APPDYNAMICS
part of Cisco

eBook
Application security is key to observability

appdynamics.com

Application security is key to observability

Pinpoint root causes of application issues in real time, from third-party APIs down to the code level, so IT teams can identify what's affecting key business metrics for quick remediation.

As complexity increases along the application delivery chain, technologists are more aware than ever that delivering less than perfect user experiences puts the organization at risk of losing customers and reputation. As such, IT teams bear the challenge of delivering always-on, flawless and secure applications — while also aligning application health to overarching business goals. This includes resolving issues quickly in a coordinated fashion across multiple IT functions, a feat that can seem daunting when full visibility into application behavior and looming threats is lacking.

A big gap in the race to deliver secure and reliable app performance comes from a lack of correlation between security incidents and how the affected application impacts top business priorities. That is, SecOps can likely say what happened and what type of threat exists but without visibility, they can't confirm the exact impact to an organization's bottom line. And because performance issues may coincide with network, device or service bottlenecks as well as security incidents, it's important to gain insights into both performance and security.

In addition, without visibility, prioritizing remediation can be difficult because the impact on business-critical apps can't be determined quickly enough. Thus, IT organizations without tools may be held accountable to stakeholders despite lacking insights to align remediation with user expectations and company goals. A proper understanding and view into application vulnerabilities can help address these concerns and overcome related challenges.

The state of application security

An increasing number of applications and APIs are developed with third-party and open source code as a way to deliver new and updated apps faster, which elevates the need for a security-first mindset. And in a world where users are more security-aware than ever, deploying vulnerable apps or negative user experiences can devastate brand reputation. Worse, unchecked security flaws can expose users and organizations to loss, harm and expenses that impact the ability to recover quickly — if at all. Therefore, protecting apps against threats is a major concern and a key element within an application security strategy.

Security stats to consider

Looking at the Ultimate Guide to Application Security, there are numerous standouts, including:

43%

43% of security breaches target applications.

40%

Nearly 40% of the average total cost of a data breach stems from lost business.

280

The average time to identify a breach is 280 days.

80%

80% of orgs failing to adopt a modern security approach will face increased operating costs.

Bringing business and security goals together

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 seek to balance one against the other. Analysts consistently 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. This makes delivering secure and reliable user experiences key components of modern security strategies, if organizations are to hit both marks, as follows:

- Alignment among all stakeholders is the essential starting point.
- Create a security practice that expands DevOps to become DevSecOps.
- Leverage new and advanced security tools to improve and safeguard user experiences.
- Take a risk management approach, recognizing that problems occur and need quick detection, identification, prioritization and resolution for a business to thrive.
- Security-first approach to app development must be designed in, tested during development and checked across the lifecycle.

> Protecting apps against threats is a major concern and a key element within an application security strategy.

A key element in such a strategy centers around adopting AI-powered and automated security capabilities, which work in unison to give SecOps and DevOps a shared view into app security and performance, as well as the context needed to develop an overarching app delivery strategy, where security is a top priority. Growing complexity in infrastructures, expanding threat landscapes, looming compliance demands and limited human and technical resources all weigh heavily on security operations (SecOps) and development/IT operations (DevOps) teams. This explains why automation tools are important and valuable for security staff to confidently delegate day-to-day remediation responsibilities to development counterparts.

Simply put, security tools make addressing security challenges easier to implement, less subject to human error and faster to prioritize and resolve. AI can automate data collection, threat identification and filtering to help orchestrate rapid incident response, and security automation allows even the smallest teams or those with limited resources to deliver maximum app protection.

> With security and user experience becoming inextricably intertwined, organizations seek to balance one against the other.

Costs of ignoring application security

Ignoring application security is too expensive for modern organizations to withstand. From a risk management perspective, this list of "scary statistics," underscore how unacceptable it is to take chances without proactive security solutions and policies in place:

- Record-breaking levels of zero-day attacks occurred in 2021 (30 in 2020 vs. 80 in 2021) and the same is expected for 2022. Thus, the cost of vulnerabilities exploited as they're discovered and before they can be patched is skyrocketing.
- CyberSecurity Ventures estimates ransomware costs reaching up to $20 billion in 2022. At 57 times the losses compared to 2015, that's indicative of exponential growth.
- The United States Federal Trade Commission (FTC) can levy fines up to $50,000 per violation per day for failing to inform users about data breaches. FTC actions can reach enormous levels: Equifax (2017: $575 million), Capital One (2021: $190 million) and Morgan Stanley (2022: $120 million).
- Likewise, the European Union General Data Protection Regulation (GDPR) and other governmental compliance requirements can hold companies financially responsible for privacy and data breaches or disclosures. British Airlines was hit with an initial levy of $230 million in 2020, later reduced to under $28 million for a breach involving 400,000 customers.

