CYBERCRIME MAGAZINE

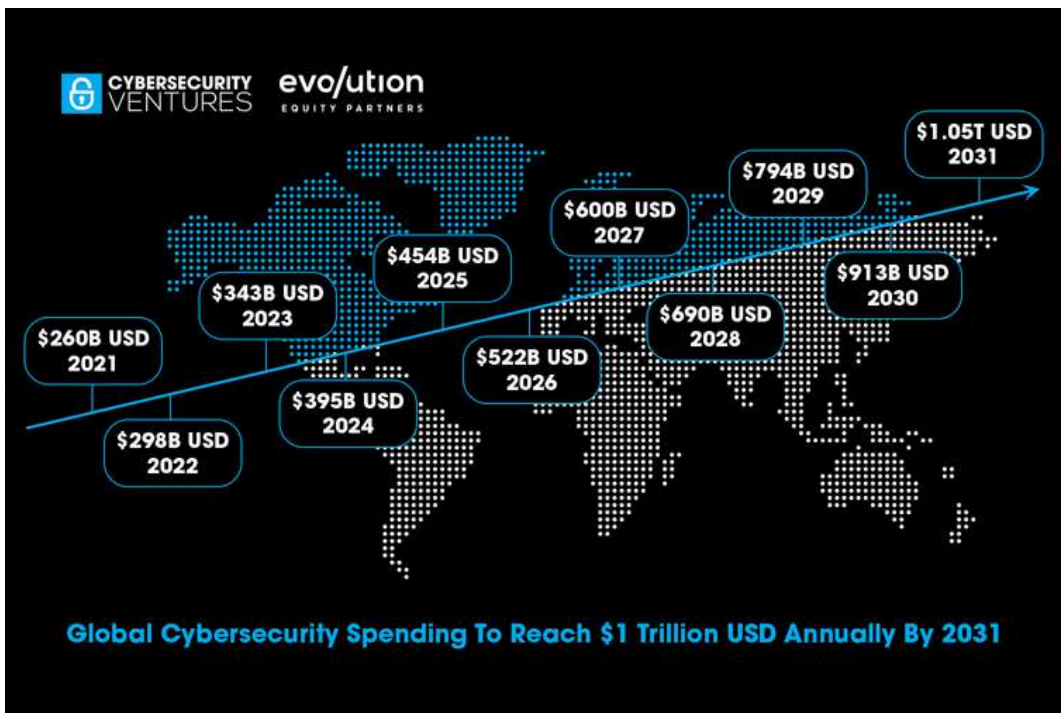
Q4 2025 | PAGE ONE FOR THE CYBERSECURITY INDUSTRY | CYBERCRIMEMAG.COM

2026 CYBERSECURITY MARKET REPORT

GLOBAL CYBERSECURITY MARKET TO REACH $1 TRILLION ANNUALLY BY 2031

Cybersecurity Ventures anticipates 15 percent year-over-year growth over the next five years

SAUSALITO, CALIF. – Nov. 14, 2025



The imperative to protect increasingly digitized businesses, governments, schools, Internet of Things (IoT) devices, and industrial control systems (ICS), as well as semiconductors, medical devices, gaming systems, cars, ships, planes, drones, trains, ATMs, and consumers from cybercrime will propel global spending on cybersecurity products and services to $1 trillion (USD) annually by 2031, according to the "2026 Cybersecurity Market Report" from Cybersecurity Ventures in partnership with Evolution Equity Partners.

"In 2004, the global cybersecurity market was worth just $3.5 billion," says Steve Morgan, founder of Cybersecurity Ventures, "and now it's one of the largest and fastest-growing sectors in the information economy."

TOTAL ADDRESSABLE MARKET

Cybersecurity Ventures predicts that global spending on cybersecurity products and services will hit $454 billion annually (USD) in 2025, up from $260 billion in 2021. This includes all countries globally, B2B and B2C, plus a portion of any markets that are converged with cybersecurity such as quantum security, physical security and surveillance, government information security and military cyber defense technology (all nations), space cyber defense, and also counts in cyberinsurance policies.

AI is expanding a $2 trillion total addressable market (TAM) for cybersecurity providers, according to a 2024/2025 study by McKinsey, a global management consulting firm and trusted advisor to leading businesses, governments, and institutions.

