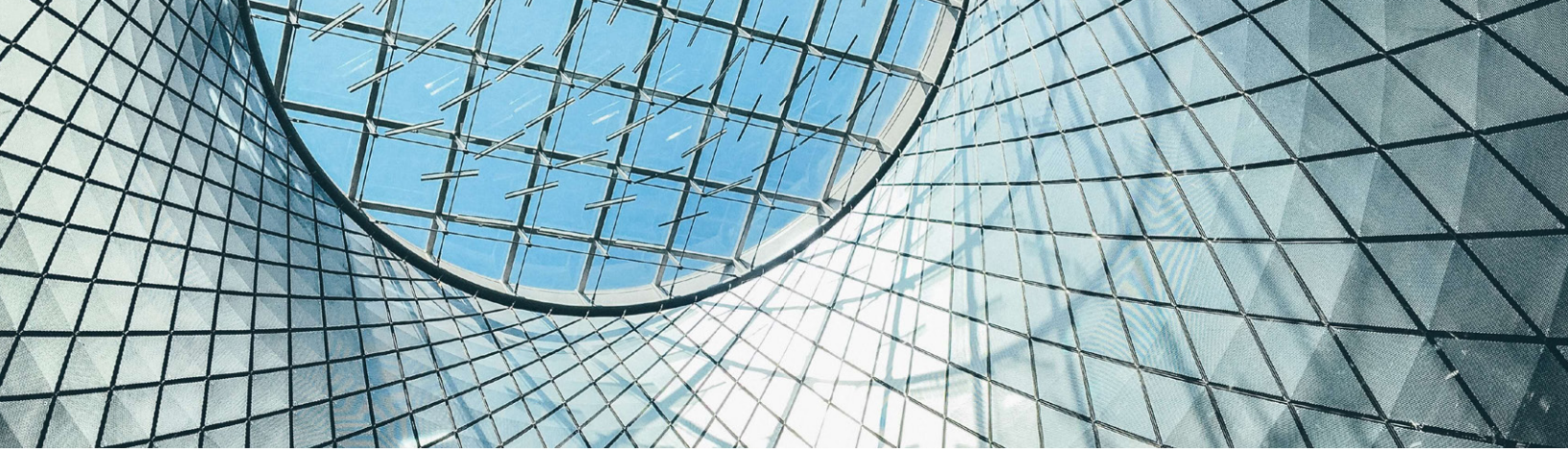

Market Insight Report Reprint

Cisco's Business Risk Observability combines application context with threat intelligence

February 28 2023

by Mike Fratto

IT observability is becoming a must-have technology for digital transformation leaders. Cisco's new offering raises the visibility of vulnerabilities and threats to critical applications, and aims to enable IT operations and security teams to better collaborate on remediation.

S&P Global
Market Intelligence

Introduction

IT observability — which we define as a system that take in a variety of platform data in the form of MELT (metrics, events, logs and traces), and outputs contextual end-to-end topologies, analysis, visualizations, recommendations and forecasts — is becoming a must-have technology for digital transformation leaders. Cisco Systems Inc. has launched Business Risk Observability with Business Risk Scoring, combining and correlating the business impact from applications' business transactions, the vulnerabilities associated with external dependencies, the likelihood a vulnerability will be exploited in the context of the business application, and active threat research, among other factors.

THE TAKE

Cisco's Business Risk Observability aims to raise the visibility of vulnerabilities and threats to critical applications, their components, and critical application dependencies, allowing IT operations and security operations teams to better collaborate on remediations, as well as improving security architectures. We expect competitors in the application monitoring, observability and application security segments to create similar capabilities as Cisco's from their own software portfolios, or by partnering with third parties. The benefit for enterprises will be contextual vulnerability management for cloud and cloud-native applications, but Cisco's offering would have broader appeal if it supported threat and vulnerability data from third parties.

Details

Enterprises expect to garner a number of benefits from observability, but as we see from 451 Research's DevOps, Workloads & Key Projects 2022 survey (see figure below), improved security and faster problem resolution and detection are top of mind. A common challenge for security vendors is connecting the output of security analytics into remediation and repairs. Making security analysis actionable is a prime benefit for customers by streamlining security processes.

Security and Troubleshooting Top Drivers for Observability

Q. What outcomes does your organization achieve by using observability? Please select all that apply.

Base: Organizations that use or plan to use observability (n=455)

Source: 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2022

Cisco's Business Risk Observability takes advantage of security capabilities across the company — such as API Security from Panoptica, and capabilities from acquisitions like Cisco Talos and Kenna Security — and generates actionable insights by contextualizing these capabilities with the business impact to business applications.

A business risk score raises the visibility of vulnerabilities and threats to critical applications, components and dependencies, allowing IT operations and security operations teams to better collaborate on remediations as well as improve security architectures. The company's Business Risk Scoring transforms application monitoring to actionable observability, because the vulnerabilities and risks they represent are presented in the context of business impact and application topology, which are typically complex and dynamic.

Business Risk Scoring is delivered through the Cisco Secure Application add-on for AppDynamics, which combines application observability and threat intelligence into a business risk score that IT and security teams can use to prioritize remediation, assess overall risk, and view threats in terms of the application.

Cisco Secure Application is an agent-based security module that scans applications for common vulnerabilities and configuration issues. It is part of the AppDynamics agent, and once it has been licensed, there is no additional installation or instrumentation, or extra cost for the Cisco Talos, Kenna and Panoptica threat intelligence data feeds — it can simply be enabled.

The new Business Risk Observability capability is designed to help IT operations and security operations better understand their vulnerability landscape, and be able to respond quickly to new kinds of attacks and vulnerabilities. Cisco Secure Application does this by taking in data feeds and security scoring from other Cisco products (Cisco Talos, Kenna Security and Panoptica) to provide a full-stack view of the application, whether it is running in a VM, a serverless function or a containerized cloud-native application. Currently, third-party vulnerability feeds cannot be ingested, but Cisco has it on the roadmap.

The vulnerabilities and threats are then mapped to application components and dependencies derived from Cisco AppDynamics, and presented to users in a dashboard, which shows a risk score that considers the criticality and severity of the vulnerability, and the component/dependency that is being displayed. The risk score is contextual based on the application's architecture and the assigned business value to the organization, and how actively the vulnerability is being exploited. Critical applications with vulnerabilities that are not being actively exploited may be deprioritized in favor of similarly critical applications with vulnerabilities that are being actively exploited.

The business risk score presents a high-level view for operations and operations managers to begin to prioritize vulnerabilities to focus on. Historical reporting shows the business-risk change over time, so organizations can understand whether their vulnerability management is improving, which translates to business risk. IT and security operations teams can drill down into vulnerabilities to get detailed information about where the component/dependency resides and the type of vulnerability it represents, such as remote code execution or data exfiltration. Cisco Secure Application can automatically block attacks and report the number of attacks that were attempted, and whether they were successful or blocked.

Business Risk Observability will help IT and security teams better collaborate (one of the biggest challenges for DevSecOps integration), working with a common dashboard and a common set of threat and vulnerability fields, thus allowing those teams to more quickly identify and remediate issues as they occur. Competitors in the application performance monitoring and observability segments have been adding more security-focused capabilities to their products, and we expect to see further integrations as software vendors attempt to differentiate their products and expand their footprint in the enterprise.

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