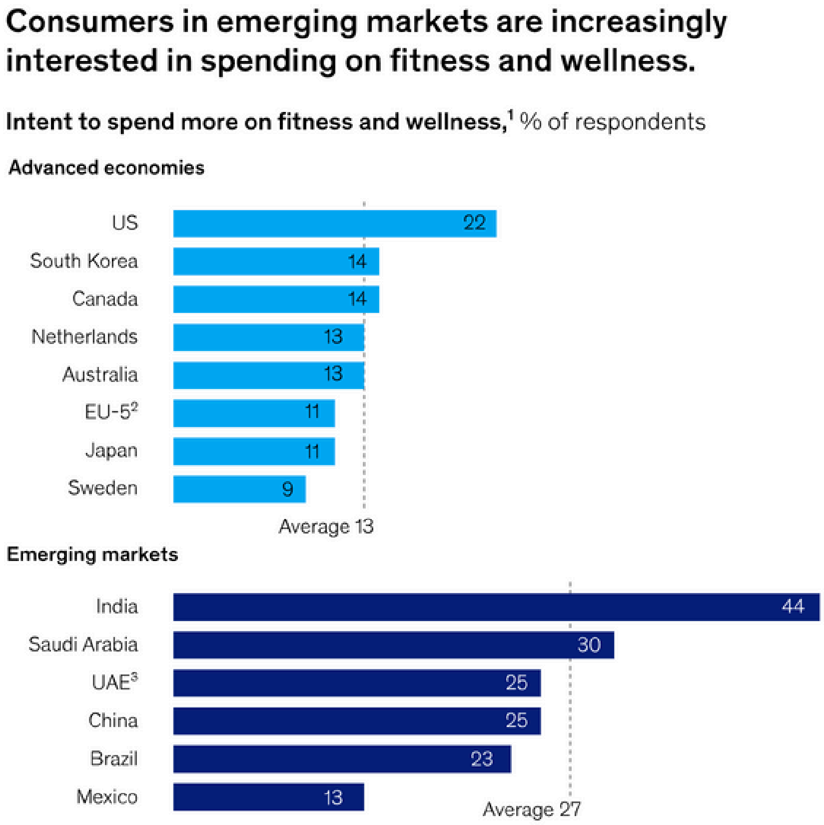
Global Wellness Market Growth:

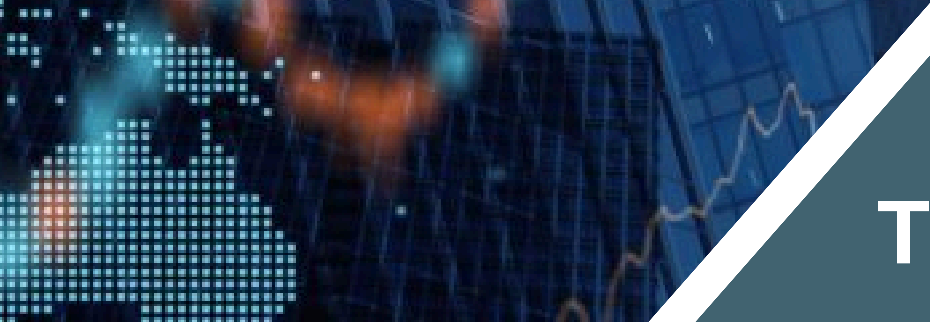
Estimates of the global wellness market are that it is worth more than $1.8 trillion and grows 5 to 10 % annually.4 Health and wellness products and services have been in high demand in advanced economies over the past several years. Today, these categories are also growing quickly in emerging markets, and in some cases, the intent to spend on health and wellness products in emerging markets is outpacing growth in advanced markets.

In emerging markets such as China, India, and the Middle East, the percentage of consumers who intend to increase their spending on wellness products and services is two to three times higher than in advanced markets such as Canada and the United States.

