



Market Insight Report Reprint

AWS rearchitects Amazon Inspector vulnerability management service

April 20 2022

by **John McNeice, Daniel Kennedy**

Inspector provides continuous scanning for vulnerabilities and configuration risks such as unintended network exposure. The rearchitected service is now real time and easier to deploy, and includes enhanced risk scoring and support for container workloads.

451 Research

S&P Global

Market Intelligence

This report, licensed to AWS, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

In November 2021, AWS launched an improved version of Amazon Inspector, its vulnerability management service. The service provides continuous scanning for software vulnerabilities and configuration risks, such as unintended network exposure. The new service is real time, and easier to deploy. It also added multi-account support, and consolidated vulnerability management for both Amazon EC2 and Amazon ECR workloads. This version includes new features such as enhanced vulnerability risk scoring and support for container workloads.

THE TAKE

AWS's new Inspector service offers a few significant advantages over the previous version. Scans are now initiated in near real time when events such as software changes are made, or new vulnerabilities are identified in the software packages on customer workloads. The new architecture and tight integration with AWS System Security Manager (SSM) and AWS Organizations make for easier administration and deployment. The new service will likely result in increased adoption by current AWS customers, and increased adoption by customers running container workloads in AWS. It will likely pose a competitive threat to third-party vulnerability scanning offerings. We expect to see Amazon Inspector move toward addressing potential open source risk, and add software composition analysis capabilities to the offering in the future.

Details

AWS's Inspector service provides continuous scanning of AWS hosts for software vulnerabilities and configuration issues, such as unintended network exposure. The new Inspector service is now near real time and event-driven, meaning that changes to cloud resources automatically kick off new scans, and it generates vulnerability findings automatically once deployed.

The rearchitected service replaces the old Inspector agent with the widely used AWS SSM and SSM agent, which inventories software packages. The SSM agent is easier to deploy, covers an expanded range of AWS asset types, eliminates the need for an outbound internet connection to a SaaS platform, and has multiple use cases beyond vulnerability management. The previous Inspector service was widely adopted but suffered from some issues – the Inspector agents were resource intensive and difficult to deploy, and scans were not real time. One goal of the new launch was to support new use cases like containers.

Inspector includes several key added features. Enhanced vulnerability risk scoring goes beyond traditional CVE scoring by determining how exploitable the vulnerability is within the context of the customer's AWS environment. This feature helps overwhelmed security teams prioritize the riskiest vulnerabilities for remediation. The new service includes support for containers – container images are scanned for vulnerabilities when they are launched in the Amazon Elastic Container Registry. It also offers simple integration with AWS Security Hub and Amazon EventBridge, ITSM offerings such as ServiceNow and SIEM providers such as Splunk, which can help streamline the vulnerability remediation process.

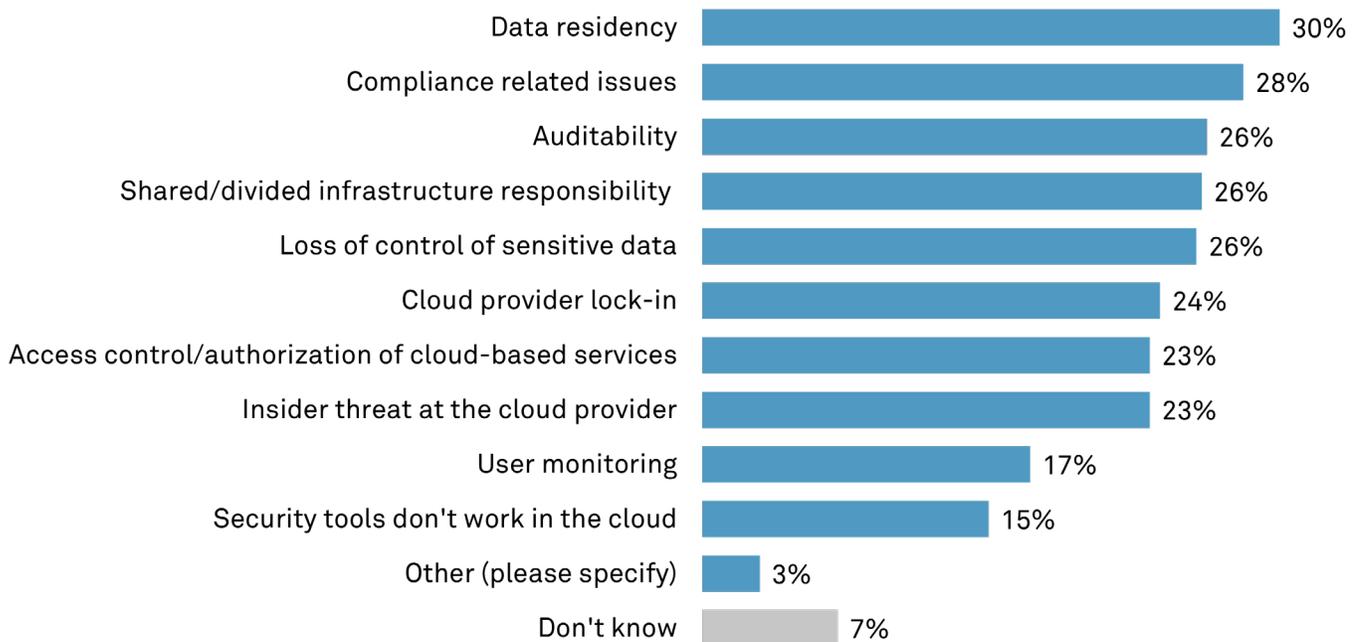
The new service will likely have an impact on traditional vulnerability management offerings (Qualys, Tenable, Rapid7) and also cloud SaaS security platforms that include vulnerability scanning as a feature. Notably, Palo Alto Prisma, a leading cloud security SaaS platform, recently added integration with Inspector. The new container-scanning capabilities are also likely to have an impact on container security platform providers, especially those that have focused on vulnerability scanning versus runtime protection.

Third-party vendors can tout advanced features and support across multicloud environments, but AWS offers easier deployment and integration, and a simplified pricing model (based on number of instances and containers scanned per month), which are often more important to customers.

The launch also improves Inspector’s application security capabilities. The service has always offered scanning for open source risk against operating systems (Linux distributions) as part of EC2 scanning, but newly launched container image code scanning capabilities move it further in the direction of being a software composition analysis tool. Specifically, Inspector offers support for C#, Golang, Java, JavaScript, PHP, Python, Ruby and Rust.

AWS leverages NIST’s National Vulnerability Database and vendor feeds for open source vulnerability data, and has also licensed the proprietary Snyk Intel Vulnerability Database. As noted earlier, risk scores go beyond CVE information, augmenting the risk calculation with exploitability, network reachability, and data from social media trends. A recent blog post describes how a user might identify instances of the Log4j vulnerability with Inspector, and take ‘shift right’ triage steps once identified, leveraging AWS WAF.

Security Concerns With the Cloud



Source: 451 Research's Information Security, Budgets and Outlook 2021

CONTACTS

The Americas

+1 877 863 1306

market.intelligence@spglobal.com

Europe, Middle East & Africa

+44 20 7176 1234

market.intelligence@spglobal.com

Asia-Pacific

+852 2533 3565

market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2022 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.