RSAC Cybersecurity Insights & Futures, Volume 1

For 2026, Experts Emphasize Securing AI and ML Models, and Ransomware Gangs Strike Back

For 34 years, the data that the community has purposefully shared with each other has allowed RSAC to serve as a window into the industry's future. Highlights of this first edition of RSAC™ Cybersecurity Insights & Futures include:

- Emphasis shifts from AI & ML-enabled security to securing AI & ML applications
- Interest in Agentic AI rises enormously
- Ransomware payments rebound
- Startups flood into post-quantum
- Investment in privacy bounces back
- Experts shift to combatting AI-driven cybercrime
- Focus on Zero Trust holds steady

Authors:

Laura Koetzle
Head of Community Research
RSAC

Dario Pasquini, PhD
Principal Researcher
RSAC

Chris Gates, PhD
Director, Research
RSAC

APRIL 28, 2025

RSAC: Conference and Membership

Cybersecurity is too big and complex to be solved alone. It requires a collective, global effort across all disciplines to tackle rapidly evolving threats. This is why RSAC has brought hundreds of thousands of the most diverse minds in cybersecurity together for 34 years and counting at our flagship event, RSAC™ Conference.

RSAC's mission is to unite the cybersecurity community to create a safer society. We do this through our RSAC™ Membership Platform and our annual Conference. RSAC Conference is the largest and most influential event in the cybersecurity industry, bringing together industry leaders, researchers, and innovators to discuss the latest advancements and challenges in cybersecurity.

RSAC Conference is comprised of four very important components:

1. Carefully curated educational presentations
2. Innovation programming and contests
3. Exhibitors who offer products and services to enterprises, governments and individuals that help them address cybersecurity challenges
4. A vibrant community of cyber professionals who engage and learn together

The Data That Inspired This Report

RSAC Conference selects presentations through a rigorous process. Our independent Program Committee is comprised of 150+ cybersecurity experts from enterprise, government, academia, and the vendor community, who evaluate submissions based on relevance, originality, and impact. All content selected for the program must meet strict neutral and educational guidelines. In 2025, **more than 2,800 submissions** were received from the cybersecurity community across the globe through our Call for Submissions process.

Additionally, RSAC Conference has become a launchpad for groundbreaking cybersecurity startups through initiatives like the RSAC™ Innovation Sandbox (ISB) contest, which has helped emerging companies secure funding and gain industry recognition. This environment fosters innovation, making it a key destination for companies looking to showcase cutting-edge security solutions. 2025 is the 20th anniversary of the ISB and **more than 200 submissions** were received from across the globe to vie for an opportunity to be a Top 10 Finalist and ultimately one declared winner.

RSAC 2025 Conference has **more than 600 exhibitors**, from start-ups to well-established platform providers. We offer RSAC™ Early Stage Expo for up and comers in the industry; RSAC™ Next Stage for rapidly growing start-ups; and a sprawling Expo with innovative solution providers from across the world.

Why We Created This Report

This vibrant community has grown into the convening authority of the cybersecurity industry. Through reports like this, we aim to educate and empower the community to stay ahead of emerging threats—and to inspire and support one another in times of need. Everything we do is for the community and by the community, to enable collaboration and foster growth.

Who We Serve

The RSAC™ Community is represented by:

140+ Countries

4,500+ Contributing Experts

40,000+ Annual Conference Participants

Global 1000 Security Executives

Senior Government Decision-makers

Top Anti-fraud Executives

Innovation Sandbox Participants Boasting $16.4B in Investments*

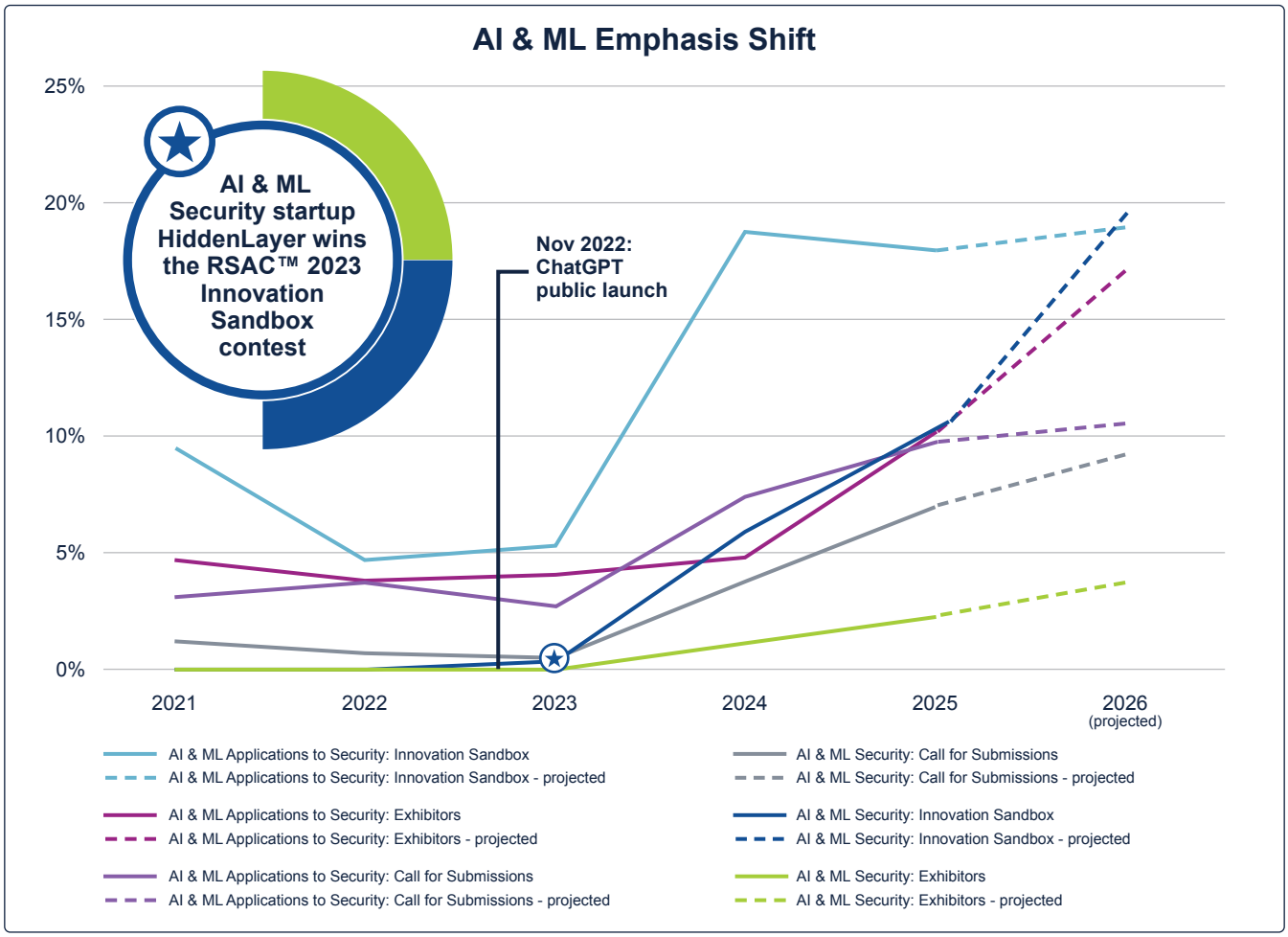
*Source: Crunchbase

In this report, we synthesize several years of the community's Call for Submissions, Innovation Sandbox, Exhibitor, and session attendance data and use our RSAC™ Cybersecurity Atlas toolset to illuminate counterintuitive trends and to predict the industry's course through 2026.

In 2023, we saw the beginning of a shift in emphasis by startups from building AI & ML applications for security tasks to securing the AI & ML applications themselves… Looking back on the shifts between these two topics[1] helps us predict future developments across the industry as a whole. For example, we had several "AI & ML Applications to Security" submissions for the RSAC Innovation Sandbox contest in 2021 and 2022, and "AI & ML Security" startups started to make waves in the contest in 2023. Indeed, the Innovation Sandbox judges selected "AI & ML Security" startup HiddenLayer as the RSAC 2023 Innovation Sandbox winner, which doubtless contributed to the interest in the space along with the fast uptake of ChatGPT after its first public launch in November 2022. Further, nearly 11% of Innovation Sandbox proposals in 2025 focused on "AI & ML Security," up from 6% in 2024.

Definitions:
- **"AI & ML Applications to Security": Using AI and ML to perform security functions**
- **"AI & ML Security": Securing the AI & ML applications themselves**

…And that shift among cybersecurity community experts accelerated in 2024 and solidified in 2025. In the RSAC Call for Submissions, we saw an early group of nearly 1.3% of entries on "AI & ML Security" in 2021 (but that was less than half of the nearly 3.3% already devoted to "AI & ML Applications to Security" that same year), followed by declines in 2022 and 2023 to as little as 0.7%. The share of Call for Submissions "AI & ML Security" proposals for 2024 then jumped to nearly 4%, and rose again to 7.1% in 2025. The "AI & ML Applications to Security" submissions grew more slowly during that period, accounting for nearly 7.7% of the total in 2024 and just shy of 10% in 2025.



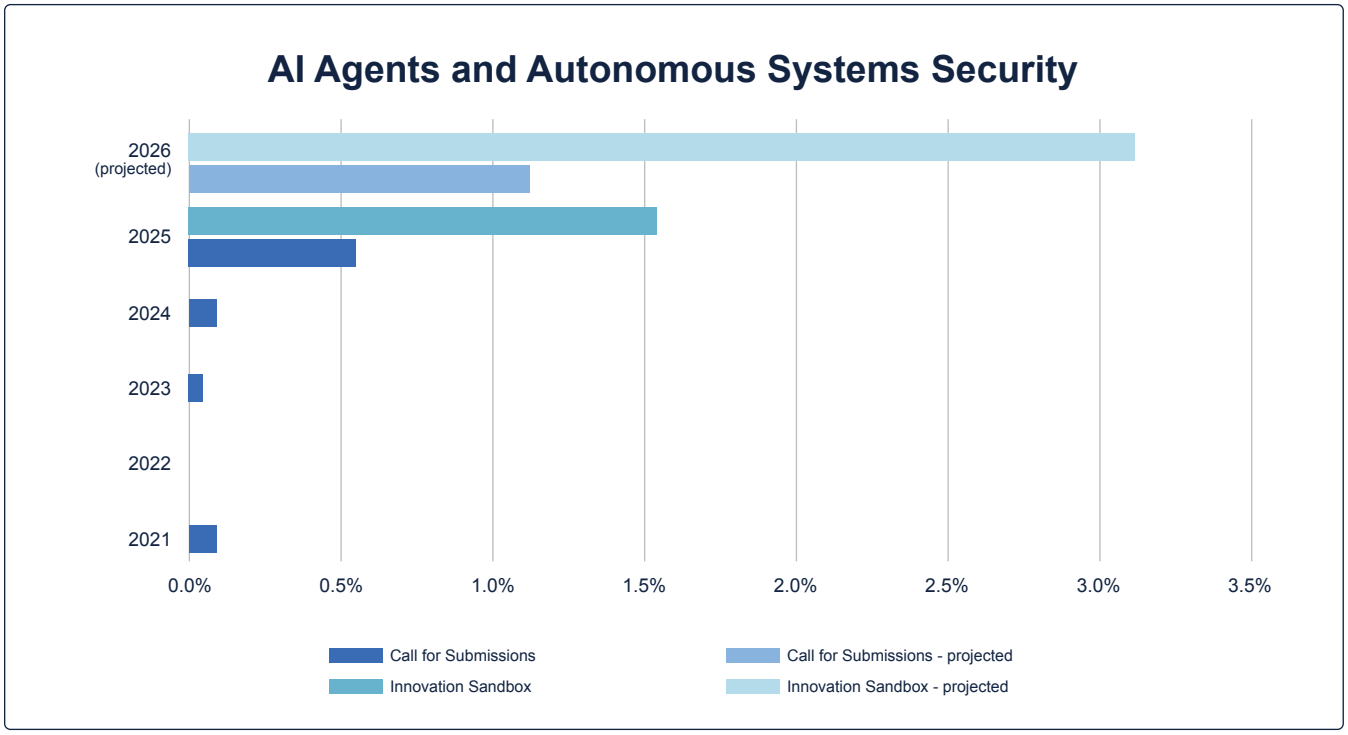
Established cybersecurity suppliers doubled down on AI & ML applications for security tasks. The percentage of mainstream "AI & ML Security" exhibitors at RSAC Conference jumped from 1.1% in 2024 to 2.3% in 2025. In contrast, around 4% of exhibitors promoted their "AI & ML Applications to Security" solutions every year from 2021-2023, with a bump to nearly 5% in 2024. And in 2025, the share of "AI & ML Applications to Security" exhibitors more than doubled, to more than 10.5%.