Read more **HERE**







Cyber Security Trends & Threats

Over View of Current Trends & Threats:

In October 2024, cybersecurity threats have become increasingly sophisticated, posing significant risks across various sectors. One major issue is ransomware, which remains a significant threat globally, particularly in sectors like manufacturing and government. Over 66% of organizations were impacted by ransomware in the past year, with the misuse of valid credentials contributing to nearly 45% of data breaches. Additionally, attacks leveraging IoT (Internet of Things) malware have surged by 400%, highlighting vulnerabilities in connected devices.

The rise of AI-generated misinformation and deepfakes is also a growing threat, complicating efforts to maintain digital trust. These technologies are being used to fuel disinformation campaigns, financial scams, and even electoral interference.

Further, large-scale botnets, such as the dismantling of the 911 S5 network of infected computers, continue to be a significant issue, enabling global cybercriminal activity ranging from financial fraud to identity theft.

These evolving threats demand robust cybersecurity measures to protect digital infrastructure, sensitive data, and business continuity.

Financial Cyber Threat:

The ever-expanding sophistication of cyber threats in the financial sector does not indicate slowing down. As quickly as there is a way to prevent a threat from occurring, there is an equally or even faster way it is exploited or bypassed. For example:

North Korean hackers are using a Linux variant of the “FASTCash” malware to exploit interbank payment processors and ATMs, enabling unauthorized cash withdrawals even when accounts lack sufficient funds. This type of cyberattack manipulates transaction messages, often evading standard detection systems. The malware primarily targets financial institutions in Africa and Asia.

How can this affect you or your business?:

This form of malware can and most probably will become a part of the increasingly popular cyber threat of Ransomware-as-a-Service (RaaS).

Three tips to protect yourself or your company from this form of attack:

- Monitor Financial Transactions: Set up real-time monitoring for abnormal transaction patterns or messages in interbank systems.
- Segment Critical Networks: Isolate payment processors and ATM systems from other corporate networks to reduce attack spread.
- Patch and Update: Regularly update all systems, especially Linux-based servers, to close vulnerabilities exploited by malware.
- Strong backup policies, network segmentation, and continuous monitoring for anomalous behaviour.

Ransomware Attacks Tripled for Microsoft Customers Last Year:

The article discusses a 275% increase in ransomware attacks on Microsoft customers from July 2023 to June 2024. Despite the rise, fewer attacks reached the encryption phase due to improved defences. The healthcare and education sectors were especially targeted, with significant disruptions. State-sponsored hackers are using ransomware as part of “hybrid warfare,” combining cyberattacks with influence campaigns. Microsoft emphasizes the need for joint public-private efforts to counter these threats and enforce stricter cybersecurity measures.

Most Impactful Data Breaches of 2024:

(January 2024): Ivanti, a VPN and remote-access provider, was compromised, with attackers stealing credentials and causing domain-level compromises. Given that government agencies widely use Ivanti, this breach posed serious risks to national security

(February 2024): Change Healthcare, One of the largest breaches this year, affecting over 15 billion U.S. medical transactions annually, Change Healthcare paid $22 million in ransom after attackers exploited insufficient security measures on their servers. This breach significantly impacted healthcare data security

(January 2024): A vulnerability in Trello’s public API allowed hackers to scrape data on 15 million users, exposing emails, usernames, and other account information. This breach created a new phishing attack vector

(October 2024): Cisco Data Breach: Reports emerge that a hacker known as “IntelBroker” and two others breached Cisco’s IT network, giving them access to a large amount of Cisco data. According to the perpetrators, stolen data includes “Github projects, Gitlab Projects, SonarQube projects, Source code” and much more.

Key Deals & Recent Funding:

Q3 2024 saw a notable downturn in cybersecurity investments, with a 51% drop in venture funding compared to the previous quarter, totalling only $2.1 billion. This decrease came after a stronger Q2, highlighting the volatility of the sector. The number of large funding rounds—those over $100 million—also fell sharply, with only four significant rounds compared to 10 in Q2. For example, Chainguard raised $140 million, reaching a unicorn valuation of $1.12 billion, and Abnormal Security secured $250 million, valuing the company at $5.1 billion.

