TMPC
STRATEGY & SECURITY

SERVICE FACTSHEET

Vendor Threat Mitigation

Third-party providers often hold access to sensitive data and systems. TMPC identifies and reduces that risk so vendors do not become the weak link, and connects vendor oversight to your insider threat and monitoring operations.

What we assess

- Vendor security posture through policy reviews and compliance audits
- Contract security, confidentiality, and data protection clauses
- Vendor access: restricted accounts and network segmentation
- Alignment with your controls, including MFA and encryption

Threats we address

- Supply chain attacks that pivot through a vendor
- Vendor staff misusing sensitive data
- Unpatched vendor systems
- Phishing that impersonates trusted vendors

How we reduce risk

- A formal vendor risk management framework for onboarding and monitoring
- Risk-tiering and standardized assessments
- Data minimization and right-to-audit clauses
- Planned off-boarding: data returned or destroyed

Built to connect

- Aligned to NIST SP 800-161r2 supply chain risk management
- Continuous monitoring and threat intelligence on vendors
- Incident response coordination with vendors
- Integrated with insider threat hub and UAM operations

How TMPC helps

Our team brings more than 30 years of combined insider threat experience and the proprietary processes built from it. For 8 years, TMPC has delivered continuous counter-insider threat and user activity monitoring support to a DoW (DoD) customer, work that drove that program to a #1 ranking among 24 DoW components by DCSA and DIA.

To talk with our team, contact info@tmpcinc.com or 813.524.6935.