SC awards 2021

HONORING THE BEST IN U.S. CYBERSECURITY

ENTRY KIT

scmagazine.com/awards
#scawards

SC Awards 2021

HONORING THE BEST IN U.S. CYBERSECURITY

OUR MISSION

The SC Awards are cybersecurity's most prestigious and competitive honor. For 24 years, we've recognized the people, the organizations and the solutions that are forging the industry's future and advancing the cause of safe and secure commerce and communications.

In 2021, the SC Awards will feature an extended and expanded celebration, honoring finalists and winners through comprehensive promotion across SC Media's full range of digital, social, and editorial channels. Industry anticipation will build over four months, culminating in the kick-off of SC Awards Week on May 3, 2021.

2021 CATEGORIES

- Trust Awards recognize information security products and services. Judges will look at the solutions, the problems and their market penetration, functionality, manageability, ease of use, scalability, customer service/support and more.
- Excellence Awards recognize the top cybersecurity companies and their leaders, delivering solutions and services to enterprises and small and medium businesses.
- Leadership Awards (formerly Reboot Awards) recognize the people leading the way in the end-user community, delivering cybersecurity expertise within their own enterprises as well as throughout the industry.

Join SC Media in celebrating the year's outstanding innovations and accomplishments. For professionals and leaders, gain a powerful person credential, bring honor to your team and to your company. For cybersecurity providers, win market validation for your products, services and solutions.

HOW TO ENTER

1. Entry is simple – review all categories to determine the best fit for the product, solution or person you are nominating. The entry process is Q&A based.

2. 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.

3. 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 both digitally and in print to support your entry. Logos alone are not acceptable images. The image should be at least 300dpi, jpeg/eps format and at least 16.5 x 23.4 inches in size.

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

Submit your SC Awards entries HERE.

CATEGORY OVERVIEW

TRUST AWARDS

1. BEST BUSINESS CONTINUITY/DISASTER RECOVERY SOLUTION
2. BEST CLOUD COMPUTING SECURITY SOLUTION
3. BEST COMPUTER FORENSIC SOLUTION
4. BEST DATA LEAKAGE PREVENTION (DLP) SOLUTION
5. BEST DATABASE SECURITY SOLUTION
6. BEST EMAIL SECURITY SOLUTION
7. BEST DECEPTION TECHNOLOGY
8. BEST IDENTITY MANAGEMENT SOLUTION
9. BEST MANAGED SECURITY SERVICE
10. BEST MOBILE SECURITY SOLUTION
11. BEST AUTHENTICATION TECHNOLOGY
12. BEST NAC SOLUTION
13. BEST RISK/POLICY MANAGEMENT SOLUTION
14. BEST SCADA SECURITY SOLUTION
15. BEST SIEM SOLUTION
16. BEST THREAT INTELLIGENCE TECHNOLOGY
17. BEST THREAT DETECTION TECHNOLOGY
18. BEST VULNERABILITY MANAGEMENT SOLUTION
19. BEST WEB APPLICATION SOLUTION

EXCELLENCE AWARDS

20. BEST SECURITY COMPANY
21. ROOKIE SECURITY COMPANY OF THE YEAR
22. BEST SME SECURITY SOLUTION
23. BEST ENTERPRISE SECURITY SOLUTION
24. BEST REGULATORY COMPLIANCE SOLUTION
25. BEST CUSTOMER SERVICE
26. BEST EMERGING TECHNOLOGY
27. BEST IT SECURITY-RELATED TRAINING PROGRAM
28. BEST PROFESSIONAL CERTIFICATION PROGRAM
29. BEST CYBERSECURITY HIGHER EDUCATION PROGRAM
30. SECURITY EXECUTIVE OF THE YEAR
31. INNOVATOR OF THE YEAR

LEADERSHIP AWARDS

32. CHIEF SECURITY OFFICERS
33. PRIVACY LEADS/DATA PROTECTION EXPERTS
34. RISING STARS
35. THOUGHT LEADERS
36. THREAT SEEKERS
37. TOP MANAGERS
38. CHIEF INFORMATION OFFICERS
39. INFLUENCERS
40. OUTSTANDING EDUCATORS
41. DIVERSITY LEADERS

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 BUSINESS CONTINUITY/DISASTER RECOVERY SOLUTION

While back-up, business continuity and disaster recovery can be different for every company, involving numerous strategies and tactics, there is no doubting the need for solutions to support over-arching BDR plans. Almost daily, organizations of all sizes are getting hit with ransomware threats, for example, which puts whole systems, databases, files and more at risk. As well, 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 BDR 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.

