CyberRisk ALLIANCE

2026 SC Awards

ENTRY KIT

To enter the SC Awards, please **click here**

WHAT ARE THE SC AWARDS?

Presented by SC Media, the SC Awards are cybersecurity's most prestigious award program, recognizing and honoring outstanding innovations, organizations, and leaders that are advancing the practice of information security.

As the SC Awards enter its 29th year, they continue to serve as a beacon of excellence. Our mission is to highlight the outstanding achievements of individuals, teams, and organizations, and unveil their success stories to our audience of 1.2 million cybersecurity professionals. Every year we recognize and celebrate information security products and services, organizations and leaders in Trust and Excellence across 30+ categories. Entering the SC Awards offers a range of benefits that make them an exceptional opportunity for organizations seeking to showcase their outstanding achievements and gain widespread industry recognition.

We invite cybersecurity companies and individuals to nominate and participate in the SC Awards.

To enter the SC Awards, please **click here**.

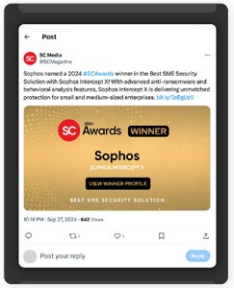
2025 SC AWARDS WINNERS

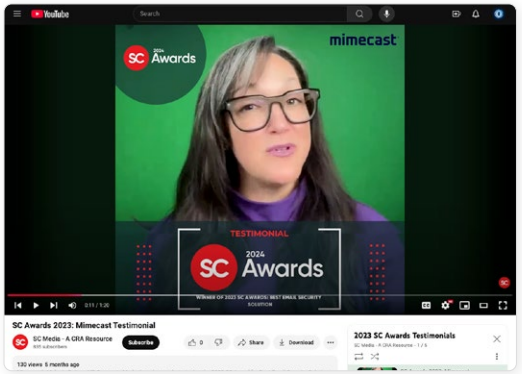
adam networks
algosec
AppSOC AI
BACKBOX
Barracuda
Bastille
CLOUD RANGE
CONCENTRIC AI
CROWDSTRIKE
CyberProof A UST Company
cynomi
DARKTRACE
DataGrail
DOPE SECURITY
eset
FORTINET
halcyon
ISACA
mimecast
nucleus
okta
PERMISO
qwiet AI
REDSEAL
SentinelOne
sumo logic
Trustwave
TENELEVEN
torq
TRACEABLE
WatchGuard

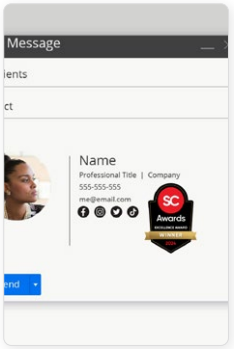
SC AWARDS WINNER AND FINALIST BENEFITS

As an SC Awards winner or finalist, you'll gain access to a range of valuable marketing and promotional opportunities throughout the awards season. These benefits ensure that your success is recognized and celebrated throughout the cybersecurity industry, helping you build a stronger presence, enhance your organization's reputation, and elevate your achievements. Here's what you get with an SC Awards:

- **Extensive Media Coverage**: Receive recognition across SC Media's website, channels, and e-newsletters, reaching an audience of 1.2 million.
- **In-Depth Feature Articles**: Detailed award profiles and articles written by SC Media editors and industry journalists, promoted across SC Media's website and social media.
- **Press Release Exposure**: A press release announcing winners and finalists, with opportunities for quotes, plus a template with SC Media's quote and logos.
- **Social Media Promotion**: Your achievement will be promoted across SC Media's and CRA's LinkedIn and X channels throughout the award season.
- **Awards Reception & In-Person Recognition**: Attend an exclusive event where winners are presented with a prestigious award.
- **Exclusive Interview Opportunities**: Winners can participate in exclusive interviews in the CRA Studio, livestreamed on CyberRisk TV.
- **Logo on Award Website**: Your organization's logo prominently featured on the SC Awards website for increased visibility.







ADDITIONAL PROMOTIONAL OPPORTUNITIES

Through our partnership with PARS International, you'll have access to digital logo badges and commemorative products to showcase your award and amplify your achievements.

