PRODUCT EBOOK

hackerone

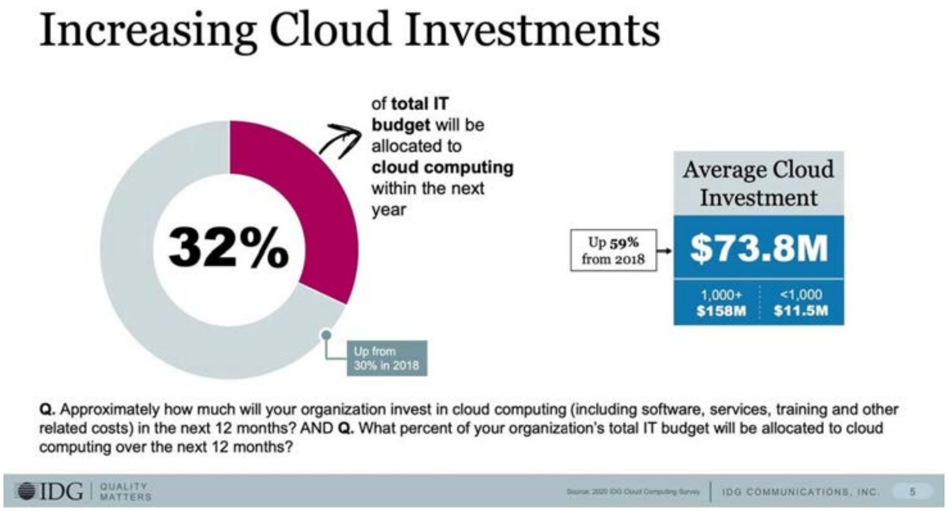
How Hacker-Powered Security Can Help Organizations Secure Their AWS Environments

Table of Contents

Security and Your Cloud Migration Projects

Acceleration of Cloud Computing, Digital Applications, and Remote Work

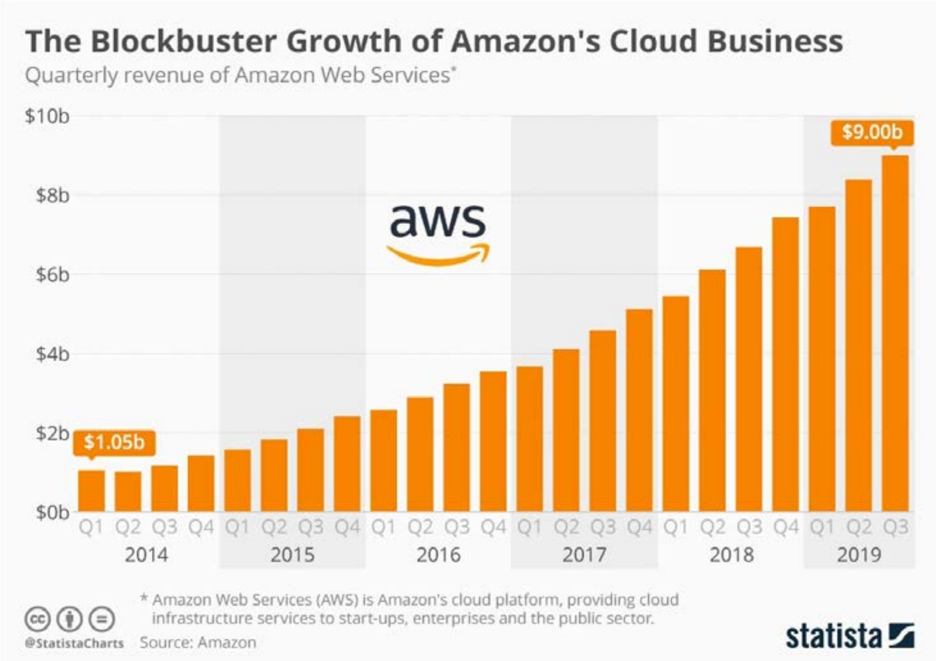
Over the last 15 years, there has been massive growth in cloud adoption for organizations worldwide. A McKinsey report states that in that time, Fortune 500 companies generated over $1 trillion in value related to cloud adoptions, and almost all of that value came from business innovation and optimization rather than IT cost reduction. Organizations are seeing the benefits of cloud infrastructure, including rapid-pace development and increased abilities to scale. They are also reallocating budgets. According to an IDG 2020 Cloud Computing survey, IT departments are now spending almost a third of their budgets on cloud computing.



Q. Approximately how much will your organization invest in cloud computing (including software, services, training and other related costs) in the next 12 months? AND **Q.** What percent of your organization's total IT budget will be allocated to cloud computing over the next 12 months?

The leading cloud infrastructure providers AWS®, Microsoft® Azure®, and Google Cloud™ have seen increasing adoption of their cloud platforms, and those numbers continue to rise.

The leading cloud infrastructure providers AWS®, Microsoft® Azure®, and Google Cloud™ have seen increasing adoption of their cloud platforms, and those numbers continue to rise.



