CROWDSTRIKE

STATE OF AI IN CYBERSECURITY SURVEY

CrowdStrike commissioned a survey of over 1,000 cybersecurity professionals to learn their thoughts on GenAI

Table of Contents

How Your Peers Are Thinking about GenAI

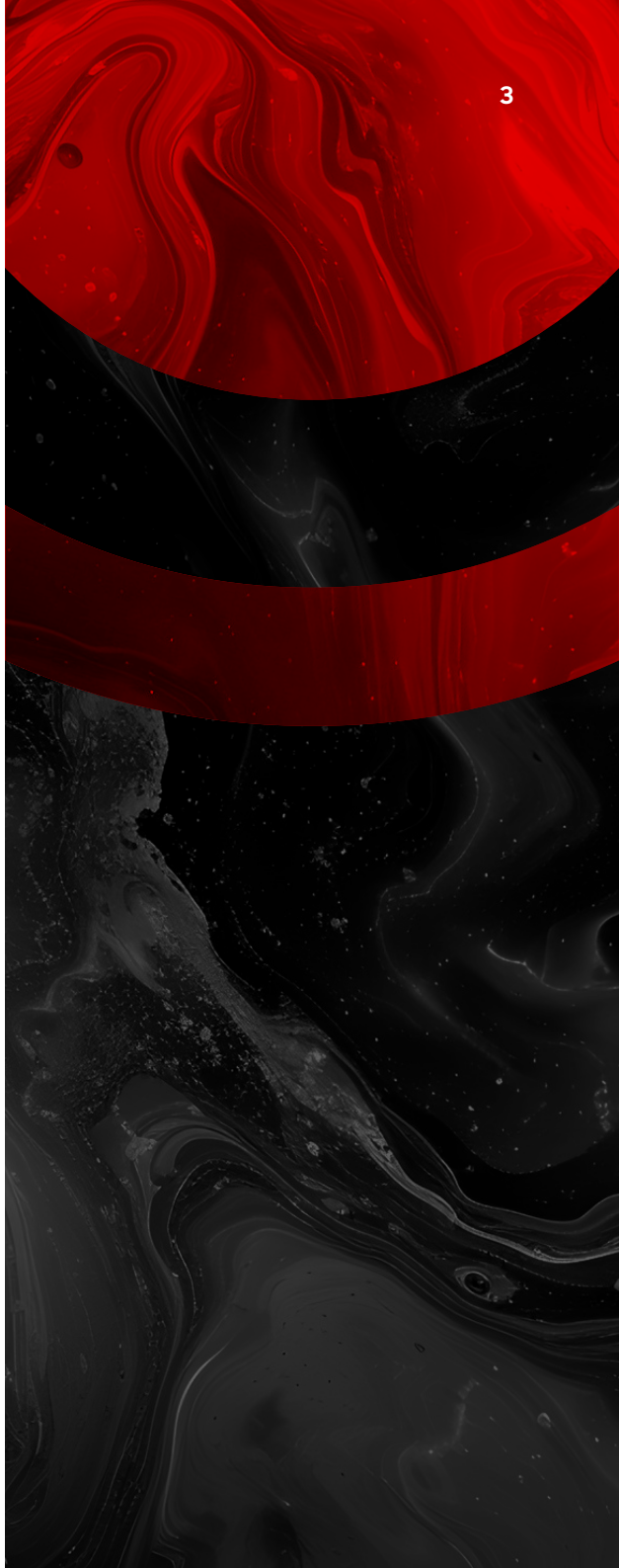
The pressure is mounting for security teams. As adversaries become faster and stealthier, security teams must adapt to stay ahead.

The emergence of generative AI (GenAI) has the potential to help them do just that. With its unique capabilities for natural language processing and synthesizing large amounts of data, GenAI can help security teams improve data awareness across silos and operate their security tools with greater proficiency. Many security leaders recognize its potential, with some going so far as to mandate AI adoption across their operations.