UPCOMING AWARDS DEADLINES AND FEES

KEY DATES

DECEMBER 2	Early Bird Rate Deadline
JANUARY 26	Final Entry Deadline
FEBRUARY 9 THROUGH FEBRUARY 27	Judging Process
MARCH 2	Finalist Announcements
MARCH 24	Winners Announced at SC Awards Reception

ENTRY FEES

$400 PER ENTRY	**$625** PER ENTRY
Discounted Entry Rate (expires December 2)	Standard Entry Rate (December 3 - January 26)

ANNOUNCEMENTS

Finalists will be announced at **scworld.com/sc-awards**

The **2026 SC Awards Winners** will be announced at an Awards Reception on Tuesday, March 24, 2026

ENTRY QUESTIONS?

Contact **scawards@cyberriskalliance.com**

JUDGES

The SC Awards are judged by an esteemed panel of impartial experts from industry-leading organizations, members of SC Media and the CyberRisk Alliance community of CISOs and Women in Cyber. Our rigorous, transparent judging process ensures that every entry is evaluated fairly, giving both products and services the recognition they deserve.

Click here to meet our judges

Apply to become a judge for the SC Awards

Enter the SC Awards and be a part in celebrating the year's outstanding innovations and accomplishments, while ensuring your company and its leaders and product and service offerings receive the recognition they deserve.

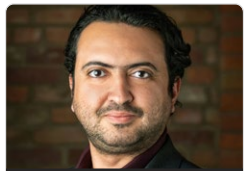
START YOUR ENTRY TODAY!

2025 JUDGES

Alissa Abdullah
Mastercard

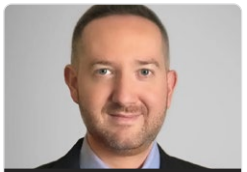
Roota Almeida
Delta Dental of NJ/CT

Miki Calero
Ohio Dept, Public Safety



Adam Ennamli
General Bank of Canada

Michael Fey
Island



Todd Grober
Ernst & Young

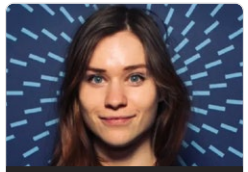
Renee Guttmann-Stark
CISOHIVE LLC

Travis Hartman
IWC3

John Johnson
Docent Institute

Ashutosh Kapse
Falcon Labs Australia

Cedric Leighton
CYFORIX

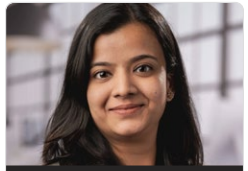


Lera Leonteva
Allen & Overy

Sean McElroy
Lumin Digital

Julian Mihai
Penn Medicine

Kelley Misata
Sightline Security



Chahak Mittal
Universal Logistics

Aunudrei Oliver
Allianz Life

Marcus Sachs
CIS

Vandana Verma Sehgal
Snyk

Gregory Wilson
Putnam Investments

ENTRY SUBMISSION PROCESS

1. The SC Awards are open to all information security vendors, service providers and professionals with current operations in North America (U.S. and Canada). This includes vendors and service providers that offer a product and/or service for commercial, government, educational, nonprofit, and more. The awards are designed to celebrate outstanding innovations, organizations, and leaders advancing information security.

2. Submitting entries is simple: review all categories to determine the best fit for the product, solution, organization or person you are nominating, then complete the entry by answering a series of questions.
Preview our entry overview guide HERE.

3. If entering multiple categories, please offer unique answers for each. Avoid copying and pasting the same answers for each category you enter to ensure the best response from our judging panels.

4. Every entry must be accompanied by an image. The image should be a visual representation of the entry. If you are a finalist, SC Media will use this image to support your entry. Logos alone are not acceptable images. Product screen captures, headquarter images, and team photos or executive headshots are all acceptable. Please try to submit images that are at least 1000 pixels wide.