* Amazon Web Services (AWS) is Amazon's cloud platform, providing cloud infrastructure services to start-ups, enterprises and the public sector.

Source: Amazon

As a result of this influx to the cloud and global access to software-based services, customers need and expect new digital applications (web, mobile, and IoT). IDC has predicted that between the modernization of traditional applications and the development of new ones, 25% of all production applications will be cloud-native by 2022. Cloud computing creates a new environment for development teams with easier access to significant resources—including on-demand services, resource pooling, and scalability—for flexible and agile testing and deployment, increased performance, and faster time-to-market. According to IDC's FutureScape 2021, by 2023, over 500 million digital apps and services will be developed and deployed using cloud-native approaches—the same number of apps developed over the last 40 years.

By 2023, over 500 million digital apps and services will be developed and deployed using cloud-native approaches—the same number of apps developed over the last 40 years.

The COVID-19 pandemic has changed the way organizations work, with many implementing full or part-time remote work policies. Forrester's Predictions 2021 indicate that by the end of 2021, the number of remote workers is expected to be three times pre-pandemic levels. Cloud computing and cloud applications are the backbone that enable remote work as per a Forbes article. Many firms were forced to quickly build or upgrade applications to reach employees and customers. As remote work, data and application access, and software development all become part of permanent corporate culture, organizations are exposed to increased risk. According to a Tanium 2020 report, C-suite executives reported a 90% increase in cyberattacks after workers went remote.

Public clouds have eliminated the need for highly trained, authorized employees who were responsible for provisioning compute and storage resources and also responsible for managing the user security configurations. The concept of self-provisioning and the popularity of pay-as-you-go has often led to uncontrolled launch of services or applications without the intervention of dedicated IT personnel or service providers. Perimeter security continues to be important. But adding services, applications, and devices within the perimeter gives limited visibility or a dated view of perimeter resources.

According to Gartner, through 2025, 90% of all organizations that don't control their public cloud will share sensitive data and nearly 100% of all cloud security failures will be the customer's fault.

The absence of perimeter security, or limited and porous perimeter security can mean costly mistakes in the cloud. These errors can include:

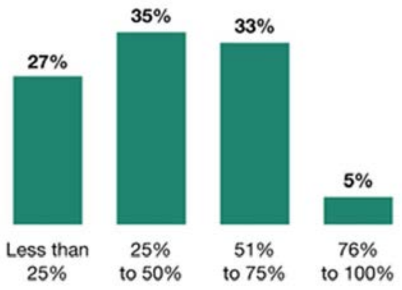
- Misconfigured S3 buckets
- Leaving ports open to the public
- The use of insecure accounts
- Unprotected APIs
- Using components with known vulnerabilities
- Inadequate management of identities, access, and privileges

Multiple publicly reported breaches started with misconfigured S3 buckets that were used as the entry point. According to in-depth research into 40,000 AWS buckets and their cloud storage permissions by Lightspin "46% of AWS S3 buckets could be misconfigured and unsafe."

In addition, organizations are sometimes unaware of what APIs are being used, let alone whether or not they are secure, transforming cloud workloads into easy web crawler targets. According to Forrester's The State of Application Security, 2021:

> *Vulnerabilities weren't limited to traditional web applications—the number of submissions for API vulnerabilities doubled, with broken access control (a common cause of API-related breaches) becoming the top reported issue. With so many organizations exposing a high percentage of applications to the internet or to third parties through APIs, APIs have become a prime target for attackers.*

Percentage of apps organizations exposed to the internet or to third-party services via APIs



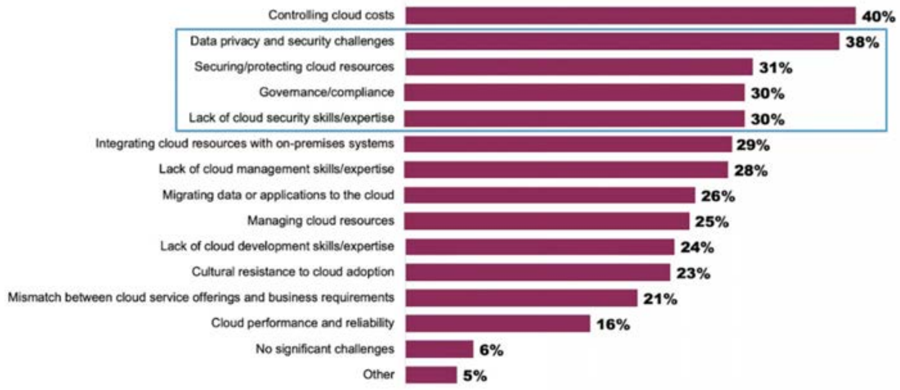
Source: "The State Of Web Application And API Protection," Radware

164041 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited

Other examples of cloud misconfiguration leading to a breach involve DMZ servers that have ports open to the world. These configuration issues continue, often leaving workloads and containers publicly exposed.