M&A front, September 2024 saw a robust 37 deals, with major acquisitions like Mastercard's $2.6 billion purchase of Recorded Future, strengthening its cybersecurity portfolio. Other notable transactions include Salesforce's $1.9 billion acquisition of Own Company, and Visa acquiring Featurespace to bolster its fraud detection capabilities.

Importance:

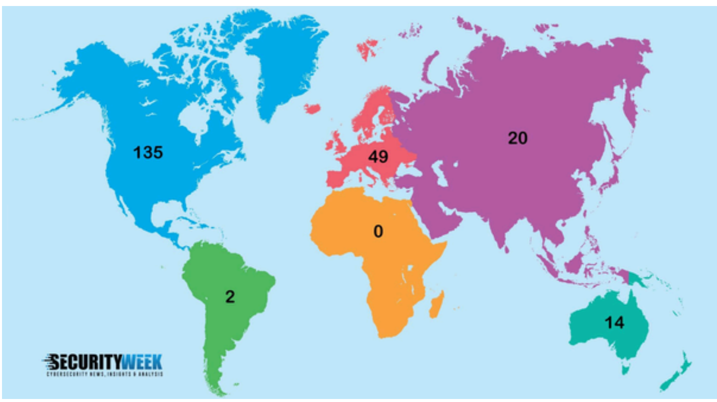
- The sharp decrease in funding and deal flow is significant because it signals shifting investor sentiment.
- Potentially due to macroeconomic conditions and the ongoing AI boom.
- However, cybersecurity remains crucial as threats evolve, and companies like Chainguard and Abnormal Security continue to attract high valuations, showing that investors still trust key players to push technological boundaries.

Governments Are Ramping up Cybersecurity Efforts:

Several governments are ramping up their cybersecurity efforts for 2024 and beyond, implementing new strategies and policies to protect against escalating cyber threats. The U.S. government, for instance, has released updates through the National Cybersecurity Strategy (NCS), which focuses on critical infrastructure protection, ransomware, AI risks, and supply chain vulnerabilities. The U.S. is rebalancing the responsibility for defending cyberspace by increasing government and private sector roles while reducing the burden on end users. The federal government has completed a significant portion of its cybersecurity initiatives in 2024 and continues to address evolving risks, especially from nation-state actors like China.

Similarly, Ghana has launched its National Cybersecurity Policy and Strategy (NCPS) in response to increasing threats from its rapid digital transformation. The strategy emphasizes building a resilient digital ecosystem, securing digital infrastructure, and strengthening collaboration between public and private sectors to minimize risks.

These cybersecurity advancements are expected to strengthen national defences, deter cybercrime, and ensure that digital economies are safeguarded from sophisticated cyber-attacks.



Private Equity Trends & Deals

Market Activity & Key Acquisitions:

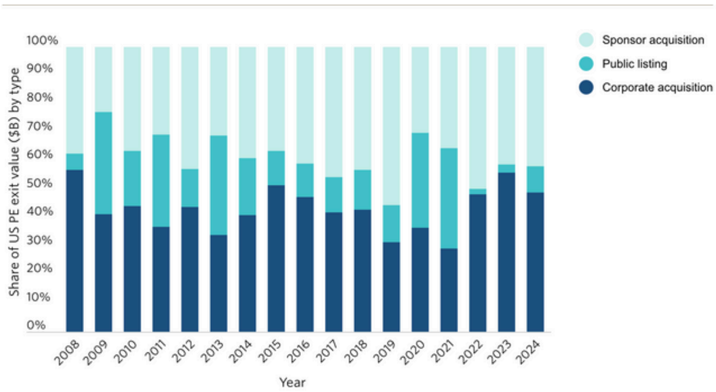
The private equity sector has seen a continued focus on infrastructure, healthcare, and digital transformation in Q3 and Q4 of 2024. One major deal includes EQT's sale of Swiss cybersecurity firm Open Systems to Swiss Post. This highlights an ongoing trend of private equity funds pivoting to sectors with growing digital infrastructure needs, particularly cybersecurity.

