ENHANCING AI SECURITY: HOW VENTRILO.AI REVOLUTIONIZES WRITING ASSISTANCE

CUSTOMER SNAPSHOT

Ventrilo.ai

INDUSTRY	Technology – Software & Services
CUSTOMER	Ventrilo.ai is an intelligent writing assistant designed to understand context and help end users write more effectively. It offers autocomplete to anticipate train of thought, and a sidebar chat to help brainstorm and refine ideas.
SERVICES PROVIDED	Application Penetration Testing; AI/ML Security Assessment

"What impressed me was how Bishop Fox worked in parallel with our ongoing development. They didn't slow us down but still managed to provide thorough testing of our systems."

— **ANDY CHOU**
CEO, Ventrilo.ai

THE CHALLENGE:

As Ventrilo.ai prepared to bring its context-aware AI writing assistant to market, the team prioritized a comprehensive security validation to proactively identify and mitigate vulnerabilities that could impact platform integrity, user trust, and operational resilience.

The company faced several specific security challenges:

- Protecting User Privacy and Data Integrity: Ensure that systems are designed to handle sensitive information according to industry standards like SOC2 and GDPR.
- Securing the Chrome Extension: Prevent the browser extension from being compromised if the user visits malicious sites.
- Safeguarding Backend Systems: Protect APIs and infrastructure from attacks.
- Defending AI Resources: Prevent theft of valuable AI tokens and GPU resources.

"We wanted to prioritize building in security and privacy from the beginning. Users of AI products are increasingly aware of the importance of how their sensitive data is being treated, so we needed to know our security was solid before launching to the public."

— **ANDY CHOU**
CEO, Ventrilo.ai

THE SOLUTION:

Ventrilo.ai brought in Bishop Fox to assess the security of the product before it reached users. The engagement focused on real-world attack scenarios, working collaboratively with Ventrilo's development team throughout the process.

GOALS OF ENGAGEMENT

- Assess API services for susceptibility to direct and indirect prompt injection
- Ensure input validation and output sanitization are properly implemented
- Test for authentication and authorization vulnerabilities
- Identify any sensitive information disclosure and session management issues

The engagement culminated in clear, actionable reporting of discovered issues with vulnerabilities prioritized by risk. A technical handoff meeting facilitated direct communication between Bishop Fox's security experts and Ventrilo's engineering team.

"Bishop Fox took the time to understand our architecture and target users. They weren't just checking boxes, they were thinking about our specific context and what would actually matter to us."

— **ANDY CHOU**
CEO, Ventrilo.ai

THE OUTCOME:

Bishop Fox's security assessment delivered substantial benefits to Ventrilo.ai, enabling them to launch their product with confidence in its security posture.

KEY RESULTS

- Critical vulnerabilities identified and remediated before launch.
- Enhanced protection of sensitive user data.
- Secured Chrome extension against potential exploitation.
- Protected valuable AI resources from unauthorized access.
- Established foundation for ongoing security practices.

"Bishop Fox's work gave us confidence that we had hardened our system against real-world attacks. The team was responsive and efficient, and their findings were clear and actionable. They worked around our development schedule, making the entire process smooth and valuable."

— **ANDY CHOU**
CEO, Ventrilo.ai

ABOUT BISHOP FOX

Bishop Fox the leading expert in offensive security, providing comprehensive assessment of modern environments with continuous attack surface management, red teaming, and penetration testing for applications, cloud, network, and products. We've worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all of the top global media companies to improve their security.

LEARN MORE AT BISHOPFOX.COM