IDC

SPOTLIGHT

Sponsored by: Cisco

When application performance and security are managed by separate teams, gaps are created that savvy, motivated attackers can exploit. The evolution from monitoring to full-stack observability provides security, development, and IT operations teams with an innovative path forward to reduce vulnerabilities and increase system reliability.

Aligning Application Performance and Security with Business Context

April 2023

Written by: Stephen Elliot, Group Vice President, I&O, Cloud Operations, and DevOps

Introduction

The role of application development teams today is shifting, with a critical focus on better understanding security risks. As more vulnerabilities and risks are unknowingly part of the code and broader software development life cycle, it's imperative for teams to increase collaboration to deliver secure, high-performing digital services.

Speed and cross-team coordination are paramount because bad actors can take advantage of gaps between siloed security and application teams, resulting in costly and damaging consequences. Traditional vulnerability and threat scanning solutions lack the shared business context needed to rapidly assess risks and align teams based on potential business impact. In fact, many organizations today track and prioritize vulnerabilities in spreadsheets — a time-consuming and very manual process. This process can be compressed and shortened using data analysis and intelligent data feeds to prioritize issues and provide transparency into the security risks that require attention.

To triage and align teams quickly, IT executives need to know where vulnerabilities and threats impact the application, the likelihood a risk will be exploited, and how much business risk each issue presents. IT organizations using full-stack observability empower security and IT operations teams to collaborate faster to locate, identify, prioritize, and respond to security issues in a modern, advanced, and effective fashion.

Having a deeper and contextualized understanding of security risks enables shared visibility and responsibility across teams, ensuring that security teams have the same priorities as IT operations, application, or DevOps teams. The alignment of these teams can help shape a faster, common response to a security threat or vulnerability in context of the problem, using a single and common source of data.

AT A GLANCE

WHAT'S IMPORTANT

Speed and cross-team coordination are paramount when dealing with application security risks to avoid potentially costly and damaging consequences of gaps and delays between siloed security and application teams.

KEY TAKEAWAYS

- Traditional vulnerability and threat scanning solutions lack context for how threats may impact business.
- Business risk scoring prioritizes application security risks and aligns teams on what matters most to the business.
- Potential revenue impacts are mitigated faster with business context awareness.
- There should be a cross-team effort to drive a great customer experience.

Challenges

Some of the challenges that exist when organizations are looking to close the gaps between development, security, and operations teams are as follows:

- For many enterprises, organizational structure remains a difficult challenge as security, development, and operations teams tend to work in silos, with established policies, procedures, processes, and tools.
- Many organizations have different levels of maturity for developing applications, with developers often used to their processes and adverse to change. Changing a development culture to include security capabilities, or establishing tool integrations between development and operations toolchains, can take time.
- Establishing a full-stack observability strategy should include key stakeholders from several teams. Garnering attention, prioritization, and staff participation for deployment of such a strategy can be difficult.
- Some security operations teams might assume they have a good-enough strategy; investing in a more aligned security and operations collaborative effort often takes education, a value-based discussion, and time to build out the conversation between teams.
- Most IT organizations lack the ability to create unified visibility across all key services, covering application, network, infrastructure, security, and cloud services components (sometimes a result of skill set shortages among teams or existing processes/tools). This causes a slowdown in incident response, exposes the end user to a poor digital experience, and pulls the IT staff away from innovation efforts.

Benefits

There are many benefits from bringing together data from business transaction monitoring and mapping, adding threat intelligence, and providing context. Teams can work together to identify security and operations issues before they impact customer experience and potentially even revenue. In addition, teams can realize the following benefits:

- DevSecOps teams can **detect vulnerabilities and threats in real time** and assess how and where those vulnerabilities will impact business-critical applications.
- Comprehensive monitoring provides a consolidated threat feed to **increase visibility and insights.**
- Teams can make **data-driven decisions** quickly based on the highest threat levels and their potential business impact.
- Cloud application security insights are unlocked **without having to deploy an additional agent.**
- Issues across the entire technology stack, including cloud-native microservices, Kubernetes containers, multicloud environments, or mainframe datacenters, are **automatically detected and resolved.**

Trends

Investment in application security is now a permanent trend as more executives understand the business outcomes it offers and realize that their business runs on applications or that their business is the applications themselves. Most customers are building, modernizing, and deploying various types of business-critical applications including traditional/on-premises, "lift and shift" to the cloud, and modern, distributed (cloud-native) architectures. These complex architectures make identifying and resolving security and operational problems harder than ever.

With the increased expectations end users now have for always-on, secure, and exceptional experiences, customers are under pressure to accelerate their digital transformation projects. The shift to modern, distributed applications can leave organizations more vulnerable due to an ever-expanding attack surface.

Outstanding application security is foundational to a brand's reputation and for creating and building trust and loyalty with users. But vulnerabilities can occur anytime, anywhere, making it difficult and time consuming to prioritize responses. Avoiding costly delays that can result in damage to revenue and brand reputation means organizations must have clear visibility into each new vulnerability and the insights needed to prioritize remediation based on their business impact.

Considering Cisco

Cisco is enhancing its full-stack observability offering with the introduction of Business Risk Observability, an early industry offering in application security. The Business Risk Observability capabilities available through Cisco Secure Application from Cisco AppDynamics include business transaction mapping to understand how and where an attack may occur with threat intelligence feeds from Cisco Talos, Kenna, and Panoptica. By seamlessly integrating features from Cisco's portfolio of security solutions, security and application teams have expanded threat visibility and the intelligent business risk insights to prioritize and respond in real time to revenue-impacting security risks and reduce overall organizational risk profiles.

Conclusion

IDC believes that a business risk observability solution that provides business context across the technology stack to empower development, DevSecOps, security, and operations teams will optimize end-to-end service performance with visibility, insights, and analytics while reducing security risks. The value of bringing together "business transaction mapping and monitoring" is the ability to locate how and where an attack may occur. Businesses can accomplish this within common application workflows, combining threat and vulnerability intelligence, business impact, and runtime behavior to identify the most pressing risks, and do so in a way that aligns key stakeholders and teams in an innovative fashion. Generally, the more that developers, security, and operations teams are provided with unified visibility into the operating condition of an end-to-end digital system, the better digital services will perform and, most importantly, the better they will serve the business. Digital services will also be more secure.

About the Analyst

Stephen Elliot, *Group Vice President, I&O, Cloud Operations, and DevOps*

Stephen Elliot manages multiple programs spanning IT Operations, Enterprise Management, ITSM, Agile and DevOps, Application Performance, Virtualization, Multicloud Management and Automation, Log Analytics, Container Management, DaaS, and Software-Defined Compute. Mr. Elliot advises senior IT, business, and investment executives globally in the creation of strategy and operational tactics that drive the execution of digital transformation and business growth.

MESSAGE FROM THE SPONSOR

Cisco is a leading provider of Full-Stack Observability solutions and Application Performance Monitoring technology via Cisco AppDynamics. Cisco AppDynamics helps customers observe what matters inside and beyond their IT environments. Combined with the power of Cisco, Cisco AppDynamics enables organizations to deliver exceptional user experiences by centralizing and correlating data into contextualized insights of critical business metrics — providing them with the power to prioritize actions based on business needs.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com