DATA SHEET

Archer® Third Party Security Risk Monitoring

Use Case for Third Party Governance

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 thirdparty 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

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 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 Archer use cases.

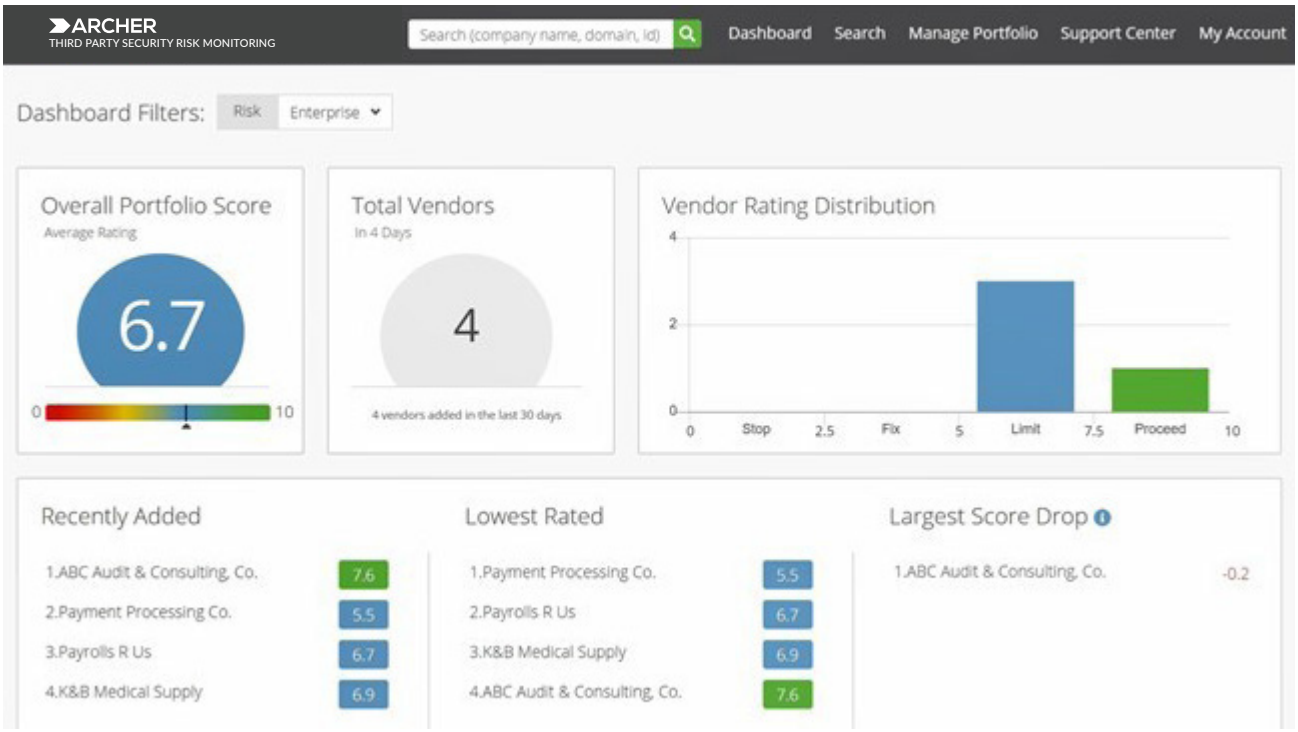
Key Features

- 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 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.



Discover More

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.

ARCHER
An RSA Business