These ongoing incidents make security among the top issues in the minds of technology executives and cloud architects according to an IDG Cloud Computing Survey, even as public cloud providers continue to invest in infrastructure security.

Public Cloud Challenges



Q. What have been the biggest challenges or obstacles to your organization's ability to take full advantage of public cloud resources? (overall)

A New Approach to Application Security in the Cloud

Security vulnerabilities are unavoidable. Most organizations realize that increasing their budgets to enhance their cybersecurity posture is not a solution to the problem. It is nearly impossible to address every security flaw even with the most sophisticated software infrastructure and applications, some of the world's most innovative developers, and industry-leading security tools. And some of these flaws can be leveraged by bad actors, potentially creating severe impacts. The only option is to find and fix vulnerabilities before they are exploited.

There is a worldwide movement happening–hundreds of thousands of hackers around the globe are hacking companies, not to steal information, but to secure vulnerabilities. Organizations like the Department of Defense and Adobe are starting to realize the benefits of using hacker-powered security. Hacker-powered security helps them achieve security and compliance objectives by uncovering critical vulnerabilities quickly and comprehensively.

HackerOne believes that ethical hackers can bring a unique approach to cloud application security. Our HackerOne community of hackers is the largest and most diverse in the world bringing varied skill sets and expertise to all engagements and delivering continuous, comprehensive testing and vulnerability discovery throughout the cloud computing ecosystem. Hackers think like malicious actors and mitigate cyber risk by searching, finding, and safely reporting real-world security weaknesses across all industries and attack surfaces before criminals can exploit them. Hackers empower organizations to build data-driven security teams that thrive in a world of ambiguity and change, teams that don't block but enable.

> **“The sensitive nature of our assets and hacker participation requirements makes HackerOne's vetting capabilites a critical component of our program's success”**

Reina Staley
FORMER CHIEF OF STAFF,
DEPARTMENT OF DEFENCE,
DEFENSE DIGITAL SERVICE

Busting the Myths of Hacker-Powered Security

Myth #1 - Hackers are not to be trusted.

During the past year alone, organizations witnessed many devastating cyberattacks. And the threat continues to rise. Though malicious hackers are responsible for these attacks, they represent a small segment of a much larger community. Ethical hackers are the majority and use technical skills and expertise to break into code and find vulnerabilities before an attack. Our HackerOne community is the largest and most diverse in the world.

Eight-two percent of the hacker community define themselves as part-time hackers and 35% have full-time jobs. Despite the majority claiming to be self-taught, many have a technical background. Thirty-seven percent of hackers have studied computer science at a post-graduate level and 20% hold post-graduate qualifications in computer science.

The hacker-powered security, or crowdsourced community, is a global group, with diverse backgrounds, technical skills, and expertise. The hacker-powered security model connects a community of skilled, creative individuals with organizations looking to mitigate risk and improve their security profiles. We encourage our hackers to go through our I.D. verification process where we verify identity and geography through a third-party provider. Many organizations may require identity or geography verification for compliance or legal reasons, or geography may impact application accessibility. This goes beyond the vetting process of many pentesters, who may only go through an interview, reference call, or criminal background check.

Myth #2 - Crowdsourced model fails to produce experienced pentesters.

It's important to use different hackers for testing different apps and subsequent tests of the same application. Organizations using hacker-powered security appreciate the advantages of working with a diversity of skilled and creative hackers. In contrast, traditional pentest engagements may have a limited pool of local pentesters, with no talent continuity.

Myth #3 - Running a hacker-powered security program (whether pentesting, VDP, or bug bounty) doesn't yield high-quality results.

False. Hacker-powered security programs help organizations uncover 7x more critical vulnerabilities than traditional security assessment methods. HackerOne encourages a layered approach to security, prioritized by organizational capabilities, needs, and goals. Automation can only find what it knows to find. Traditional penetration tests add value to many security programs and extend beyond "check the box" compliance requirements. But continuous pentesting programs augment an organization's security strategy. Hacker-powered security uses human creativity to find complex, high-risk, and critical vulnerabilities that automation can't.

Myth #4 - Crowdsourced programs are too risky.

Cyber risk outweighs any potential risk your organization may associate with running a vulnerability assessment, Vulnerability Disclosure Program (VDP), or a bug bounty program. Your externally accessible apps are already targets and may be under attack. Hacker-powered security allows your security team to get more vulnerability findings and visibility into unknown vulnerabilities reducing risk and increasing security.

HackerOne closely monitors public researcher communications and activity. Researchers are penalized for not complying with our Standard Disclosure Terms and Code of Conduct.