At the same time, the hype has reached a fever pitch. The avalanche of conversation and content about GenAI has made it hard for security teams to understand what's possible and what's not. Misconceptions abound.

To help organizations navigate this uncertainty, CrowdStrike surveyed over 1,000 global cybersecurity leaders and practitioners on their key criteria shaping GenAI adoption, perceptions of current GenAI offerings and overall sentiment on GenAI.

With speculation swirling in the market, this survey reveals how security teams are *actually* thinking about GenAI — and the results might surprise you.



Top 5 Takeaways

1. **Security teams want a platform-based approach**
   80% of respondents prefer GenAI delivered through a cybersecurity platform (versus a point solution).

2. **GenAI must be purpose-built for cybersecurity**
   76% of respondents prefer GenAI tools purpose-built for cybersecurity, as opposed to domain-agnostic tools.

3. **It's about augmentation, not replacement**
   Respondents overwhelmingly believe GenAI will ultimately optimize the analyst experience, not replace human labor.

4. **Measurable ROI is a top priority**
   The top economic concern about GenAI isn't about cost — it's about providing a measurable ROI.

5. **Safety and privacy remain top concerns**
   Wary of GenAI risks, users ranked safety and privacy guardrails among the top features they want to see in GenAI tools.

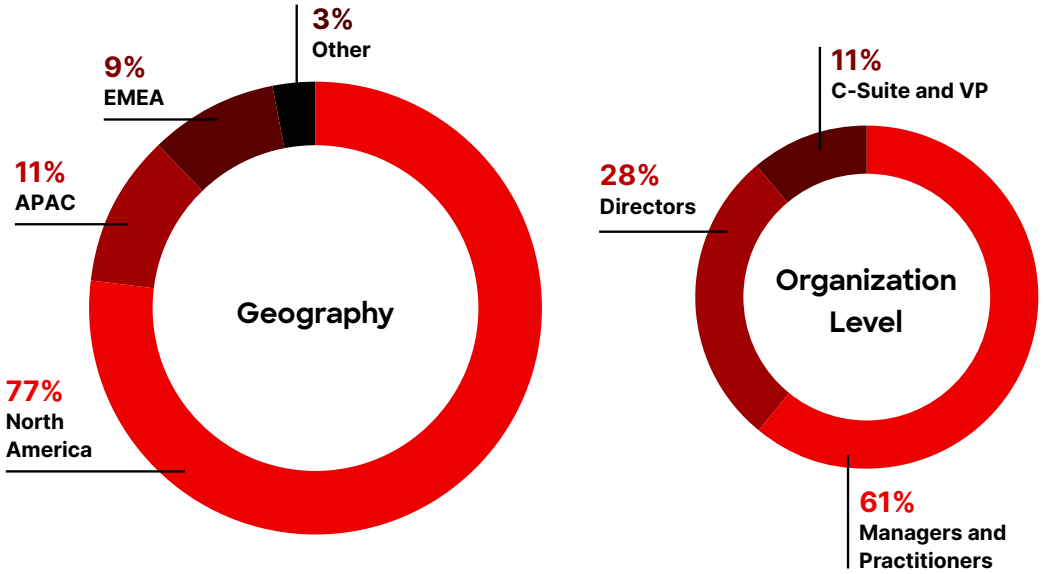
Survey Methodology

CrowdStrike worked with research firm ViB to survey 1,022 global cybersecurity and IT professionals in June and July 2024. Questions centered on perceptions, attitudes and concerns toward GenAI cybersecurity offerings. Respondents were also asked about their purchase drivers, decision criteria and current buying journeys for GenAI. In total, 31 questions were asked. CrowdStrike analyzed the responses to provide this document highlighting trends and key findings.

What is GenAI?

