
2023
AWARDS
Honoring the Best in U.S Cybersecurity
ENTRY KIT

2023 AWARDS
Honoring the Best in U.S Cybersecurity

2023 SC AWARDS

The SC Awards are cybersecurity's most prestigious and competitive honor. For 26 years we've recognized the solutions, organizations and people that are innovatively advancing the practice of information security. Last year, the awards program attracted an impressive 800 entries – a 21% increase over 2021. The record interest in our awards program, year after year, reflects the extraordinary trust and value that continue to attract new entrants and industry mainstays. View our 2022 SC Award Winners **HERE.**

2023 CATEGORIES

We're excited to expand entry opportunities and debut new award categories that reflect the dynamic shifts in our industry. This year we added a new Trust Award category for Best API Security Solution, new Excellence Award category for Investor of the Year, an expanded Trust Award category to recognize industrial security solutions, and modified Excellence Award categories focused on the cyber tech startup community. There are 35+ cybersecurity categories to choose from across our two award types:

- **Trust Awards** recognize outstanding information security products and services.
- **Excellence Awards** recognize top cybersecurity companies, their leaders, investors and financial partners.

Winners and finalists will be featured in an extended celebration through comprehensive coverage across SC Media's full range of digital channels and community of 1.6M+ infosec professionals. Selected executives, companies and products will be unveiled on August 21, 2023, with individual profiles of every winner as well as Winners Circle virtual roundtables.

Join SC Media 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 and showcase your astounding achievements!

ENTRY PROCESS

1 SC Awards are open to all information security vendors, service providers and professionals. It honors organizations and individuals with current operations in North America (U.S. and Canada)

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.

3 If entering multiple categories, offer unique answers for each. That is, 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, headquarters 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 Awards entry **HERE**.

2023 SC AWARDS

SCHEDULE & ENTRY FEES

DISCOUNTED ENTRY DEADLINE

FEBRUARY 22

FINAL ENTRY DEADLINE

MARCH 13

FINALIST ANNOUNCEMENTS

MAY 15

WINNERS ANNOUNCEMENT

AUGUST 21

Finalists and winners will be announced online at scmagazine.com/sc-awards

ENTRY QUESTIONS

Please contact Wendy Loew at Wendy.Loew@cyberriskalliance.com

SPONSORSHIP QUESTIONS

Please contact Dave Kaye at Dave.Kaye@cyberriskalliance.com

ENTRY FEES

Discounted Entry Rate
(expires February 20, 2023)

$400
PER ENTRY

Standard Entry Rate

$595
PER ENTRY

2023 SC AWARDS

CATEGORY OVERVIEW

TRUST AWARDS

1. BEST API SECURITY SOLUTION
2. BEST AUTHENTICATION TECHNOLOGY
3. BEST BUSINESS CONTINUITY/DISASTER RECOVERY SOLUTION
4. BEST CLOUD SECURITY POSTURE MANAGEMENT SOLUTION
5. BEST CLOUD WORKLOAD PROTECTION SOLUTION
6. BEST COMPUTER FORENSIC SOLUTION
7. BEST DATA SECURITY SOLUTION
8. BEST DATABASE SECURITY SOLUTION
9. BEST EMAIL SECURITY SOLUTION
10. BEST IDENTITY MANAGEMENT SOLUTION
11. BEST INDUSTRIAL SECURITY SOLUTION
12. BEST MANAGED DETECTION AND RESPONSE SERVICE
13. BEST MANAGED SECURITY SERVICE
14. BEST MOBILE SECURITY SOLUTION
15. BEST RISK/POLICY MANAGEMENT SOLUTION
16. BEST SASE SOLUTION
17. BEST SIEM SOLUTION
18. BEST THREAT DETECTION TECHNOLOGY
19. BEST THREAT INTELLIGENCE TECHNOLOGY
20. BEST VULNERABILITY MANAGEMENT SOLUTION
21. BEST WEB APPLICATION SOLUTION

EXCELLENCE AWARDS

22. BEST CUSTOMER SERVICE
23. BEST EMERGING TECHNOLOGY
24. BEST ENTERPRISE SECURITY SOLUTION
25. BEST IT SECURITY-RELATED TRAINING PROGRAM
26. BEST PROFESSIONAL CERTIFICATION PROGRAM
27. BEST REGULATORY COMPLIANCE SOLUTION
28. BEST SECURITY COMPANY
29. BEST SME SECURITY SOLUTION
30. DEAL OF THE YEAR
31. INNOVATOR OF THE YEAR
32. INVESTOR OF THE YEAR
33. MOST PROMISING EARLY-STAGE STARTUP
34. MOST PROMISING UNICORN
35. SECURITY EXECUTIVE OF THE YEAR
36. SECURITY MARKETING CAMPAIGN OF THE YEAR

TRUST AWARDS

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

1.BEST API SECURITY SOLUTION (NEW)

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

2. 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.