In 2026, RSAC expects those trends to continue: more startups will pile into securing AI & ML applications, and nearly 17% of exhibitors will vie to apply AI & ML to everything. Given the rapid evolution of large language models (LLMs), we expect growth in RSAC Call for Submissions proposals from the cybersecurity community on "AI & ML Security" to outpace growth in "AI & ML Applications to Security" entries in 2026. Further, RSAC predicts that the share of "AI & ML Security" startups will narrowly outstrip the percentage of "AI & ML Applications to Security" entries in the 2026 edition of the RSAC Innovation Sandbox contest. We expect the percentage of "AI & ML Security" exhibitors to rise to more than 4% at RSAC 2026 Conference, but they'll be greatly outnumbered by the suppliers of AI & ML solutions to every conceivable security problem, who will account for nearly 17% of the total.

Nearly 20% of RSAC™ 2026 Innovation Sandbox competitors will be "AI & ML Security" startups.

"AI Agents and Autonomous Systems Security" appeared from (almost) nowhere in 2025, and we expect it to double its share of both expert submissions and startups in 2026. Given their ubiquity in Q2 2025, it's easy to forget that powerful, autonomous AI Agents are a very new challenge for most of the cybersecurity community. But our data tells the story—vanishingly few experts were focused on "AI Agents and Autonomous Systems Security" (now often referred to as "Agentic AI Security") until the 2025 Call for Submissions, when its share of entries leaped to 0.6%. And the percentage of Innovation Sandbox startups tackling Agentic AI security challenges also skyrocketed in 2025, to nearly 1.6% of the total. Because autonomous agents are a fertile area for technology and productivity improvement, RSAC expects that more than 3% of Innovation Sandbox contestants and nearly 1.2% of Call for Submissions proposals in 2026 will focus on Agentic AI Security.

In 2026, Agentic AI Security's shares of both RSAC™ Call for Submissions and Innovation Sandbox entries will at least double.

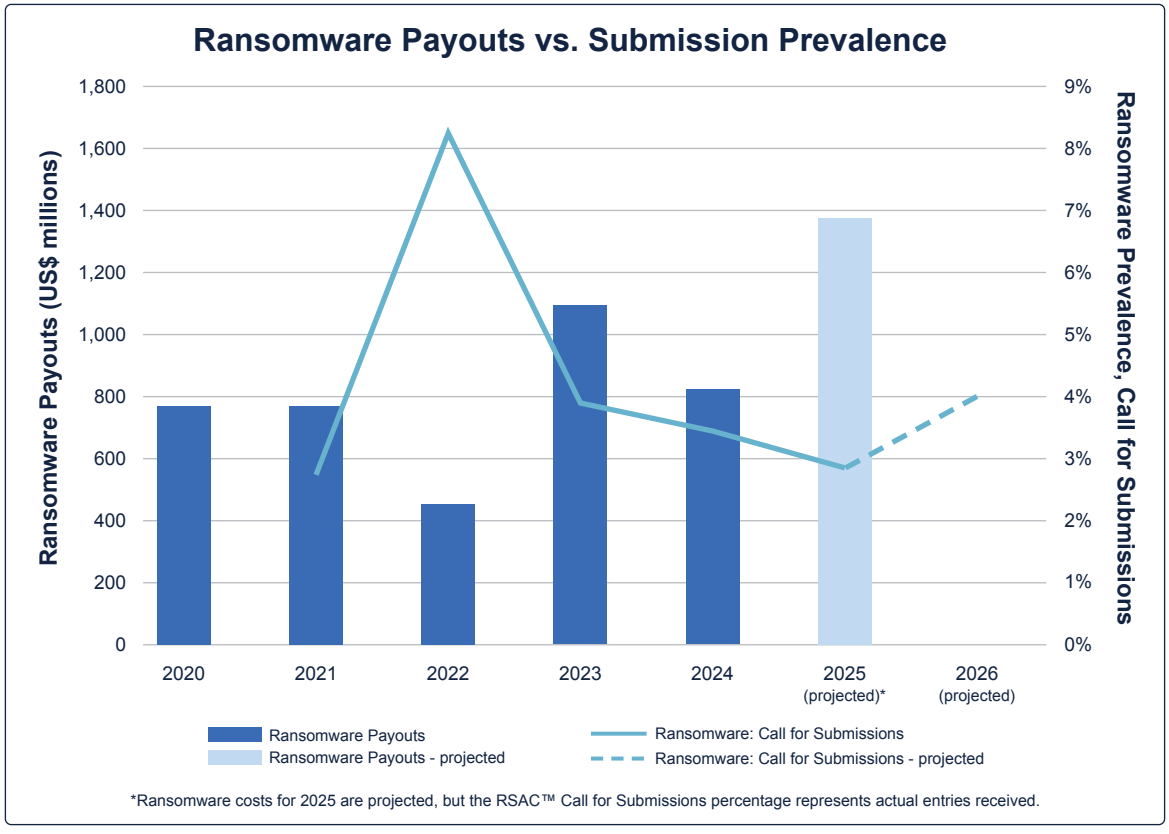


The emphasis on ransomware at RSAC Conference has declined significantly since its most recent peak in 2022. Whereas 8.2% of our RSAC 2022 Call for Submissions entries centered on ransomware, less than 3% of the submission pool focused on ransomware in 2025. At first glance, that seems strange when we look back on the rapid proliferation of ransomware incidents during this period; there were approximately 2,600 documented attacks in 2022, 4,506 in 2023, and 5,414 in 2024.[2] However, when we consider that cybersecurity teams have developed considerable expertise at applying many of the best practices for dealing with ransomware—including network segmentation, isolated backups, regular exercises, and establishing decision trees on whether (and in which situations) an organization will pay a ransom—this makes sense.

