Packetlabs

CASE STUDY

HUBSPOT

Protecting Trust: HubSpot's Impressive Commitment to Cybersecurity Excellence

ABOUT HUBSPOT

HubSpot is an AI-powered customer platform that connects businesses' marketing, sales, and customer service teams with the tools and resources they need to grow better.

With over 248,000 customers and a global footprint spanning 14 offices, cybersecurity isn't just a priority—it's the foundation everything else builds upon. That's why HubSpot takes an "assumed breach" approach to penetration testing to prevent potential risks with the most extensive cybersecurity measures.

HubSpot obsesses over providing value for customers. Alongside their numerous annual "Best Software Company" accolades in the areas of customer satisfaction, products, and more, a strong security posture is a cornerstone of what sets them apart in the competitive global SaaS market.

+248K
CUSTOMERS

+1700
APP INTEGRATIONS

135
COUNTRIES SERVED

14
GLOBAL OFFICES

+8,000
EMPLOYEES

THE CHALLENGE

From Prevention to Protection: HubSpot's Proactive Security Approach

With over **82% of breaches originating from the cloud in 2025**, HubSpot's cybersecurity team recognized that proactive penetration testing was critical to identify risks. That's exactly what they partnered with Packetlabs to achieve.

THE PRIMARY OBJECTIVE

When partnering with Packetlabs, HubSpot's primary objective was to ensure the confidentiality of customer data and guarantee access control best practices for their global team.

This objective aligned with the three main pillars of HubSpot's cybersecurity strategy:

Regulatory Compliance

HubSpot implements controls and processes that comply with current industry best practices and international guidelines for cloud security. They undergo rigorous SOC 2 Type 2 audits annually to validate the security, availability, and confidentiality of customer data and HubSpot products.

Operational Continuity

HubSpot ensures ongoing availability of their platform and customer data while mitigating security risks that would threaten the continuity of service, so customers can access what they need, when they need it.

Customer Services & Information Integrity

HubSpot takes measures to ensure customer information is free of corruption or alteration. As a part of this, they pledge to deliver consistent, exceptional customer support while always safeguarding user confidentiality and privacy.

To support these three cybersecurity pillars, HubSpot partners with industry leaders like Google Cloud Platform (GCP) and Amazon Web Services (AWS) to ensure the highest levels of network and physical security. Both providers use audited security, including ISO 27001 and SOC 2 compliance.

> ***Infrastructure access is restricted and regulated through an access control model. Access is limited to only those employees whose roles require it. Privileges must be assigned based on team, unit, and job requirement***
>
> ***- Parker McGee***
> ***Engineering and Infrastructure Security Lead***

THE STRATEGY: FINDING A PARTNER AS THOROUGH AND COMMITTED AS HUBSPOT IS

When evaluating pentesting vendors, Packetlabs stood out for their tester capabilities and comprehensive approach.

"[The Packetlabs team] really took the time to understand what we were looking for–and went beyond the checkbox to uncover all potential vulnerabilities," says McGee. **"The team even offered services that were initially out of scope. Our original agreement included a limited number of tests but, as the ethical hackers at Packetlabs started working with us, there were additional opportunities identified."**

For this campaign, Packetlabs took an "assumed breach" approach to penetration testing. Their OSCP-minimum certified ethical hackers began under breach conditions using a compromised endpoint system. From there, they investigated what kinds of data could be accessed through this entry point (such as a laptop or mobile device), how far the threat actor could potentially reach before encountering safeguards (such as people, processes, or technology), and whether existing technical defense mechanisms could effectively minimize the impact.

The Packetlabs team conducted a high-level penetration test across HubSpot's entire infrastructure, methodically examining even seemingly innocuous areas for potential vulnerabilities.

HubSpot integrated the Packetlabs testers like team members to ensure they could effectively simulate both external and insider threats.

By going well beyond standard automated vulnerability assessment (VA) scans or surface-level pentests, HubSpot gained unprecedented insight into both existing and hypothetical weaknesses–and clear strategies to address them.

> *"Some pentesting vendors give a list of inconsequential hypothetical vulnerabilities, which they then offer to remediate for an extra fee. Whereby an in-depth "assumed breach" approach allows my team to focus on where we're vulnerable and to determine where to put our effort–and, because Packetlabs leaves remediation with my team, I can rest assured that their discovered vulnerabilities are both authentic and high-impact.*
>
> *- Parker McGee*