PE firms remain active in healthcare technology, as seen in Blackstone's acquisition of Altruist Health, a provider of AI-driven healthcare solutions, for approximately $1.5 billion in October 2024. Such deals underline the attractiveness of technology-driven healthcare as an investment focus.

PE Firms Enlist More IPO Exits in Q3:

According to PitchBooks PE breakdown of the US, it suggests that the exit environment is on the mend, with five exits via IPO.

Private equity has seen considerable improvement in exit value from IPOs compared to last year. IPOs in 2023 accounted for just 3% of exit value; that number for 2024 stands at 9.4% as of the third quarter's end.



US Banks are Easing on LBO:

Banks are gradually resuming their involvement in financing leveraged buyout (LBO) deals. By the third quarter of 2024, the year-to-date value of syndicated LBO loans had almost doubled, reaching $50.8 billion, compared to $28.6 billion during the same period in 2023. While this represents a significant increase, if this trend continues through the final quarter, the total loan volume for 2024 will still fall about 53.6% below the record highs seen in 2021 and remain 33.2% below the average annual volume observed in the three years leading up to the COVID-19 pandemic.

Notable PE Firms Activity in the Middle East Region:

CVC Capital Partners - In 2024, CVC made headlines with a $3.3 billion deal involving Dubai-based GEMS Education. Their focus on education and healthcare reflects broader investment trends across the region, especially within the UAE and Saudi Arabia, where there is a surge in healthcare infrastructure projects.

Gulf Islamic Investments - This firm has invested heavily in Saudi healthcare, with notable deals like a $164 million investment in Abeer Group, a major healthcare services provider. Such investments align with Saudi Arabia's Vision 2030 to enhance its healthcare capabilities and diversify the economy.

Oman Investment Authority (OIA) - OIA's $5.2 billion Oman Future Fund is being used to develop national infrastructure projects and attract foreign investment across key sectors, including healthcare and tech, over the next five years.

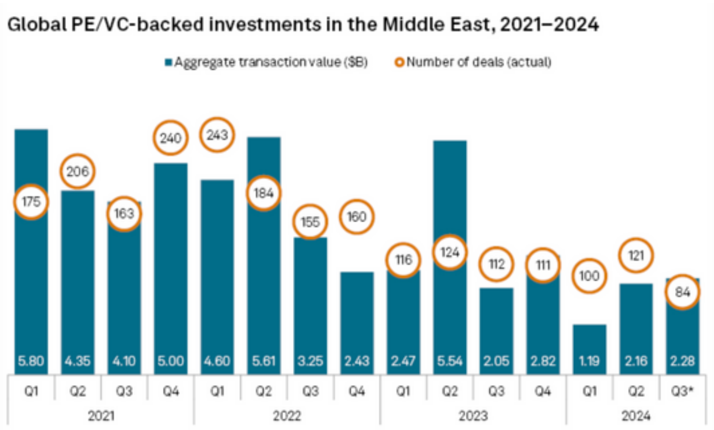
Private equity deal value in the Middle East on the rise:

Private equity and venture capital investments in the Middle East have increased so far in 2024, targeting businesses that are outside the oil and gas sector

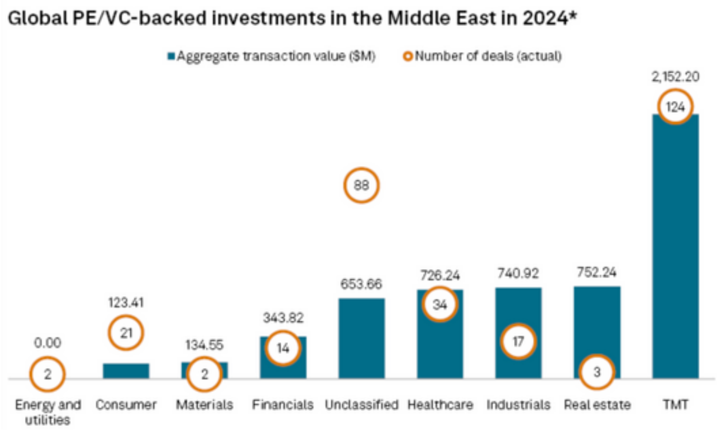
.

