bugcrowd

Ultimate Guide to **Crowdsourced Security**

FOR FINANCIAL SERVICES ORGANIZATIONS

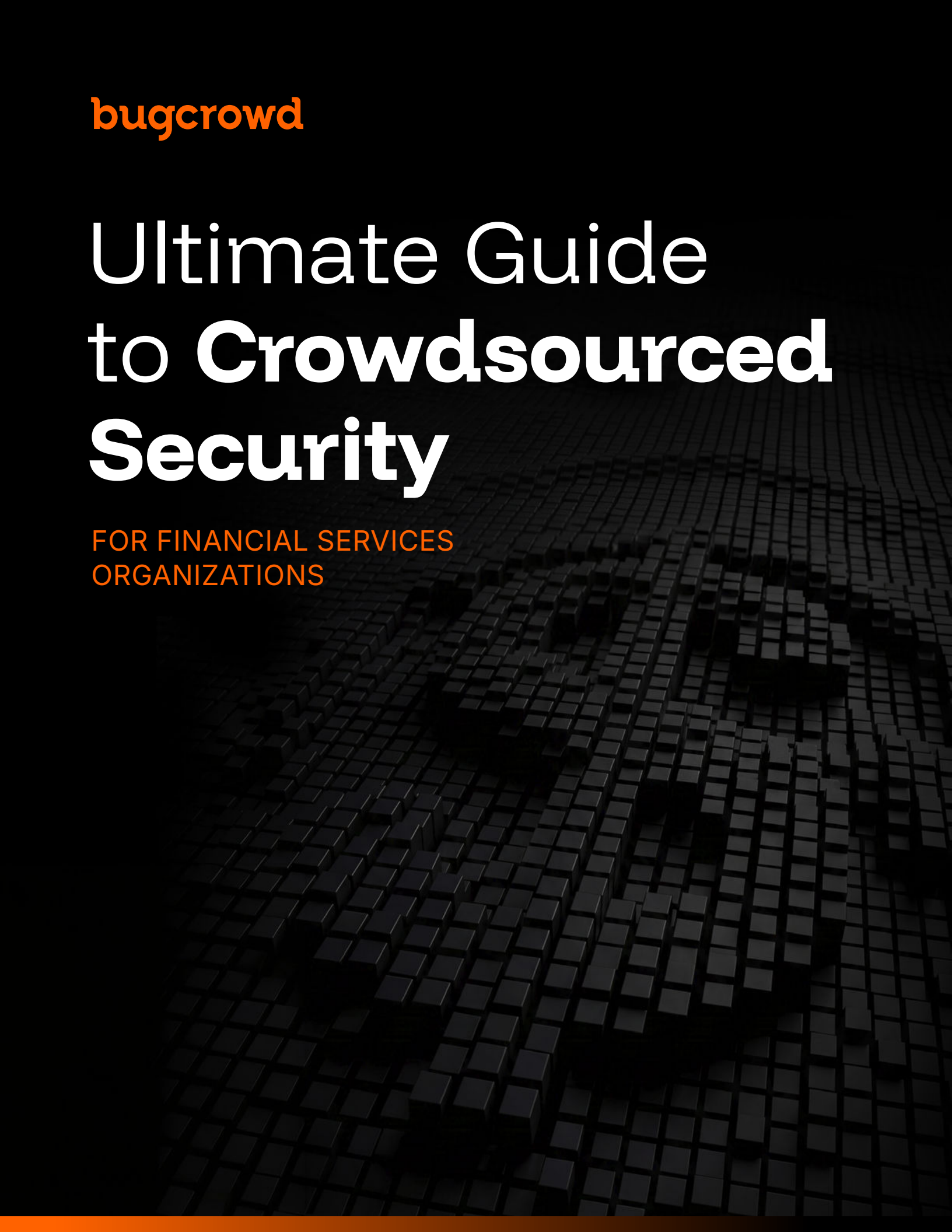


Table of Contents

Introduction

The financial services industry processes trillions of dollars every day, making it an ideal target for attackers. In 2024, 97% of US banks experienced a third-party breach, and targeted attacks against the financial industry increased by 109% in 2024 compared to 2023.