CYBERCRIME MAGAZINE

INQUIRIES: INFO@CYBERSECURITYVENTURES.COM

evolution EQUITY PARTNERS

CONTACT:EVOLUTIONEQUITY.COM/CONTACT-US/

Nearly 15 percent of cybersecurity spending comes from outside the chief information security office (CISO), according to a McKinsey study

“One of the areas that is extremely compelling is the opportunity to build a security layer around agentic AI,” says Richard Seewald, founder and Managing Partner at Evolution Equity Partners. “If you think about the volume of agents that will be put into the market, the opportunity to create cybersecurity companies that defend and protect that layer are significant.”

Richard Seewald
Founder & Managing Partner
Evolution Equity Partners

McKinsey’s study is particularly relevant to the CISOs and vendors, the cybersecurity buyers and sellers, who made a pilgrimage to this year’s RSA Conference USA 2025 in San Francisco. “Based on the organizations we have served, cyber budgets are still under tremendous pressure to reduce cost when, in reality, they are often under-budgeting when framed in terms of the organization's risk profile,” Justin Greis, Partner and North American Cybersecurity Practice Leader at McKinsey, told Cybercrime Magazine while at the RSA Conference.

“More often than not, when we are engaged to analyze and possibly reduce cybersecurity costs, we typically end up increasing the cyber budget because the cyber risks uncovered exceed management's and the board's risk appetite,” adds Greis. “More and more CISOs are requesting and reporting their budgets, not just in dollars and cents, but framed in terms of risk to critical business processes, products, services, or strategic goals/objectives.”

Evolving market dynamics are changing the way cybersecurity providers reach potential customers, according to McKinsey.

Today, nearly 15 percent of (corporate) cybersecurity spending comes from outside the chief information security office (CISO), and non-CISO cyber spending is expected to grow at a 24 percent CAGR over the next three years, according to the McKinsey study, which goes on to state that this has changed from a decade ago, when almost all cybersecurity spending came from the CISO organization.

The TAM figures from McKinsey are global and primarily focused on B2B, but not B2C or other markets converged with cybersecurity, such as physical security and surveillance, automotive security, and others.

Going forward, providers will need to increasingly cater to non-CISO customers, the McKinsey study posits, with most non-CISO cyber spending coming from buying centers responsible for cloud, product, network, and audit and compliance.

CYBERCRIME MAGAZINE
INQUIRIES: INFO@CYBERSECURITYVENTURES.COM
evolution EQUITY PARTNERS
CONTACT:EVOLUTIONEQUITY.COM/CONTACT-US/

The U.S. and Western Europe will account for more than 70 percent of global security spending in 2025, according to IDC

SECURITY SPENDING

The increasing complexity and frequency of cyberthreats—accelerated by generative AI (GenAI) and AI in general—are driving organizations worldwide to adopt more advanced defensive measures.

According to the latest forecast from the International Data Corporation (IDC) "Worldwide Security Spending Guide," global security spending is expected to reach $377 billion in 2028. This covers security software, hardware, and services – both managed services and professional services.

The U.S. and Western Europe will account for more than 70 percent of global security spending in 2025, according to IDC. However, all geographic regions were expected to see consistent growth in security spending in 2025, with the highest increases in Latin America, Central and Eastern Europe, and the Middle East and Africa.

The IDC guide quantifies both core and next-generation security spending for 28 industries and five company sizes across 39 technology markets and 48 countries.

Stefano Perini, PhD, co-author of the IDC guide, told Cybercrime Magazine that their spending figures include corporate and consumer security, as well as Internet of Things (IoT) and Industrial Internet of Things (IIoT), which is a network of interconnected sensors, instruments, and devices used in industrial sectors.

The IDC spending figures do *not* include security for ICS (Industrial Control Systems), according to Perini, for example:

PLCs (Programmable Logic Controllers), which are ruggedized industrial computers used to automate processes in manufacturing, machinery, and assembly lines;

SCADA (Supervisory Control and Data Acquisition), which are systems of software and hardware components used to monitor and control industrial processes remotely across large geographical areas;

DCS (Distributed Control System), computerized systems used in industrial settings, such as power plants and manufacturing facilities to monitor and control automated processes.

Perini also told Cybercrime Magazine that the IDC spending figures do *not* include security systems embedded in ships (maritime security) and planes (aviation security), and also do *not* include security systems related to automobiles, gaming systems, and medical devices, as well as consumer-wearable medical devices.

Cybersecurity Ventures predicts that the world will spend $522 billion on cybersecurity products and services in 2026

Forrester forecasts that worldwide information security spending will reach $200 billion in 2026, while Gartner projects $240 billion for 2026. Cybersecurity Ventures predicts the figure will be $522 billion in 2026.