2. BEST CLOUD COMPUTING SECURITY SOLUTION

These technologies are deployed to protect data and/or applications in a cloud environment. They may also protect the cloud computing infrastructure itself. Cloud computing security concerns are numerous for both providers and their customers – and include security and privacy worries, compliance issues and legal/contractual problems. Solutions or services in this category can provide for the protection of data or applications in the cloud, protection for traffic flowing between companies and their cloud service providers, policy management and encryption capabilities, privileged user access and controls or more.

3. 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.

4. BEST DATA LEAKAGE PREVENTION (DLP) SOLUTION

Products in this category include those that help organizations safeguard their intellectual property and customers' critical data persistently – inside and outside the company. Network-based and endpoint data leakage prevention products will be considered. Products should prevent data from unauthorized exit from the network or protect data on the endpoint – whether the endpoint is connected to a network or not. Products typically are policy-driven and should include scanning of all data, regardless of protocol or application leaving the network, and/or keep track of peripherals, such as removable storage and attached to the endpoint – reporting that inventory to a central location or administrator. All entrants should have the capability of being managed by a centralized administrator. Those products considered part of this category include network DLP products, which are typically gateways; those products protecting only endpoints; and hybrid products that operate at both the gateway to the network and at the endpoint. Specifically, for endpoint DLP, traffic should be monitored, and encryption should be available.

5. 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 – from encryption to access management to logging and monitoring. Be sure to explain the specific ways the solution protects these corporate crown jewels and the features present to ensure exposures are mitigated.

6. 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. These email security products should be evaluated on their effectiveness, manageability, non-intrusiveness, ease of use and other factors that impact the implementation of this type of product in the enterprise environment. They typically provide features such as email encryption, digital signatures, automatic shredding of messages and attachments, and more.

7. BEST DECEPTION TECHNOLOGY

Deception technologies automate the creation, deployment, and management of digital traps (decoys), lures and deceits, which are blended among existing IT resources. Hidden in plain sight, these tools are intended to engage and prompt the attacker into revealing their trade craft, tools and techniques, in real-time, which provides the enterprise security teams with the facts to pre-emptively launch effective counter measures.

8. BEST IDENTITY MANAGEMENT SOLUTION

Products in this category address the identity management lifecycle in an enterprise environment, including password management, user provisioning and enterprise-access management.

9. BEST MANAGED SECURITY SERVICE

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

10. 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, BlackBerries and more. Products in this category deal with not only a collapsing perimeter, but also consumer-owned and -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. If your product is used to secure this type of small device/ handheld, it may fit. 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.

11. 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.

12. BEST NAC SOLUTION

Protecting host-based computing platforms and network resources from threats that are brought in by employees, vendors, contractors and guests involves a number of solutions and policies. From anti-virus and firewalls to IDS/IPS solutions, the products in this category run the gamut. However, to control access to network resources at the endpoint, the tools companies often rely on are network access control (NAC) products. These solutions can be used to validate the existence of certain security measures and validate that they are properly configured and up to date. They also can validate the existence of current OS patches and can be used to manage the complexity associated with overseeing permissions and authorizations for various groups of users. Most will integrate with a common directory structure, some will provide local authentication capabilities, while others will match something on the endpoint – such as an agent or MAC address – to the authentication before allowing access to the protected network resources.

13. 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 for companies to centrally manage the product.

So, 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.

14. BEST SCADA SECURITY SOLUTION

Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) operational and information technologies reinforce critical infrastructure security. While traditional and long- standing vendors are making their move toward SCADA ecosystems, new players are joining the fray with IoT/ IIoT-related solutions. For this category, we're looking for technologies that help safeguard critical ICS/SCADA systems from an array of attacks, whether spearheaded by nation- state bad actors, organized criminals, or malicious attackers on the hunt for a quick buck.