Generative artificial intelligence (GenAI) in cybersecurity refers to AI systems that can create new content — such as threat detection patterns, automated incident response playbooks and phishing email simulations — by learning from vast datasets. The technology can be delivered through embedded product features or conversational interfaces such as assistants or chatbots.

Audience Statistics

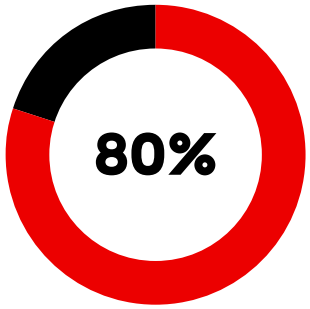


Primary Industry

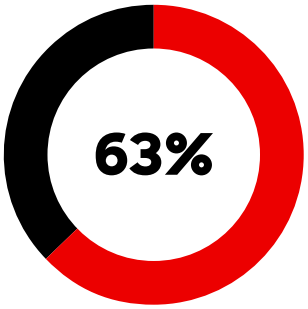
- Manufacturing
- Business Services
- Healthcare
- Telecommunications
- Colleges and Universities
- Insurance
- Media and Internet
- Retail
- Government (State and Local)
- Transportation

KEY FINDING 1

A Platform-Based Approach Is Preferred



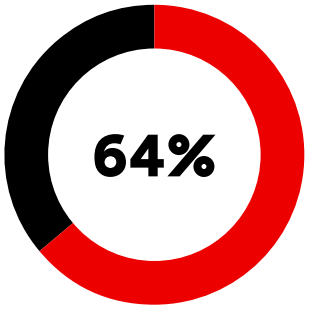
prefer GenAI delivered through a platform (versus point solutions)



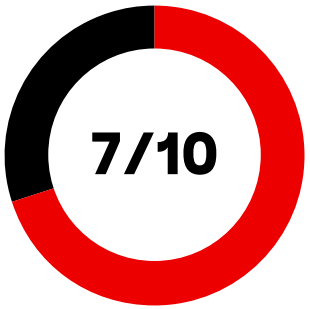
would change security vendors to use the GenAI of another vendor

#1

preferred feature: GenAI tool integration

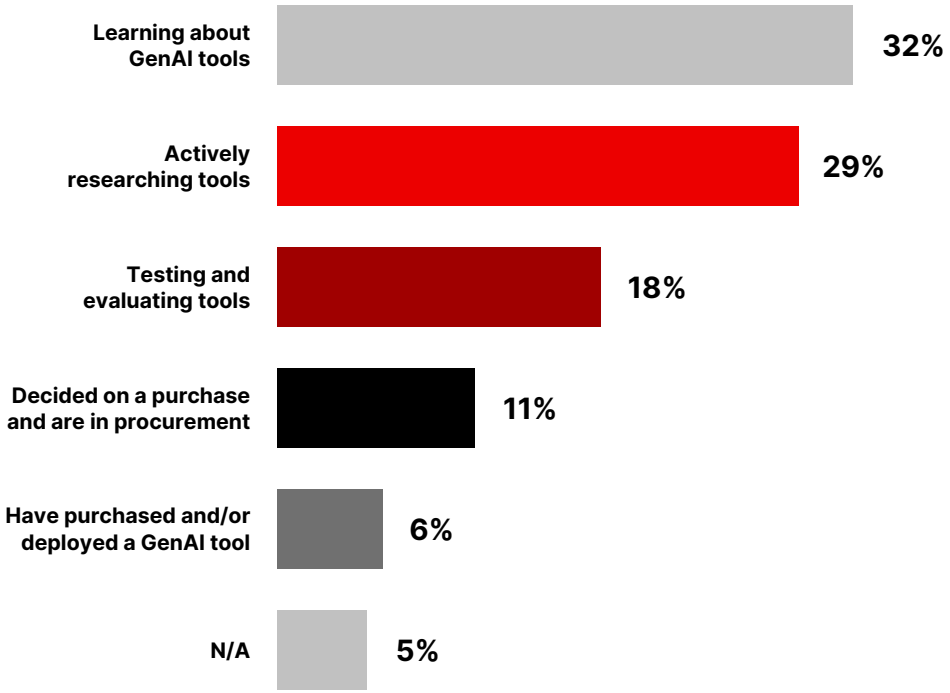


of respondents are researching GenAI tools or have already purchased one



intend to make a purchase in the next 12 months

How far along are cybersecurity professionals in their GenAI buying journeys?