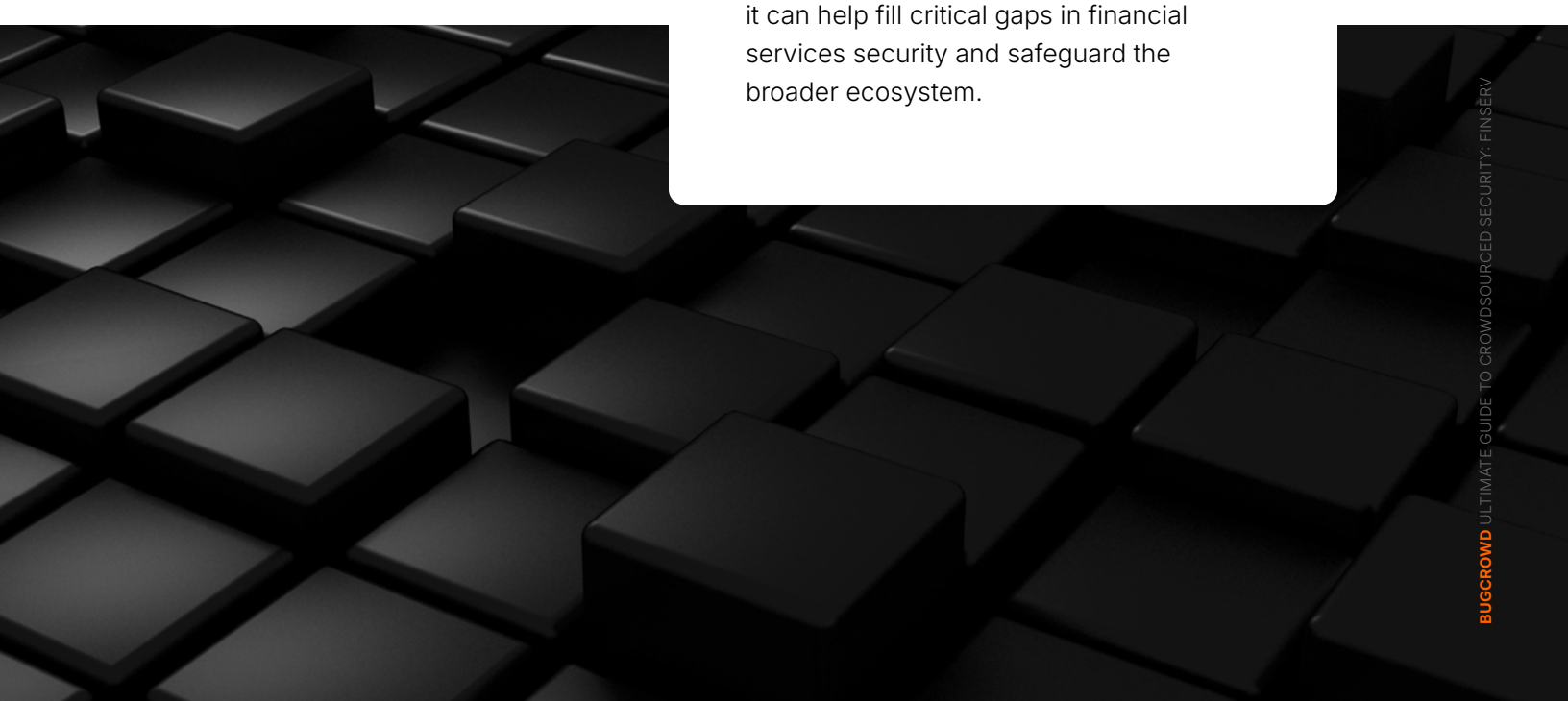
These statistics signal a deeper problem that extends far beyond mere coincidence. Financial institutions are routinely targeted by adversaries, including nation-state-backed groups and cybercriminals. Additionally, insider collusion, fraud, and hacktivist groups pose constant threats.

> **When financial organizations are attacked, businesses and individuals lose access to critical financial services. Not only do these attacks disrupt commerce and daily economic activities, but they are also very costly.**

The average cost of a breach for financial institutions is $6 million. A breach can also damage brand trust and lead to more regulatory scrutiny, fines, and expensive audits.

Crowdsourced security can help financial services organizations overcome these challenges. By leveraging human intelligence and SaaS technology, financial services organizations can access specialized expertise on demand to scale their security teams and meet compliance requirements.

In this guide, we will dive into crowdsourced security and explore how it can help fill critical gaps in financial services security and safeguard the broader ecosystem.



The challenges of securing financial services organizations

Financial services organizations operate in one of the most challenging cybersecurity landscapes. Several factors make these institutions particularly difficult to defend:

Large and complex attack surfaces

Financial institutions have a wide variety of product surfaces, like cloud systems, internal APIs, cryptocurrency custody, and blockchain-based payment rails. They also rely heavily on third-party integrations (e.g., payment processors or credit reporting integrations), which extend their functionality but exponentially expand their attack surface. Each surface introduces its own security risks, such as cloud misconfigurations, third-party API vulnerabilities, and smart-contract vulnerabilities.