The region comprising 12 countries including oil-rich Saudi Arabia, the United Arab Emirates and Iran — attracted $2.28 billion for the third quarter to Sept. 27, according to S&P Global Market Intelligence data. The amount is already slightly higher than the $2.16 billion deal value for the full second quarter and nearly double the $1.19 billion in the first quarter.

However, the annual total is on track to fall well short of the $11.60 billion of capital attracted in 2023, particularly given the backdrop of continuing military conflict involving Israel, Palestine, Lebanon and Iran.



The technology, media and telecommunications industry recorded the most activity with 124 deals totalling over $2.15 billion. Real estate had the second-largest deal value at $752 million, followed by the industrial sector with $741 million. Energy and utilities ranked the lowest with only two undisclosed deals even with rising private equity investment in global fossil fuel and renewable energy companies this year.



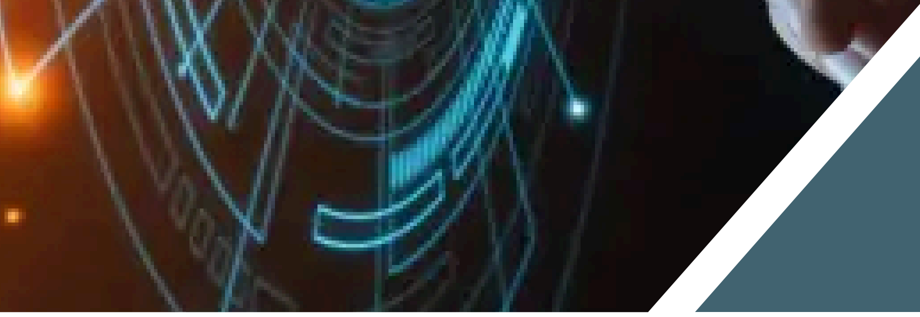
Real estate, industrials, and GenAI make up the top 3 deals

The region's largest deal so far this year is the acquisition by Lunate and Olayan Financing Co. WLL of a ***49% stake*** in ICD Brookfield Place from Investment Corp. of Dubai and ICD-Brookfield Management Ltd. for ***$735 million***. After the deal closed, Lunate and Olayan each owned a 24.5% stake in the Dubai, UAE-based business centre.

The second-largest deal is Apollo Global Management Inc.'s planned ***$600 million*** purchase of a ***50% stake*** in iron blending and distribution company Vale Oman Distribution Center LLC. The Vale SA subsidiary operates a maritime terminal in Sohar, Oman, with an integrated iron ore blending and distribution centre that has a nominal capacity of 40 metric tons per year.

Third is Silver Rock Group's ***$325 million*** investment in UAE-headquartered generative AI company Pathfinder Global FZCO.

The top three deals in the region consist of real estate, industrials, and an investment in a company called GenAI.



Venture Capital Trends & Deals

Investment Trends and Notable Deals:

Venture capital investments in cybersecurity and AI-related startups have slowed overall, but certain high-profile deals stand out:

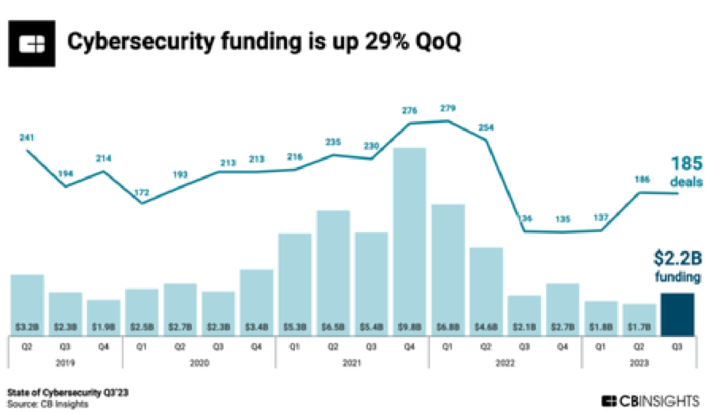
In July 2024, Vanta raised $150 million in a Series C round led by Sequoia Capital, valuing the company at $2.45 billion. This round highlighted the growing demand for compliance automation, especially in sectors dealing with sensitive data.