Early stages of adoption

Respondents acknowledge that GenAI remains in its infancy, but feel confident enough to initiate the buying journey. Almost **two-thirds (64%) are researching GenAI tools** or have already purchased one. Of those who have started their GenAI buying journeys, nearly **7 in 10 (69%) intend to make a purchase in the next 12 months.**

Integration is the top priority

When considering a GenAI purchase, the top-ranked capability *and* leading operational concern for organizations is **how GenAI integrates with existing security tools.** These results show how GenAI's value is linked to how well it works within the broader technology ecosystem.

GenAI drives platform preference

Nearly **two-thirds (63%) of respondents said their organization would consider overhauling their security tools** to use the GenAI tools of another vendor. GenAI is seen as not only an accessible interface to security tools but a capability that can help teams extract deeper insights and more value across tools — making it a decisive factor when choosing security platforms.

Why platform matters

A platform-based approach to cybersecurity integrates multiple tools, data and processes into a unified system. When delivered as an integrated component of a platform, GenAI can accelerate and augment the benefits of a platform approach. It can streamline onboarding, enabling analysts to get up to speed faster and interact with their tools in a more intuitive way (such as by using natural language). Delivering GenAI through a platform can also simplify procurement and deployment complexities, facilitating more seamless adoption.

KEY FINDING 2

Security Teams Want GenAI Built by Cybersecurity Experts

Breach prevention remains a top priority

74% of respondents have either been breached in the previous 12-18 months or are worried they may be vulnerable to a breach. Perhaps not surprisingly, the majority of respondents cited their primary motivation for considering GenAI tools is to better detect and respond to attacks. This motivation outranked widely speculated drivers for AI adoption, including skills shortages (12%) and leadership mandates (10%).

Cybersecurity expertise beats general AI leadership

When selecting a GenAI tool, **respondents prioritize vendors with deep cybersecurity expertise**, strong incident response capabilities and leadership in threat intelligence. These factors outweigh more general AI leadership, such as a vendor's investment in AI research or partnerships with large language model providers.

Purpose-built GenAI for cybersecurity

The emphasis on breach prevention and vendor expertise suggests security teams would avoid domain-agnostic GenAI tools, which may lack the specialized context required to provide actionable assistance in alignment with security best practices. **83% of respondents said they would not trust tools that provide unsuitable or ill-advised security guidance.**

Top 3 purchase drivers for GenAI security

- #1 To improve my organization's ability to detect and respond to attacks
- #2 To improve my organization's operational efficiency
- #3 To mitigate the impact of skills shortages

Top 3 vendor selection criteria

- #1 Validated leadership in cybersecurity
- #2 Expertise in incident response
- #3 Vendor-led threat intelligence research

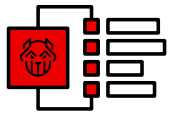
Top 3 target security outcomes

- #1 Faster mean time to respond
- #2 Improved detection fidelity
- #3 Reduced risk exposure

KEY FINDING 3

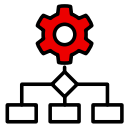
The Robots Will Augment Us, Not Replace Us

Top Security Workflows for GenAI Tools

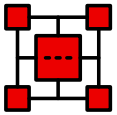


Threat Intelligence Analysis and Summarization

Assisted Detection Investigation and Analysis

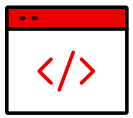


Automated Response and/or Workflow Implementation



Assisted Vulnerability Management and Patching

Enabling Self-Service Answers to Questions by Non-Security Teams (IT, Engineering, etc.)