Legacy systems

Many financial tech stacks are built on legacy technologies that generally lack modern security features, aren't frequently updated, and require specialized engineering knowledge to maintain and secure. These outdated systems have become prime targets for ransomware groups because they're easier to exploit and compromises within them are harder to detect. In fact, 65% of financial services organizations have experienced a ransomware attack in the past year. As a result, security teams have to invest additional resources to secure these systems, which can strain already overburdened teams.

In addition, attackers don't need to compromise many of these systems to wreak havoc. They frequently aim to penetrate high-value systems, such as SWIFT terminals, internal fund-transfer APIs, and trading platforms, where even limited access can be used to manipulate transactions or move money covertly. As a result, institutions have large surface areas to protect, which can lead to gaps that attackers can exploit.

High-value target status

Financial organizations store sensitive user payment, identity, and financial information, which makes them high-profile targets for both opportunistic criminals and sophisticated nation-state actors. For example, entities like the Lazarus Group (backed by wealthy nation-states like Russia and North Korea) intentionally target banking infrastructure and cryptocurrency platforms to conduct economic espionage, destabilize a country's financial sector, or evade sanctions.

Furthermore, financially motivated cybercriminals, such as FIN7 and Clop, view financial institutions as money machines. These attackers carry out ATM "jackpotting" heists and fraudulent wire transfers.

> **Given the high payout for hacking financial institutions, threat actors are willing to invest significant time and resources to overcome defenses and successfully execute attacks, putting financial services organizations at a disadvantage.**

Limited access to skills and capacity

There's a global talent shortage of full-time cybersecurity professionals. In 2024, there were 4.8 million open cybersecurity roles, a 20% increase from the prior year. Even when organizations can find talent, they often struggle to find those with specialized expertise (e.g., cloud security architecture, API penetration testing, fraud detection, and cryptocurrency), making it difficult for internal teams to maintain full coverage of their systems.

Stringent compliance and regulatory requirements

Financial organizations must satisfy customers and regulators by meeting various regulatory frameworks across different markets. These requirements are also often evolving, especially for newer technologies like cryptocurrency, which can add another layer of operational pressure. Maintaining these attestations requires balancing administrative tasks and implementing actual security practices, which can put pressure on already limited resources.

The risks of AI for financial services organizations

Many industries are rushing to adopt AI, and the financial services industry is no different. According to a Bank of England survey, 75% of financial services organizations are already using AI, with a further 10% planning to use it over the next three years.

However, rapid adoption is introducing new challenges:

→ Securing AI-generated code

Many financial institutions are relying on AI coding assistants and agents to generate code and accelerate development. However, this code is often insecure. One study found that half of AI-generated code snippets had vulnerabilities that attackers could exploit.

→ AI safety

AI models are trained on human data, which often contains biases. Without auditing and correcting these biases, financial services organizations might inadvertently promote misinformation or make unfair decisions. This harms consumers and may lead to additional regulatory scrutiny.

→ AI-accelerated threats

Just as financial services are using AI in development, attackers are increasingly turning to AI tools to develop and deploy new and sophisticated attacks quickly. Anthropic recently disclosed a cybersecurity attack carried out primarily by Claude Code.

→ Secure large language models

LLMs

Financial organizations are using LLMs to improve the efficiency of key services, such as customer support and fraud detection. However, if proper safeguards are not implemented, attackers can jailbreak LLMs to spread false information, carry out crimes, or extract sensitive information.