While cyber investments dipped, AI and healthcare technology have seen steady interest. AI-powered fraud detection companies like Featurespace and innovative healthcare tech firms continue to attract significant funding, with a strong emphasis on using AI to optimise operations

Why It Matters:

Venture capital's shifting focus from cybersecurity to AI and healthcare technology reveals broader trends in the investment landscape.

While cyber remains critical, AI's potential in sectors like fraud detection and healthcare optimisation has captured the attention of major VC firms, indicating a pivot in where capital is flowing.

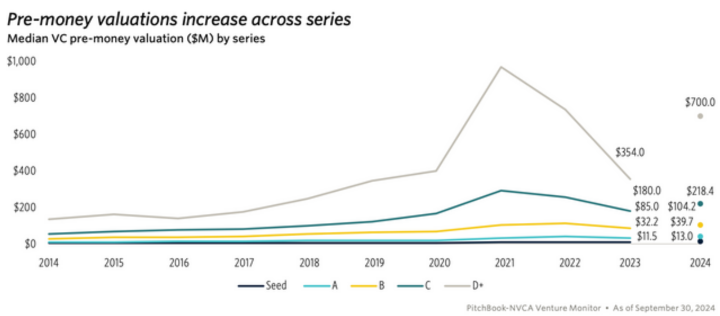


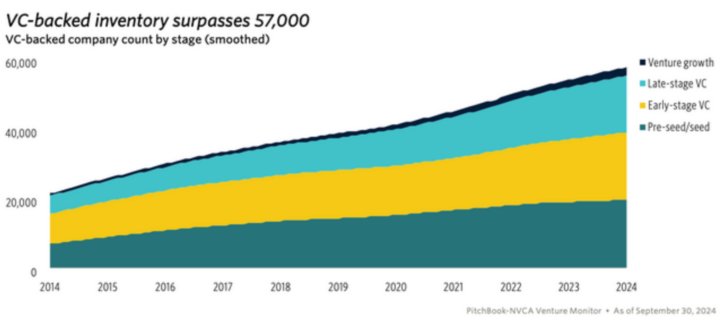
Venture-backed Companies are Choosing to Stay Private for Longer:

Companies are staying private for longer as they wait for a friendlier dealmaking environment. The growing backlog of companies currently unable or unwilling to exit has caused the US private company inventory to balloon to 57,674, a record high.

Late-stage and venture-growth startups, which are typically prime candidates for public listings, have taken on a growing percentage of this population, making up 32.4% of private companies, compared with 30.0% three years ago.

Considering that the inventory increased by 25.9% during this period, this change is significant and contextualizes just how much the lack of IPOs has affected VC.





AI Companies are Commanding the Most Attention in Venture:

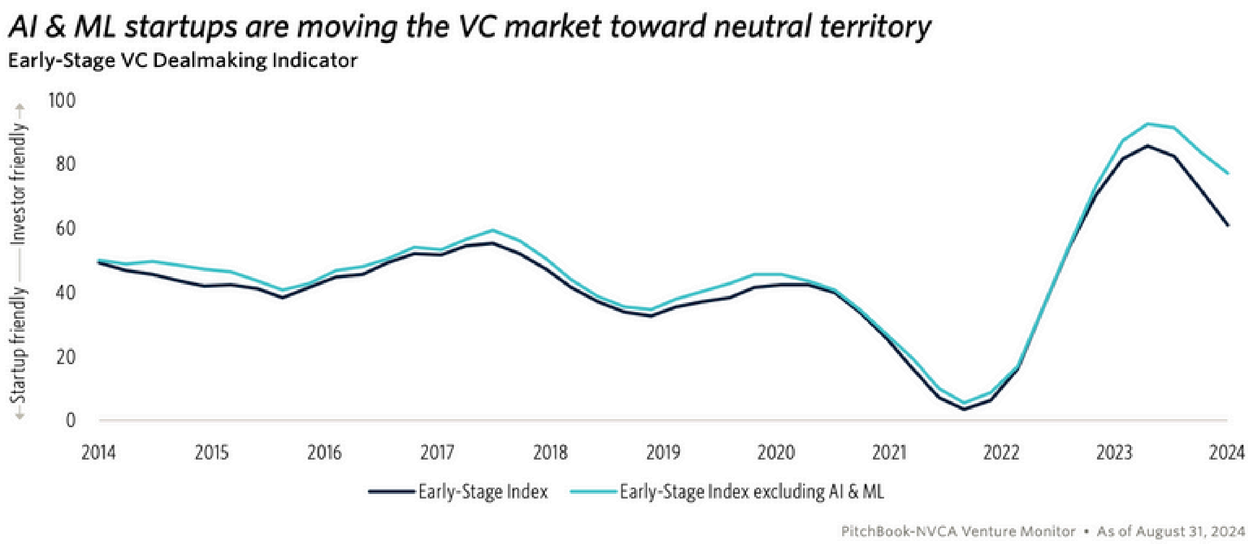
Deal sizes and valuations are generally trending upward across most investment stages when compared to 2023, which initially appears promising. However, a closer analysis shows that these numbers are being skewed by large AI deals and startups that raised funds two to three years ago during a period of record-high valuations.

AI companies are drawing the most attention in the venture capital space. The biggest deal in Q3 came from Anduril Industries, a defence tech firm that integrates AI into weapon systems, securing $1.5 billion in a Series F round at a pre-money valuation of $12.5 billion.

Another major deal was Safe Superintelligence, which raised $1 billion in its first-ever funding round at a $4 billion pre-money valuation, despite having no product or defined business model yet. Investors were drawn to the company's impressive founding team, which includes AI experts like OpenAI co-founder Ilya Sutskever.

This trend exemplifies the dominance of AI in the venture capital landscape. For instance, Safe Superintelligence's $1 billion deal represents over 20% of first-time funding in Q3 alone. Although many investors are cautious, preferring to reinvest in established portfolio companies, AI startups are exceptions to this trend.

Investors are more willing to commit significant capital to AI firms without requiring the same financial benchmarks—like profitability and strong unit economics—that other startups must meet.



Family Office Trends & Deals

Expanding Investment Horizons:

Family Office has been increasingly venturing into alternative investments, with a strong focus on tech startups and sustainability projects. In 2024, there has been a notable shift toward direct investments in cybersecurity startups and renewable energy projects. Family offices are increasingly bypassing traditional funds and directly backing companies like Tamnoon, a cybersecurity firm that raised $12 million in Q3 2024.

One example is the involvement of FO in backing renewable energy initiatives, particularly those that integrate cutting-edge AI to optimise energy use. This trend has been visible in deals like the $300 million family-office-led round in Elysium Energy, an AI-driven energy optimisation platform, in September 2024.

Why It Matters:

Family offices are playing a larger role in financing innovative tech and energy sectors. Their ability to make nimble investment decisions without the constraints of institutional mandates allows them to capitalise on high-growth opportunities, particularly in cybersecurity and sustainable technologies, setting a trend for 2025.

Family offices are increasingly becoming influential players in financing innovative sectors like technology and renewable energy. These privately held investment entities, often managing the wealth of ultra-high-net-worth families, can make rapid investment decisions without the bureaucratic hurdles typically faced by institutional investors.