Since 2012, HackerOne has invested heavily in building resources and creating opportunities for the hacker community to learn and grow their skill sets. Twenty-five percent of hackers surveyed are learning from online resources, including Hacker101 and Hacktivity. Hacker101 is HackerOne's dedicated resource for hackers, providing free online webinars and lessons for anyone who wants to learn how to hack for good. Hacker101 capture-the-flags (CTFs) empower learners to find bugs in a simulated environment. Over 66,000 hackers found 420,000 flags in CTF challenges in the past year alone, up from 49,000 hackers finding 317,000 flags in 2019.

Busting the Myths of Hacker-Powered Security

Myth #1 - Hackers are not to be trusted.

Myth #2 - Crowdsourced model fails to produce experienced pentesters.

Myth #3 - Running a hacker-powered security program (whether pentesting, VDP, or bug bounty) doesn't yield high-quality results.

Myth #4 - Crowdsourced programs are too risky.

Myth #5 - Crowdsourced pentesting is hype and more expensive compared to traditional pentesting.

Myth #5 - Crowdsourced pentesting is hype and more expensive compared to traditional pentesting.

As the number of companies practicing DevSecOps increases, so does the demand for agile and rapid pentesting. Traditional pentesting is gone. Organizations need a new way of testing that fits with new security practices. HackerOne's SaaS platform retains knowledge of past and ongoing tests, minimizing the need for extensive knowledge transfer and streamlining test and tester onboarding. HackerOne also allows the delivery of incremental test results through its platform for immediate triage and remediation. Traditional pentesting delivers results upon completion when a report is generated, and vulnerability findings are out-of-date. In addition, hacker-powered pentesting yields high-fidelity test findings, meaning fewer false positives and more impactful outcomes.

The cost of a penetration test is based on the amount of human work required to deliver the test successfully, and the work depends on the infrastructure complexity. Traditional pentests are typically based on fixed budgets along with a targeted, predetermined scope. Hacker-powered security engagements are highly flexible in terms of cost, and deliver a more comprehensive view into your system's vulnerabilities. An experienced pentesting team of hackers is a cost-effective way to improve your security profile, find unknown security issues, and mitigate risk. The results are better security and reduced risk, all delivered faster and with more insights. That not only improves your security posture, but it also shows customers you're devoting more effort to ensuring the security of their data, and you're doing it faster and at a lower cost. That's a powerful differentiator that puts you ahead of your competitors.

Traditional Pentesting vs Hacker-Powered Pentesting

	Traditional Pentest	Hacker-Powered Pentest
Scheduling	Typically a four to six week lead time to get started.	Get started in days.
Time-Frame	Point-in-time.	Point-in-time.
Talent	One to two testers are usually assigned to different engagements	Diverse and vetted pentester community with three to five testers assigned to different engagements. Tap into a vast rotating talent pool.
Tester Communication	Interact with project manager(s) but communications with pentesters may vary.	Communicate directly with pentesters to discuss issues and drive engagement via HackerOne platform.
Testing Process	Little to no interfacing with the security team throughout the testing process. The focus is on the final report.	Transparency of your pentest progress across kick-off, testing, retesting, and remediation phases.
Vulnerability Notifications	Critical or severe vulnerabilities aren't disclosed until the final report at the end of the engagement.	Act on vulnerabilities as they are surfaced and reduce remediation lag time. Always aware of vulernabilities.
Vulnerability Management	Tests are purely transactional with each engagement independent from the other.	End-to-end vulnerability lifecycle management beyond initial reporting.
Integrations	No integrations with customer workflows.	Integrations with Jira, GitHub, Slack, etc.
Reporting	Final pdf report consolidates findings, but it's not organized to make important findings accessible, understood, and actionable.	Summarized, actionable report for both executive stakeholders and auditors. Detailed recommendations highlighted.
Pricing	Pentesters paid hourly, regardless of results.	Pentesters paid for coverage and effort.

Hacker-Powered Security for AWS Environments

Hacker-powered security uses the hacker community to find unknown security vulnerabilities and reduce cyber risk. It helps organizations advance their security maturity by providing three primary benefits:

1. Access to skills and expertise that aren't otherwise readily available.
2. Access to a large community of highly skilled, expert hackers to tackle a significant volume of work.
3. On-demand access to knowledge to handle work surges without hiring full-time staff.

To grow the AWS expertise of HackerOne pentesters, HackerOne sponsors hackers to earn AWS Certifications by completing AWS-specific curriculum. AWS Certifications ensure pentesting-experienced hackers have the requisite understanding of AWS environments to more effectively pentest and quickly identify AWS application vulnerabilities. Hacker certification ultimately expands the expertise of HackerOne's hacker community and offers a broader range of skill sets for AWS customers seeking to enhance their cloud security.

Hacker-powered security connects organizations with the global hacking community via three distinct types of engagements:

- Vulnerability Disclosure Programs (VDPs) set guidelines for hackers and security researchers to submit vulnerabilities found in defined assets and systems. Many hackers appreciate the challenge, and VDPs harness that creativity to generate new vulnerabilities continuously.
- Bug bounty programs are like VDPs, but they directly incentivize hackers financially to search for vulnerabilities in defined systems and assets. Organizations publicize a reward structure—along with guidelines of what is and isn't allowed—to attract the attention and expertise of top hacking talent.
- Hacker-powered assessments and penetration tests harness the same skill sets as VDPs and bug bounty programs but in a more traditional, engagement-based model. These engagements take place over a particular time with a well-defined cost structure—hackers with specific skills and expertise address predetermined assets and testing requirements.