Financial exposures aren't limited to fines and penalties, either. Opportunity costs are incurred while remediating and reputational damage and loss of trust also weigh on the bottom line. In fact, companies often pay to rehabilitate users whose credit is impacted and when breaches lead to identity theft. Therefore, risks aren't worth taking without seeking protective cover of some kind.

Runtime application security plays a vital role

Runtime application security is worthwhile and important for companies to adopt when implementing security technologies. Runtime application self-protection (RASP) monitors inputs to running applications and boosts application security. In general, RASP screens all inputs, and blocks those indicative of potential attacks. It also covers the application runtime environment and blocks changes to environment variables, access controls and privileges plus out-of-bounds (or unusual) memory and storage access and more. As such, valid or typical requests are allowed through while invalid or suspect ones are denied.

Using open source software

Most organizations (90% by some estimates) use one or more open source software (OSS) components in their codebases. The code for OSS components is generally available for public inspection, modification and enhancement. It's also usually built within an open, collaborative community that's updated and maintained by volunteers, which can lead to vulnerabilities. Well-known OSS examples include Linux, Apache, WordPress and Firefox.

Cisco Secure Application technology

For Cisco Secure Application, RASP resides within an app's runtime environment to monitor and filter inputs and actions or changes. Because customers have runtime agents in place, additional agents are not needed for RASP nor does it add application overhead or latency to protect against unwanted and unexpected inputs and attempts to subvert runtime security. This provides a safeguard needed to avoid zero-day exploits.

> The DevSecOps team needs to understand how a vulnerability impacts the organization within the context of its risk to harming business goals.

For example, Cisco Secure Application proved effective against Log4Shell and LogJam vulnerabilities in the Apache Log4j Java logging library, as used in millions of servers. This zero-day exploit, rated a maximum CVSS severity score (10.0), is both accessible and exploitable for attackers. It allows them to take full control over affected servers and applications and comes with added exposures and concerns. AppDynamics released a detailed security advisory within 24 hours, assisted customers to identify and mitigate Log4J vulnerabilities at runtime in Cisco Secure Application and block related exploits. Problem solved! See the February 2022 Log4j blog post for details.

Correlating business transactions across apps

Understanding how application performance and security relate to overarching business goals is critical. Without that context, when a vulnerability arises how will organizations know the risks posed, where to look, what to patch and the degree of priority required? For example, is the incident impacting business-critical apps in which case it's a top priority or does it require a fix but isn't an immediate emergency? The DevSecOps team needs to understand how a vulnerability impacts the organization within the context of its risk to harming business goals. Gaining a shared view and real-time insights into application health enables technologists to quickly assess risks within a business context and effectively prioritize remediation efforts. This big picture understanding can help drive remediation priorities based on user impact, financial risk, potential losses and possible fines or penalties — or any other priority dictated by stakeholders.

Integrations are important and essential

Integrations deliver insight from one toolset into some other toolset. In this case, it refers to insights from specific security tools into development and test tools, as well as OSS components, libraries and development platforms. Most importantly, integrations put insight and monitoring results into terms that provide remediation information and data designed for DevSecOps teams. For example, the Splunk integration for Cisco Secure Application plugs into the Splunk framework to send information and advice designed to work with only minor modifications and adjustments that are tailored to make remediation as simple as possible.

The enduring importance of application security

A security landscape includes all technologies leveraged by companies for a competitive edge — namely, revenue generating and customer service applications that assist staff to get work done. And maintaining security is a group effort requiring collaboration between operations, development and security across a set of shared objectives from a security-first perspective. That means day-to-day security concerns fall under the development umbrella with input from operations and security teams. And a shift-left security approach puts it at the beginning of the app development lifecycle, which coupled with rapid remediation can lower risks while providing the best possible user experiences.

This fundamental change in approach to security comes with adoption of more advanced, integrated tools to provide maximum protection and visibility directly to developers. AI-driven tools and automation can accelerate remediation, boost response accuracy and deliver the line of sight into apps that support secure and well performing applications. RASP plays an important role in filtering out unwanted and insecure inputs or behaviors within applications, resulting in a better security posture. Cisco Secure Application provides these capabilities for organizations to limit risk while accelerating delivery of secure and flawless user experiences.

Ready to transform your organization’s security posture?

Watch the Introduction to Cisco Secure Application demo and learn how it works.