3. BEST BUSINESS CONTINUITY/DISASTER RECOVERY SOLUTION

Almost daily, organizations of all sizes are getting hit with cyberattacks, which puts whole systems, databases, files and more at risk. Also, nation-state attacks and unexpected weather events have prompted companies to be more prepared for down-time and quick recovery 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.

4. BEST CLOUD SECURITY POSTURE MANAGEMENT SOLUTION

The majority of cloud breaches stem from misconfigurations, demonstrating the critical need for organizations to properly address risks associated with a cloud infrastructure. Solutions for this category should help ensure security in the configuration and management of cloud environments. They may include any security tools that are designed to identify misconfiguration and compliance risks in the cloud and monitor the cloud infrastructure in real time enforcement of security policy.

5. 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.

6. BEST COMPUTER FORENSIC SOLUTION

Products in this category fall into two subcategories: network and media.

Network: The network tools must be exclusively intended for forensic analysis of network events/data. If the product is a SIEM with forensic capabilities, it should be placed in the SIEM category.

Media: Media tools cover just about all other non-network forensic tools, including those tools that collect data from media over the network and live forensic tools. This also includes specialized forensic tools that are not intended to analyze network data.

7. 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.

8. BEST DATABASE SECURITY SOLUTION

Protecting its critical information is the number one priority for many organizations. An integral component of this is to secure corporate databases. Entries here should include solutions that help customers safeguard mission-critical database environments. Features of these offerings can run the gamut but should not focus on securing data itself or data in transit, which would fall under Best Data Security Solution. Be sure to explain the specific ways the solution manages and maintains data in a secure way, helping to prevent exposures.

9. BEST EMAIL SECURITY SOLUTION

Email security addresses the ability to exchange email messages with assurance, as well as the ability to filter email messages based on content, source, or other criteria. Solutions should ensure the privacy of sensitive messages, limit the repercussions of email forgery, and manage other aspects of safeguarding email within the organization. These products are enterprise-centric and should have, but are not required to have, some form of centralized management. They may include spam filters, junk mail filters, malware filters, 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 email encryption, digital signatures, automatic shredding of messages and attachments, and more.

10. 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.

11. 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.

12. BEST MANAGED SECURITY SERVICE

These offerings provide a turnkey approach to an organization's primary technical security needs. These offerings can either be a colocated 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.

13. BEST MOBILE SECURITY SOLUTION

More and more employees are using smaller and smaller devices with loads of applications to access corporate data. Some examples include iPhones, iPads, Android devices, and more. Products in this category deal with not only a collapsing perimeter, but also consumer-owned and consumer-controlled devices being used to get at corporate resources. At a minimum, these devices likely will require strong endpoint security, point-to-point encryption and more. This is a broad category. 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.

14. 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.

15. 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.

16. BEST INDUSTRIAL SECURITY SOLUTION

As operational technology and industrial control systems increasingly gets integrated into the IT network, and supply chain attacks become more prevalent, new considerations emerge for protecting industrial systems and ensuring the integrity of critical infrastructure. Entrants into this category provide solutions to support industrial security, defined by the National Institute of Standards and Technology as the protection of industrial installations, resources, utilities,
materials, and classified information essential to protect from loss or damage. Specific goals of implementation should be to safeguard OT/ICS, including supervisory control and data acquisition systems (SCADA), from an array of attacks, whether spearheaded by nation-state bad actors, organized criminals, or malicious attackers on the hunt for a quick buck.

17. BEST SIEM SOLUTION

Security information and event management (SIEM) tools are used to collect, aggregate and correlate log data for unified analysis and reporting. Typically, these tools can take logs from many sources, normalize them and build a database that allows detailed reporting and analysis. While forensic analysis of network events may be a feature of a SIEM, it is not the only feature, nor is it the primary focus of the tool.

18. 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 automate the creation, deployment, and management of digital traps (decoys), lure and deceit to engage and prompt the attacker into revealing their trade craft, tools and techniques.

19. 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.

20. 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.

