From niche to necessity: global bug bounty adoption accelerates, led by the U.S.

BY ELEANOR BARLOW · FEBRUARY 5, 2026

Bug bounty growth insights across the US

Bug bounty programs have evolved from a niche security tactic into a core component of modern defense strategies worldwide. In this blog, we focus on the US: one of the most invested and fastest-adopting markets, where organizations, driven by higher security maturity, are increasingly using bug bounty to uncover complex vulnerabilities that traditional testing often misses.

What does this growth look like in terms of statistics?

According to LucIntel's 'Bug Bounty Platforms Market Report: Trends, Forecast, and Competitive Analysis 2030', the expansion of bug bounty programs in the US has been especially rapid.

In fact, **North America holds the largest share of the global bug bounty market, at nearly 49%.**

This growth has been driven by major tech firms such as Google, Microsoft, and Facebook, and as focus has moved towards AI integrations and ML enhancements, a 'push for more inclusive and diverse researcher communities' has been backed by significant investments in both private and public sectors.

When discussing Microsoft's partnership with Intigriti, Madeline Eckert, Microsoft, commented that 'We look at the researcher community as our partners and not our adversaries. We see all occasions to partner with the researchers as an opportunity to secure our customers.'

63% of Fortune 500 companies across the US and Canada are running a bug bounty program, and 'over 54% of cybersecurity budgets are allocated to proactive threat hunting, with bug bounty programs representing a key investment.'

Is there an expansion of bug bounty in the US beyond tech and financial companies?

While tech and finance dominate the scene, with 42% of US-based tech companies using continuous vulnerability disclosure programs, all industries, from retail and automotive to gaming, media, and telecommunications, are implementing bug bounty programs as a necessity.

'Adoption is highest amongst companies with over 1,000 employees, accounting for nearly 61% of all contracts awarded to bug bounty platforms in the US, reflecting the growing emphasis on advanced vulnerability management strategies.' - Regional insights and forecast to 2033

For companies with over 1000 employees, security is no longer purely an IT department responsibility and is handled by a dedicated security expert/s. At 1000+ employees, scale, maturity, and risk unite; companies establish legal and disclosure frameworks and the operational capacity to remediate external reports. Their attack surface is large enough that internal tools and periodic testing no longer provide sufficient coverage, making continuous, crowdsourced testing economically attractive. Security budgets and procurement processes also, overall, become necessary rather than ad hoc, allowing variable bounty costs to be absorbed and justified in terms of risk reduction.

> **"Every organization, regardless of the industry or size, has bugs. Proactive disclosure shows that you are not only finding but fixing them before they're found by the malicious actors, and signals to the world that security is taken seriously and backed by action."**
>
> **Jennifer Chaney, Head of Marketing, Intigriti**

How does this growth demonstrate a fundamental shift in perception?

Companies across the US are leveraging the power of continuous, real-world security testing across their digital assets to identify vulnerabilities that might otherwise remain undetected and risk exploitation.

Based in the US, our very own Strategic Engagement and Community Architect, **Chris Holt**, commented on the shift he has observed in the industry, stating that

> **"Bug Bounty has been growing throughout the US for decades and has been through some significant phases. First, there were private programs. Then the era of live hacking was born. This was then destroyed by the COVID-19 lockdowns. Now, post-COVID, we are in an era of substantial growth again as companies are incredibly focused on harnessing the power of the crowd."**

'Bug bounty programs have undergone a fundamental shift in perception, evolving from being seen as a luxury reserved for tech giants to an essential security component for organizations of all sizes. This transformation reflects a growing recognition that traditional point-in-time security assessments alone are insufficient against today's threat landscape.' - Rise in bug bounty programs

How does Intigriti support bug bounty growth in the US?

While Intigriti is headquartered in Europe, we've seen major growth in customers in the US over the last few years, and we're continuing that growth trajectory as we put more boots on the ground in the US in 2026 and beyond.

Below are just a few of the US customers who trust us for their bug bounty needs.

- **The Coca-Cola Company**, headquartered in Atlanta, Georgia, brought its VDP program to Intigriti to further its community growth and provide some exciting changes around reward structure. Reporting that they are 'proud of our researcher community and the impactful findings they have provided over the years.' - The Coca-Cola Company Vulnerability Disclosure Program

- Tech giant, **NVIDIA**, headquartered in Santa Clara, California, highlighted that 'Working with Intigriti's global community of AI experts allows a collaborative and diverse approach to identify risks and strengthen the security of the AI ecosystem.'- Intigriti teams with NVIDIA to launch bug bounty and vulnerability disclosure program (VDP)

David Reber, Chief Security Officer at NVIDIA, stated that 'To secure the full stack of AI infrastructure, it takes more than just advanced technology; it requires collaboration across every layer'.

- **Intel**, based in Santa Clara, California, emphasized in a case study with Intigriti, that the most important element is 'The hackers, the security researchers, the people outside the company doing the work to find vulnerabilities and feed that information to us. Without them, it doesn't matter who our internal customers are. If we have no feed of vulnerabilities, then we're not producing any value.'- How Intel partners with Intigriti to sustain a world-class hacker community

In fact, a report published in February 2025 shows that nearly half of all vulnerabilities that Intel disclosed in 2024 were identified because of a Bug Bounty Program. 'Intel's deep engagement with the security research community drives the success of its Bug Bounty program, resulting in 53% of the vulnerabilities addressed in 2024.'- *2024 Intel Product Security Report* (Slide 24).

- **Grafana Labs** has its headquarters in New York. 'After talking to customers and researchers, it stood clear that Intigriti has the best triage services... and since that's what's important to us, the decision was easy to go with Intigriti.' - David Andersson, Manager of the Security Engineering Team, Grafana Labs

What industries does Intigriti support in the US?

From handling report triage and payments and providing the tools and legal frameworks that make responsible vulnerability reporting and reward distribution feasible, Intigriti supports bug bounty programs for US-based companies in many different industries.

These include:

- **Software** companies like Dropbox (California), DOMO (Utah), Anaconda Inc (Texas), Digital Ocean (Colorado), Liferay (Austin), PDQ (Utah), Qualified (California), Proof (Massachusetts), and Quickbase (Massachusetts).

- **Financial services,** such as Flywire (Massachusetts), Tremendous (New York), Donorbox (Virginia), or Uphold (California).
- **Manufacturing companies**, like Advanced Micro Devices (California), or Rivian (California).
- **Education** services, like Datacamp (New York).
- **Media** companies, like WP Engine (Texas) or Yahoo (California).

Are you a company based in the US? What's holding back your bug bounty journey?

If you're a company based in the U.S without a bug bounty program, it's worth asking the question, 'What's the delay?'

The threats are real, and the solutions are proven. Partner with us and turn potential risk into a strategic advantage.

Contact the team today to schedule a chat, and one of our experts will be in touch.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.