When it comes to AWS environments, it's important to point out that many AWS services are based on the Software-as-a-Service (SaaS) model, which means the end-user does not own the environment and it cannot be pentested in the same way as a traditional on-premise environment or Infrastructure-as-a-Service (IaaS) model. However, the configuration and identity of those SaaS services can be tested from a black box engagement or even through a security audit.

Three Primary Benefits of Hacker-Powered Security:

1. Access to skills and expertise that aren't otherwise readily available.
2. Access to a large community of highly skilled, expert hackers to tackle a significant volume of work.
3. On-demand access to knowledge to handle work surges without hiring full-time staff.

Areas That Cannot be Tested Within the AWS Cloud

- Services or applications that belong to AWS
- The physical hardware, underlying infrastructure, or facility that belong to AWS
- EC2 environments that belong to other organizations (such as partners or vendors)
- Security appliances that are managed by other vendors without their permissions
- Amazon's small or micro Relational Database Service (RDS).

There are additional areas that cannot be tested within the AWS cloud worth highlighting due to legal and technological constraints:

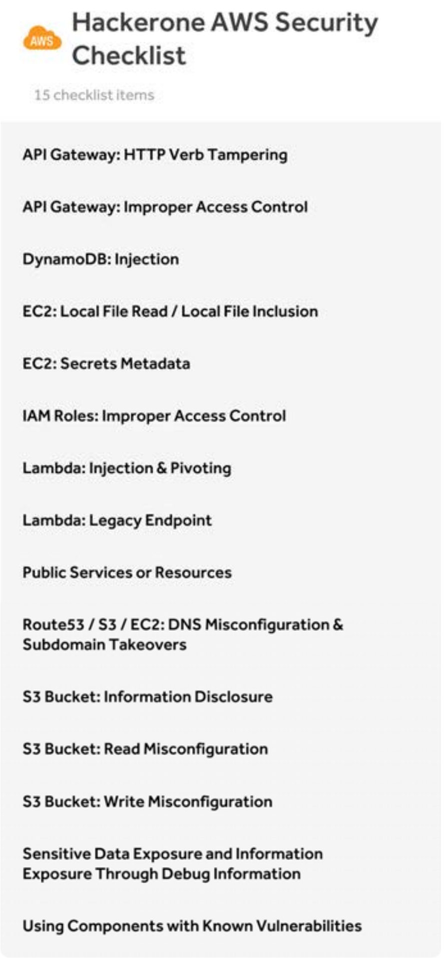
- Services or applications that belong to AWS
- The physical hardware, underlying infrastructure, or facility that belong to AWS
- EC2 environments that belong to other organizations (such as partners or vendors)
- Security appliances that are managed by other vendors without their permissions
- Amazon's small or micro Relational Database Service (RDS)

Pentesting AWS must instead focus on user-owned assets, identify and access management user permissions configuration, and use the AWS APIs deeply integrated into the AWS ecosystem.

HackerOne's approach is to help organizations understand their current cloud security gaps and how to tap into an experienced community to bolster their security posture. Solving misconfigurations and security gaps in the cloud is a great first step. Cloud providers have an enormous, robust, complex set of services available to make life easier for organizations building in the cloud. But what's lacking is the diverse skill set needed to cover all of those services—it is humanly impossible. So, when your developers are building for a cloud environment, it is understandable that they may not have a deep understanding of security, for example. However, the problem is, they are still tasked to develop a secure app. And while the finished product may appear to meet the functional requirements, it may have some severe security gaps—based on a lack of knowledge.

HackerOne can help provide:

- An "always-on" security layer to capture third-party vulnerabilities spotted within your cloud environment
- Continuous testing across your various assets, including web, mobile, network, and APIs
- Targeted pentesting when releasing new products or meeting compliance requirements