Dealing with ransomware has become an established part of cybersecurity defense, and ransomware payouts declined meaningfully in 2024. And experts are diving further into those strategies for practical ransomware defense; in the 2025 Call for Submissions proposals, interest in Zero Trust network segmentation rebounded from its 2024 low. And in 2025, the share of submissions on enhancing tabletop exercises rose to its peak for the 2021-2025 period. Today, cybersecurity professionals have many tools that they can use to help mitigate the damage of ransomware attacks. And happily, enterprises and their partners in law enforcement succeeded in stemming the financial impact of ransomware in 2024; total ransoms paid declined from an estimated US $1.1B in 2023 to US $814M in 2024.[3]

But that positive trend won't last; we predict higher ransomware payment totals in 2025 and an uptick in expert interest in 2026. Why the gloom and doom? Because in cybercrime, past is often prologue; the industry also saw a decline in ransomware payouts between 2021 (US $766M) and 2022 (US $457M) prior to that high of US $1.1B in 2023.[4] January 2025 saw a record number of reported ransomware attacks (590), which is 34% higher than the monthly average for 2024.[5] As such, RSAC predicts that the overall unhappy pattern will continue: the number of ransomware attacks will continue to rise, ransomware payments will rebound to more than $1.3B in 2025, and we'll see a small upswing in 2026 Call for Submissions proposals about ransomware.

Entries on ransomware will rebound to 4% of the RSAC™ 2026 Call for Submissions total.



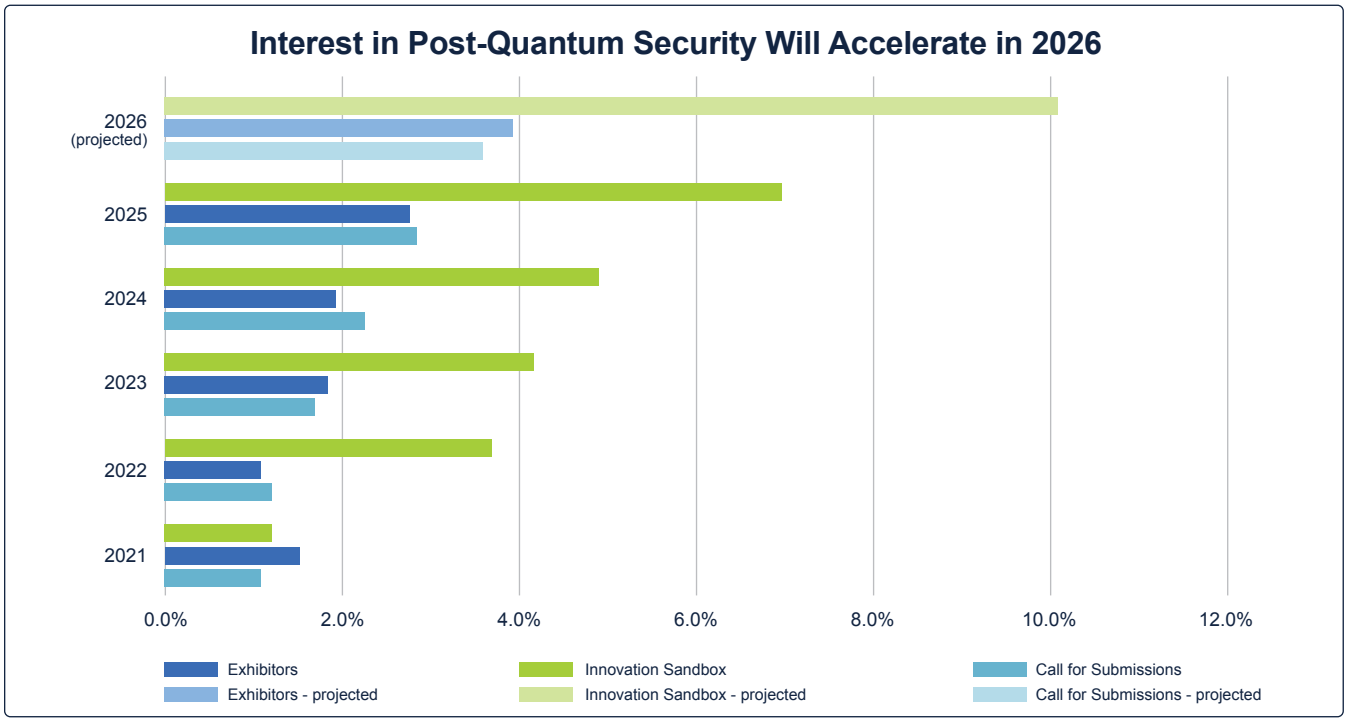
After a busy 12 months in post-quantum cryptography heading into RSAC 2024 Conference… Interest in post-quantum security has grown steadily, climbing from just 1.2% of RSAC Call for Submissions entries in 2021 to 2.2% in 2024. At RSAC 2024 Conference in May, the community had just emerged from a 10-day roller-coaster ride with a paper claiming to have rendered lattice-based cryptosystems vulnerable to quantum attack, and the swift discovery of a bug in the paper's algorithm rendering those claims invalid. Hence, it's unsurprising that experts from organizations with 50,000-plus employees who attended RSAC 2024 Conference were 72% more likely than the average attendee to spend time diving into postquantum cryptography.

…Engagement with post-quantum security has continued to grow, and we predict an acceleration in 2026. In August 2024, the US's National Institute for Standards and Technology (NIST) released its first three finalized post-quantum encryption standards. So it's no surprise that for RSAC 2025 Conference, 2.7% of Call for Submissions proposals, more than 5% of 2025 Innovation Sandbox startups, and nearly 2.7% of exhibitors focused to a substantial degree on post-quantum security. And RSAC expects this trend to accelerate; in 2026, we estimate that post-quantum security will drive nearly 3.6% of Call for Submissions entries—plus more than 10% of Innovation Sandbox startups—and be a selling point for nearly 4% of exhibitors in 2026.

