The Ultimate Guide to Application Security

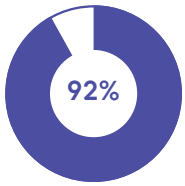
Table of Contents

Faster development, increased security risks

With the rise of cloud computing and greater emphasis on app development (especially with low-code and no-code solutions gaining popularity) in the last decade, application security has never been more important—or more challenging.

Digital transformation is at the forefront of many companies' business strategies as they continue to adapt to a digital-first world. But faster innovation and iteration, spurred by rapid cloud adoption and the availability of low-code and no-code platforms, also made it possible to develop and run more apps across more platforms, leaving applications particularly vulnerable to gaps in security.

Combine that with a pandemic that accelerated global dependence on technology and remote work, and you have a virtual explosion of cloud adoption and application development. The sheer volume of applications spread across multiple entities makes monitoring security throughout the DevOps pipeline difficult and inefficient—especially when security is most often applied as an afterthought rather than intentionally built-in from day one.



92% of enterprises now use a multi-cloud strategy to drive their operations, accelerating organizations' development while stretching their capacity for robust security. [1]

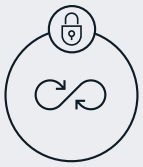
Building security checks from the start

With the high cost of security breaches (averaging $3.86 million globally[2]) and a staggering 43% of cybersecurity breaches targeting applications[3], enterprises need to find more efficient, effective, and automated ways to proactively build security into their app development and release processes.

Enter: DevSecOps.

DevOps vs. DevSecOps: what's the difference?

DevOps focuses on collaboration between application teams throughout the app development and deployment process. Development and operations teams work together to implement shared KPIs and tools, app security comes later.



DevSecOps is a way to integrate the management of security earlier on throughout the development process, as application security begins at the outset of the build process, instead of at the end of the development pipeline.

[1] "2021 State of the Cloud Report," Flexera.com

[2] "Cost of a Data Breach Report 2020," IBM.com

[3] "2020 Data Breach Investigation Report," Verizon.com

Traditional application development distinguishes DevOps from SecOps, creating organizational silos that follow a linear path from development and release to security management. But in today's rapid digital transformation and increasingly complex cloud environments, leaving security as an afterthought can have dire consequences for your application security and long-term business continuity.

DevSecOps integrates application security throughout the development cycle from the beginning. This is accomplished through both security automation, which integrates security gates throughout development without slowing down the process, as well as a strategic and cultural shift to built-in security. More importantly, it empowers everyone to take responsibility for security and pushes developers to identify and prioritize security issues at every step, resulting in better, more secure products and improved security management before, during, and after release.

For example, development teams may consider security questions from the start and include them as part of strategic planning, such as:

- What level of security controls are needed within an app?
- How important is speed to market?
- What is the business' risk tolerance?

IT and business leaders must embrace security technologies that can monitor security at every step at the app level, alert teams to potential and active security threats wherever the app connects, and automatically remediate the threat.

Rapid change leaves app security stuck in the past

The app landscape has changed dramatically in the last few years, yet app security has remained largely the same. Fifteen years ago, applications and app clients were all housed on-premise, making security and risk containment a straightforward process. But as the use of cloud technology has grown, application environments have become more complex and more difficult to secure.

Now, with rapid iteration enabled by the cloud and driven by the widespread adoption of Agile methodologies, app delivery now occurs via an in-node model to an app stack that's sprawled across various entities and platforms.

Companies have widely adopted multi-cloud environments to replace their single on-premise infrastructure and tap into virtually unlimited compute and storage capacity. But it also means that application components may run on a mix of platforms like Azure, Google, AWS, and on-premise databases that can create visibility gaps and increase the risk of a security event.

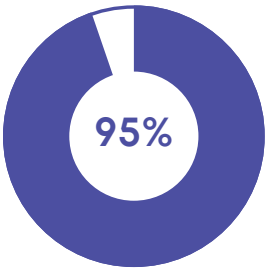
While cloud transformation empowers teams to build and deploy applications faster with greater agility, many organizations continue to apply outdated security strategies that no longer reflect the needs or realities of the modern application development landscape.