Writing and Editing Queries or Scripts

Analyst Onboarding and Answering Product Functionality Questions

Job displacement is a low concern

Despite popular misconceptions, **concerns about job displacement in favor of an "autonomous SOC" are minimal.** In fact, this concern ranked lowest among operational concerns with GenAI, even among practitioners. While GenAI can help address skills shortages, respondents believe it won't be doing this by automating away human labor.

Improving the analyst experience

Respondents see GenAI as a means of improving the analyst experience, as reflected in the top-ranked operational outcomes they expect to realize, including **enhancing productivity, reducing burnout and accelerating onboarding.** This reveals an understanding that GenAI can be a force multiplier and a task accelerator.

Accelerating data-driven decision-making

The most requested workflows for applying GenAI revolve around boosting analyst productivity and streamlining data analysis to inform decision-making. This includes workflow automation and **minimizing tedious, time-consuming tasks**, such as summarizing threat intelligence, writing scripts and compiling cross-domain data for investigations.

KEY FINDING 4

Measurable ROI Is More Important than Cost

Top-ranked economic concerns around GenAI adoption

#1 Quantifying the ROI of GenAI spend

#2 Costs of licensing GenAI tools

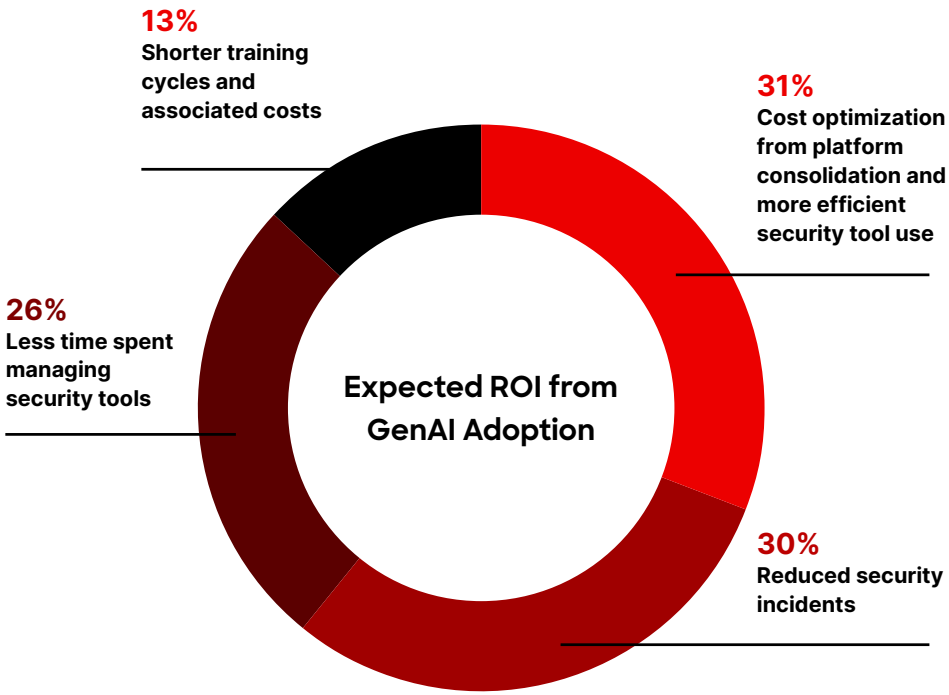
#3 Unpredictable or confusing pricing models

ROI as the top economic concern

Return on investment (ROI) remains the top economic concern related to GenAI, outranking concerns around the costs to license GenAI tools.

Faster returns on AI spend with a platform approach

Responses suggest that organizations believe **platform-delivered GenAI can help teams realize faster economic returns** from AI investments. Respondents expect to realize incremental savings associated with broader platform consolidation efforts, including **procurement efficiencies, reduced security incidents, fewer training cycles and reduced maintenance costs**.