Post-quantum security will account for nearly 3.6% of RSAC™ Call for Submissions entries and 4% of exhibitors in 2026.

Experts have become *less* interested in cryptocurrency and blockchain since 2023... They see cryptocurrency as a vehicle for fraud and ransom payments, and blockchain as a solution to fewer problems than thought. The cybersecurity community's interest in cryptocurrency and blockchain has never been enormous—2023 was the high-water mark, with 1.4% of Call for Submissions proposals featuring blockchain, cryptocurrency, or associated terms, and that percentage declined to under 0.5% in 2024 and to less than 0.2% for 2025. The RSAC 2025 Innovation Sandbox contestants focused on cryptocurrency, blockchain, or Web3 emphasize their work in identifying vulnerabilities in the smart contracts used to create and manage cryptocurrencies and other types of tokens. And note that RSAC is one place you'll never see "cryptocurrency" shortened to "crypto"; cryptography was here first.

RSAC™ 2024 Conference attendees from the largest firms were 72% more likely than average to prioritize post-quantum.

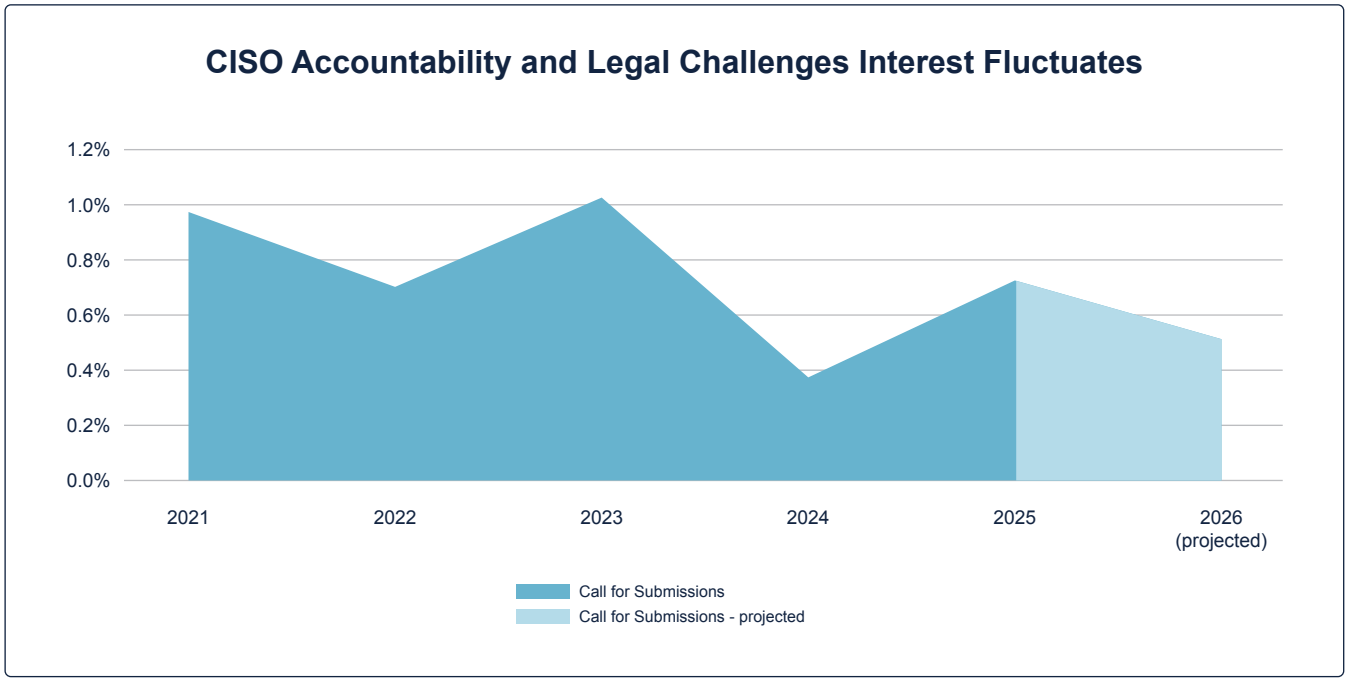


…And that interest level won't change much in 2026, with one exception: smart contracts. RSAC believes that the 2025 Innovation Sandbox submissions that focused on smart contracts are a harbinger of things to come for 2026 and beyond. Cryptocurrencies have already invaded the mainstream financial system—any retail investor can now buy shares in a bitcoin exchange-traded fund (ETF). Further, the current US administration's enthusiasm for cryptocurrencies (and disinclination to apply securities regulation to them) will lead to more mainstream financial institutions providing "picks and shovels" services to investors and companies seizing on what they hope will be another cryptocurrency gold rush. This means that more application security experts at those financial firms will need to check those smart contracts for both logical and coding errors.

Emphasis on handling CISOs' personal accountability for cybersecurity breaches has fluctuated since 2021…The percentage of RSAC Call for Submissions entries focused on "CISO Accountability and Legal Challenges" peaked in 2021 with just shy of 1% of proposals, and then again in 2023 with just over 1%. That 2021 spike was driven by US government investigations of data security incidents at firms like Equifax and Uber that resulted in individual criminal prosecutions of technology and cybersecurity executives. The high-water mark in Call for Submissions entries in 2023 related to CISO legal accountability isn't surprising given that the US Securities and Exchange Commission (SEC) proposed regulation requiring individual liability for CISOs for cybersecurity failures in March 2022.