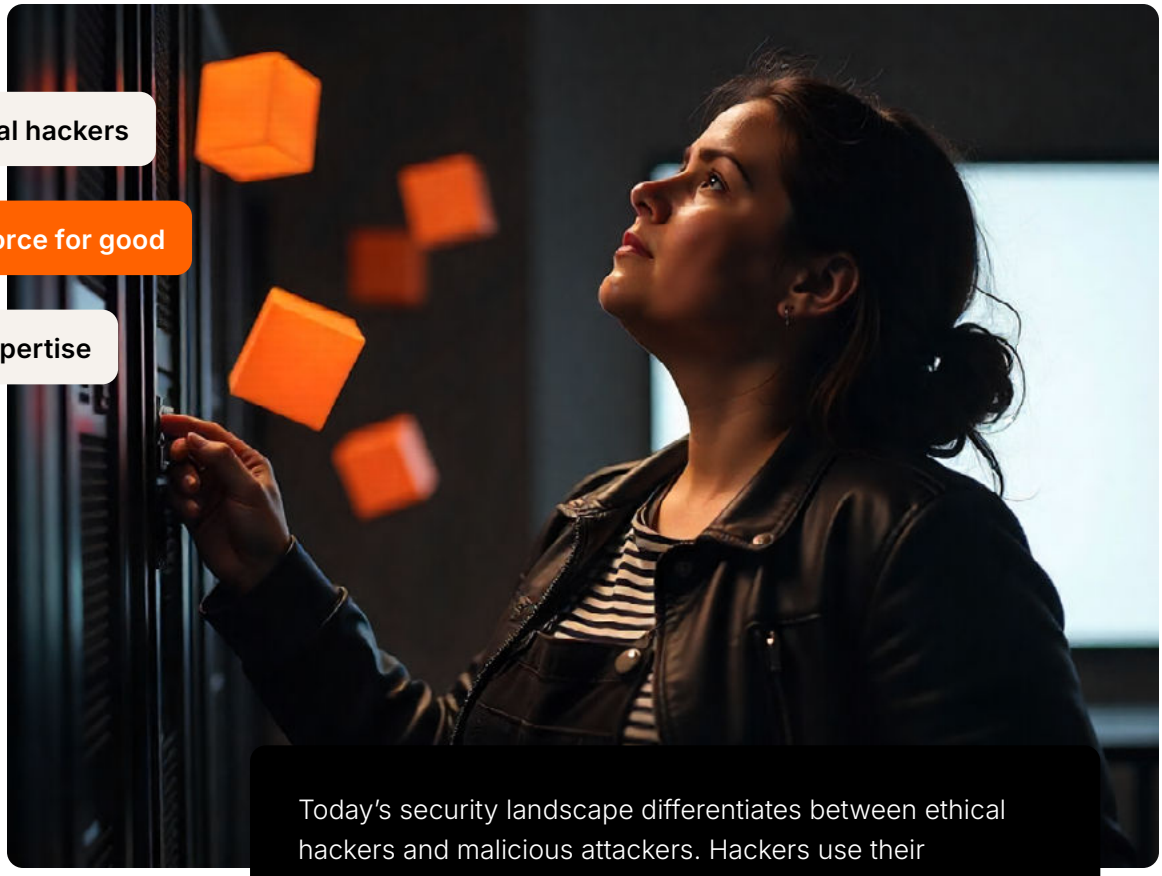
Ethical hacking 101

The term “hacking” often carries negative connotations and is frequently associated with criminal activity. However, at its core, hacking is simply expertise in programming and solving complex computer problems—a skill set that can be used for beneficial or harmful purposes.

ethical hackers

a force for good

expertise



Today’s security landscape differentiates between ethical hackers and malicious attackers. Hackers use their expertise to strengthen cybersecurity defenses and protect organizations. Hackers can be a force for good, with 85% of them believing that it’s more important to report a vulnerability than make money from it. **In this guide, we refer to ethical hackers as “hackers.”**

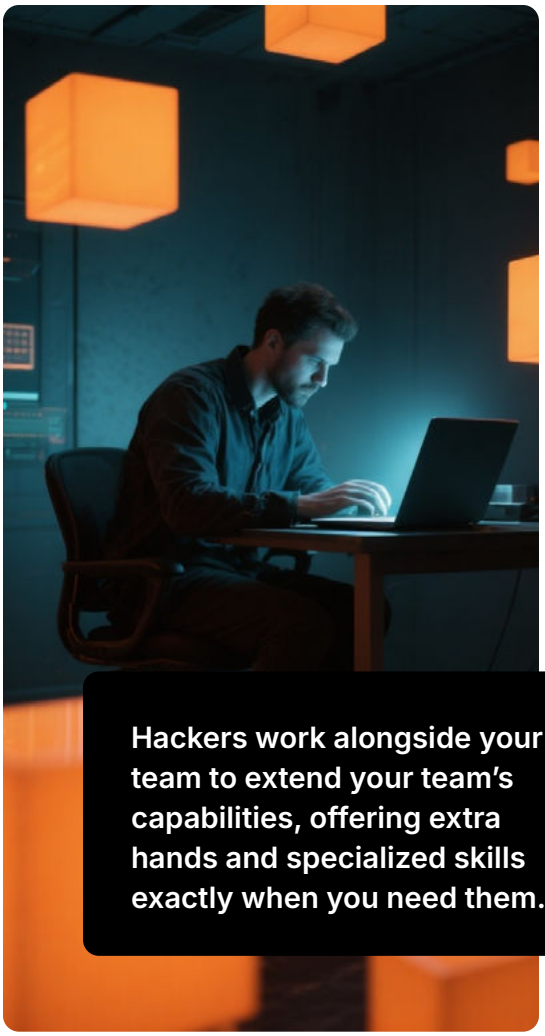
What is crowdsourced security?

