cisco
AppDynamics

Protecting what matters most with business risk observability

Introduction

Today's savvy application users expect high-performing, secure digital experiences across every device, all the time. In pursuit of meeting these user demands, **IDC predicts** 750 million cloud native applications will be created globally by 2025 and **Gartner** expects 95% of new digital workloads will be deployed on cloud native platforms in the same timeframe, representing a 30% surge in cloud native adoption over the next two years. While shifting landscapes across technologies is nothing new, this round of change is happening faster than ever. And without a rock-solid strategy for both app performance and security — organizations risk losing market share — no matter where their application infrastructure lies.

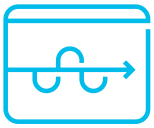
While the number of cloud assets organizations manage has increased by 133% year-over-year, the number of security vulnerabilities has jumped disproportionately — by a staggering 589%. This growing security challenge was also surfaced in a recent EMA survey when half of the IT leader respondents reported that security is often an afterthought in their application delivery ecosystems. It's a mindset that needs to change and with DevSecOps adoption on the rise, organizations clearly see the value of collaboration across applications and security teams.

The shift to modern application architectures enables accelerated app delivery across on-premises, public cloud and multi-cloud environments, which is good, but the distributed nature of these environments has greatly increased the attack surface across the application lifecycle. As this complexity continues to mount, app and security teams need to work together with the right (shared) tools to maximize productivity and minimize business risk.

What is business risk observability?

Business risk observability, facilitated by **Cisco Secure Application,** allows IT teams to pinpoint root causes of application health and security issues coming from third-party APIs down to the code level, in real-time. In doing so, it automates identification of vulnerabilities affecting critical business metrics for quick remediation. An industry-first evolution in application security, business risk observability leverages security intelligence from Cisco security products to understand the likelihood of exploits and brings insights to a shared dashboard that enables cross-functional collaboration to address application security risks.

Within the tool, vulnerabilities are automatically discovered, mapped to business-critical transactions – and assigned a business risk score. The result is a continuously updated, ranked list of remediation recommendations based on likelihood of impact and what will be impacted. These insights are key for app and security teams to see what needs immediate attention and for IT and business leaders to ensure that the latest security intelligence is being leveraged to protect what matters most to the organization.



Log4j vulnerability highlights the value of a combined security and observability approach

The initial Log4j vulnerability (CVE-2021-44228) is a zero-day vulnerability that was disclosed in the popular Apache Log4j Java logging library, quickly followed by three additional vulnerabilities (CVE-2021-45046, CVE-2021-45105 and CVE-2021-44832). Log4j is used directly or as a dependency by millions of servers for both enterprise applications and cloud-based services. The Log4j vulnerability allows attackers to gain full control of affected servers and applications.

After disclosure of the first Log4j vulnerability, Cisco AppDynamics security experts took immediate action to help customers defend business-critical applications against the threat. The AppDynamics security team directly facilitated customer efforts to identify Log4j vulnerabilities at runtime and block exploits — without friction or overhead.

Cisco Secure Application sits alongside your code and runs wherever it does. This means that it can detect and block exploits when your application is executing code based on a request or a response no matter the origin of the traffic. In the case of Log4j, Cisco Secure Application can enforce a single policy across all applications and block any specified vulnerable class from making any type of network connection, no matter what the trigger was for that behavior.

When companies began putting together their Log4j response plan, questions immediately arose as to how to prioritize and coordinate between siloed application and security teams. Many didn't have a complete, readily available software bill of materials (SBOM) for their applications and services, which made it difficult for them to identify what was vulnerable and connect all the need-to-know stakeholders through shared data.

Cisco Secure Application eliminates this gap by leveraging the metadata that AppDynamics already uses to monitor the health of applications to maintain continuous context across different stakeholder groups. It correlates security details with application insights for unified visibility into the impacted service area and breaks down the barriers between application and security teams to allow for rapid response.

How business risk observability can help mitigate AppSec challenges

Applications are a vital part of most business transactions and keeping up with user demands while handling an overwhelming influx of security threats is critical to business health. With security and user experience becoming inextricably intertwined, organizations need to balance one against the other. Analysts report that increasing alert volumes pose problems for security teams due to more than **90% of organizations** being unable to address all security alerts on a same-day basis. Delivering secure and reliable user experiences are key components of enterprise security strategies.

