hackerone

RIGHTSLINE GUARDS THE ENTERTAINMENT INDUSTRY'S INTELLECTUAL PROPERTY WITH HACKERONE ASSESSMENTS

—

Rightsline manages intellectual property for the highest-profile names in media and entertainment. To meet customer security requirements and fend off targeted cyber attacks, the company needed a security partner to go beyond traditional penetration testing and provide an accurate simulation of real-world threats.

rightsline

Rightsline is the world's only true, multi-tenant, software-as-a-service rights and contract management platform. Their secure cloud technology platform offers real-time assistance, pipeline management, contract visibility, and inventory management that powers many of the world's leading companies within the media and entertainment ecosystem.

Rightsline manages sensitive intellectual property for the highest-profile names in the media and entertainment industry.

As an organization holding a vast amount of sensitive personal and financial information on behalf of its customers, security is naturally a top priority.

Matt Bricker, CTO at Rightsline, explains:

"Having a robust security posture is the price of entry in our space. Data security is central to our value proposition, and it's one reason we have such strong customer retention. We pride ourselves on using the most secure data protection products and services on the market to ensure customer data remains secure and confidential."

KEY STATS

Solution	Engagement Length	Vulnerabilities Uncovered	Integrations
HACKERONE PENTEST	2 WEEKS EACH	32	SLACK JIRA

BATTLING STATE-SPONSORED THREATS AND CUSTOMER REQUIREMENTS

Customers trust Rightsline to protect highly sensitive intellectual property. To demonstrate its commitment to security and meet contractual obligations, the company has established compliance programs, including annual SOC 2 certification. However, compliance was just the start of Rightsline's commitment to security.

Organizations that hold highly sensitive information are an enticing target for cybercriminals. Rightsline faces a barrage of cyberattacks, including widespread generic threats, probing by Chinese and Russian state-sponsored groups, and targeted attacks by APT groups.

The security team at Rightsline aims to be as proactive as possible, striking a balance between technology and process vs. thoroughness and overhead. As veterans in the cybersecurity space, the team adheres to best practice principles from leading industry-standard sources like AWS, CIS, and OWASP.

Security testing is a core part of the team's ongoing program. However, the security team has faced several challenges in this area. After working with several traditional penetration testing vendors, the team wasn't satisfied with the depth and coverage. At the same time, they didn't have the capacity internally to keep up with the required security testing cadence.

"Having a third-party partner test our platform eliminates bias and provides the objective input needed to assure our customers that we take security seriously," explains Bricker. "There are plenty of penetration testing providers that focus on media and entertainment, but they weren't digging deep enough, so we weren't getting all the security benefits we needed from them. We wanted a partner to deliver deep, thorough security testing, and we needed them quickly before any challenges had a material cost impact to the business."

REAL-WORLD SECURITY TESTING

Aside from depth, the security team at Rightsline had two major concerns about traditional security testing:

1. **The consultative model relied too heavily on the expertise of a small number of individuals.**
2. **Traditional pentests aren't representative of real-world threats.**

Rightsline wanted to move away from traditional penetration testing and adopt a distributed, hacker-powered approach to address this. Being innovators themselves, they were drawn to the solid technical foundation and creativity of the hacking community. The security team recognized that distributed testing from the diverse hacker community could simulate real-world attack vectors more accurately than traditional penetration testing and provides the best formula for obtaining different tester skillsets, mindsets, and approaches, which is vital to help Rightsline achieve high-quality, actionable outputs.

Once they had settled on hacker-powered security as their preferred approach, the security team began assessing their options. Immediately, HackerOne leaped to the top of the list. Bricker explains:

"HackerOne's reputation in the bug bounty market was top notch. Their community lends itself to real-world simulation and removes the bias from working with a more traditional vendor. You get pentesters with different backgrounds and areas of expertise, and HackerOne provided the flexibility and assurance we needed to meet budgeting, SOC compliance, and internal security needs."

MATT BRICKER

CTO, RIGHTSLINE

Rightsline first employed HackerOne Pentest in 2019. During the first engagement, the company needed to complete a pentest within a condensed timeline in Q4 to meet budget requirements and satisfy SOC 2 obligations within the annual audit period.

With HackerOne, the security team got the test up and running in under two weeks, which wasn't possible with a traditional penetration testing provider. They were also able to take advantage of a flexible cost model, scaling the engagement up and down as needed with complete visibility of the impact on application coverage, timeline, and testing depth.

GREATER COVERAGE, FEWER INCIDENTS, AND FASTER SALES

Aside from flexibility, the first thing Rightsline noticed about HackerOne Pentest was the quality of program management. Working closely with the program management team, the security team arranged test and retesting easily and was impressed with the speed of delivery and process transparency.

Rightsline also made use of the dedicated Slack channels to communicate with the pentest team and internal stakeholders. The security team noted that the pentests were flexible and responsive, quickly answering questions to keep the pentest on track and ensure Rightsline was entirely up to date at all times. The pentest team was extremely thorough, providing comprehensive coverage of in-scope assets.

The team at Rightsline was impressed with the transparency offered by the HackerOne platform. Bricker commented that using the platform to see evidence documentation in real-time provided assurance that all security and compliance objectives would be met.

Using the platform's seamless integration with Jira made it simple for Rightsline to process, reproduce, and address reported vulnerabilities.

Bricker was clear that HackerOne Pentests provided a greater ROI than traditional penetration testing.