5. All entries must be submitted and paid for online by either Visa, Mastercard or American Express.

SUBMIT YOUR SC AWARD ENTRIES

Category Overview

TRUST AWARDS

01. Best AI/ML Data Analytics Security Solution
02. Best API Security Solution
03. Best Application Security Solution
04. Best Authentication Technology
05. Best Business Continuity/Disaster/ Ransomware Recovery Solution
06. Best Cloud Security Management Solution
07. Best Cloud Workload Protection Solution
08. Best Continuous Threat Exposure Management Solution
09. Best Data Security Solution
10. Best Endpoint Security Solution
11. Best Identity Management Solution
12. Best Insider Threat Solution
13. Best Managed Detection And Response Service
14. Best Managed Security Service
15. Best Risk/Policy Management Solution
16. Best SASE Solution
17. Best Secure Messaging Solution
18. Best Supply Chain Security Solution
19. Best Threat Detection Technology
20. Best Threat Intelligence Technology
21. Best Vulnerability Management Solution

EXCELLENCE AWARDS

01. Best Compliance Solution
02. Best Customer Service
03. Best Emerging Technology
04. Best Enterprise Security Solution
05. Best IT Security-Related Training Program
06. Best Professional Certification Program
07. Best Security Company
08. Best SME Security Solution
09. Innovator (Executive or Practitioner) of the Year
10. Investor of the Year
11. Most Promising Early-Stage Startup
12. Security Executive of the Year

Trust Awards

Back to Categories

Awarding information security products and services in the industry. Judges will be looking at the cybersecurity solutions, the problems and their market penetration, functionality, manageability, ease of use, scalability, customer service/support and more.

01

BEST AI / ML DATA ANALYTICS SECURITY SOLUTION

New generative artificial intelligence (GenAI) and machine learning (ML) technologies have helped cybersecurity elevate existing solutions and drive the creation of new ones. This category focuses on excellence in leveraging the GenAI/AI/ML in applications such as detecting anomalies in large language/data models, juggling threat intel with vulnerability research, behavioral analytics, or building predictive threat models. Solutions nominated for this category focus on the data analytics side of GenAI/ML to better extract, visualize and analyze both ongoing and potential threats.

02

BEST API SECURITY SOLUTION

The rapid transition to cloud computing, reliance on multiple cloud environments, and the prevalence of mobile devices and applications to support business operations, have led to piling threats tied to application programming interfaces – or APIs – that define how software interacts. Failure to lockdown an API can result in unauthorized access to otherwise secure networks and serve as an avenue in for adversaries. Products in this category help prevent or mitigate attacks on APIs by addressing any of three API security categories described by the OWASP Foundation:

- API Security Posture, providing visibility into the security state of a collection of APIs
- API Runtime Security, detecting and preventing malicious requests to an API
- API Security Testing, evaluating the security of a running API by interacting with the API dynamically

Trust Awards (Continued)

Back to Categories

03
BEST APPLICATION SECURITY SOLUTION

The OWASP Automated Threat Handbook provides key industry standards by which organizations should set their security controls to detect and mitigate threats occurring through malicious internet-based automation attacks. Such assaults, from spamming, credential stuffing, CAPTCHA defeat, fraudulent account creation, Denial of Service (DoS) and still more, can cause monetary and brand damage to companies experiencing them. This is where technologies such as web application firewalls (WAFs) and bot mitigation technologies and services come into play. WAFs typically use deep-packet inspection, provide logging and reporting, block real-time traffic, provide alerting capabilities and auto-update features, perform web caching, provide content filtering, offer web-based access to reporting and/or logging, protect traffic from reaching the underlying operating system, and filter application traffic to only legitimate requests. Bot mitigation solutions, have also proven increasingly useful to organizations trying to avoid falling victim to malicious web automation attacks. Contenders entering the category can offer these technologies in tandem or alone.

04
BEST AUTHENTICATION TECHNOLOGY

Products here provide enhanced security to end-users or devices by offering credentials for access to an authenticator or authentication server. Software and hardware that specializes in the biometric authentication of users is also included here. These solutions may use a tangible device (something you have) for authentication and knowledge (something you know) for authentication. For biometrics, the solution provides identification and authentication using any of the following methods: finger/thumb print/retinal scan/voice recognition/hand/palm geometry/facial recognition. Please note that solutions that include behavioral analytics for authentication fall into this category.

Trust Awards (Continued)

Back to Categories

05

BEST BUSINESS CONTINUITY/DISASTER/RANSOMWARE RECOVERY SOLUTION

Almost daily, organizations of all sizes are impacted by cyberattacks, which puts whole systems, databases and files at risk. Nation-state attacks and unexpected weather events have also prompted companies to be more prepared for down-time and interested in quick recovery strategies to keep their businesses up and running. Solutions for this category can support various components of backup, business continuity and disaster recovery plans and efforts - from supporting back-up protocol when systems have been threatened or taken offline to addressing infrastructure demands to get back up and running in the event of physical disasters or online attacks by insiders and outside malicious actors, inside or outside the organization.

