IoThinkTank | IOT AWARDS

INTELLIGENCE & SECURITY

IoT Security Excellence Award

Safeguarding the Future of Connected Technologies

ENTRY GUIDE

Award details, dates, and past winners: **iothinktank.com/iot-security-excellence-award/**



About the award

The IoT Security Excellence Award recognizes the technologies, platforms, and strategies that protect connected systems from emerging cyber threats. As IoT deployments expand across industries, security has become one of the most critical foundations for maintaining trust, protecting data, and ensuring operational resilience.

This award honors organizations delivering innovative security solutions designed specifically for connected environments. From device authentication and encryption to secure communication architectures, threat detection platforms, vulnerability management, transparency programs, and resilient infrastructure, the winning technologies demonstrate leadership in protecting modern IoT ecosystems.

Why IoT matters in security

Connected devices now operate at the center of industrial systems, healthcare infrastructure, transportation networks, smart cities, and consumer environments. Each connected endpoint represents both an opportunity and a potential security risk. Without strong protections in place, vulnerabilities can expose sensitive data, disrupt operations, or compromise critical systems.

Modern IoT security requires a comprehensive approach that spans device authentication, encrypted communications, identity management, vulnerability analysis, software transparency, network monitoring, and threat detection. Innovations in these areas allow organizations to scale connected technologies while maintaining the security and reliability required for mission-critical environments.

The IoT Security Excellence Award recognizes the technologies and programs that help organizations protect their connected systems while enabling continued innovation across the IoT landscape.

Who should enter

- IoT cybersecurity platforms
- Secure IoT communication technologies
- Industrial IoT security platforms
- Vulnerability management teams
- Device authentication and identity management solutions
- Threat detection and monitoring platforms
- Edge and cloud security solutions
- Secure IoT infrastructure providers

Entries are welcome from organizations delivering security products, platforms, architectures, transparency programs, or operational practices that protect IoT devices, networks, data, and ecosystems.

What to include

Describe the threat or risk, security architecture, deployment scope, device and network coverage, operational integration, validation, responsible disclosure, and measurable risk reduction. Explain the solution's technical approach, implementation maturity, integrations, scale, security, reliability, and practical value.

- Quantified improvements in risk reduction, detection time, response time, coverage, remediation speed, compliance, resilience, false positives, or operational efficiency
- Deployment details, including locations, devices, users, systems, operating conditions, and implementation timeline
- Customer, client, or end-user identification when the entry relies on a real-world deployment
- Supporting evidence, including case studies, performance data, dashboards, customer validation, images, videos, technical documents, or information URLs
- Any confidentiality, regulatory, embargo, or publicity restrictions

Supporting collateral should make the entry easier to verify and evaluate. Include the strongest evidence available, and clearly distinguish measured results from estimates, projections, or planned outcomes.

Eligibility

The award is open to organizations and individuals developing or deploying connected technologies in commercial products, enterprise fleets, industrial systems, critical infrastructure, buildings, healthcare, transportation, utilities, and public-sector environments. Commercial products, platforms, public-sector programs, research-led deployments, pilots, and customer implementations are eligible when the entry includes enough evidence for meaningful evaluation.

Submitted work should be active, deployed, launched, or meaningfully advanced during the current awards cycle. Entrants may submit their own solution or a customer deployment with appropriate authorization.

Each product, platform, deployment, or project requires a separate submission and entry fee.

How it's judged

Every entry is scored out of 100 on five criteria. This award uses the Product & Technology weighting, so evidence of real-world results counts most.

Innovation & Differentiation	25
Evidence & Measurable Impact	35
Execution & Scalability	25
Category Fit	10
Leadership & Industry Contribution	5

For this award, judges look for

- Innovation in IoT security technologies, architecture, transparency, or lifecycle protection
- Effectiveness in protecting connected devices, networks, applications, and data
- Scalability across complex IoT environments, device fleets, and ecosystems
- Security validation through testing, certifications, risk reduction, third-party analysis, or deployment proof
- Real-world impact through customer outcomes, ecosystem improvements, operational resilience, or measurable security progress
- Contribution to IoT trust by advancing standards, transparency, software accountability, or secure development practices

Tips for a strong entry

Lead with the problem and the result.

Open with what wasn't working and what changed because of your solution. Judges should know why it matters by the end of your first paragraph.

Put numbers on it.

Evidence carries the most weight in scoring. Give before-and-after figures, and say which results are measured and which are estimates.

Name the customer.

A real deployment with a named customer is the strongest proof you can offer. If the name can't be published, tell us in writing when you submit.

Show it working.

Case studies, dashboards, screenshots, short videos, and technical documents help judges verify what you describe.

Write for this award.

Explain why your work fits this category specifically. A strong entry for one award can score poorly in another if the fit isn't clear.

Keep it tight.

Clear, specific answers beat long ones. Cut anything that doesn't help a judge understand the solution or its results.

How to enter

1. **Prepare your entry.** Gather the required organization, contact, product, deployment, and supporting information before beginning the application.
2. **Complete the application.** Describe the solution, connected technology, deployment environment, integrations, measurable outcomes, and supporting evidence.
3. **Submit payment.** The entry fee is charged when the application is submitted. Entries are not complete until payment is received.

You can save a draft and finish it anytime before the deadline. Deadlines close at 11:59 pm Pacific.

Current dates and fees

Entry dates and fees change each cycle. Find them, and get an email when entries open, on the award page.

iothinktank.com/iot-security-excellence-award/

Past winners

2026 WINNER

Quectel

Quectel won the 2026 IoT Security Excellence Award for its Security Capability Infrastructure, an integrated program spanning independent assessment, incident response, vulnerability disclosure, software supply-chain assurance, cryptographic key management, and internationally recognized certification.

2024 WINNER

Quectel

Quectel was named the 2024 IoT Security Excellence Award winner for a comprehensive security program that redefined how IoT module security can be tested, documented, improved, and communicated across the product lifecycle.

What winners get

- ✓ Recognition across IoThinkTank digital channels
- ✓ Official winner badge
- ✓ Dedicated winners page and newsroom coverage
- ✓ Visibility within the broader IoT community

Entry fees are charged at submission and are non-refundable. Customer or client identity should be included in your submission. If you need names excluded from public materials, notify us in writing at the time of submission. By submitting, you agree to the **Submission Guidelines**, **Privacy Policy**, and **Terms and Conditions**. IoThinkTank Awards are independent and unaffiliated with other award programs. Questions? Contact **awards@iothinktank.com**.