Crowdsourced security harnesses the collective skills and experiences of the world's hacker and pentester communities. These highly capable individuals are given the direction, scope, and incentives to identify and report vulnerabilities to organizations.

Hackers come from all over the world, bringing hundreds of unique skill sets that can help organizations identify hidden risks in their attack surface before attackers do.

Many crowdsourced researchers have deep specializations, such as in core banking app exploitation, API abuse, or crypto-related attack paths. They leverage this extensive knowledge to replicate the same techniques used by groups targeting financial institutions, finding more vulnerabilities.

Crowdsourced security's innovation lies in combining this crowd expertise with a SaaS platform that connects organizations of all sizes with specialized security talent on demand. Unlike traditional security, which relies on ad hoc consulting arrangements, crowdsourced security emphasizes community and collaboration.



Hackers work alongside your team to extend your team's capabilities, offering extra hands and specialized skills exactly when you need them.

Benefits of crowdsourced security

By using crowdsourced security, financial services organizations can unlock the following benefits:

Continuous coverage

As you add new products or technologies (or simply update existing ones), crowdsourced security allows you to secure these assets with minimal operational overhead. As a result, your security teams can focus on remediating security flaws or implementing new security features rather than scaling their testing processes.

Elastic capacity

Crowdsourced security extends your team's capacity on demand, giving you additional experts exactly when you need them. Whether you're rolling out new code or monitoring a growing attack surface, you can scale this support up or down to match the business's needs and prevent your internal team from burning out.

Specialized expertise

Hackers bring their knowledge of specific parts of the stack (cloud, API, mobile, AI/LLMs, and cryptocurrency), enabling financial services companies to find novel vulnerabilities that their internal teams or a checklist security approach might miss.

Strategic, risk-based prioritization

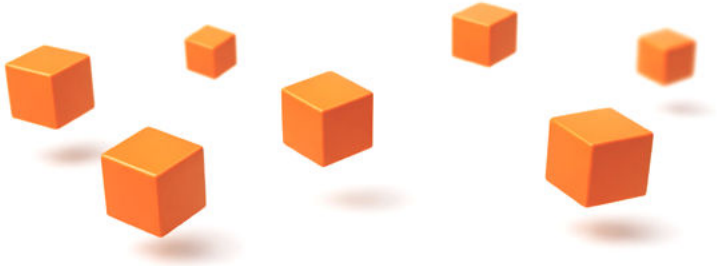
Instead of relying on sifting through noisy data or guessing which issues to fix first, crowdsourced testing shows you which vulnerabilities attackers can really exploit. This allows security leaders to direct resources where they produce the highest ROI, reduce operational and regulatory risk, and align security investments with broader business goals.

Regulatory readiness

Access vetted experts who can deliver the evidence you need to meet payment and privacy regulations (e.g., GDPR and PCI-DSS) or certifications (e.g., SOC2 or ISO 270001), keeping customers secure and regulators happy.

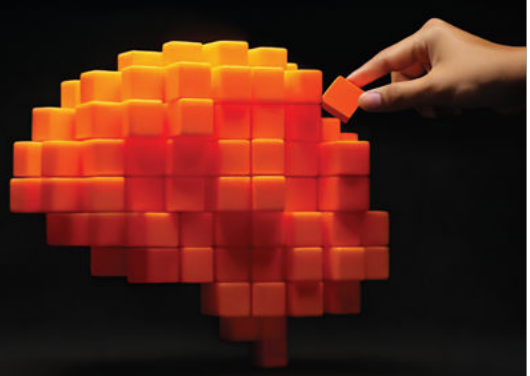
Integrated insights

With the right crowdsourced security platforms, startups can take actionable insights from crowdsourced security testing right into their software development life cycle, so you can quickly fix vulnerabilities and keep shipping.



OVERVIEW

Common crowdsourced security solutions



PTAAS

Pen testing and pen testing as a service

In a traditional pen test, hired hackers use knowledge of various attack vectors to attempt to break through a company's system defenses. Pentesters operate as a team, working within a defined scope for a set period and reporting the vulnerabilities detected. However, these tests can take a long time to set up and ramp up, making them hard to run continuously.

PTaaS solves these operational challenges by implementing many aspects of pen-testing delivery as software. For example, with a PTaaS engagement, once testing is underway, you can monitor results in real time rather than waiting weeks for a final report.

Additionally, with streamlined onboarding and delivery, organizations can easily repeat these tests at scale, contributing to continuous assurance.

Contrary to popular belief, PTaaS *complements* VDPs and MBBs by providing organizations with systematic, continuous analysis at scale. As a result, organizations that adopt these programs together find up to five times as many high-impact vulnerabilities.