Devs struggle to manage security across disconnected systems with limited visibility

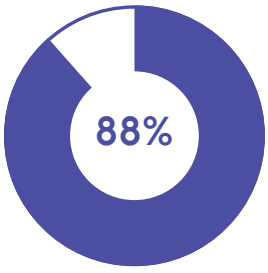
Another challenge facing today's DevOps leaders is the difficulty of identifying and handling security risks across multiple disconnected systems and platforms. With application development housed across multi-cloud environments, the attack surface has expanded—and with it, the scope and complexity of security risks have grown exponentially, leading to an influx in attacks.

One Vanson Bourne survey[4] cited bot attacks, software supply chain attacks, and API attacks as the top application security challenges facing enterprises today—making it virtually impossible for devs to keep up, let alone take a proactive posture. There are simply too many potential vulnerabilities for human teams to handle on their own.

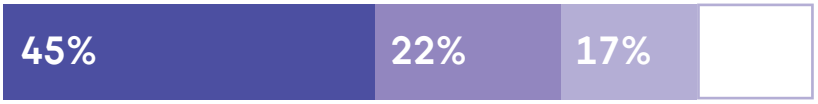
The state of app and cybersecurity



95% of cybersecurity breaches are caused by human error



88% of organizations worldwide experienced spear phishing attempts



45% of breaches featured hacking, 22% involved phishing and 17% involved malware

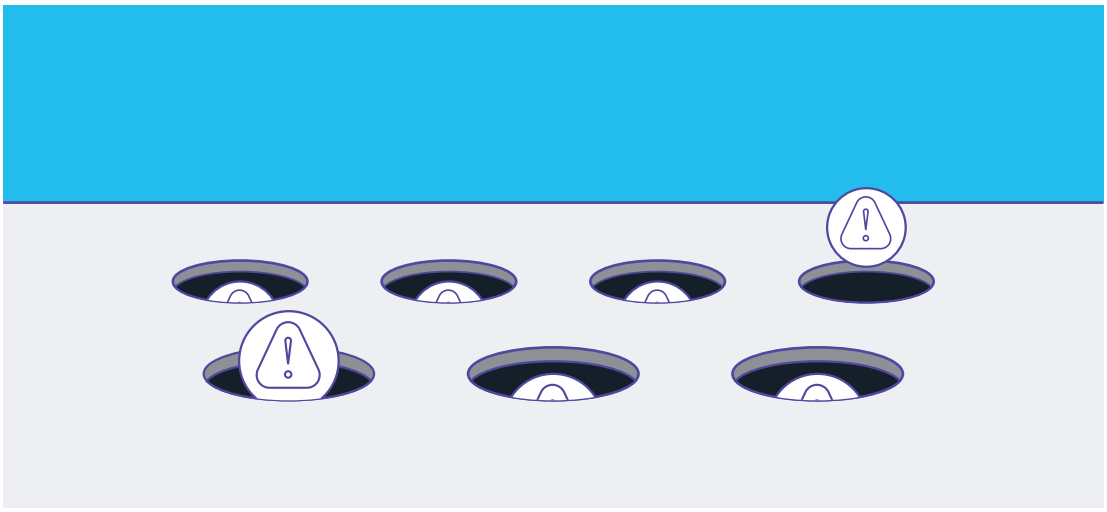
86% of breaches were financially motivated and 10% were motivated by espionage

Source: 134 Cybersecurity Statistics and Trends for 2021. Varonis.com

Additionally, teams have limited visibility into app components running on different platforms. In order to connect the dots and stitch together a full picture of the security landscape, organizations need multiple tools, which can be cumbersome to adopt and costly to implement. Even then, a patchwork of solutions increases complexity — often raising more questions than answers — leaving teams one step behind when it comes to security mitigation.

[4] "The state of application security in 2021" VansonBourne.com

For example, basic network security monitoring solutions simply alert that there is a problem, but don't necessarily show where it is, what it is, or how to fix it. Without a way to prioritize alerts based on business impact or potential risk severity, security teams are left playing a time-consuming game of whack-a-mole.