To hit both marks, organizations must work collaboratively across application delivery including all IT and business stakeholders. The move from DevOps to DevSecOps is a critical component, beginning to hit its stride, with **90% of orgs** reporting they are in some phase of the DevSecOps journey. Other recommendations include adopting a risk management and security-first approach where automated security tools continuously discover and alert problems within design, testing and production. Business risk observability empowers cross-functional teams with shared tools that breakdown silos, automate vulnerability discovery, prioritize vulnerabilities based on context and provide a common view into the overall impact.

Business risk observability helps:

- **Operations teams** prioritize vulnerabilities based on business impact, vulnerability information, threat intelligence and application context.
- **Application development teams** quickly understand vulnerabilities at a granular level and gain understanding of location and threat impact within applications.
- **Line-of-business owners** make high-level, data-driven decisions based on risk levels and associated business consequences.

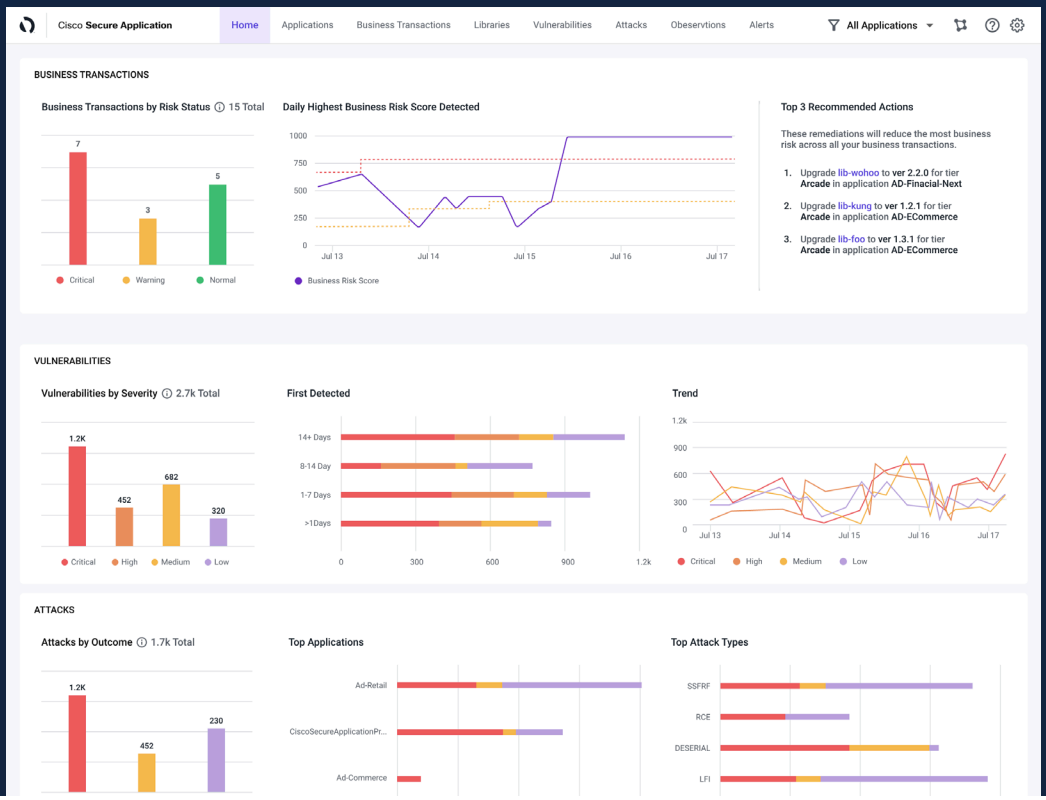


Figure 1: Cisco Secure Application provides visibility and context to application vulnerabilities, helping ensure alignment between IT and business leaders.

Choosing the right tools for the job

Cisco Secure Application helps organizations protect production applications by detecting and blocking threats at runtime. With it, technologists can see individual lines of code as they are executed and gain actionable insights, regardless of where the application is hosted or where the traffic originated. Cisco Secure Application uses the rich context from Cisco AppDynamics solutions to deliver application performance and security monitoring with business risk observability. Let's take a closer look at how this unified tool plays an integral part in a comprehensive monitoring strategy for hybrid and cloud-based applications.

> Cisco Secure Application helps organizations protect production applications by detecting and blocking threats at runtime.