21. BEST WEB APPLICATION 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 web 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 like 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, also have 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.

EXCELLENCE AWARDS

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.

22. 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.

23. 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 2022 (January-December). The company should also have an office in North America and provide ready support and service to customers.

24. 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.

25. 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.

26. 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.

27. BEST REGULATORY COMPLIANCE SOLUTION

Nominated solutions should 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 noted by the likes of the FFIEC or the PCI Security Standards Council.

28. 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.

29. 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.

30. DEAL OF THE YEAR

This award recognizes excellent performance by an investment banking firm or professional. Contenders should detail and discuss their unique and creative approach to a merger, acquisition, or initial public offering of a cybersecurity company, which closed during calendar year 2022. The deal should involve companies where the primary focus of technology or services is to support efforts to identify, respond to, or mitigate threats to information security, or protect data and networks, and where the transaction seeks to support the company's strategy and further enhance its capabilities.

31. INNOVATOR OF THE YEAR

Contenders should be from the vendor and security services and consultancy community – not from the end-user community. Whether they be the 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 and instead recognize the type of innovation that is required to best protect the data and systems that are the lifeblood of enterprises.

32. INVESTOR OF THE YEAR (NEW)

Contenders should be venture capital or angel investor or firm that contributed to any stage of funding to cybersecurity startups during the 2022 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.

33. 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.

34. MOST PROMISING UNICORN

Nominated unicorn businesses with great promise can come from any IT security product/service sector and should be a privately held startup company with an applied valuation basis at or above $1 billion. They are still relying on investment dollars but have developed their core product offering and target market, and proven viability. These businesses are seeking market validation and accelerated scale, potentially with near term interest in M&A or IPO. While this award will be presented to a business, and not product, information about flagship products garners much consideration.

35. 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.

36. SECURITY MARKETING CAMPAIGN OF THE YEAR

Differentiating technology solutions in a crowded marketplace and quickly building awareness and demand are important challenges facing vendor marketing teams. This category recognizes outstanding efforts within the IT security product/service sector to creatively communicate product or service benefits to target customers. Nominees should demonstrate how a 2022 campaign (launched between January – December) demonstrated an understanding of the market dynamics and contributed to strategic positioning for the product or service.

ENTRY KIT FAQ

WHAT IF MY ENTRY HAS CONFIDENTIAL INFORMATION?

You will be offered the opportunity to submit information separately that should be kept confidential (i.e. submitted only to the judges). For everything else, SC Media reserves the right to publish details.

WHAT IS THE COST TO ENTER SC AWARDS 2023?

The fee for entering the SC Awards Trust and Excellence categories is $595 per entry. To receive a discounted entry rate of $400, entries must be finalized, submitted and paid in full by February 22.

WHAT IS THE DEADLINE TO SUBMIT?

The discounted entry deadline date is extended to February 22. The final entry deadline is March 13.

CAN I SUBMIT AN ENTRY INTO MORE THAN ONE CATEGORY?

Yes, you can submit an entry into more than one category, but we advise you to offer unique answers for each.

CAN I CHANGE MY WRITTEN ENTRY AFTER I'VE SUBMITTED AND PAID?

No. Unfortunately you will not be able to access your entry once it has been submitted and paid for.

CAN I REMOVE AN ENTRY AFTER IT HAS BEEN SUBMITTED AND PAID FOR?

No. If you have an issue please contact Wendy Loew at Wendy.Loew@cyberriskalliance.com

WHEN ARE FINALISTS ANNOUNCED?

Finalists will be announced on our website, scmagazine.com/sc-awards the week of May 15, 2023.

Date subject to change.

WHEN ARE WINNERS ANNOUNCED?

Winners will be announced August 21, 2023.

WHO DO I CONTACT FOR ENTRY INQUIRIES?

Wendy Loew at Wendy.Loew@cyberriskalliance.com

WHO DO I CONTACT FOR SPONSORSHIP INQUIRIES?

Dave Kaye at Dave.Kaye@cyberriskalliance.com

2023 SC AWARDS

JUDGING PROCESS

SC Award category winners are decided by an expert panel of jurors. They represent a cross-section of SC's audience – which is comprised of information and IT security personnel at large, medium and small enterprises from all major vertical markets, including financial services, healthcare, government, retail, education and other sectors. These jurors are hand-picked by SC Media's editorial team for their breadth of knowledge and experience in the information security industry. 2023 categories that recognize the investor community will be judged by a separate panel of jurors from the founder and entrepreneur market.