…Paralleling ups and downs in litigation, regulation, and enforcement. Two important things happened well before the submission deadline for RSAC 2024 Conference: a) the SEC formally adopted its new cybersecurity rules; and b) the EU's update to the Network and Information Security directive (NIS2)—which also imposes some personal liability for corporate officers who fail to insure compliance—came into force. Hence, it's difficult to explain both the decline in interest in CISO legal accountability in 2024 to less than 0.4% of Call for Submissions proposals and the fact that C-Level attendees at RSAC 2024 Conference were just 7% more likely than average attendees to join those

Timeline: CISO Accountability Legislation and Regulation, 2020-2025

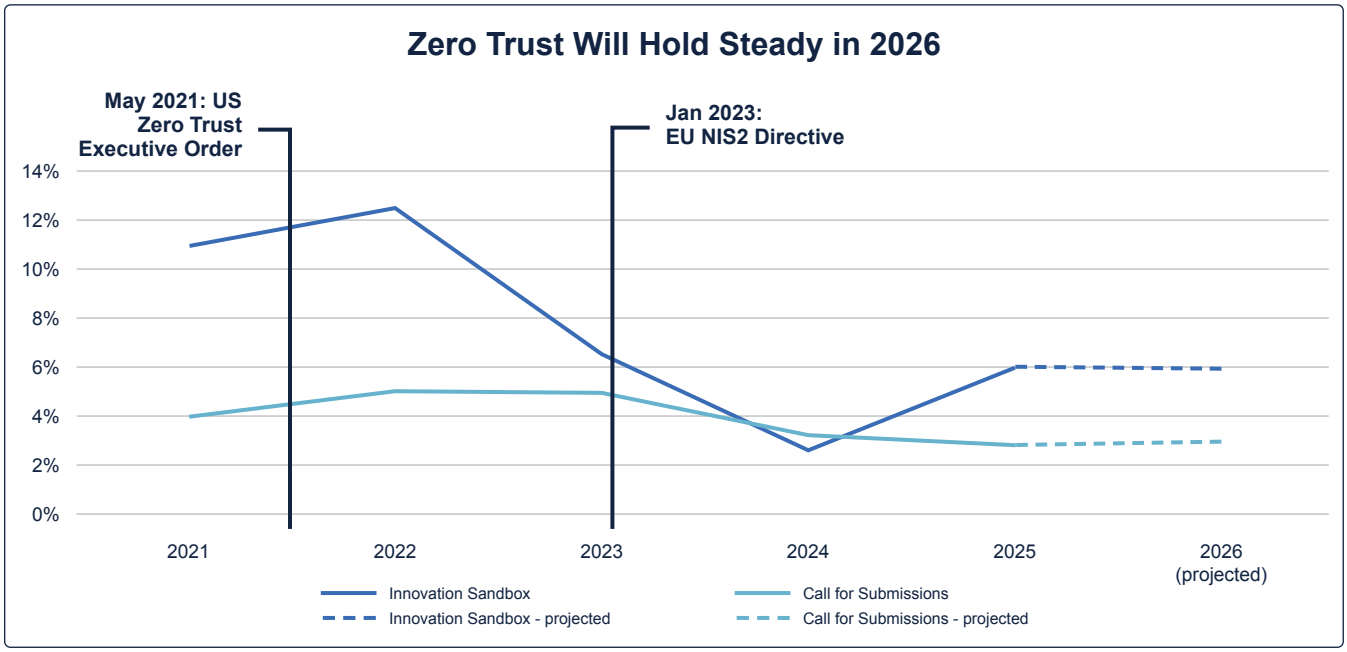


sessions. But the rebound in "CISO Accountability and Legal Challenges" Call for Submissions entries for RSAC 2025 Conference makes sense, given that the court allowed some of the charges against SolarWinds CISO Timothy Brown to proceed in the SEC v SolarWinds lawsuit, and that the EU deadline for transposing the NIS2 Directive into national law was in October 2024.

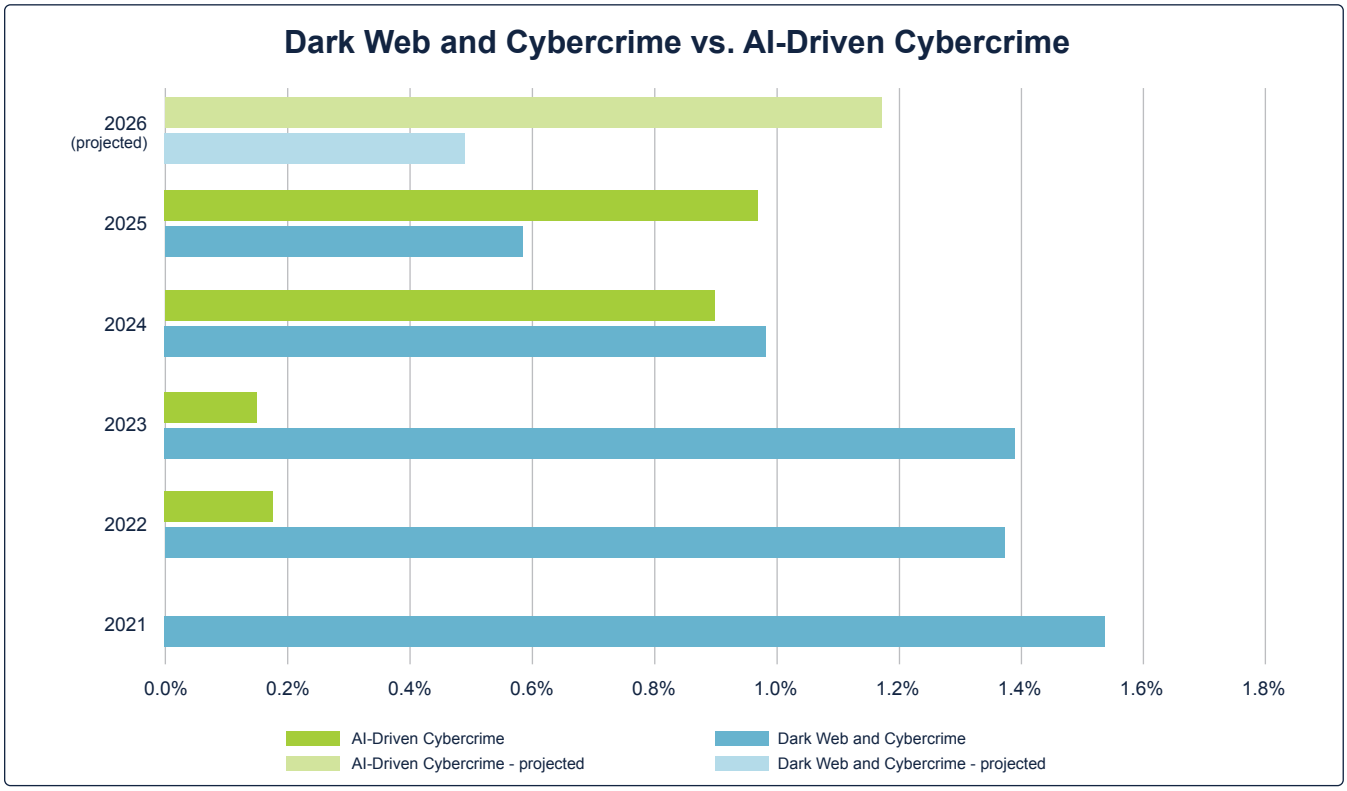
We expect less focus on CISOs' personal accountability in the US in 2026 because of changed SEC enforcement priorities, while interest by CISOs with liability under the NIS2 Directive will continue. Because many signs as of Q2 2025 point to the US SEC narrowing its cybersecurity enforcement focus and a higher threshold for what it will consider material cybersecurity disclosures, we're likely to see a decline in emphasis from US experts and CISOs on "CISO Accountability and Legal Challenges" at RSAC 2026 Conference. However, because all the EU member states who missed the October 2024 deadline will have successfully enshrined the NIS2 Directive in national law and begun enforcement by mid-2025 at the latest, cybersecurity experts and CISOs with NIS2-subject European operations will continue to be concerned about minimizing personal liability risk. Thus, we expect to see 0.5% of Call for Submissions proposals for 2026 focus on "CISO Accountability and Legal Challenges."