Business risk observability for **hybrid application environments**

Cisco Secure Application expands security visibility and provides risk insights and actionable recommendations to protect hybrid applications. Fully integrated with several Cisco security products, it automates real-time continuous monitoring to discover and prioritize remediation for business-critical vulnerabilities and threats so organizations can proactively prevent revenue-impacting security risks — and reduce their overall risk profile. Purpose built to protect applications from the inside out without adding friction or overhead — Cisco Secure Application helps orgs shift from a reactive to proactive security approach while maintaining speed and uptime.

Key security innovations for hybrid application environments include:

- **Business transaction mapping:** Locate how and where an attack may occur within common application workflows like login, checkout or complete payment to instantly understand the potential impact to the application and the bottom line.
- **Integrated security intelligence feeds:** Cisco Talos, Cisco Vulnerability Management and Panoptica provide valuable risk scores from multiple sources to assess the likelihood of exploits.
- **Business risk scoring:** Goes beyond the Common Vulnerability Scoring System (CVSS) score by measuring and incorporating exploitation predictability and the associated security risk. It enables teams to avoid delays and accelerate collaborative responses by combining threat and vulnerability intelligence, business impact, application context and runtime behavior to identify the most pressing risks.

Why automation is critical for application security

In today's fast-moving and complex application delivery environments, organizations need solutions that can work faster than humanly possible. Attackers already leverage automation and AI to launch sophisticated attacks at massive scale — it's time to use these same capabilities for good. Automation provides a constant snapshot of what's happening in real-time based on identifying and alerting anomalies found across large volumes of data, while AI-powered tools enable efficient resource allocation for faster innovation — rather than chasing and triaging risks. Together, automation and AI/ML help organizations turn the tables on attackers.

Business risk observability for **cloud native environments**

The cloud is an integral part of business strategy for enterprises worldwide. According to the **Flexera 2023 State of the Cloud Report**, 65% of respondents are heavy users of the public cloud and half of all enterprise workloads today are in the public cloud. This trend is expected to continue as Gartner expects 95% of new digital workloads to be deployed on cloud native platforms by 2025. But the journey to the cloud isn't just about moving workloads from on-premises data centers to the public cloud. It's also about maturing your organization's cloud operations. Within the cloud, top challenges organizations struggle to address include managing cloud spend (82%), security (79%) and lack of cloud expertise/resources (see **Figure 2**).

Cisco Secure Application on the Cisco Observability Platform helps organizations secure cloud native applications based on real-time vulnerability analytics and business risk observability. It enables teams to rapidly locate, assess and prioritize risk and remediate security issues based on potential business impact. Cisco Secure Application delivers runtime data security that detects and protects against sensitive data leaks — and harnesses the power of Cisco security products by integrating with Panoptica and Cisco Vulnerability Management to provide expanded threat visibility and business risk insights with actionable recommendations. Working seamlessly with Cisco Cloud Observability, Cisco Secure Application delivers a unified tool for cloud native environments that maps application security to business strategy (see **Figure 3**).