KEY FINDING 5

Guardrails Are Required for Safe and Responsible Adoption

GenAI safety and privacy controls

Respondents are torn on whether the rewards of GenAI outweigh its risks. To adopt GenAI with peace of mind, respondents say **safety and privacy controls are needed for GenAI maturity**, both ranking among the top feature requirements for GenAI tools.

Concerns about data exposure and attacks

The top security concerns for GenAI are **data exposure to underlying large language models (LLMs) and attacks on GenAI tools**, validating frequently cited risks around GenAI use.

New GenAI security policies

As GenAI adoption grows, organizations increasingly rely on both technology and policy frameworks to ensure responsible use. Almost **9 in 10 respondents (87%) have implemented new security policies** or are developing policies to govern GenAI adoption within the next year.

Top security concerns for GenAI adoption

#1 Sensitive data exposure to underlying LLMs

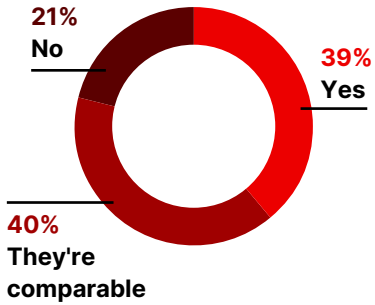
#2 Adversarial attacks on GenAI tools

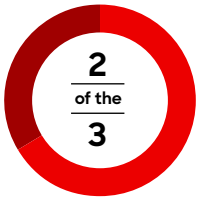
#3 Lack of guardrails or controls in GenAI tools

#4 AI hallucinations

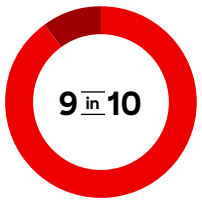
#5 Insufficient public policy regulations for GenAI use

Do the rewards outweigh the risks of GenAI?





Top GenAI feature requirements involve safety and privacy controls



Respondents have either implemented new security policies or are developing policies to govern GenAI adoption within the next year

In Summary

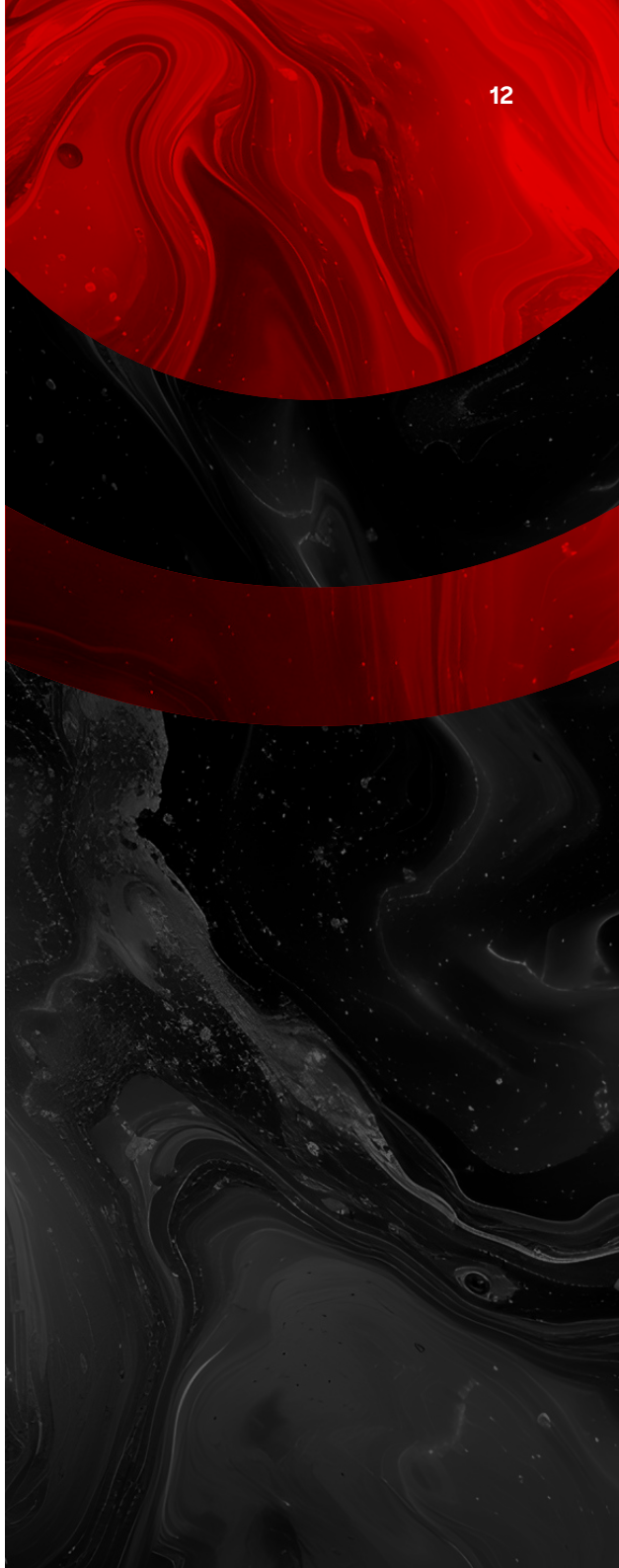
We're entering the era of GenAI in cybersecurity. Recently the domain of early adopters, GenAI is nearing mainstream adoption as security teams realize its many benefits.