06

BEST CLOUD SECURITY MANAGEMENT SOLUTION

Cloud breaches stem from a number of common cloud management issues including misconfigurations (CSPM), workload protection (CWPP) Security Incident and Event Management (SIEM), Secure Access Service Edge (SASE) and more. Solutions for this category help ensure security in the configuration and management of cloud environments and may also include any security tools that are designed to monitor the cloud infrastructure in real time enforcement of security policy.

07

BEST CLOUD WORKLOAD PROTECTION SOLUTION

Business decisions vary in the types of assets that are maintained in the cloud, and for each of those assets, there are often distinct security considerations. Solutions for this category provide protection to the containers and servers and code that reside in the cloud. They may help define risks associated with cloud workloads, and should contribute to their performance, availability, and security.

Trust Awards (Continued)

Back to Categories

08
BEST CONTINUOUS THREAT EXPOSURE MANAGEMENT SOLUTION

Continuous Threat Exposure Management (CTEM) involves identifying, assessing and mitigating vulnerabilities in an organization's publicly accessible IT assets and services. Entrants to this category show a best-of-breed technology for web application scanning, domain certificate monitoring, network perimeter scanning, third-party service assessment, misconfigured cloud assets and unpatched software and systems.

09
BEST DATA SECURITY SOLUTION

As first stated by The Economist, the world's most valuable resource is no longer oil, but data. That also means that data for many organizations present the greatest potential risk. Solutions in this category focus first and foremost on the protection of data from unauthorized access and data corruption throughout its lifecycle. They may include data encryption, data discovery and classification and data loss prevention.

10
BEST ENDPOINT SECURITY SOLUTION

Increasingly endpoint devices with applications are exchanging data on corporate networks. Examples for this broad category include employee laptops, handsets, tablets and also IoT devices such as security systems, cameras and virtual machines. Products in this category center around the collapsing network perimeter and those devices that have director or indirect access to corporate resources. Each of these devices require strong endpoint security, point-to-point encryption and more. Security can be for data at rest in the device itself, secure access to data in the enterprise, and encryption for data in motion between the enterprise and the device. It also includes anything from hard disk encryption solutions, and tools that track lost mobile devices to USB/thumb drive security solutions.

Trust Awards (Continued)

Back to Categories

11
BEST IDENTITY MANAGEMENT SOLUTION

As a core pillar of zero trust, identity security protects all types of identities across the enterprise human or machine, to detect and prevent breaches. Products in this category address the identity management life cycle in an enterprise environment, including password management, user provisioning and enterprise-access management.

12
BEST INSIDER THREAT SOLUTION

Modern insider threats in organizations and businesses range from intentional malicious acts, unintentional errors, or negligence. Solutions nominated for this category should include ones that help cybersecurity teams reduce the impact of credential sharing, accidental data exposure, risky shadow IT, social engineering and network and lateral network access control.

13
BEST MANAGED DETECTION AND RESPONSE SERVICE

These offerings provide remotely delivered security operations center capabilities to detect, investigate and mitigate incidents. MDR services typically combine advanced analytics, threat intelligence, and human expertise.

Trust Awards (Continued)

Back to Categories

14
BEST MANAGED SECURITY SERVICE

These offerings provide a turnkey approach to an organization's primary technical security needs. These offerings can either be a collocated device at the client's organization facility or can be a completely outsourced solution where the application to be protected would reside at the vendor's data center.

15
BEST RISK/POLICY MANAGEMENT SOLUTION

These products measure, analyze and report risk, as well as enforce and update configuration policies within the enterprise, including but not limited to network, encryption, software, and hardware devices. Contenders' products should offer a reporting format that covers the frameworks of multiple regulatory requirements, such as Sarbanes-Oxley, Gramm-Leach-Bliley and other acts and industry regulations. As well, this feature should be network-centric, providing reporting to a central administrator and allowing companies to centrally manage the product.

Overall, entrants' products should be enterprise-centric; collect data across the network, including threats and vulnerabilities; report associated risk, endpoint configuration, enforcement, auditing and reporting; provide remediation options (but are not exclusively patch management systems); and, finally, offer centralized reports based on regulatory requirements and local policies.