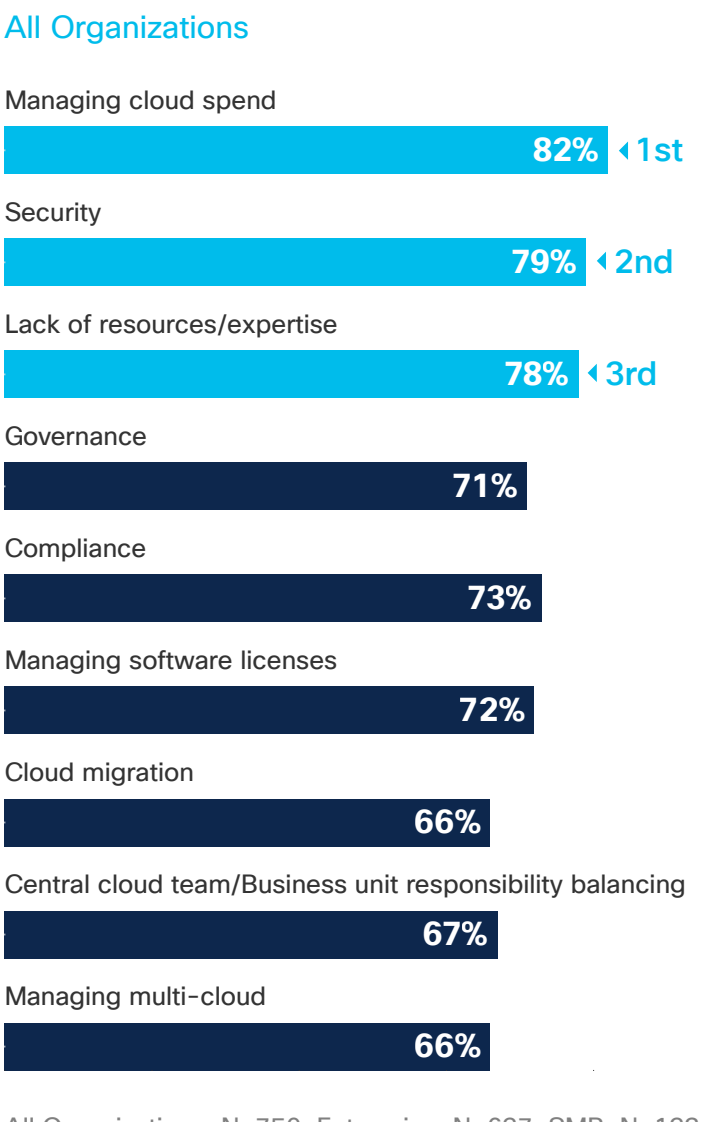


Figure 2: Top cloud challenges. (Source: Flexera 2023 State of the Cloud Report)

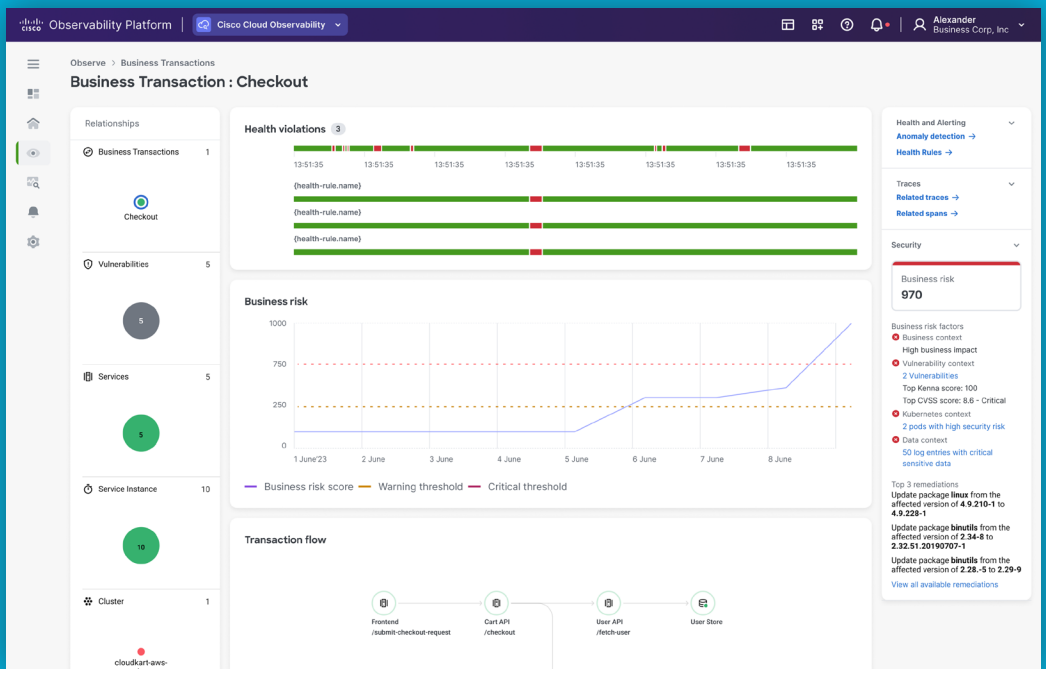


Figure 3: Cisco Secure Application provides a rich interface with security insights and actions to address the most pressing security risks.

With Cisco Secure Application organizations can:

- **Locate and highlight** security issues across application entities to quickly isolate issues and apply fixes to reduce mean time to remediation (MTTR).
- **Prioritize** security vulnerabilities using business risk scoring that combines application context, business impact and the latest security intelligence.
- **Remediate** security issues with tailored, actionable recommendations and tools for masking sensitive data to accelerate mitigation.

Working seamlessly with Cisco Cloud Observability, Cisco Secure Application delivers a unified tool for cloud native environments that maps application security to business strategy.

Continue your journey today

Learn more about Cisco Secure Application, Cisco Cloud Observability and AppDynamics — then, register for a live demo to see how business risk observability can help your organization protect what matters most.

MKT_1664_2023