TRUST AWARDS (CONT.)

15. 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.

16. 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 cybercriminal 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 analysis 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.

17. BEST THREAT DETECTION TECHNOLOGY

Closely aligned to threat intelligence technologies and processes, threat detection techniques have necessarily graduated from more simple network-based detection solutions to technologies focused on improving detection times, alerting and mitigating attacks as they are happening given the evolution of cyberattackers and the tactics they now employ. Not only can a wide range of organizations now readily fall victim to an attack, their systems now often already have been infiltrated with various types of malware they may still be persisting in their networks through the leveraging of various points of entry and methods of obfuscation. As such, contenders entering this category should offer solutions that offer detection and/or remediation capabilities for the entire network, including mobile devices, cloud applications, IoT-based devices and more.

18. BEST VULNERABILITY MANAGEMENT SOLUTION

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.

19. 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. A tried and true arrow in a one's quiver, these solutions are helpful on this front. As well, 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.

20. 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.

21. ROOKIE SECURITY COMPANY OF THE YEAR

Nominated companies should be new to the IT security field – offering an initial, strong, flagship product that is within two years of its initial release. Nominees can come from any IT security product/service sector and will be continuing efforts in further product development, customer growth and overall fiscal and employee growth. Please note in your submission the launch date of your initial flagship offering. If this initial offering or any of your other products have been on the market for longer than two years, please do not submit a nomination in this category.

22. 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

23. 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.

24. 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. Nominees must be prepared to offer references of customers who are engaged in, or have already completed, real, fully fledged deployments, and should be ready to address specific questions posed to them during the judging process.

25. 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. For this new category, 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.

26. 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 new 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 just hit the market in the last six to 12 months, and entries should have some customers available who can act as references. The company should also have an office in North America and provide ready support and service to customers in this country.

27. BEST IT SECURITY-RELATED TRAINING PROGRAM

This category is targeting companies and organizations that provide end-user awareness training programs for organizations looking to ensure that its 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.

28. 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.

29. BEST CYBERSECURITY HIGHER EDUCATION PROGRAM

This category includes the best cybersecurity undergraduate or higher education program which currently has a cybersecurity degree program. These are for schools throughout the United States. Qualification is based on the quality of instruction, programs and how well these prepare students for the marketplace.

Please note: There is no fee to enter this category.

30. SECURITY EXECUTIVE OF THE YEAR

Contenders should be from the vendor and security services and consultancy community – not from the end-user community, which are being recognized in the Leadership Awards. 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. Nominees should be prepared to answer further questions during the judging process, offer at least two references, and be open to holding confidential interviews with members of the SC Media editorial team, if warranted.

Please Note: A high resolution image of the nominee must be submitted with the entry.

31. INNOVATOR OF THE YEAR

Contenders should be from the vendor and security services and consultancy community – not from the end-user community, which are being recognized in the Leadership Awards. Whether they be the chief scientist of a large cybersecurity vendor or the CEO of one of the most promising tech startup, 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.

Nominees should be prepared to answer further questions during the judging process, offer at least two references, and be open to holding confidential interviews with members of the SC Media editorial team, if warranted.

Please Note: A high resolution image of the nominee must be submitted with the entry.

LEADERSHIP AWARDS

Formerly the Reboot Leadership Awards, the SC Media Leadership Awards recognize executive and professional leaders in the end-user community for their unique, inventive and inspiring contributions that improve security, shape the industry, provide thought leadership, and otherwise have a positive impact on cybersecurity. Multiple individuals will be honored in each category. Vendor, reseller and consultancy leaders do not qualify for the Leadership Awards and should instead consider the Excellence Award categories for executives and innovators.

32. CHIEF SECURITY OFFICERS

Primary cybersecurity leaders spearhead viable IT security programs, gain the support of their company's executive leaders and colleagues, and helped to propel the CISO/CSO (or other appropriate equivalent title) position to a footing of influence within their organization and wider industry.