Trust Awards (Continued)

Back to Categories

16
BEST SASE SOLUTION

Efforts by businesses to implement a zero trust model require effective management of network visibility of user activity and access. Solutions for this category should contribute to that effort, offering secure access service edge (SASE) to combine wide area networking, or WAN, and network security services into a single cloud offering. They should enable secure, policy-based access to the appropriate application or data regardless of user or device location.

17
BEST SECURE MESSAGING SOLUTION

Messaging security addresses the ability to exchange messages securely whether it be email, a collaboration platform or cross-platform messaging apps to send text, voice or video communications. Solutions should ensure the privacy of sensitive messages, limit the repercussions of forgery, and manage other aspects of safeguarding messaging within business communications. These products are enterprise-centric and should have, but are not required to have, some form of centralized management. They may include spam filters, content filters, malware safeguards, unauthorized content (sometimes called "extrusion protection" or "data leakage protection"), phishing and other types of undesirable content. However, these are not simply anti-spam filters. They typically provide features such as encryption, digital signatures, automatic shredding of messages and attachments and more.

Trust Awards (Continued)

Back to Categories

18
BEST SUPPLY CHAIN SECURITY SOLUTION

Cybersecurity supply chain risks are vulnerabilities and threats that exist within the supply chain of information technology systems and products. These types of threats are behind the massive SolarWinds breach and costly hacks tied to the MOVEit vulnerability. Entrants to this category should provide solutions that might add code and component transparency, validate development tools and address third- and fourth-party risks.

19
BEST THREAT DETECTION TECHNOLOGY

Closely aligned to threat intelligence technologies and processes, threat detection techniques have necessarily graduated from simpler network-based detection solutions to technologies focused on improving detection times, alerting and mitigating attacks as they are happening. Not only can a wide range of organizations now readily fall victim to an attack, bad actors can often infiltrate systems undetected, leveraging various points of entry and methods of obfuscation. As such, contenders entering this category should deliver solutions that offer detection and/or remediation capabilities for the entire network, including mobile devices, cloud applications, IoT-based devices and more.

This category includes deception technologies that detect threats, then automates the creation, deployment, and management of digital traps (decoys), lures and deceits to engage and prompt the attacker into revealing their trade craft, tools and techniques

Trust Awards (Continued)

Back to Categories

20 BEST THREAT INTELLIGENCE TECHNOLOGY

Contenders in this category should help cybersecurity teams research and analyze cybercrime and other threat trends and any technical developments being made by those engaging in cyber-criminal activity against both private and public entities. These technologies facilitate the understanding and contextual relevance of various types of data, often an overwhelming amount, collected from internal network devices, as well as from external sources (such as open source tools, social media platforms, the dark web and more). Armed with these more digestible analyses on risks and cyberthreats, cybersecurity teams should be able to enhance their tactical plans preparing for and reacting to an infrastructure intrusion prior to, during and after an attack, ultimately improving their overall security posture so their long-term security strategy is more predictive rather than simply reactive.

21 BEST VULNERABILITY MANAGEMENT SOLUTION

An increasingly sophisticated threat landscape requires ongoing efforts to track potential security gaps within networks and systems. With that in mind, these products perform network/device vulnerability assessment and/or penetration testing. They may use active or passive testing and are either hardware-or-software-based solutions that report vulnerabilities using some standard format/reference.

Excellence Awards

Back to Categories

Awarding the top cybersecurity companies and service providers in the industry, as well as some of its finest products/services that cater to both enterprise and SME organizations.

01
BEST COMPLIANCE SOLUTION

Nominees include solutions that help organizations comply with specific regulatory requirements demanded of companies in the healthcare, retail, educational, financial services and government markets. Solutions should help customers meet mandates noted in such legislation as HIPAA, SOX, GLBA, FISMA, or in guidelines around cyber incident reporting. Also noted are industry guidelines that include cyber governance and FFIEC or those that center on the PCI Security Standards Council.

02
BEST CUSTOMER SERVICE

Support as well as service of products and assistance sold are critical components of any contract. For many organizations that seek out help from information security vendors and service providers, the aid they receive from customer service representatives is crucial to the deployment, ongoing maintenance and successful running of the technologies they've bought and to which they have entrusted their businesses and sensitive data. We're looking for vendor and service providers that offer stellar support and service – the staff that fulfilled its contracts and maybe even goes a little beyond them to ensure that organizations and their businesses are safe and sound against the many threats launched by today's savvy cybercriminals.

