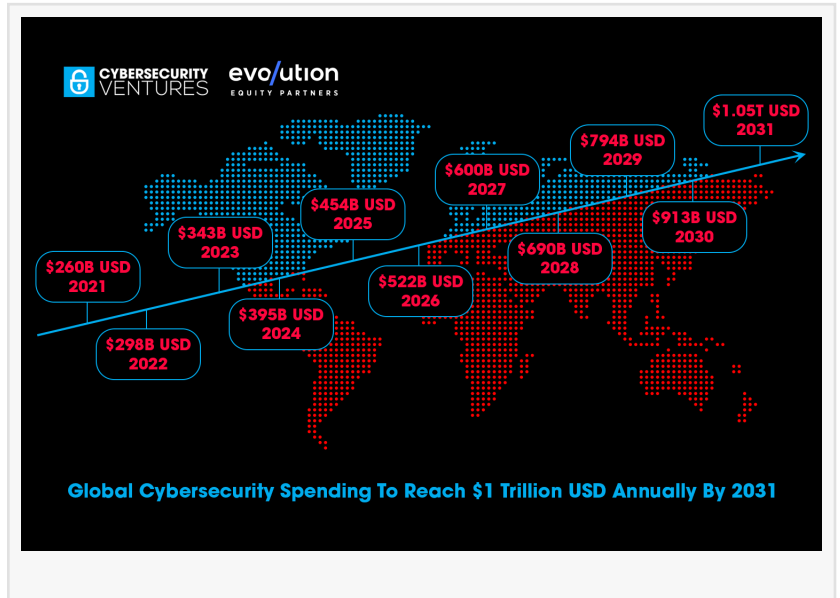


Global Cybersecurity Market To Reach \$1 Trillion Annually By 2031

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

SAN FRANCISCO, CA, UNITED STATES, April 28, 2025 /EINPresswire.com/ -- The imperative to protect increasingly digitized businesses, governments, schools, Internet of Things (IoT) devices, and consumers from cybercrime will propel global spending (1) on cybersecurity products and services to \$1 trillion (USD) annually by 2031, according to the "Cybersecurity Market Report" due out from

[Cybersecurity Ventures](#) and [Evolution Equity Partners](#) on Jun. 16, 2025.



Global spending on cybersecurity products and services is expected to reach \$454 billion annually (USD) in 2025, up from \$260 billion in 2021.

“

Global spending on cybersecurity products and services is expected to reach \$454 billion annually (USD) in 2025, up from \$260 billion in 2021.”

Cybersecurity Ventures

“In advance of the report, we are releasing our cybersecurity market prediction today at the RSA Conference 2025 in San Francisco” says Steve Morgan, founder of Cybersecurity Ventures. For 32 years, the RSA Conference has been a driving force behind the world's cybersecurity community.

AI is expanding a \$2 trillion total addressable market or TAM (2) for cybersecurity providers, according to a

2024/2025 study by [McKinsey](#), a global management consulting firm and trusted advisor to the world's leading businesses, governments, and institutions.

“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.”

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.

“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,” says Justin Greis, Partner and North American Cybersecurity Practice Leader at McKinsey.

“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.”

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.

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.

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.

(1) Spending is actual dollars spent, or expected to be spent. The spending prediction figures from Cybersecurity Ventures includes all countries globally, B2B and B2C, plus a portion of any markets that are converged with cybersecurity such as physical security and surveillance, as well as automotive security, medical device security, military cyber defense technology, and others. It also counts in cyberinsurance policies.

(2) TAM 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. 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.

ABOUT

Cybersecurity Ventures is a leading cybersecurity market watcher and the publisher of Cybercrime Magazine, Page ONE for the global cyber economy, and a trusted source for cybersecurity facts, figures, and statistics.

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.

Malcomb Farber
Cybersecurity Ventures
+1 631-680-8660

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/807326191>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.