“A large portion of information security related spending is not accounted for as being information-security related,” says Morgan. This was called out nearly a decade ago in an Inc. Magazine article, and it’s still true today. “If all of the unaccounted expenditures could be tallied by the analysts, then the IT security spending figures would be much higher,” adds Morgan.

The delta between the spending figures from Cybersecurity Ventures and the IT analyst firms are due in large part to the number of security categories and attack surfaces that are covered.

“Historic analyst reports are rooted in ‘IT security’ (servers, networking gear, data centers and IT infrastructure, PCs, laptops, tablets, and smartphones) and not fully evolved to ‘cybersecurity,’ which includes non-computer devices and non-IT centric platforms and environments – which covers entire sub-markets, i.e. aviation security, automotive security, IoT security, and IIoT (Industrial Internet of Things) security,” says Morgan. “All of those market segments, plus others, combine to make up the cybersecurity market, as we see it.”

Steve Morgan, Founder of Cybersecurity Ventures

Even IT security services are difficult to fully size. Tech is a cottage industry, which includes tens of thousands of VARs (value-added-resellers), IT solution providers, and SIs (systems integrators), who wrap IT security services around the IT infrastructures they implement and support–but (most of) these firms don’t break out and report cybersecurity revenues as a separate bucket.

Despite its current market size, cybersecurity has a lot of headroom to grow. "We are still in the early innings of a secular trend in the cybersecurity space that involves increased spend by large enterprises, smaller businesses and consumers alike, a rapidly expanding attack surface, market consolidation and demand for next generation products and services that makes this a very compelling segment for investment," says Dennis Smith, Founder and Managing Partner at Evolution Equity Partners.

Cybersecurity Ventures predicts that cybercrime will cost the world $10.5 trillion annually by 2025, up from $3 trillion in 2015

CYBERCRIME WILL GET MUCH WORSE

"The World In 2030," a Bank of America research paper, cites Cybersecurity Ventures, whose analysis shows that cybercrime – such as hacking, fake videos and stealing personal data – is expected to cost the world $10.5 trillion by 2025, making it the world's third largest economy behind the U.S. and China. And with the exponential rise of AI deep fake videos and phone calls, these crimes will become more effective and harder to stop.

Part of the reason why those losses are so high, according to Adam Evans, Royal Bank of Canada's SVP and CISO, is that businesses too often underestimate the risks, and too often under-invest in protecting themselves.

GOBankingRates, a Gen Digital media property, reports that the rise in online threats will cause both businesses and governments to spend much more on cybersecurity (especially in the U.S.).

This includes areas like banking, defense, and infrastructure, and it could increase profits for security companies and open the door to online security innovation.

"Cybersecurity is the only line item that theoretically has no spending limit," says Morgan. "There is a budget before a company suffers a cyberattack or a series of them, and then there's the actual spend that takes place afterwards. What business or consumer isn't going to do and spend whatever it takes to recover from being hacked?"

While all other tech sectors are driven by reducing inefficiencies and increasing productivity, cybersecurity spending is driven by cybercrime.

In 2015, Bank of America CEO Brian Moynihan declared that the nation's second-largest lender had an unlimited cybersecurity budget. "Moynihan was brutally honest," says Morgan. "But really, what he said then is true now and in the future for Fortune 500 and Global 2000 enterprises all the way down to Main Street businesses. He just had the courage to say it without worrying about the repercussions."

The bottom line, according to GOBankingRates: Online risks will drag down growth unless security spending keeps up, but cybersecurity itself could end up becoming its own business sector.

In fiscal 2025, Microsoft generated approximately $37 billion in cybersecurity revenue, according to Investing.com

TECH GIANTS

A significant amount of corporate, government, and small-to-midsized (STM) spending in our space has gone to Microsoft, who in fiscal 2025 generated around $37 billion in cybersecurity revenue, representing about 14 percent of its total revenue, according to Investing.com, and its security business can reach $50 billion by 2030 if it grows at a mid-teens CAGR.

Trailing Microsoft, amongst the tech giants, Cisco's security business is approximately $8 billion for the last year tracked, and IBM Security generates billions in annual revenues but doesn't presently report it separately. Nearly a decade ago, IBM publicly stated its annual security revenues were $2 billion.

Google also doesn't break out its security revenues separately, but they made an enormous push into the space in 2025 when they announced their intentions to acquire Israeli cybersecurity startup Wiz for $32 billion. Google acquired Mandiant, another major cyber brand, for $5.4 billion in 2022.

Earlier this year, Google revealed a new unified security platform that analysts think can help it battle Microsoft for a bigger chunk of the enterprise infosec market. Google Unified Security (GUS) combines the search giant's existing threat intelligence, security operations, and cloud security services, plus Chrome Enterprise, and it also adds agentic AI.