VDP

Vulnerability disclosure program

A VDP is a structured framework that invites hackers to submit vulnerabilities they discover in an organization's infrastructure or application directly to the organization. Think of it as a "neighborhood watch" for finding vulnerabilities. VDPs are widely recognized as a security best practice and are often the first step for an organization investing in its security program.

RTaaS

Red teaming and red teaming as a service

Traditional security testing often identifies vulnerabilities in isolation, but that's not how real-world attackers work. That's why many organizations turn to red team engagements, in which they task a group of security professionals (i.e., the "red team") with conducting a simulated attack against the company's technology, people, and processes. According to Forrester, red teaming testing typically results in a 25% reduction in security incidents and a 35% reduction in the cost of security incidents.

Think of red teaming as an advanced exercise that simulates, but doesn't replicate, what threat actors can do to your system. Red team members might execute any of the following:

- **Chain common vulnerabilities and misconfigurations rather than viewing them in isolation**
- **Expose gaps in non-technology assets by compromising internal employees or exploiting weaknesses in physical security**
- **Probe for indirect attack paths through less secure third-party partners or existing technology tools used by financial organizations**

Despite its value and capability, red teaming is underutilized because it's challenging to build and grow skilled red teams that can scale with your attack surface.

Traditional red team consultancies rely on a handful of highly skilled operators who juggle intense, back-to-back projects, leading to burnout and talent shortages.

That's why Bugcrowd introduced Red Team as a Service (RTaaS), which brings the scale and agility of crowdsourcing to red teaming. By blending the power of our global operator community with a range of fully managed engagement models, RTaaS simplifies the implementation and scaling of red team exercises. As a result, organizations can complement and expand their internal security efforts with on-demand red team expertise that integrates easily with existing security workflows.

MBB

Managed bug bounty programs

Bug bounty programs are result-focused security initiatives that encourage hackers to uncover and report security vulnerabilities in an organization's infrastructure and applications. They're similar to VDPs, except they offer a financial reward based on the criticality of the reported vulnerability.

This "pay-for-impact" model comes with several advantages. First, it can help organizations attract top talent quickly and uncover more vulnerabilities than automated scanners. Second, it makes it easier for programs to retain top hackers.

Bug bounty programs are especially valuable for fast-paced teams that deploy frequent updates, as they provide scalable security coverage with minimal additional effort from internal teams.

How crowdsourced security can meet regulatory requirements

There has been a flurry of cybersecurity regulations and frameworks targeting financial services organizations across domains such as data privacy, information security, and payment security.

Here's a breakdown of the most impactful requirements and how crowdsourced security can help meet them.

Information security certifications

ISO/IEC 27001 and SOC 2 are the leading information security frameworks for digital-first companies, providing standardized approaches to protecting sensitive data and demonstrating security competence to customers, regulators, and partners. Here's how crowdsourced security can meet these frameworks' security guidelines:

- **ISO** requires organizations to implement a system for identifying vulnerabilities in key assets and recommends establishing a bug bounty program to meet this requirement.
- **SOC2** has several requirements (such as CC7.1) for implementing detection systems to identify new vulnerabilities. Bug bounty programs, VDPs, and pen testing can be used to meet these requirements.

Data privacy regulations

In the last two decades, governments have passed significant privacy laws in response to growing concerns about how organizations use and manage user data, especially sensitive financial information. These efforts have led to three pieces of landmark legislation:

General Data Protection Regulation (GDPR)

Requires organizations operating in the EU to implement secure data processing practices to protect citizens' privacy

- **California Consumer Privacy Act (CCPA)**
  Requires for-profit businesses operating in California to implement reasonable security measures to protect residents' data and privacy
- **Gramm–Leach–Bliley Act (GLBA)**
  Requires financial institutions in the United States to protect the privacy of their customers' personal information. Institutions must implement appropriate safeguards to protect information and conduct regular testing to ensure they are functioning as expected.

These regulations mandate robust data protection practices, with severe penalties for non-compliance; GDPR violations alone can trigger fines up to 4% of global annual revenue. Crowdsourced security programs that combine vulnerability discovery (VDPs/MBBs) with penetration testing provide a comprehensive approach to meeting these regulatory requirements.

Payment security

The Payment Card Industry Security Standards Council (PCI SSC) has established data security standards (PCI-DSS) for any organization that accepts consumer payment cards. These guidelines highlight crowdsourced requirements to effectively meet critical security requirements. These include the following:

- **PCI-DSS 4.0 / 6.3.1,** which recommends bug bounty programs as a potential solution for assessing vulnerabilities in internally developed software.
- **PCI-DSS 4.0/6.4.1,** which requires periodic vulnerability assessments that can be met through pen testing (including PTaaS).