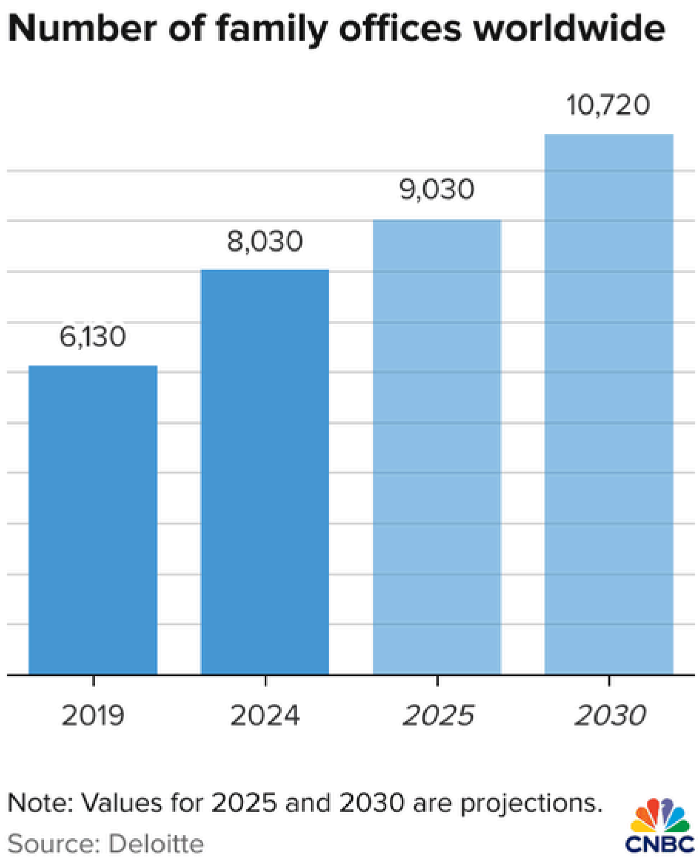
This agility allows family offices to tap into high-growth areas such as cybersecurity, artificial intelligence, and sustainable energy technologies.

In 2025, family offices are poised to shape emerging trends by prioritizing investments in cybersecurity as cyber threats escalate, particularly in sectors like financial services and healthcare. Their growing focus on sustainable technologies, including clean energy and climate tech, aligns with global shifts toward decarbonization and energy security.

Moreover, family offices often have a long-term investment horizon, making them ideal backers for companies driving deep technological innovation and infrastructure improvements in these areas.

This trend reflects family offices' capacity to influence markets by backing cutting-edge solutions while enjoying more control and flexibility than traditional investment firms.

As a result, their role in the venture ecosystem is expected to expand, potentially driving even more capital into transformative technologies over the next several years.



Final Thoughts

As we approach the close of 2024 and look toward 2025, distinct trends are emerging across key sectors like cybersecurity, private equity, venture capital, and family offices, each reflecting the broader market's pivot toward technology-driven solutions.

In cybersecurity, while overall funding has seen a reduction, the importance of robust security frameworks remains undiminished.

Threats such as ransomware, AI-driven attacks, and supply chain vulnerabilities are evolving rapidly. This is prompting renewed M&A activity in the sector, with larger companies acquiring smaller, innovative cybersecurity firms to enhance their defences and service offerings.

With growing concerns over data breaches and nation-state-sponsored cyber attacks, the sector will remain vital for businesses and governments, even in an environment of more selective funding.

Private equity (PE) and venture capital (VC) are leaning heavily into healthcare and AI innovation, two sectors that continue to attract substantial investments. PE firms are increasingly backing healthcare-related startups, particularly those focused on AI-driven diagnostics, telemedicine, and personalized healthcare solutions.

VC activity has also surged around artificial intelligence, where startups focused on generative AI, AI infrastructure, and cybersecurity applications are commanding high valuations.

This trend is expected to persist, as both PE and VC firms see healthcare and AI as pivotal in addressing long-term global challenges, from ageing populations to digital security.

Meanwhile, family offices are playing a growing role as direct investors in these sectors, with a strong focus on cybersecurity and sustainability projects. Unlike institutional investors bound by mandates, family offices have greater flexibility to allocate capital swiftly and strategically, especially in fast-growing areas like renewable energy and green technologies.

Their willingness to invest in these long-term solutions underscores a broader market transition toward sustainable and tech-centric opportunities, setting a course for 2025 and beyond.

Together, these developments illustrate a wider market shift towards innovative, technology-driven solutions that address the most pressing issues in healthcare, security, and sustainability.

As these sectors converge, the emphasis on innovation and resilience will likely shape investment strategies well into the future.

QWANTIV TECHNOLOGIES