Not only is this frustrating for security teams, but it's also costly and unsustainable for business. In addition to the upfront costs of identifying and remediating issues (not to mention the reputational impact on a company), the cost of non-compliance can be steep—particularly if a data breach involves personally identifiable information (PII). Regulatory penalties for security violations can range from $50-$50,000 per record under HIPAA (up to $1.5 million per year) and up to $100,000 per violation under the GLBA.[5]

280

The average time to identify a breach in 2020 was 280 days.[6]

App security is still a second thought

Perhaps the biggest issue enterprises face today when it comes to application security is that security remains separate from the initial development lifecycle. Following a traditional DevOps approach of rapidly developing and deploying apps, security is still largely applied post-deployment. In other words, devs focus primarily on meeting product requirements and business needs while leaving security as an afterthought.

Ignoring or deprioritizing security during the development process can lead to increased human error when teams push releases faster in favor of meeting business or customer needs. And once the app is released, it's much more difficult to uncover what caused an issue and identify a fix. But waiting until production to worry about security is often too late—and even relying on periodic third-party audit solutions to bridge those security gaps is insufficient.

[5] "Cybersecurity Laws and Penalities," CyberInsureOne.com

[6] "Cost of a Data Breach Report 2020," IBM.com

Because applications and their components are so dispersed, periodic third-party audits of the overall app stack can take weeks or even months to complete since they may only have limited visibility and access to the company's security landscape. And every day waiting for an audit is a day that data is at risk.

When the average global cost of a data breach is $3.86 million, closing those security gaps is a top priority. Enterprises that want to stay ahead of security threats and build greater resilience into their applications and development processes will need to rethink how they do security.

Driving end-to-end security with DevSecOps

As application development accelerates, security must keep pace. Research suggests that 80% of businesses that fail to shift to a modern security approach will face both increased operating costs and a lower response to attacks by 2023.[7]

Today's business leaders recognize that the old approach to DevOps security no longer works in a complex, rapid development environment. The Gartner Hype Cycle for Agile and DevOps, 2020, reports that DevSecOps is "Climbing the Slope" with mainstream adoption and maturity just five years away.[8]

That's why enterprising IT and security leaders are increasingly seeking to close those security gaps and baking security into every facet of its app development and delivery process through a series of cultural and process changes, including:

Encouraging collaboration between DevOps and security teams

Integrating security into your DevOps program can further eliminate operational silos and encourage collaboration between DevOps and security teams. To start, "shift left" and introduce security testing earlier in the development process, working with your security team to analyze and assess security risks and priorities during planning phases to set the foundation for development.

Building a mature approach to DevSecOps allows you to strengthen your security posture and scale security operations, without sacrificing speed.

Automating security with robust AI

Automation is key to a successful DevSecOps strategy. Seek solutions with robust automation to strengthen your security posture using artificial intelligence (AIOps).

> "The self-learning algorithms in AIOps platforms can spot internal malicious activity and unauthorized access across the entire network ecosystem—including on-premises data centers and virtualized cloud deployments," which is crucial as organizations increasingly move their applications to the cloud.[9]

[7] Collins, John and Sadowski, Gorka. "Embrace Remote Security Operations," Gartner.com, Sept. 3, 2020

[8] Horvath, Mark. "Hype Cycle for Application Security 2020" Gartner.com, July 27, 2020

[9] "AIOps uses AI automation to boost security" MIT Technology Review Insights

AIOps extend human capabilities in multiple cybersecurity tasks, including monitoring, assessing, and resolving security issues—freeing up your security team to focus on higher-value issues and enabling them to collaborate more effectively and strategically throughout the development lifecycle.

This is where DevSecOps shines. When you teach AI security tools to identify threats and resolve them independent of an admin, you reduce human error, increase efficiency, and drive greater agility in development—enabling your team to ship and deploy applications even faster.

Aligning security to the business to protect your bottom line

According to a report by IBM, nearly 40% of the average total cost of a data breach stems from lost business—including increased customer turnover, lost revenue due to system downtime, and the increasing cost of acquiring new business due to a diminished reputation.[10]

Part of the problem is that security teams typically haven't had targeted insights into what risks to focus on and which threats will have the most impact on the business. A mature DevSecOps approach integrates security processes and tools into the development lifecycle to enable full visibility into the security landscape and contextualize security in a meaningful way.

This allows you to identify which of your app services and business transactions are experiencing security incidents and prioritize security tasks based on risk and impact to the application, user, and business.