33. PRIVACY LEADS/DATA PROTECTION EXPERTS

Privacy and security often are cast as at odds with each other when, in reality, they are two sides of the same coin. These professionals have excelled in imposing privacy controls while supporting and adhering to the tenets of cybersecurity within their organizations.

34. RISING STARS

These nominees and their accomplishments caught the attention of the industry and are ones to watch going forward.

35. THOUGHT LEADERS

What would cybersecurity – or any segment of IT – be without the vision of those who mull problems and issues, initiate conversation and think about solutions, policies, programs, best practices and more. These team players are not only thinkers, but doers who have devised or created solutions, helped to establish standards, initiated best practices, or otherwise have undertaken other initiatives that have contributed greatly the cybersecurity industry as a whole.

36. THREAT SEEKERS

These innovative, bright, and adventurous denizens of cybersecurity dash around the globe from behind their keyboards, chasing down and uncovering threats, vulnerabilities and bugs that left unchecked could bring organizations – public and private – to their knees.

37. TOP MANAGERS

These superstars of management have taken the principles of security and translated them into business objectives. They lead by example and set the tone for the companies that they head up.

38. CHIEF INFORMATION OFFICERS

The CISO and CIO often work hand in hand. The CIO's support is often critical for the IT professionals to get the resources and the budget they need to move forward with cybersecurity initiatives.

39. INFLUENCERS

From policy makers to politicians to technologists, these nominees have influenced and shaped cybersecurity. They have helped move cyber beyond being just a vision to reality. These pros have undertaken projects or initiatives alone or with a group that impacts a wider segment of the cybersecurity industry beyond their own organization's and/or affects other business, government, or other markets in a positive way.

40. OUTSTANDING EDUCATORS

As cybersecurity moves to the mainstream and the skills gap widens, training the next generation of CISOs is critical. Academics lead the way as they head both undergraduate and graduate programs at universities, professional organizations, state economic boards and non-profits. Leading the charge in teaching future generations of CISOs never has been so critical.

41. DIVERSITY LEADERS

Increasingly, companies and organizations are recognizing not only their responsibility, but also the tangible benefit of ensuring a diverse workforce that can leverage the experience and skills that can come with differences in race, ethnicity, gender, sexual orientation, socio-economic status, and age. Individuals that support a company or organization's efforts to ensure a diverse workforce that acknowledges and benefits from a multitude of viewpoints is critical for business success and the betterment of society.

ENTRY ELIGIBILITY

SC Awards 2021 is open to all information security vendors, service providers and professionals. It honors vendors, service providers and professionals executing work in North America. Information security professionals from end-user companies should enter Leadership Awards categories, which spotlight security professionals and individual CSOs/CISOs working in North America. Vendors and service providers should apply to Trust and Excellence Awards categories.

It is encouraged for vendors and service providers to nominate their thought-leading customers. After all, the Leadership categories have been created to honor the accomplishments of their end-user customers. These leaders should be based in North America.

Please note: If vendors or service providers enter Leadership Awards, they will be disqualified after editorial review of entrants in these categories and will receive no refund of related entry fees.

KEY INFO

DEADLINE FOR ENTRIES

DEC 18TH
2020

EXTENDED ENTRY WINDOW

Late entries will be received until

JAN 15TH
2020

FINALIST ANNOUNCEMENTS

FEBRUARY
2021

Finalists will be announced
online at www.scmagazine.com

WINNERS ANNOUNCEMENT

Winners will be announced during
SC Awards Week beginning

MAY 3
2021

ENTRY QUESTIONS

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

SPONSORSHIP QUESTIONS

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

ENTRY FEES

Trust Awards Categories

$400
PER ENTRY

Excellence Awards Categories

$400
PER ENTRY

Leadership Awards Categories

$300
PER ENTRY

There is no fee to enter
Best Cybersecurity Higher
Education Program.

Extended deadline entries will
be an additional $195 per entry.

SC awards 2021

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 jury). For everything else SC Media reserves the right to publish details in the Awards Book of the Night.

WHAT IS THE COST TO ENTER SC AWARDS 2021?

The fee for entering the Trust and Excellence Awards categories is $400 per entry.

The fee for the Leadership Awards categories is $300 per entry.

There is no fee to enter Best Cybersecurity Higher Education Program.