As adoption accelerates, one truth is clear: The value of GenAI tools lies in their ability to integrate with the platforms and tools that security teams already use. Security teams want to deploy GenAI as part of a platform to get more value from existing tools, elevate the analyst experience, accelerate onboarding and eliminate the complexity of integrating new point solutions.

Security teams also want GenAI tools built for cybersecurity by cybersecurity experts. Organizations will evaluate their GenAI investments based on the outcomes that matter most: faster response times, more accurate decision-making and measurable ROI achieved through streamlined security operations.

While GenAI is still in its infancy, many wonder about the long-term adoption of GenAI in cybersecurity. Across the industry, the cost for vendors to develop this technology (and for organizations to license it) will demand tangible outcomes. While GenAI is not a silver bullet, this survey shows that organizations believe it can have significant benefits.

The future of GenAI in cybersecurity will be defined by tools that not only advance security but also uphold the highest standards of safety and privacy.



CrowdStrike's Approach to Generative AI

CrowdStrike pioneered the use of AI in cybersecurity in 2011 and we've been innovating ever since. CrowdStrike first unveiled its GenAI assistant, Charlotte AI, in 2023. Named "*Best AI Security Co-Pilot*" by the 2024 Cyber Defense Global Infosec Awards, Charlotte AI empowers security teams to use plain-language queries and embedded GenAI across their CrowdStrike Falcon® platform modules to surface cross-domain insights, automate time-intensive workflows and make faster, more accurate decisions. Trained on petabytes of security telemetry and insights from CrowdStrike threat researchers and incident response experts, Charlotte AI is purpose-built to assist security teams, while providing critical guardrails for data transparency, data privacy and role-based access — enabling safe and responsible GenAI adoption.

Additional Resources

- Read the 5 questions security teams must ask to use GenAI responsibly.
- Learn how Charlotte AI's multi-AI agent architecture enables security teams to accelerate workflows, while enabling safe and responsible GenAI adoption.
- See how CrowdStrike enables organizations to protect their AI security posture (AI-SPM) with CrowdStrike Falcon® Cloud Security.
- Learn how CrowdStrike enables organizations to prevent sensitive data leakage or exposure with CrowdStrike Falcon® Data Protection.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: www.crowdstrike.com/free-trial-guide

© 2024 CrowdStrike, Inc. All rights reserved.