Prioritizing securing your cloud

As businesses increasingly adopt cloud computing, along with new low-code and no-code app development tools, perimeter-only security will no longer be sufficient. Instead, runtime application self-protection (RASP) provides visibility from inside the apps so you can secure them wherever they live and however they are deployed.

Validating data requests directly inside the app helps to prevent vulnerabilities from being exploited and provides threat intelligence that identifies attacks down to the code level. RASP technology gives developers targeted insight into their application environments that allow them to respond to threats at scale—whether that's in containers, on-premises, or in the cloud—and integrate security throughout the entire application lifecycle.

Put security at the center of your business

Cisco Secure Application provides a modern solution to a modern application security problem. This industry-first application security solution combines security and performance insights to streamline vulnerability management and protect your business from attacks and other security vulnerabilities.

Protect applications from the inside out

From mainframes to microservices, Cisco Secure Application detects threats continuously and defends your business against attacks in real-time.

Simplify the lifecycle of vulnerability fixes and see what is happening inside the code to prevent known exploits. Secure Application operates directly in the app runtime and works seamlessly with the systems and applications you're already using, including Java apps and all major languages.

[10] "Cost of a Data Breach Report 2020," IBM.com

Detect vulnerabilities in minutes through unified business, security, and performance insights and automatically block threats to safeguard customer data, organizational IP, and your brand equity.

Automation is key to a successful DevSecOps strategy. Seek solutions with robust automation to strengthen your security posture using artificial intelligence (AIOps).

Prioritize responses by business impact

Secure Application empowers you to automatically detect and resolve issues across your entire technology stack, including cloud-native microservices, Kubernetes containers, multi-cloud environments, or mainframe data centers.

Using combined application and security monitoring, you can get targeted insights and unified visibility into your application security landscape, so you can see how and where vulnerabilities can impact your business, put decision-making into context, and focus on incidents that matter most.

Break down silos between AppOps and SecOps

Secure Application's holistic monitoring system leverages AI to enhance risk remediation and enable security to keep pace at scale. Boost security maturity with a solution that integrates security at every level to accelerate development and solve bottlenecks. With a unified context between AppOps and SecOps, your teams can collaborate effectively and efficiently to focus on what the business needs.

Benefits:

- Full-stack observability for clear visibility into your security landscape.
- 24/7 monitoring driven by AI so you never miss a threat.
- Real-time notifications and detailed info for better on-the-spot decision-making and post-mortem analysis.
- Better collaboration between DevOps and SecOps teams for faster development cycles.
- Robust analytics that drive increased business performance and agility.

Go from reactive to proactive security today

Today's enterprises can no longer afford to approach app security as an afterthought, yet applications are more challenging to secure than ever before. IT teams—especially DevOps and security teams—need more effective, automated, and teachable tools to keep up with the rapid pace of expansion in the app ecosystem.

But while most solutions simply monitor and alert without context, providing limited value to the business while leaving IT teams stuck guessing about—and reacting to—security threats, Cisco Secure Application protects your IT perimeter with one seamless solution.

Secure Application is simple to deploy and easy to manage. It integrates your security operations seamlessly, working across applications, systems, and languages to monitor and detect vulnerabilities in real-time, enabling your teams to proactively address security throughout the lifecycle of your applications—from development to ship. When you understand the risks, who will be affected, and what the potential impact could be to your business, you can make strategic, informed decisions to secure your data.

With Cisco Secure Application, DevOps and security teams can work together with greater agility and collaboration without sacrificing speed or innovation.

To learn more about how Cisco Secure Application can secure your business, schedule a demo or try for free today.

About AppDynamics

AppDynamics is the Application Intelligence company. With AppDynamics, enterprises have real-time insights into application performance, user performance and business performance, enabling them to move faster in an increasingly sophisticated, software-driven world. AppDynamics' integrated suite of applications is built on its innovative, enterprise-grade App iQ Platform that allows its customers to make faster decisions that enhance customer engagement and improve operational and business performance. AppDynamics is uniquely positioned to enable enterprises to accelerate their digital transformations by actively monitoring, analyzing and optimizing complex application environments at scale.

To learn more about AppDynamics, visit https://www.appdynamics.com