According to Gartner, worldwide security services revenue exceeded $77 billion in 2024, and Big 4 consulting giant Deloitte had the largest market share with 16.6 percent. That puts Deloitte's annual security services revenues at more than $12.7 billion. Deloitte has an army of more than 40,000 security services professionals.

The tech giants have also been big cybersecurity spenders over the past five years. Following a 2021 convene at the White House, several major technology companies, including Apple, Amazon Web Services (AWS), and IBM, announced new cybersecurity initiatives from 2021 to 2025.

Microsoft quadrupled its cybersecurity investment to $20 billion from 2021 to 2025, up from the $1 billion per year they had been spending on cybersecurity since 2015.

Google's CEO announced the search giant would invest more than $10 billion from 2021 to 2025 in cybersecurity. The money was to include helping to secure the supply chain and strengthening open-source security.

Only around 15 pure-play cybersecurity companies generate $1 billion or more in annual revenues as of 2025, according to various sources

BIG CYBER

The largest pure-play cybersecurity companies compiled by Cybersecurity Ventures with annual revenues of $500 million or more for the last financial year reported, according to Yahoo! Finance for publicly traded companies, and various sources for privately held companies, altogether account for around $48.5 billion in annual revenues:

- Palo Alto Networks (NASDAQ: PANW), Santa Clara, Calif. $9.22 billion
- Fortinet (NASDAQ: FTNT), Sunnyvale, Calif. $5.96 billion
- CrowdStrike (NASDAQ: CRWD), Austin, Texas. $4.34 billion
- Gen Digital (NASDAQ: GEN), Tempe, Ariz. $3.94 billion
- F5 (NASDAQ: FFIV), Seattle, Wash. $3.09 billion
- Zscaler (NASDAQ: ZS), San Jose, Calif. $2.67 billion
- Okta (NASDAQ: OKTA), San Francisco, Calif. $2.61 billion
- Check Point Software (NASDAQ: CHKP), Tel Aviv, Israel. $2.56 billion
- ProofPoint (privately held), Sunnyvale, Calif. $2 billion
- Cloudflare (NYSE: NET), San Francisco, Calif. $1.67 billion
- CyberArk (NASDAQ: CYBR), Newton, Mass. $1.67 billion
- 360 Security Technology aka Qihoo 360 (SHA: 601360), Beijing, China. $1.1 billion
- Sophos (privately held), Abingdon, U.K. $1 billion
- LevelBlue (privately held), Plano, Texas. $1 billion
- Infoblox (privately held), Santa Clara, Calif. $938 million
- Rubrik (NYSE: RBRK), Palo Alto, Calif. $886.5 million
- Kaspersky (privately held), Moscow, Russia. $822 million
- Tanium (privately held), Kirkland, Wash. $700 million

CYBERCRIME MAGAZINE

INQUIRIES: INFO@CYBERSECURITYVENTURES.COM

evolution EQUITY PARTNERS

CONTACT:EVOLUTIONEQUITY.COM/CONTACT-US/

The 50 largest publicly traded IT security companies by market cap have a total market cap of more than $700 billion

- SailPoint (NASDAQ: SAIL), Austin, Texas. $699.6 million
- Netskope (NASDAQ: NTSK), Santa Clara, Calif. $615.5 million
- Varonis (NASDAQ: VRNS), New York, N.Y. $551 million
- BlackBerry (NYSE: BB), Waterloo, Canada. $534.9 million
- Barracuda Networks (privately held), Campbell, Calif. $500 million

This list does not include a small number of pure play cybersecurity companies, for instance McAfee (owned by privaty equity firm Advent International) which now focuses mainly on consumer security, and may generate as much as $2 billion or more in annual revenues, but their revenues are not reported or even estimated by any reliable sources. Similarly Trellix (owned by private equity firm STG), which combined McAfee's enterprise products and FireEye when it formed the company in 2022, and their revenues, perhaps as much as $1.5 billion, are not publicly available.

The 50 largest publicly-traded IT security companies by marketcap have a total marketcap of more than $700 billion as of the date this report was published.

Dozens of large well-known brands, ranging from tech vendors to defense contractors to consulting houses, have major cybersecurity businesses, but don't report those revenues separately. For example, a short list of names are Akamai, Broadcom, DataDog, EY, HPE, Honeywell, Leidos, Palantir, and Thales.