The share of RSAC™ 2026 Call for Submissions entries focused on CISOs' personal liability will fall to just 0.5%.

Zero Trust isn't going anywhere—in 2025, community experts are working on Zero Trust and AI Integration, and RSAC expects a similar level of investment in 2026. Forrester Research introduced the Zero Trust model in 2010, and a 2021 US Executive Order required government departments to work towards a Zero Trust architecture (the latter of which drove the 2022 peak in Zero Trust Call for Submissions and Innovation Sandbox entries). Between 2010 and 2021, Zero Trust evolved from a concept to an architecture implementable with off-the-shelf cybersecurity products. The ideas behind Zero Trust haven't changed, and they've proven extensible to a set of challenges no one was contemplating 15 years ago. For example, the "Zero Trust and AI Integration" Subtopic nearly doubled its share of Call for Submissions proposals between 2024 and 2025, and the percentage of Innovation Sandbox startups focused on Zero Trust bounced back to nearly 6% of the total in 2025. Given that the US Executive Order on Zero Trust remains, and that the EU's NIS2 Directive also requires essential entities to adopt Zero Trust principles, RSAC expects the cybersecurity community's level of commitment to Zero Trust in 2025 to continue through 2026.

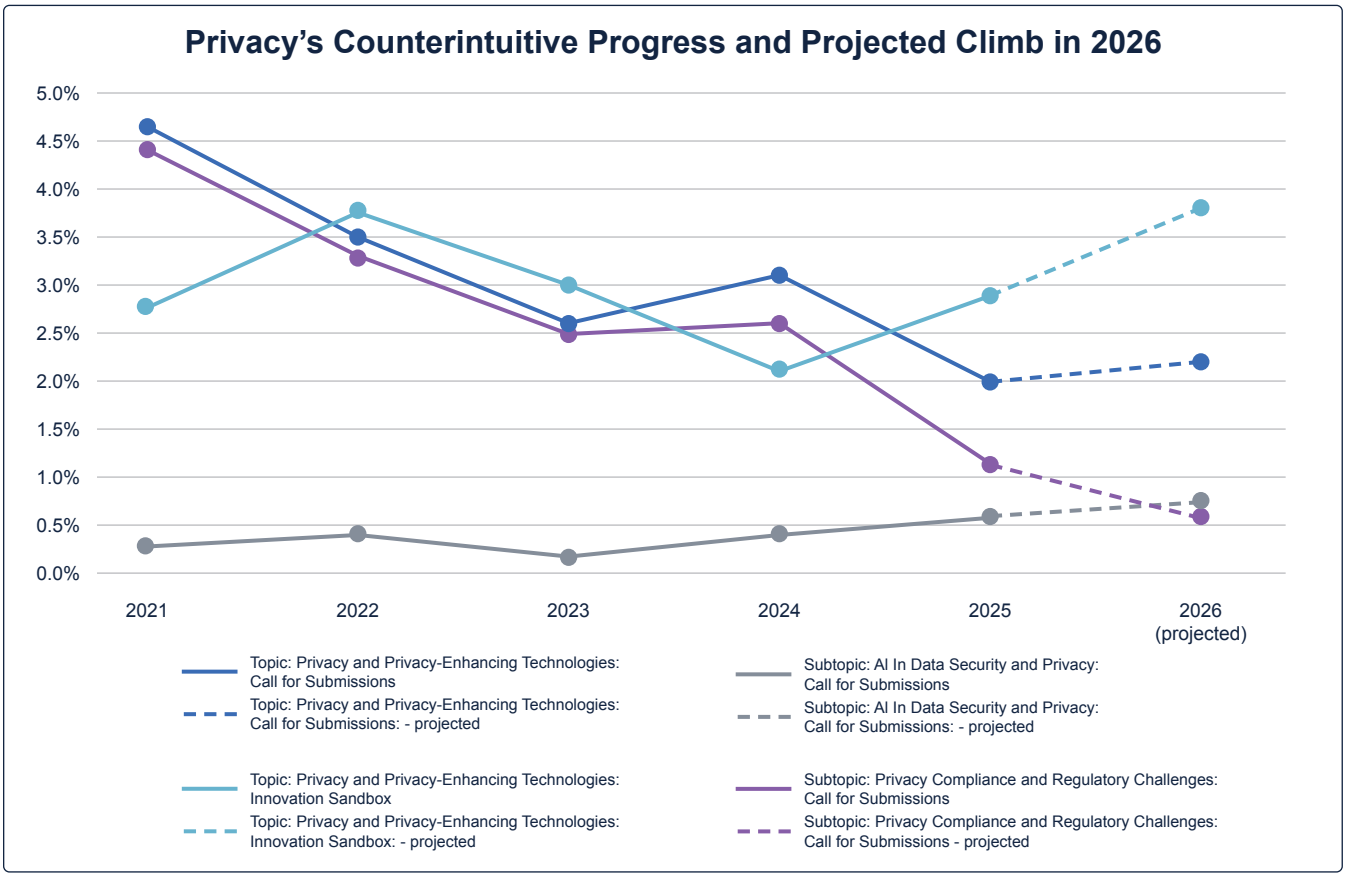


Cybersecurity experts have shifted resources from patrolling the Dark Web to combatting AI-driven cybercrime, and that move will accelerate in 2026. Nearly 1.4% of RSAC 2022 Call for Submissions entries focused on the "Dark Web and Cybercrime," while just one (total) of those proposals zeroed in on "AI-Driven Cybercrime"—and that was a demonstration of how Deepfakes could be used to commit insurance fraud. But then the LLMs that launched a thousand phishing emails exploded onto the scene in November 2022. Hence, for RSAC 2025 Conference, concern about AI-driven cybercrime grew to nearly 1% of submissions, while entries related to the Dark Web and cybercrime declined to less than 0.6% of the total. In 2026, we expect investment in combatting AI-driven cybercrime to rise again, to nearly 1.2% of entries, while interest in the Dark Web side will continue to level off.



RSAC's data reveals a counterintuitive trajectory for interest in privacy—but in 2026, we expect healthy growth in privacy startups. Given the steady drumbeat of regulatory and technical developments in privacy since the EU began enforcing the General Data Protection Regulation (GDPR) in 2018, we'd have expected privacy's share of RSAC Call for Submissions proposals to have been consistent (and high) from 2021-2025. But the data proves that assumption wrong—we started at nearly 4.6% in 2021 and it's fallen steadily each year to less than half that level in 2025. This decline is almost entirely due to decreased focus on "Privacy Compliance and Regulatory Challenges"—those entries accounted for more than 4.4% of Call for Submissions entries in 2021, but that percentage plummeted to just 1.2% of the total in 2025. Some of that plunge has been offset by an increase in interest in areas like "AI in Data Security and Privacy," but not nearly all. Interestingly, the RSAC Innovation Sandbox startups come a lot closer to following the pattern we'd anticipated; they started at 2.7% in 2021 and have fluctuated up and down to land at more than 2.9% in 2025. In 2026, RSAC predicts: 1) a modest rise in the share of Call for Submissions proposals devoted to privacy, driven primarily by developments in AI and privacy; and 2) sizeable growth in the percentage of Innovation Sandbox startups focused on privacy, to more than 3.8%.