How financial services organizations use crowdsourced security

Leading financial institutions of all sizes are using crowdsourced security to protect their platforms and customers.

Here are two examples of organizations that have successfully implemented crowdsourced programs:

National Australia Bank (NAB)

NAB is one of the four largest financial institutions in Australia and the 21st-largest bank in the world by market capitalization. With this scale comes an expanding attack surface that requires extensive security coverage, which is why they turned to crowdsourced security. Their first step was to launch a VDP with Bugcrowd, providing a pathway for hackers to report feedback. After seeing initial signs of success, they launched an MBB to actively engage the hacker community for its expertise.

Through both programs, they were able to quickly identify and act on many critical findings before attackers could exploit them, with a low false-positive rate. They also used these findings to demonstrate the maturity of their security program to customers, partners, and the broader financial community.

Website →

Rapyd

Rapyd creates technology for businesses that removes the back-end complexities of cross-border transactions. As the company grew, it sought to elevate its security posture through continuous testing, particularly for its API products. Therefore, they turned to crowdsourced security as a solution, leveraging a private MBB and PTaaS assessments for continuous and point-in-time testing.

In 2023, they discovered and remediated 15 critical vulnerabilities with an average time to remediation of 18 days, almost half the industry average. Building on this success, Rapyd launched a public bug bounty program to support its continued growth and security needs.

Website →

Checklist: How to evaluate crowdsourced security platforms

Not all crowdsourced security platforms are created equal, and the differences can significantly impact the success of your program.

Here are some factors to consider when evaluating platforms:

Scalability

Many crowdsourced security vendors are "one-trick ponies" that treat every solution as an ad hoc, consulting-heavy engagement. Invest in a platform that offers multiple programs to meet emerging use cases and can easily flex capacity as your business needs change.

Low overhead

Ensure the platform provides a fully managed experience, including program design, researcher management, and triage, so your team isn't burdened with extra administrative work or costs. This guarantees that you get quality results.

In-built compliance deliverables

Ensure the platform maps findings to relevant regulatory frameworks (PCI-DSS, SOC2, ISO 27001, DORA, or FFIEC) and supports audit-readiness with clear evidence trails. This reduces compliance overhead and helps you demonstrate due diligence.

Measurable outcomes

Select a platform that provides analytics on program performance, such as remediation speed, risk reduction, and cost savings, so you can demonstrate ROI and show how crowdsourced testing strengthens overall security posture.

Integrations

For a crowdsourced security program to have the most impact, it must be integrated into your organization's broader workflow, including DevOps and the software development lifecycle. Confirm that the platform offers integrations with the tools in your stack (e.g., JIRA, Jenkins, and PagerDuty).

Customized matching

Many platforms use a "spray-and-dump" approach when inviting hackers to their programs, resulting in slower engagement and lower-quality results. Choose a platform that matches you with the right hackers for your program to reduce noisy reporting and ensure high-quality results.

About Bugcrowd

Bugcrowd helps financial services organizations implement security programs that continuously monitor assets while meeting key compliance requirements—regardless of the complexity of an organization's infrastructure.

We have over 12 years of experience designing, launching, managing, and improving successful crowdsourced security and penetration testing engagements for over 1,200 customers across all sizes and industries.

Here's an overview of what we have to offer:

Elastic expert capacity

We provide an unlimited capacity of hackers across various skill sets (e.g., API, LLMs, cryptocurrency, and cloud configuration) that you can't afford to hire in-house. Programs can scale their capacity up and down depending on their needs.

Rich, actionable insights

Your program is guided by a dedicated Technical Customer Success Manager and supported by automated insights from our Security Knowledge Graph.

Clear compliance proof

We deliver clear, credible reports aligned with the SOC 2, ISO 27001, CCPA, GLBA, and GDPR that you can use to demonstrate security maturity to regulators, customers, and partners.

Personalized hacker matching

Bugcrowd uses proprietary CrowdMatch technology to assess each hacker's portfolio (e.g., their skills, report volume, and earned rewards) against your project's scope to build the best possible team for your needs.

Low triage overhead

We have an in-house, globally distributed triage team that filters noise and validates findings so you only see actionable results. Bugcrowd saves your team time without compromising on security outcomes.

Seamless workflow integrations

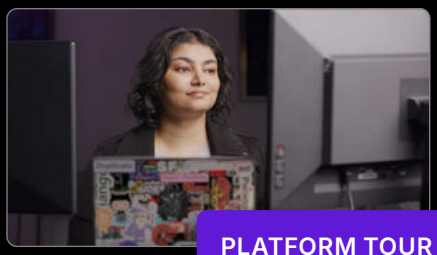
Plug Bugcrowd directly into the tools you already use, like Jira, Slack, ServiceNow, and PagerDuty. We also offer event-based webhooks for event notifications and a rich, easy-to-use API for building custom integrations.