Hackerone AWS Security Checklist

15 checklist items

API Gateway: HTTP Verb Tampering

API Gateway: Improper Access Control

DynamoDB: Injection

EC2: Local File Read / Local File Inclusion

EC2: Secrets Metadata

IAM Roles: Improper Access Control

Lambda: Injection & Pivoting

Lambda: Legacy Endpoint

Public Services or Resources

Route53 / S3 / EC2: DNS Misconfiguration & Subdomain Takeovers

S3 Bucket: Information Disclosure

S3 Bucket: Read Misconfiguration

S3 Bucket: Write Misconfiguration

Sensitive Data Exposure and Information Exposure Through Debug Information

Using Components with Known Vulnerabilities

Figure 1: Checklist in HackerOne that specifies AWS-specific methodology

HackerOne Cloud Security Capabilities for AWS customers

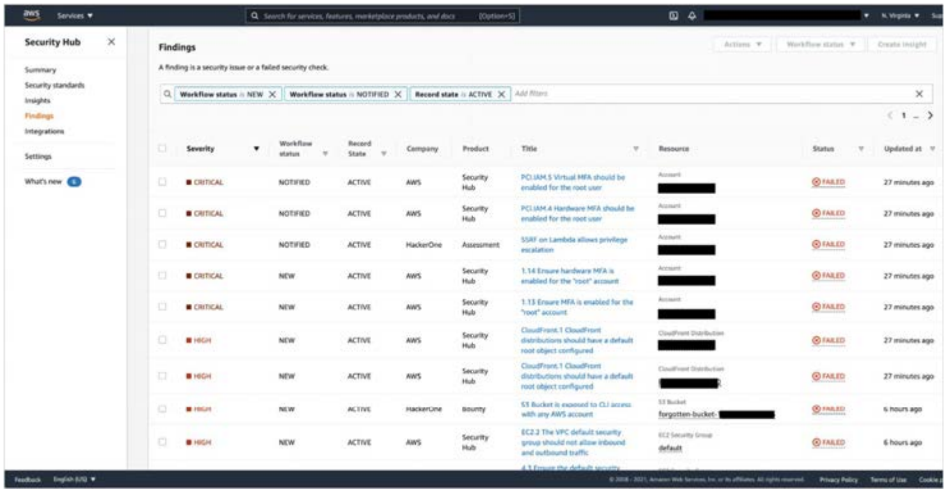
For AWS customers looking to improve security in their cloud applications, HackerOne provides:

- Vulnerability pentests specific to AWS environments
- Integration with AWS Security Hub for fast, effective security actions
- Access to highly skilled background-checked, AWS Certified hackers

HackerOne provides a range of security assessments to meet the needs of our customers ranging from web, mobile, network, and APIs. HackerOne Assessments: Application Pentest for AWS is explicitly tailored for AWS-deployed applications. These pentests discover risks in organizations' AWS environments following a methodology using top HackerOne platform cloud vulnerabilities. As a result, AWS customers prevent data leaks, subdomain takeovers, unauthorized access to applications, and more.

AWS Security Hub provides organizations a comprehensive view of their security alerts and security posture across their AWS accounts. The integration reduces the manual process of comparing and taking action on vulnerability findings between HackerOne and Security Hub with workflow automation to accelerate security actions. By consolidating and routing vulnerability intelligence from HackerOne to AWS Security Hub, the integration delivers greater visibility into crucial gaps that could lead to a cyberattack.

AWS customers can sync all HackerOne vulnerability findings and use AWS Security Hub as the single console for management and prioritization. They can also compare AWS Security Hub findings with those found by the HackerOne community to see duplicates, understand status, and plan remediation, as shown in Figure 2 below.



Findings

A finding is a security issue or a failed security check.

Workflow status is NEW | Workflow status is NOTIFIED | Record state is ACTIVE

□	Severity	Workflow status	Record State	Company	Product	Title	Resource	Status	Updated at
□	CRITICAL	NOTIFIED	ACTIVE	AWS	Security Hub	PCI.IAM.5 Virtual MFA should be enabled for the root user	Account [redacted]	FAILED	27 minutes ago
□	CRITICAL	NOTIFIED	ACTIVE	AWS	Security Hub	PCI.IAM.4 Hardware MFA should be enabled for the root user	Account [redacted]	FAILED	27 minutes ago
□	CRITICAL	NOTIFIED	ACTIVE	HackerOne	Assessment	SSRF on Lambda allows privilege escalation	Account [redacted]	FAILED	27 minutes ago
□	CRITICAL	NEW	ACTIVE	AWS	Security Hub	1.14 Ensure hardware MFA is enabled for the "root" account	Account [redacted]	FAILED	27 minutes ago
□	CRITICAL	NEW	ACTIVE	AWS	Security Hub	1.13 Ensure MFA is enabled for the "root" account	Account [redacted]	FAILED	27 minutes ago
□	HIGH	NEW	ACTIVE	AWS	Security Hub	CloudFront.1 CloudFront distributions should have a default root object configured	CloudFront Distribution [redacted]	FAILED	27 minutes ago
□	HIGH	NEW	ACTIVE	AWS	Security Hub	CloudFront.1 CloudFront distributions should have a default root object configured	CloudFront Distribution [redacted]	FAILED	27 minutes ago
□	HIGH	NEW	ACTIVE	HackerOne	Bounty	S3 Bucket is exposed to CLI access with any AWS account	S3 Bucket forgotten-bucket-[redacted]	FAILED	6 hours ago
□	HIGH	NEW	ACTIVE	AWS	Security Hub	EC2.2 The VPC default security group should not allow inbound and outbound traffic	EC2 Security Group default	FAILED	6 hours ago
						4.3 Ensure the default security			

