



**ZenSár**

# Vulnerability Assessment and Penetration Testing

---

**CASE STUDY**

## Vulnerability Assessment and Penetration Testing

Brainshark, a provider of on-demand presentation solutions, helps its customers deliver business communications that are both powerful and convenient. More than 600 world-class companies rely on Brainshark's software as a service (SaaS) offerings to communicate critical information to employees, customers, and partners. Both Brainshark and its customers share the mutual goal of achieving the highest level of IT security and data protection.

Brainshark is often asked by its prospects to provide documentation validating the security of its SaaS applications. Brainshark's customers are some of the largest organizations in the world, and they use Brainshark within their daily business communications for marketing, selling, training, and other corporate communications. Their customers' security standards are high and Brainshark makes it a priority to meet and exceed these requirements. During the negotiation and prospecting stages of the sales cycle, Brainshark's sales team is often asked by customers for third party documentation or "proof" of the company's strength of security.

While Brainshark knew its systems were secure and could prove it with its own documentation, customers often required verification from an external company. "To address customer and prospect questions, we needed to undertake a third party security assessment," said Arnie Greenfield, vice president and CTO of Brainshark. "One of our main requirements was that the company was a well-respected and experienced organization whose name would resonate with our clients and prospects. Zensar met our requirements, and the requirements of our customers."

The main challenge was that Brainshark needed to validate the security of its offerings to meet customer requests.

### Solution Overview

Zensar's Vulnerability Assessment and Penetration testing procedures are based on industry best practices perfected over hundreds of engagements at client sites. For Brainshark, Zensar conducted a three-pronged assessment, including vulnerability tests, a port scan and penetration testing. The vulnerability assessment included tests for SQL injection, cookie manipulation, access control weaknesses, session state, and cross-site scripting.

The focus of the tests was to identify host as well as application security concerns. Once the assessment was completed, Zensar and Brainshark partnered to review the results, discuss remediation of the few non-critical concerns the assessment brought to light, and complete a report to be delivered to a specific customer that had requested a meeting to review security.

The client was quick to applaud the work of Zensar's security team and Brainshark, and expressed satisfaction with the results of the security assessment. "Our customer was very comfortable with the results of the assessment. The client was already confident in the ability of our solution to improve business productivity, now with confidence in our security posture, the client can truly achieve maximum benefits from our solution," added Greenfield.

## Business Benefits

- As a result of the security assessment by Zensar, Brainshark now has peace of mind that comes with an expert, third-party validation of its security policies. Its customers also trust the results of the assessment, and are investing further in leveraging the Brainshark solution.
- “We now have a ‘stamp of approval’ from one of the top security consulting organizations to confirm the security and integrity of our solutions. This goes a long way in easing our sales cycle and ensuring continued customer confidence in the security of our solutions,” said Greenfield.