Privacy startups will account for more than 3.8% of the total for RSAC™ 2026 Innovation Sandbox.



Even with the best possible data and analysis, predictions are never 100% accurate, especially in a volatile field like cybersecurity. RSAC looks forward to evaluating our predictions for 2025 and 2026 with the benefit of hindsight; we'll highlight the things we got right and analyze the areas where we went wrong. RSAC™ Members can expect new editions of RSAC Insights & Futures regularly that will feature exclusive data like this and original research. And RSAC Members who'd like to explore some of our data for themselves can access the RSAC™ Cybersecurity Atlas toolset.

RSAC Cybersecurity Insights & Futures, Volume 1: Summary of Predictions
Growth in RSAC Call for Submissions entries on “AI & ML Security" will outpace growth in "AI & ML Applications to Security" proposals in 2026.
Nearly 20% of RSAC Innovation Sandbox competitors will be “AI & ML Security” startups in 2026, while “AI & ML Applications to Security” startups will account for almost 19%.
More than 4% of RSAC 2026 Conference exhibitors will focus on “AI & ML Security,” while nearly 17% will promote “AI & ML Applications to Security” solutions.
The shares of both Call for Submissions and Innovation Sandbox entries about Agentic AI Security will at least double for RSAC 2026 Conference.
Ransomware payouts will rebound to more than US $1.3B in 2025.
Entries on ransomware will snap back to 4% of the 2026 Call for Submissions total.
Experts will spend more time with smart contracts in 2026, but interest in blockchain and cryptocurrencies will remain low.
Post-quantum security will account for nearly 3.6% of Call for Submissions proposals, more than 10% of Innovation Sandbox startups, and 4% of exhibitors in 2026.
The share of Call for Submissions entries focused on CISOs’ personal liability will fall to just 0.5% in 2026.
RSAC expects the cybersecurity community's level of commitment to Zero Trust in 2025 to continue through 2026.
Privacy’s share of Call for Submissions proposals will rise modestly to 2.1% in 2026.
The percentage of privacy-focused competitors in Innovation Sandbox will rise more sharply to 3.8% in 2026.
RSAC expects investment in combatting AI-driven cybercrime to grow again, to nearly 1.2% of 2026 Call for Submissions entries, while interest in patrolling the Dark Web continues to level off.

Endnotes

1 RSAC chose the list of the top-level Topics by drawing from those used in our content Library and those extracted from the Call for Submissions data by RSAC’s LLMs. RSAC’s LLMs assign each Call for Submissions entry to the best-fit Subtopic.

2 Ransomware attack totals: 1) 2022: Institute for Security and Technology2022 RTF Global Ransomware Incident Map: Attacks continue worldwide, groups splinter, education sector hit hard - Institute for Security and Technology; 2) 2023: Ransomware_Attacks_Surge_in_2023.pdf; 2024: Ransomware Annual Report 2024

3 Ransomware payout totals: 1) 2017-2023: Annual ransomware payments global 2023 | Statista; 2) 2024: Ransomware payments declined in 2024 despite massive. well-known hacks - Ars Technica

4 Ransomware payout totals: 1) 2017-2023: Annual ransomware payments global 2023 | Statista

5 January 2025 ransomware attack total: Record number of ransomware attacks in January 2025

RSAC Cybersecurity Insights & Futures, Volume 1 | April 28, 2025

We look forward to bringing you many more reports like this one.
Visit the library in the RSAC Membership Platform for additional cybersecurity resources.

RSAC
Cybersecurity, Together™

OneRSAC.com