Ready to get started? Take a 5-minute tour to see how the Bugcrowd Platform can connect you with trusted hackers to help you continuously secure your digital assets and stay ahead of attacks.

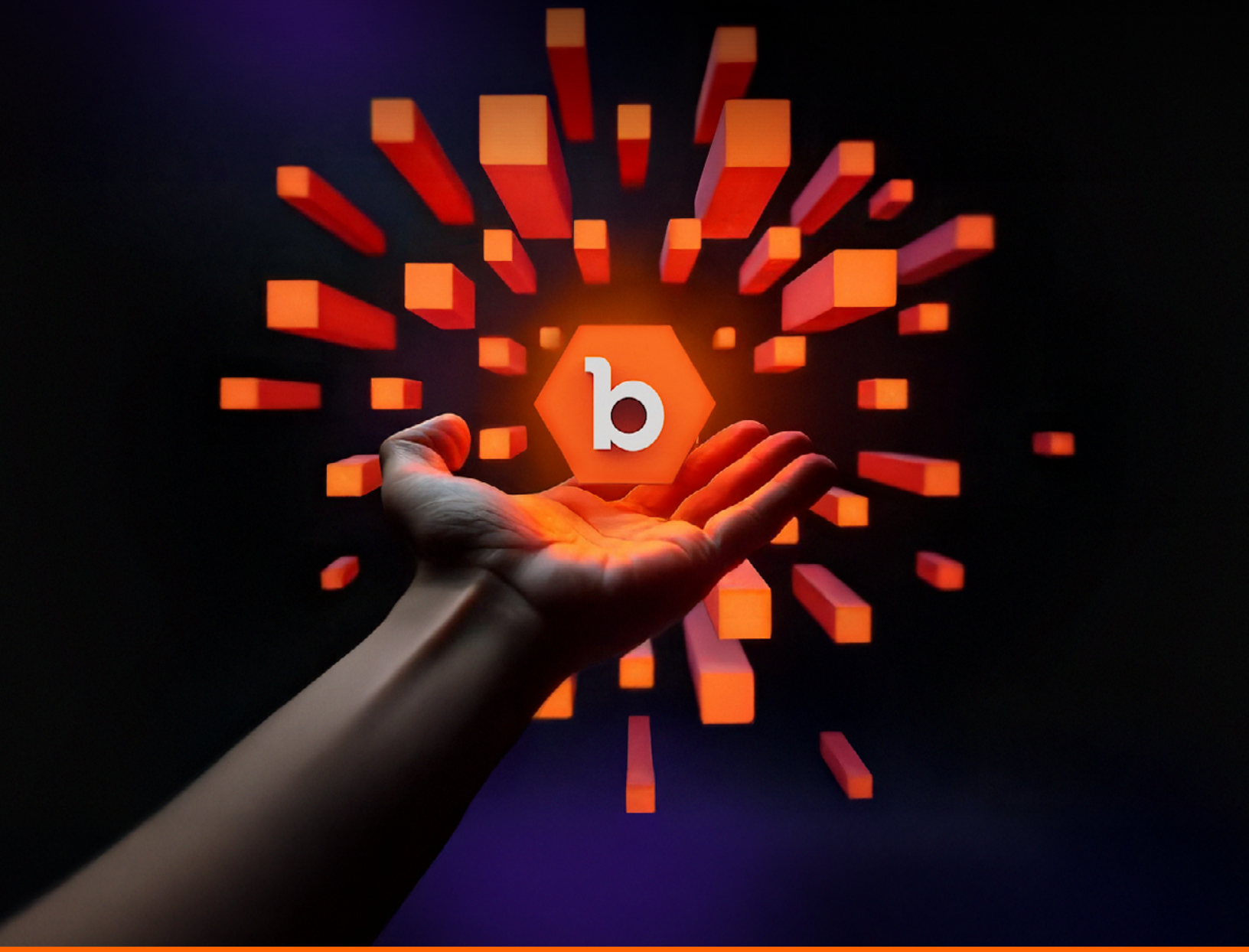
TAKE A 5-MINUTE TOUR

See the Bugcrowd Platform in action

Take a 5-minute tour to get an overview of how the Bugcrowd Platform connects you with trusted hackers to help you take back control and stay ahead of attackers.



PLATFORM TOUR ▶



Unleash Human Creativity for Proactive Security

TRY BUGCROWD