WHAT IS THE DEADLINE TO SUBMIT?

The entry deadline is December 18. Extended entry window is open until January 15 with an additional charge.

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 to 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/awards in February 2021.

Date subject to change.

WHEN ARE WINNERS ANNOUNCED?

Winners will be announced during SC Awards Week beginning May 3, 2021.

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

JUDGING INFO

INTERESTED IN JUDGING?

To be considered as a juror for the SC Awards 2021, please click HERE and complete the application form by December 1, 2020. After this date, applications will be reviewed and jurors chosen by the editorial team, led by our VP of editorial, to participate on individual panels which cover our Trust and Excellence categories. For these panels, we look to rely on cybersecurity experts working at end-user companies often relying on vendor and service providers in this space to help guide and support their own internal cyber resiliency strategies and tactics. We also seek out other knowledgeable and experienced vendor-neutral professionals to participate, such as consultants, industry analysts or those serving in information security positions overseeing cyber resiliency and risk management/planning at public entities, non-profits and, again, private end-user companies.

Please understand that judging for the SC Awards is a serious commitment, requiring all panelists to devote some time to judge submissions fairly and objectively so that IT security solutions/services providers, industry leaders and their teams can be recognized and honored for their exemplary work and contributions to the wider field. We do expect a healthy interest from our SC audience to participate, but submitting an application does not guarantee a spot as a juror.

TRUST AWARDS

Finalist and winners in these categories are chosen by IT security professionals from the SC Media readership who have been vetted by the SC editorial team to participate as part of a judging panel for this particular group of awards. Members of this panel, which will be made up of approximately 100 professionals, primarily are from end-user organizations. They are chosen to participate as jurors for the Trust Awards categories based on their industry expertise and background. Typically, they lead information security divisions, play roles in implementing information security policies and plans for their organizations, and/or have in-depth knowledge or experience with testing, deploying or managing IT security products/services. 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, health care, government, retail, education and other sectors. Having volunteered their time and, most importantly, their knowledge of and experience with the contenders in these categories, these industry professionals are tasked with carefully considering each of the competitors in relation to the categories for which they entered. To reach their decision, not only will they review the materials provided by entrants, but also will consider whether the product or service in each category actually is the most effective in helping companies address the problems for which the product or service was designed. They also are asked to consider the functionality, manageability, ease of use and scalability of the product or service, as well as the customer service and support provided for it. Too, they have been encouraged to peruse any applicable product reviews that SC Magazine has published in the last year to help in making their final decisions, along with any other relevant industry and/or analyst reports. They also may suggest that certain entrants be moved between categories if they deem them unsuitable for one but appropriate for another.

After the jurors decisions are in, SC Media's product reviews team steps in to review the finalists in each to ensure, yet again, that they accurately jibe with the category for which they entered. In the event that a particular product or service is not an appropriate fit for a category, the product reviews team and VP of editorial will convene to make a final decision on whether it should remain in the running. (No refunds will be provided if a product is eliminated for failing to meet the criteria for not fitting in the category to which it was submitted.)

SC awards 2021

HONORING THE BEST IN U.S. CYBERSECURITY

JUDGING INFO (CONT.)

EXCELLENCE AWARDS

With the exception of the Editor's Choice Award, for which there are no formal submissions, winners in these categories are decided by a second expert panel of jurors. These jurors are hand-picked by SC Media's editorial team for their breadth of knowledge and experience in the information security industry. They come from end-user companies, analyst and consulting communities, academia and other vendor-neutral organizations. Jurors are advised to review the materials provided by entrants, as well as check out any applicable research or analyst reports and/or product reviews appearing in SC Media. There will be one winner chosen per category.

EDITOR'S CHOICE AWARD

Based on information culled from SC Media's events, through research conducted by the SC Media editorial team for various features and news articles, and conversations with and feedback from readers, analysts, vendors and the Editorial Advisory Board, this award is given to a group, person, company or product at the discretion of SC Media editorial team.

The award winner will be announced during SC Awards Week in May 2021. This award enables the editorial team to pay homage to those individuals or entities that are making a positive impact on the industry.

Please note: This category cannot be entered directly.