Figure 2: HackerOne findings in AWS Security Hub console

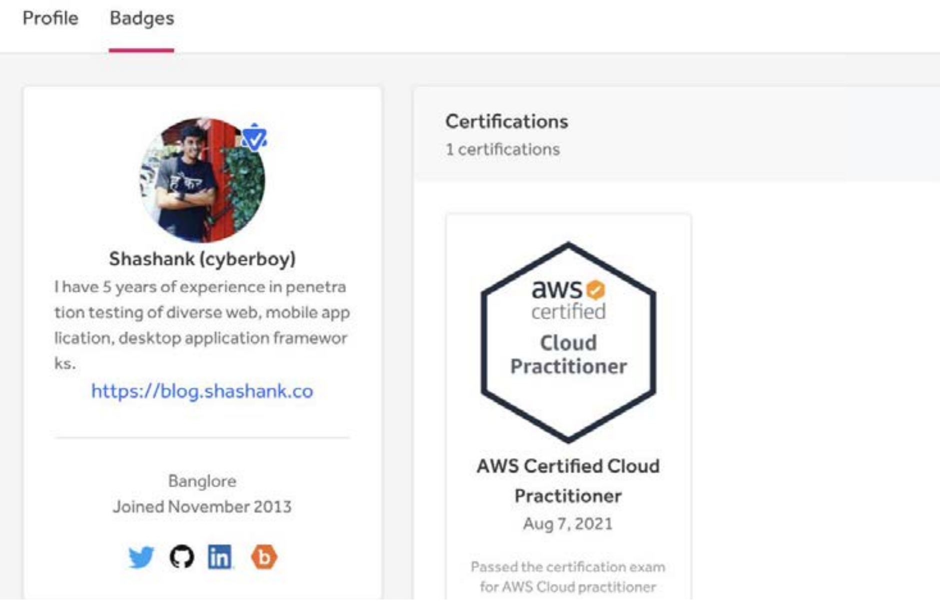
HackerOne Provides:

Vulnerability pentests specific to AWS environments

Integration with AWS Security Hub for fast, effective security actions

Access to highly skilled back-ground-checked, AWS Certified hackers

Organizations worldwide are harnessing the power of human intelligence to surface and resolve vulnerabilities faster. The hacker community's context-driven expertise cannot be matched by any tool. Every time a hacker finds a complex high-risk or critical vulnerability that links several low-severity vulnerabilities together or finds a unique bypass to a software patch, it proves that automation doesn't beat human creativity. Your organization can work with highly-skilled, certified experts with specialized, proven expertise specific to your AWS cloud environment. You will extend your attack surface coverage and address vulnerabilities from multiple threat angles, including cloud misconfigurations, unauthorized access, and data exposure. Instead of switching pentest vendors to find diverse testing expertise, find it all in this talented community of certified hackers.



Profile Badges

Shashank (cyberboy)

I have 5 years of experience in penetra tion testing of diverse web, mobile app lication, desktop application framewor ks.

https://blog.shashank.co

Banglore
Joined November 2013

Certifications
1 certifications

AWS Certified Cloud Practitioner
Aug 7, 2021

Passed the certification exam for AWS Cloud practitioner

Figure 3: HackerOne hacker Shashank (cyberboy) with his AWS Cloud Practitioner certification

Customer Spotlights

WNDRVR

Wind River

Wind River is a global leader in software for the intelligent edge. Its technology powers billions of connected devices and systems across market segments ranging from aerospace to industrial, defense to medical, and telecommunications to automotive. The company's software runs the most important modern infrastructure computing systems across various use cases—from collaborative robots to commercial and military drones, connected cars to the corresponding factory floor—and the communication networks that support these mission-critical intelligent systems.

The company is now expanding to a Software as a Service (SaaS) delivery model for its offerings, with applications built on the AWS cloud. While Wind River's systems and operations remain the same, the software used to power intelligent connected systems is now also delivered remotely, leveraging the scale provided by cloud infrastructure.

As an integral part of the connected world matrix, security is of paramount importance to Wind River. The company needed a comprehensive penetration test of all its applications, its web-based assets, and internet-facing IP addresses to ensure its systems were fully hardened against cyber threats.

As an integral part of the connected world matrix, security is of paramount importance to Wind River. The company needed a comprehensive penetration test of all its applications, its web-based assets, and internet-facing IP addresses to ensure its systems were fully hardened against cyber threats.

Key Stats

Solution

H1 Pentest

Engagement Length

Two Weeks

Outcomes

- **Hardened attack surface**
- **Tested AWS E2 instances**
- **Satisfied ISO 27001 testing requirement**
- **Instant retesting**
- **Cut issues from future code**

Customer Spotlights

WNDRVR

"Traditional penetration tests might have been OK ten years ago, but they don't provide the intensity and range of testing skills we need to make sure our assets are watertight. We need a testing partner that goes beyond a preplanned methodology to find issues a hacker could find and exploit in the real world." Rich Kellen, Vice President and Chief Information Security Officer at Wind River.