Excellence Awards (Continued)

Back to Categories

03
BEST EMERGING TECHNOLOGY

What cutting edge technologies with some innovative capabilities are bursting onto the scene to address the newest information security needs facing organizations? This category welcomes both new vendors and old pros looking to provide products and services that look to help shape the future by addressing fast-evolving threats through the creation of these types of offerings. Solutions should have been brought to market during calendar year 2025 (January-December). The company should also have an office in North America and provide ready support and service to customers.

04
BEST ENTERPRISE SECURITY SOLUTION

This includes tools and services from all product sectors specifically designed to meet the requirements of large enterprises. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

05
BEST IT SECURITY-RELATED TRAINING PROGRAM

This category targets companies and organizations that provide end-user awareness training programs for organizations looking to ensure that their employees are knowledgeable and supportive of the IT security and risk management plans. It also is considering those training companies or organizations that provide programs for end-user organizations' IT security professionals to help them better address components of their IT security and risk management plans, such as secure coding, vulnerability management, incident response/ computer forensics, business continuity/disaster recovery, etc.

Excellence Awards (Continued)

Back to Categories

06
BEST PROFESSIONAL CERTIFICATION PROGRAM

Programs are defined as professional industry groups offering certifications to IT security professionals wishing to receive educational experience and credentials. Entrants can include organizations in the industry granting certifications for the training and knowledge they provide.

07
BEST SECURITY COMPANY

Nominees should be the tried-and-true, longer-standing companies which have been offering products and services to customers for at least three years. Nominations can come from all sectors. Areas that will be accounted for in the judging process include product line strength, customer base, customer service/support, research and development, company growth and solvency, innovation and more.

08
BEST SME SECURITY SOLUTION

This includes tools and services from all product sectors specifically designed to meet the requirements of small to midsized businesses. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

Excellence Awards (Continued)

Back to Categories

09
INNOVATOR (EXECUTIVE OR PRACTITIONER) OF THE YEAR

This category has been expanded to include Executives and Practitioners from the vendor, security services, and consultancy community. Candidates can't be from the end-user community. Whether the nominee be a chief scientist of a large cybersecurity vendor or the CEO of one of the most promising tech startups, those entering this category lead the research and development efforts for their company, ensuring the cybersecurity industry does not fall behind adversaries. This category is meant for those individuals that demonstrate an innovative approach to best protecting the data and systems that are the lifeblood of enterprises.

10
INVESTOR OF THE YEAR

Contenders should be venture capital or angel investor or firm that contributed to any stage of funding to cybersecurity startups during the 2025 calendar year and can demonstrate how they supported product development and growth. Entrants should be able to demonstrate a unique and creative approach and a commitment to the cybersecurity market and understanding of gaps in existing technologies and services. Entrants should also be able to demonstrate support for investments that go beyond dollars to prepare entrepreneurs for an expected transition from startup to enterprise.

Excellence Awards (Continued)

Back to Categories

11 MOST PROMISING EARLY-STAGE STARTUP

Nominated businesses with great promise can come from any IT security product/service sector and should be a privately held startup offering a strong, flagship product that is within two years of its initial release. They should be focused on continued product development, customer growth, business development and overall fiscal and workforce expansion. Please note in your submission the launch date of your initial flagship offering. While this award will be presented to a business, and not product, information about flagship products garners much consideration.

12 SECURITY EXECUTIVE OF THE YEAR

Contenders should be from the vendor and security services and consultancy community – not from the end-user community. Those entering this category are the veterans and perennial influencers in the cybersecurity development community, with a history of leadership in companies that have their pulse on the needs of the user community and have a proven track record in delivery of products and services that meet the requirements of enterprises and small and medium business across the various market verticals.

Submit your SC Award entries today!

CLICK HERE TO SUBMIT YOUR ENTRY

We wish you the best of luck and look forward to reviewing your entries!

- The SC Media Editorial Team and CyberRisk Alliance

BILL BRENNER — **CYBERRISK ALLIANCE | SVP, AUDIENCE CONTENT STRATEGY**

InfoSec content strategist, researcher, director, tech writer, blogger and community builder. Senior Vice President of Audience Content Strategy at CyberRisk Alliance.