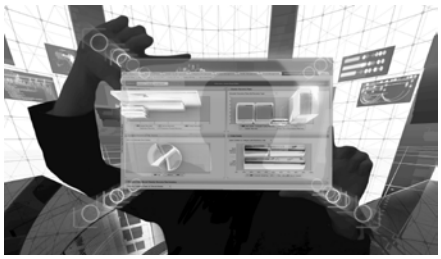
RSA ARCHER® CONTINUOUS MONITORING

Prioritize security risk data and automate control assessments



AT-A-GLANCE

- Prioritize security risk data with “worst first” security risk scores & ranking
- Automate control assessments
- Incorporate current risk metrics into FISMA reports and authorization artifacts
- Out-of-the-box integration with Assessment & Authorization (A&A)

CHALLENGES

An Information Assurance professional is faced with a constantly changing and dynamic cyber landscape in which federal agencies operate. Current tools deployed by an agency are largely inadequate in adapting to constantly changing security requirements. As a result, the agency can often be late in responding to the latest security threats.

SOLUTION

The RSA Archer Continuous Monitoring (CM) solution is purpose-built to meet the unique needs of federal agencies. The CM solution provides several capabilities essential to every Information Assurance (IA) Program including near-real-time insight into the security posture of every device in the enterprise. The CM solution is designed to ease the burden of securing information systems, maintain appropriate levels of information system security, and manage ongoing compliance for a large number of information systems. The solution provides continuous monitoring capabilities that allow an agency/department to easily determine if controls are implemented and operating as intended and ranks assets by security risk for faster remediation. In addition to targeting individual high-risk devices, the RSA Archer CM solution can inform the Authorizing Official (AO) on a wide range of risk decisions for Assessment & Authorization (A&A) and FISMA compliance activities.

Authorizing Officials can use the CM dashboards for authorization and risk decisions. Also, control assessors and auditors can use the CM dashboards and reports for assessment determinations. The ability of the RSA Archer platform to integrate with a variety of tools and formats allows for more scanner and sensor integrations and more risk inputs, and allows users to leverage more of their existing tools.

KEY BENEFITS

- Manage with risk-based approach by prioritizing security risk data and focusing on “worst first”
- Stay current with the latest requirements with ongoing content development process
- Achieve cost and operational efficiencies by implementing continuous monitoring and automating control assessments
- Leverage existing scanners and sensors and integrate new tools, including those which are Security Content Automation Protocol (SCAP)-enabled
- Effective reporting with aggregation of metrics and reporting at multiple levels of organization
- Ease of A&A deployment by making use of out-of-the box integration with CM, whereby A&A process leverages risk metrics directly from RSA Archer CM solution
- Enhance operational security by integrating with other RSA Archer solutions such as Incident Management, Vendor Management, and Contingency Planning.
- Streamline processes with guaranteed common format and interoperability among RSA Archer solutions that precludes the need to reformat, re-enter, or transform data feeds, reports or documents between tools

KEY FUNCTIONALITY

– ***Detailed insight***

Use a single dashboard to view precise count of failed configuration checks on one host or across the enterprise. In addition, view the number of vulnerabilities, missing patches, or out-of-date antivirus definitions. Know at a glance the hosts, their associated deficiencies, and the context such as host's owner, manager, and organization.

– ***Control assessments***

The RSA Archer CM solution allows for the automation of many technical control assessments. For other controls that are not completely automatable, the solution can provide valuable insights to control assessors to make informed assessment decisions.

– ***Scoring and ranking***

The solution provides security metrics aggregated from many different scanners and sensors. The security metrics are further computed to provide meaningful host risk scores. RSA Archer provides a monitoring dashboard environment that can be used to drive rapid risk improvement. This dashboard provides "worst first" risk scoring by ranking the risk scores by host, information system, and organization.

– ***Integrations with wide variety of third party tools***

RSA Archer integrates with a variety of security tools, sensors, and scanners such as vulnerability and configurations scanners, and asset management tools. Using powerful integrations, the CM solution can accommodate the CAESARS FE model by allowing for complex scoring, analysis, and hierarchical data roll-up. In addition, the data integrations can be made using SCAP, traditional XML, API, RSS, and data imports.

– ***Enhance return on your investment by integrating with RSA Archer Assessment & Authorization (A&A) and other essential RSA Archer solutions***

RSA Archer A&A serves as the system of record for all hardware, software, and information assets. These assets are uniquely tied to Information System boundaries for A&A (formerly known as Certification & Accreditation or C&A). When integrated with the A&A solution, the CM solution can use information system security categories to perform even more contextual scoring.

Adding RSA Archer Contingency Planning, Incident Management, or Vendor & Supply Chain Management will automatically tie the incidents and contingency tests to the Information Systems and organizational components defined in the A&A solution. Because RSA Archer solutions are built on the same platform, they are interoperable and share data easily, out of the box. As a result, the integrated solutions provide more complete and contextual IA tracking and reporting.