During the engagement, ethical hackers focused on identifying high-risk vulnerabilities including EC2 instances that were at risk of exploitation. By focusing on the tools and techniques, hackers simulated the attacks Wind River's assets could face in the real world. The engagement also included a methodology-driven component to meet compliance, business, and risk management needs.

After the engagement, Wind River received a summary report of the vulnerabilities discovered, with clear remediation guidance. After analyzing each vulnerability's root causes, the company's engineering and security teams put procedures in place to eliminate entire classes of vulnerabilities from future code. This proactive approach is part of Wind River's plan to future-proof the security posture of its assets.

> **"The threats we face now are much more sophisticated and varied than they were just a few years ago," concludes Rich Kellen. "To combat a higher class of threats, you need a higher class of security testing, and you need to take a more proactive approach in responding to the issues and vulnerabilities found. HackerOne Pentest gives us the comprehensive and diverse testing we need to protect against advanced threats and ensure our products meet the rigorous security standards we've set over the last 40 years."**

Rich Kellen

VP & CHIEF INFORMATION SECURITY OFFICER, WIND RIVER

Customer Spotlights

aws

Large Banking Institution

An American Fortune 500 financial institution specializing in credit cards, auto loans, banking, and savings accounts made a strategic decision a few years ago to leverage the cloud's agility, scalability, and elasticity in order to provide exceptional banking experiences for their customers. By the end of 2020, they had transitioned 100% off their own data centers and moved to the public cloud.

Despite major investments in the security of their infrastructure and working closely with AWS to implement a comprehensive cloud security strategy, the company recently discovered that an outside individual had gained unauthorized access and obtained certain types of personal information about millions of its credit card customers.

As a result, the organization wanted to identify the threats that exposed their data and comply with regulations and laws involving data protection relating to their business. Now as a cloud-native company, they employed layers of preventative security, including penetration tests and vulnerability scans. While these methods were effective, they couldn't catch everything.

HackerOne was selected to conduct a targeted security assessment of the environment focused on AWS infrastructure and its services. The requirements stemming from the pentesting project had to cover impactful vulnerabilities or misconfigurations, which commonly affect cloud environments. HackerOne's experienced pentesters were asked to exploit attempted attack scenarios, whether successful or not, demonstrate how the attack was performed, and to provide the rationale behind it. The scenarios covered information leakage, web proxy attacks, misconfigurations leading to takeover or information disclosure, and any possibilities of DNS exfiltration.

HackerOne was selected to conduct a targeted security assessment of the environment focused on AWS infrastructure and its services. The requirements stemming from the pentesting project had to cover impactful vulnerabilities or misconfigurations, which commonly affect cloud environments.

Customer Spotlights

The pentesting results were astounding. The most severe issue identified was an Insecure Direct Object Reference (IDOR) found at the endpoint via the app ID, allowing an attacker to view another user's app's client secret. Another severe issue was a Semi-Blind Server Side Request Forgery (SSRF) that allowed for abusing the whitelisted domain policy to achieve arbitrary image hosting. The company's security team noted that this could also be used to disrupt service through the automating of requests between the servers and could pose a potential brand impact if abused to share inappropriate content through the corporate domain. A third severe issue of Cache-Poisoning Denial of Service (CPDOS) flaw was discovered across multiple hosts. Using this flawed behavior, the hacker proved how they could render the asset unavailable to all users by forcing it to cache the wrong response. The HackerOne team also called out a DOM-XSS report that highlighted the potential for Session Hijacking, User Impersonation, or other various client-side attacks against a specific domain.

HackerOne's Application Pentesting for AWS environments helped this global enterprise uncover and address major security issues to achieve their strategic goal of delivering secure and exceptional customer experiences to their customers.

HackerOne's Application Pentesting for AWS environments helped this global enterprise uncover and address major security issues to achieve their strategic goal of delivering secure and exceptional customer experiences to their customers.

Get Started With HackerOne’s Security for AWS Applications

HackerOne’s all-in-one continuous security testing platform directly addresses the needs of organizations using AWS solutions. AWS customers now have access to highly-skilled AWS Certified hackers, AWS-specific pentests, and hacker-powered vulnerability insights to make their cloud applications less exploitable. To learn more, visit our HackerOne and AWS page.

hackerone

HackerOne has vetted hackers for hundreds of organizations including:

GM · Starbucks · Lufthansa · European Commission · Twitter

Spotify · TSRC Tencent Security Response Center · PayPal · UBER · HYATT

Hack the Army · Google · New Relic. · Nintendo · Adobe

HBO · Dropbox · Snapchat · yahoo! · priceline

shopify · slack · yelp · verizon media · TOYOTA

With over 2,000 customer programs, more companies trust HackerOne than any other vendor

Contact Us

www.hackerone.com / sales@hackerone.com