TENCHI

# Third-Party Security Posture Management

Overview

**Third-Party Security Posture Management (3SPM)** is a proactive and data-driven strategy to manage an organization's expanded attack surface. Third-party cyber risk management programs are often built around processes where either third-parties attest to their own security and compliance posture or an external vendor provides a score based solely on an outside-in view. This risk acceptance and transference approach leaves much to be desired by security-minded leadership.

## The Challenges of Third-Party Cyber Risk Management Today

### Missing the Big Picture

Existing solutions focus on pre-contract information based on external scans or self-attested information through questionnaires. Organizations lack any real visibility into third parties' actual security posture.

### Point-in-Time Visibility

Most tools and processes are focused on pre-contract or yearly assessments, or outside-in scans updated typically monthly. A modern third party's security posture changes multiple times per day, and having continuous vigilance and assurance is essential to actually prevent incidents.

### High Third-Party Variance

An organization's external entities can range from vendors and providers to partners and sales channels. Because a business often relies on a third-party entity for a mission-critical function, its attack surface quickly expands.

### Significant Resource Constraints

Effective management of third-party cyber risk requires tangible reduction in risk. Because of the sprawling nature of third parties within any business, teams face limitations in budget, relationships, and expertise, making it exceedingly difficult to manage any business-critical external entity. At scale, manual and tech-assisted review processes break down due to the over-reliance on questionnaires.

### Lack of Control and Accountability

The nature of third parties is that their business, technology, and security decisions are made by them. Coupled with the lack of visibility into the outcomes of their actions, it is difficult to hold them accountable for good security hygiene and practices.

### Lack of Risk Reduction

Even the most comprehensive TPCRM products today provide a form of risk assessment and add layers of compliance and security requirements to have something to point to in the event of a security incident. While this is important as a method of enforcing rigorous security controls and industry standards, risk is not actually reduced (it is only mitigated and transferred).

## How Tenchi Systematically Reduces Third-Party Risk

Zanshin is the world's first Third-Party Security Posture Management Solution, built by a team of cloud and security experts at Tenchi Security. Zanshin is deployed internally with a third party, allowing organizations (for the first time ever) to gain actual visibility into their expanded cyber risk. It scans the environment, alerting on security issues with infrastructure, compliance, identity, and more.

Zanshin's access is read-only, non-invasive, and does not report private details back to first parties.

By giving first parties real visibility into the security practices, processes, and posture of their third parties, businesses can hold their external entities much more accountable and take informed actions.

Zanshin's effectiveness is then compounded by folding Tenchi back in, where Tenchi's cloud and security experts work directly with third-party security and IT teams to remediate the issues found in third parties, taking third-party vulnerability management, negotiation, and reporting off the plate for already busy security teams.

### Third-Party Observability

By contextualizing the security data, businesses can understand the health of their third parties' security programs in a completely new way. They gain access to metrics like remediation timeliness and non-compliance frequency. Comprehensive daily checks provide alerts on multiple security disciplines, such as IAM, at-rest encryption, endpoint security. This level of vigilance also then holds third parties accountable to contractual security obligations (made even easier through Zanshin's custom SLA configurations).

### Tangible Risk Reduction

Risk management is not complete without the actual reduction of risk. Tenchi's Remediation Success team works directly with third parties to prioritize, explain, and encourage swift remediation of critical security issues. With Security Score, Tenchi gives organizations a numerical and letter grade benchmark of security posture, refreshed at regular intervals using internal and external data from agentless API connections for a more accurate view than ratings based only on external data.

Customers report an almost immediate positive impact to their third-party security risk with Tenchi's involvement!

## Improve Their Posture, Reduce Your Risk

- **Automated Scans, Real-Time Monitoring:** Zanshin continuously performs scans to detect issues in real-time and track remediation progress.
- **Pre-Contract Due Diligence:** Evaluate vendor security posture before onboarding. This provides a clearer view than questionnaires by allowing cooperative reviews with shared data or anonymous checks against public information.
- **Remediation Success Team:** Focus on more important tasks while our dedicated team of security experts assists third parties in fully remediating security findings.
- **Free and Unlimited Security Questionnaires:** Gain extensive access to security questionnaires to further assess and ensure compliance and security hygiene.
- **Customizable SLAs and Reporting:** Customize SLAs to meet your specific security requirements and business needs for continuous third-party vigilance.
- **Inside-Out Visibility:** Zanshin scans third-party IaaS, PaaS, SaaS, endpoints, and security disciplines often ignored by external scoring solutions.
- **Observability Metrics:** Understand third-party risk holistically with unique and important metrics like remediation timeliness.
- **Comprehensive Compliance Mapping:** Map your security controls and practices to industry best practices, regulatory requirements, or your custom standards.
- **Non-Intrusive Third-Party Data:** Get immediate buy-in from third parties as we only report security metrics, negating any first-party liability.

## Cloud and Security Expertise Built In

### Threat Research

Zanshin's security checks are always updated with the latest findings from its dedicated security research team.

### Industry Leadership

As leaders in cyber risk management, we build Zanshin with security outcomes in mind.

TENCHI

Book a Demo at https://tenchisecurity.com/book-a-demo