"The challenge of quantifying this type of program is that it's hard to measure. You can't measure an incident that didn't happen. But we know there's value when an incident doesn't happen. The absence of a measurable occurrence IS the measurement. What we do know is we're receiving more critical vulnerabilities from HackerOne pentests than we did from traditional testing providers. We didn't have a ton of critical tickets, but in less than a year, the number we received let us know where we needed to get more active."

Best of all, by pointing to clearly documented pentest results, Rightsline can easily and immediately demonstrate compliance with customer requirements, which helps the company's sales team close new deals more quickly.

IMPROVING INTERNAL SECURITY CONTROLS

Rightsline has implemented a straightforward process for internal vulnerability management. The team looks at the level of effort needed to fix a vulnerability and weighs that against how obscure it is. For example, if a vulnerability takes ten steps and a huge degree of expertise to exploit or requires user authentication, the team considers it obscure. Based on this analysis, the team prioritizes vulnerability findings and decides how to remediate them. The HackerOne platform provides clear instructions to reproduce each vulnerability, fitting easily into Rightsline's process.

Using the documentation and guidance provided, Rightsline also feeds pentest findings directly into the software development lifecycle (SDLC). The company's security and engineering teams have revamped the code review process based on pentest results and identified and fixed a deficiency that solved multiple issues in a single stroke.

"Our processes were already pretty tight, but it's great to have a resource to help us refine them further," explains Bricker. "Not only does this help us improve our internal security controls, the documentation provided by HackerOne also makes it easy for us to explain to C-Suite executives or less technical leaders what we're doing. The reports from HackerOne's platform enable us to consistently categorize the findings of each pentest, see how fast we're remediating issues, and support our goals to constantly improve our processes."

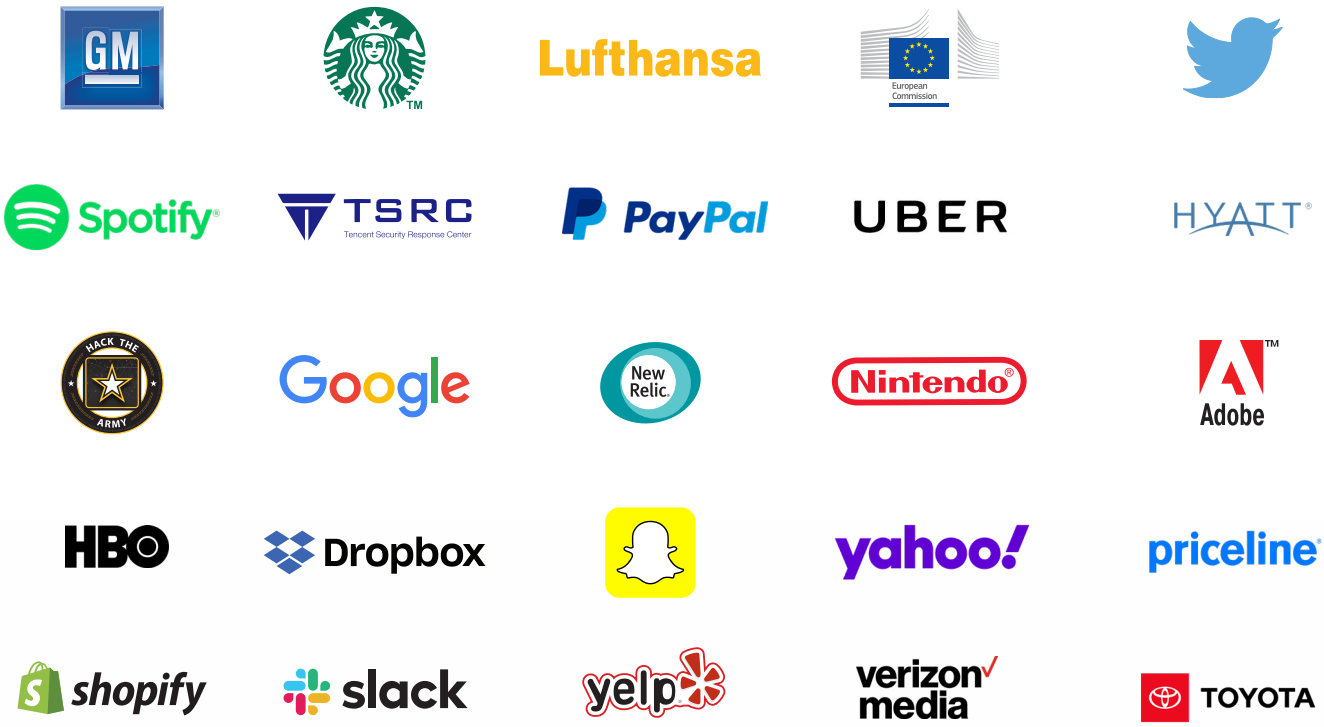
WHAT'S NEXT FOR RIGHTSLINE?

Based on the success of their initial HackerOne Pentests, Rightsline plans to expand its program to twice-annual testing. The team is also considering using feature-specific testing to support its rollout of more critical business functions that will handle even more sensitive data. Bricker explains:

"We are actively looking to increase our security posture. We're hiring Sr DevOps resources with specific security backgrounds and engaging in more security-specific training for senior Engineering resources. To support our efforts, it's natural for us to expand our pentest program to facilitate a higher testing frequency. And since HackerOne has provided us with more and higher quality findings than traditional penetration testing providers, we'll definitely be continuing our partnership with them."

hackerone

HACKERONE HAS VETTED HACKERS FOR HUNDREDS OF ORGANIZATIONS INCLUDING:



With Over 2,000 Customer Programs,
More Companies Trust HackerOne
Than Any Other Vendor

CONTACT US