DATA SHEET

RSA ARCHER®
CONTINUOUS MONITORING

USE CASE FOR PUBLIC SECTOR SOLUTIONS
THE CHALLENGE
Security controls are being assessed infrequently. Assessments are done using tools from different vendors, with proprietary data formats and limited data sharing. There are more findings than the available staff can manage. Remediation of findings is not prioritized using all available contextual data. Continuous monitoring (CM) is a mix of manual and automated assessments. Every vendor who produces automated scanner or sensor tools markets their product as "continuous monitoring solutions." However, they do not provide for manual assessments, and most only check for one defect type (vulnerability or misconfiguration), while CM guidance from NIST (National Institute of Standards and Technology) and DHS (U.S. Department of Homeland Security) defines many defect types. Updates to FISMA (Federal Information Security Management Act) and recent OMB (Office of Management and Budget) guidance create pressure to move CM planning forward, but lack of precedent leaves organizations guessing about finer implementation details.

Until this point, the lack of CM in the federal community up has meant that defects and vulnerabilities remain open for long periods of time. It is also difficult to share data or build the "big picture" of risk due to the disparity of tools and incomplete and outdated assessment results. There is not enough staff to perform all of the assessments and remediate all findings. Lack of context and visibility means that the most critical defects are not always remediated first. For example, should a critical finding on a moderate system be fixed before a moderate finding on a critical system? Most organizations do not have the insight and metrics to perform defect rankings, especially with consideration for information system criticality.

OVERVIEW
RSA Archer® Continuous Monitoring serves as a hub for many types of scanner and sensors, allowing the organization to build an aggregate risk view at any level of the enterprise. At the lowest end, individual defects can be monitored and scored. Defects are aggregated at each level of the hierarchy, from the individual device up to the Department level. In this way, a risk score can be designated at any layer and the amount of relative risk introduced can be measured. This allows limited resources to be focused on the remediation efforts that will provide the greatest benefit.

With RSA Archer Continuous Monitoring, you can make a faster, more targeted response to emerging risks. Your staff will be able to mitigate the findings in the order in which they will most reduce risk. When used in tandem with RSA Archer Assessment and Authorization, it can enhance your FISMA and OMB compliance activities by verifying that information systems are abiding by authorization agreements (ATOs or Authorization to Operate) and are operating within acceptable levels of risk. This translates to a more secure environment with more insight and the ability to make better, more informed risk decisions.
KEY FEATURES

• Current, authoritative hardware and software inventories
• Current defect libraries
• Integration of scanners and sensors into common environment, in common format
• Scoring and ranking algorithms for each defect, device, and layer of the organizational hierarchy
• Defect tracking and remediation

KEY BENEFITS

RSA Archer Continuous Monitoring provides:

• Reduced exposure time
• Reduced risk overall
• Increased visibility / better decision making
• More current risk data
• Increased assurance (confidence based on current data)
FOR MORE INFORMATION
To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at rsa.com. If you are an existing RSA Archer customer and have questions or require additional information about licensing, please contact RSA Archer at archersupport@rsa.com or call 1-888-539-EGRC.