GOVERNMENT PROTECTION

The U.S. spends more than $25 billion on cybersecurity every year to defend federal systems against increasing threats from hackers, ransomware groups and state-sponsored actors, according to Palo Alto Networks. Deltek estimates the federal cybersecurity market more at $18.8 billion in 2026, growing to $20.7 billion in 2028. The U.S. has the largest cybersecurity budget out of all nations for protecting its government against cyber threats.

If governments globally spent around .075 percent of their GDP on cybersecurity to protect their information technology infrastructures similar to the U.S., then all nations combined would spend around $64.5 billion USD annually to do so. But it's unlikely that the least developed countries (LCDs) would be spending (on cybersecurity) proportionally on par with the U.S. There is no current source that Cybersecurity Ventures is aware of that reports on each nation's annual internal government cybersecurity spending.

One cybersecurity company deployed more than 25,000 advanced cell-phone-detection systems on locomotives nationwide over the past decade

MORE THAN INFORMATION SECURITY

The totality of the cybersecurity market is far larger than information security, a point that Scott Schober, Cybercrime Magazine's Chief Security Officer-at-Large, drives home for us.

"As the U.S. rail network continues to modernize with thousands of passenger trains and tens of thousands of locomotives operating across the country, cybersecurity and operational safety must evolve together. The integration of IoT systems on trains and locomotives has brought new efficiencies—but also new attack surfaces," says Schober.

"At Berkeley Varitronics Systems (BVS), we've deployed more than 25,000 advanced cell-phone-detection systems on locomotives nationwide over the past decade to help eliminate operator distraction and enhance cyber-physical resilience. Protecting the transportation sector is not just about safety—it's a vital component of national cybersecurity strategy as global spending surges," says Schober, CEO at BVS.

BVS has built up a substantial cybersecurity business around sectors that are not so obvious to many people in our field, including some analysts who track the market.

"Cybercriminals are targeting the physical edges of our financial and retail ecosystems every day—ATMs, fuel pumps, and payment terminals—with increasingly sophisticated credit/debit card skimming devices. These threats bridge the digital and physical worlds, demanding proactive defense. At BVS, we've engineered next-generation skimmer-detection solutions that safeguard banks, fuel distributors, and payment processors from these emerging attacks."

Securing U.S. ports of entry with technology is another facet of cybersecurity, according to a blog post by Schober. A growing concern in maritime security is the use of GPS and Bluetooth Low Energy (BLE) trackers, such as Apple AirTags, Samsung SmartTags, and Tile devices, to monitor shipments illicitly. These small, inexpensive devices can be discreetly hidden within cargo, enabling unauthorized tracking of containers. Such practices can facilitate the theft of goods, unauthorized surveillance, and the circumvention of customs regulations. However, wireless security tools are being introduced to detect an assortment of wireless hackers, contraband and illegal tracking.

Total addressable market (TAM) is the total revenue opportunity available to a product or service if 100 percent market share is achieved

DEFINITIONS

Spending, which is used by Cybersecurity Ventures in this report, is actual dollars predicted to be spent, or to have previously been spent, for a specified time period. Forrester, IDC, and Gartner also refer to spending (whether it is calculated, forecasted, or predicted) in their reports.

Total Addressable Market (TAM), which McKinsey refers to in its study, which also appears in this report, is the total revenue opportunity available to a product or service if 100 percent market share is achieved. TAM does not represent actual dollars spent, or expected to be spent.

Spending and TAM are not competing terms. They offer different ways to analyze the same market, in this case cybersecurity.

CYBERCRIME MAGAZINE

INQUIRIES: INFO@CYBERSECURITYVENTURES.COM

evolution EQUITY PARTNERS

CONTACT:EVOLUTIONEQUITY.COM/CONTACT-US/

The Cybersecurity Market Report is authored by the editors at Cybercrime Magazine and published in partnership with Evolution Equity Partners

ABOUT

Cybersecurity Ventures is the world's leading market-watcher and a trusted source for cybersecurity facts, figures, and statistics. We provide cyber economic market data, insights, and ground-breaking predictions to a global audience of CIOs and IT executives, CSOs and CISOs, information security practitioners, cybersecurity company founders and CEOs, venture capitalists, corporate investors, business and finance executives, HR professionals, and government cyber defense leaders.

Evolution Equity Partners is an international venture capital investor led by technology entrepreneurs who have built software companies around the world and who leverage tremendous operating, technical, product development and go-to-market expertise to help entrepreneurs win. Evolution partners with bold visionaries building market-leading companies that defend and protect what matters most.

MEDIA CONTACT

Editors at Cybercrime Magazine
info@cybersecurityventures.com