THE CHALLENGE
As organizations embark on their digital transformation journey, they increasingly rely on third parties to help fuel rapid innovation in products, services and business processes that require strong information security. While many of these third parties have formal contractual relationships including security obligations, others do not. Furthermore, third parties rely on their own third parties (also known as fourth parties).

While business activities can be outsourced to third parties, organizations retain the risks associated with their third-party relationships. To manage risk within acceptable boundaries, it is important to understand these risks, as well as the controls that third-party providers have in place.

OVERVIEW
RSA Archer® Third Party Security Risk Monitoring delivers transparent security measurements, analytics and analyst-level insight to dramatically improve your third-party information security risk management program. It provides organizations with visibility, insight and actionable intelligence into their third- and fourth-party IT risk environments. You can quickly assess the effectiveness of each third party’s security controls with standalone capabilities or as a supplement to questionnaire-based control assessments.

The RSA Archer Third Party Security Risk Monitoring use case discovers and analyzes each third party’s IT footprint. Using artificial intelligence (AI), algorithms automatically assess the risk posture of various third-party IT assets to understand how well third parties manage information security. You can leverage Third Party Security Risk Monitoring as a stand-alone solution for monitoring third-party risk or as the basis for implementing a broader IT and third-party risk management program when deployed with complementary RSA Archer use cases.
KEY FEATURES

- Receive an actionable view of security issues for each of your vendors
- Pinpoint potential exposures and root causes for 40+ security criteria
- Obtain on-demand assessments of an organization’s security practices
- Demonstrate risk control quality to regulators and standards bodies
- Proactively identify common exposures throughout your vendor portfolio

KEY BENEFITS

With RSA Archer Third Party Security Risk Monitoring, you can:

- Respond more quickly to deteriorating third-party controls that might lead to information security breaches
- Gain objective insight into your third-party security performance and IT landscape
- Enhance visibility to high-risk third parties to allocate limited risk management resources
- Engage vendors with accurate, actionable security performance insights and corrective actions
- Continuously monitor vendor security performance
- Optimize use of analysts’ time and outside auditor resources

ABOUT RSA

RSA Archer® Suite enables organizations to manage the broad dimensions of business risk and confidently pursue digital opportunity. The suite is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to informational change. For more information, go to rsa.com.