THE RESULTS

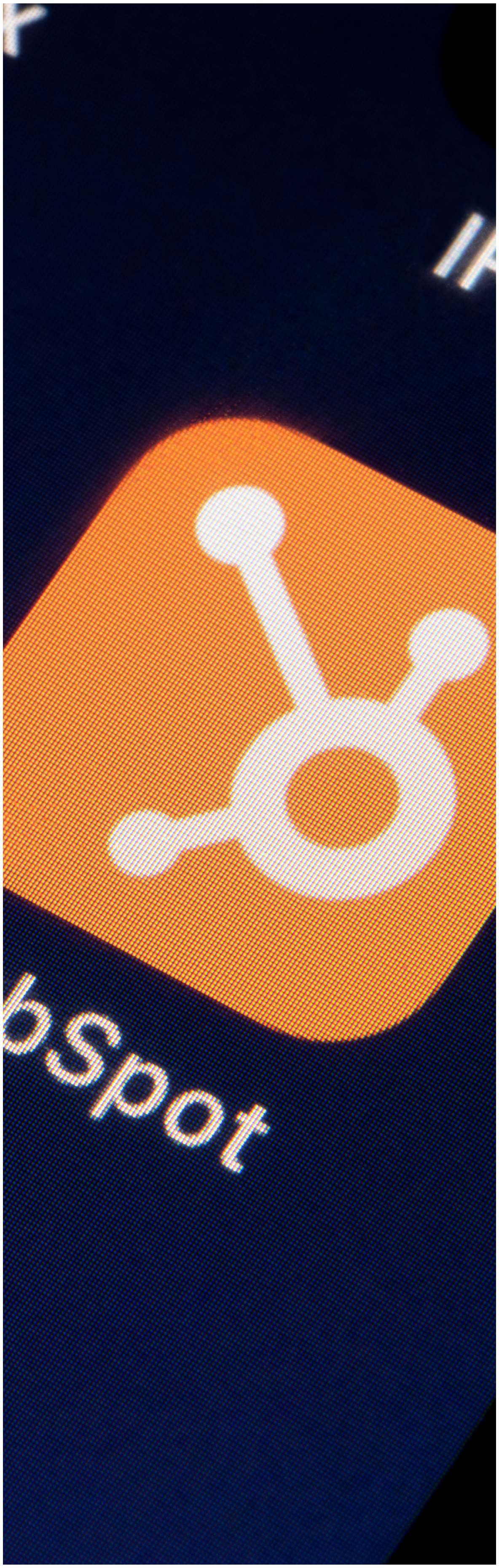
Packetlabs' 100% tester-driven penetration testing approach uncovered potential hard-to-detect vulnerabilities and hypothetical attack vectors that could be exploited. Their detailed, actionable report helped HubSpot's IT team strengthen its global infrastructure and provided in-depth guidance on staying ahead of evolving cyber threats.

"Assumed breach assessments are designed to mimic a threat scenario in which an attacker has already gained access to the internal network via some manner of compromise," Arman Aryanpour, ethical hacker at Packetlabs, explains. "With HubSpot, we achieved this by introducing a 'Patient Zero' PC to their networks. Once the 'PZ' is given power and wired Internet, it will act as an infected PC and will be used to gather intel. Through this, we gleaned valuable insights regarding user credentials, potential vulnerabilities in embedded devices, and network protection–and packaged this in an actionable report.

"Here at Packetlabs, our goal is to identify risks before they become headlines. Taking an assumed breach approach to pentesting is one of the most impact-driven ways pentesting vendors can do this in 2025."

For regulatory compliance, reputation, and business continuity, HubSpot describes Packetlabs as a critical part of their first line of defense against potentially catastrophic cybersecurity attacks, with penetration testing as a crucial component in identifying potential vulnerabilities before threat actors do. "With Packetlabs' 'no egos ever' approach to partnership, both of our teams learnt from each other and challenged each other," McGee states. "That level of open communication, commitment to results, and thorough testing is rare."

HubSpot's Engineering and Infrastructure Security Lead recommends Packetlabs to their peers for our ethical hackers' expertise and coverage-based approach. In addition to the outstanding service, Packetlabs' SOC2 Type II and CREST accreditations gave HubSpot the peace of mind that their information was well protected, and their access control was best-in-class.



Packetlabs

As a CREST and SOC 2 Type II penetration testing firm, Packetlabs' best-in-class methodologies and 100% tester-driven pentesting go well beyond industry standards. Our methodologies dig deeper into your cybersecurity to deliver actionable results. We offer several solutions that push the envelope on security—and guarantee full regulatory and cyber insurance compliance.

Packetlabs was founded on the belief that, in today's ever-changing threat landscape, organizations—and the people who trust in them—deserve more than a VA scan.

Originally formed by an ethical hacker after seeing vulnerability assessments presented as penetration tests, we value the importance of not providing our clients with a false sense of security.

Today, we partner with organizations across all sectors and industries to provide award-winning, 360-degree solutions that are over 95% manual. By partnering with Packetlabs, organizations can identify vulnerabilities faster, generate actionable results, ensure regulatory compliance, and scale their security operations to stay ahead of threat actors.

Ready to Strengthen Your Security Posture?

There is no room for compromise.

Get A Quote.

1-855-758-5227

www.packetlabs.net

X **@pktlabs** in **/packetlabs-ltd-** f **@packetlabs**