3rd Party Risks

In the interconnected ecosystem of modern business, the reliance on third-party vendors and supply chains has become a cornerstone of enterprise operations. With the ubiquity of encrypted communications, the challenge of maintaining security while adhering to legal, regulatory, and privacy requirements has intensified third-party Risk Management (TPRM) Governance.

The surge in encrypted communications is a double-edged sword; while it protects information in transit, it also offers a veil of secrecy that malicious actors can exploit. Enterprises must grapple with numerous challenges. The encrypted nature of communications can be a hiding place for attackers and other malicious activities, making it difficult for enterprises to ensure their networks remain uncompromised. In regulated industries, third-party risk management governance is not just a best practice but often a regulatory necessity.

To address these challenges, Venari Security offers a unique approach to managing the risks associated with third-party encrypted traffic. Venari Security ensures enterprises have a strategy for gaining visibility of third-party encrypted communications. This encompasses identifying, assessing, and controlling risks presented by third-party engagements.

By ensuring that all third-party vendors meet the defined legal obligations for encrypted communications, Venari Security helps organisations maintain compliance, allowing enterprises to monitor their encrypted communications to ensure policies are adhered to and maintained to manage TPRM effectively. The ability to detect suspicious communications and identify violations in real time is a critical component of the Venari Security offering. This proactive stance on security helps enterprises to mitigate risks before they escalate into breaches.

Venari Security provides real-time information crucial for Governance, Risks, and Control (GRC) teams. This enables a dynamic response to suspicious behaviour and enhances the overall risk posture of the enterprise. The necessity for encrypted traffic analysis in managing third-party and supply chain risk cannot be overstated. As enterprises expand their reliance on third-party vendors, the need for sophisticated tools to analyse encrypted traffic in real-time becomes increasingly critical. Venari Security offers organisations a way to meet the third-party/supply chain communication challenges of today's business environment and establish a robust governance framework that can adapt to the evolving landscape of cyber threats. By implementing such solutions, enterprises can safeguard their operations, protect their reputations, and ensure the integrity of their data in the face of third-party risks.

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.
16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.