

Systematically reduce your third-party cyber risk

Overview

Tenchi is a Series A funded company on a mission to radically improve the effectiveness of **third-party cyber risk management**.

Problem

Critical third parties, but without the right security solution, organizations are left overextended.

Current solutions mean first parties blindly accept risk while third parties have little to no incentive to actually improve their security posture outside of minimal compliance requirements.

Solution

Tenchi provides both a product and service for a comprehensive solution to actually reduce third-party cyber risk.

Through our Third-Party Security Posture Management solution, Zanshin, we help first-parties gain deeper visibility into the third party environments.

Security issues found by Zanshin are then facilitated by our Remediation Success team directly with the third party itself, saving first parties countless hours of work.

"Zanshin has helped us accelerate the process of identifying and fixing vulnerabilities in our partners' environments, and in a short time, over 90% of the risks that could expose customer data and information to cyber threats have already been resolved."

Cristiano Adjuto
Chief Information Security Officer
B3 [Brazilian Stock Exchange]



An effective TPCRM program requires 3 pillars



Cooperation from Third Parties

Proactive collaboration between first and third-parties allows for an aligned goal of reaching a more secure supply chain.



Comprehensive Security Data

Real visibility and wide coverage (endpoints, IAM, PaaS, etc) are how a first-party can truly understand the risk they adopt when working with a third party.



Continuous Assessment

Continuous monitoring (daily outside-in and inside-out testing) allows first parties to enforce a secure posture year round, rather than trusting point-in-time audits

Transform your TPCRM Program With Zanshin



Material Risk Reduction

Using Zanshin leads third parties to resolve an average of 80% of critical and high severity findings during the first 8 weeks of engagement.



Vigilance, not due diligence

Shifts from a reactive, point-in-time assessment model to a proactive, continuous monitoring approach.



Always-on Accountability

Hold third parties to a higher standard with enforceable security metrics like remediation timeliness over time.



Inside-Out Security Visibility

Get security data directly from the third-party source and from an inside-out point of view with a non-destructive scanning.



Investment In Risk Reduction

Build long-lasting relationships with third parties by investing in their security posture and remediation success.



Accelerate the Business

Send unlimited security questionnaires and help third parties remediate issues quickly for faster security team approval.

Why Tenchi

Third parties actually enjoy working with Tenchi, allowing for **immediate and proactive cooperation** with their first parties

- ✓ Non-intrusive Access and Data Masking: Zanshin only reports back security results so that first-parties are not liable for private third-party data.
- ✓ Third Parties Love Tenchi: Our customer success team works directly with third-parties to remediate vulnerabilities.
- ✓ First-Party Investment: Because of Zanshin's unique licensing model, third parties are able to "opt in" to a first party investing in improving their security posture.

Licensing

Yearly subscription based on the number of third parties monitored, with progressive discounts on the number of licenses and contract term.

Feature	Starter License	Business License
External Attack Surface (ASM)	✓	✓
Questionnaires (SAQ)	✓	✓
IaaS and PaaS		✓
SaaS		✓
Endpoints (Q4 2024)		✓
Recommended usage	Relevant but less critical Third parties.	Third parties that support critical businesses or have access to sensitive data.

Effective TPCRM Drives Business Forward



Accelerate business deals

Greater visibility and enforceable accountability allow first-party security teams and business teams to be aligned at the start.



Create long-term relationships

Improving third-party security posture allows for more trust and an open line of communication.



Reduce financial losses

Actual reduction of security risk protects both the third party and first party from potential breaches.