mend.io

Five Principles of Modern Application Security Programs

EXECUTIVE SUMMARY

Companies of all sizes and across all industries and geographies have one unfortunate thing in common: They're prime targets for cyberattacks. If that seems a bit alarmist, consider that cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025 – up from $3 trillion in 2015. That growth has led experts to conclude that cybercrime represents the greatest transfer of economic wealth in history.

As a foundational element of the digital world, applications have come under particular focus for threat actors. In fact, 71 percent of IT and security leaders say their portfolio of applications has become more vulnerable to attack in the past year. However, traditional application security (AppSec) strategies often prove ineffective – 63 percent of organizations still find it difficult to monitor, detect, and prevent attacks at the application level. To adapt and defend against the constantly evolving threat landscape of today's digital world, organizations need to build a modern AppSec strategy based on resiliency.

Such an approach allows organizations to prevent, detect, remediate, and recover from the wide range of threats affecting applications – a vital strategy for supporting today's increasingly digital business ecosystem. As companies grapple with the cost of cybercrime – loss of data, money, reputation, and customer trust, to name just a few – it's vital to understand five key principles of modern application security that enable companies to respond quickly to threats and minimize damage, while also continuing to operate even while under attack.

FORCES FOR CHANGE

The hits keep coming for application security teams today. First, they must revamp application security to support increasing business dependence on applications and a commensurate barrage of application-based attacks. Meanwhile, government regulations around data privacy and improving cybersecurity have added further complications.

But at the same time, the nature of application development increases vulnerability and expands attack opportunities for malicious actors. The increased dependence on open source software components, combined with a steep increase in custom-built applications, has led to massive growth of application code vulnerabilities.
Threat actors not only leverage open source vulnerabilities, but they also contribute malicious code to open-source projects with the knowledge that reviewing code for security implications varies widely across projects.

THE HITS KEEP COMING

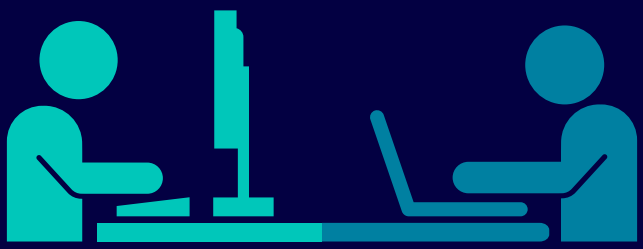
A rapidly changing digital world drives AppSec reinvention

Average attacks per company up 31%[1]

Applications top cause of external breaches[2]

Increased government requirements to improve cybersecurity[3]

By 2025, 60% of organizations will consider cybersecurity risk in business decsions.[4]



Apps run the world: average of 976 applications per company[5]

OSS use continues to skyrocket — 77% companies increased usage[6]

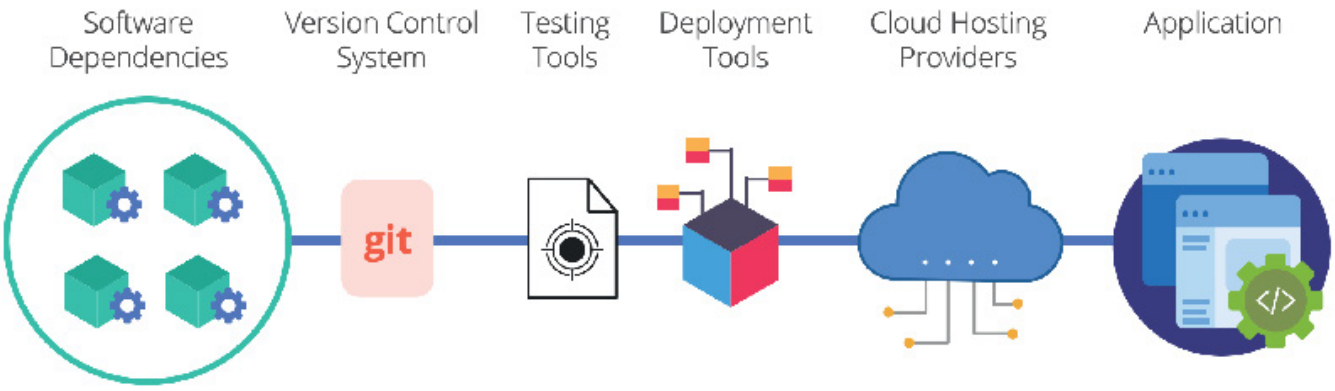
Open source vulnerabilities more than doubled from 2018 to 2020[7]

Software supply chain attacks to triple by 2025[8]

IT and security professionals say two of the biggest challenges with open source in applications stem from lack of staff experience and proficiency (47 percent), as well as keeping up with updates and patches (42 percent). Other factors that contribute include:

- Increased software complexity: Today's software, in conjunction with the ubiquity of application programming interfaces (APIs), adds additional complexity and further expands the attack surface, particularly when combined with increased dependence upon the cloud and IoT expansion.
- Cloud-native apps: Within the next five years, a third of global companies are expected to move more than 75 percent of workloads into the cloud to reduce costs, gain operational resiliency, and access the latest and best technologies. The problem, however, is that 32 percent of companies admit that security is not a part of their cloud plans, and another third admit that cloud security is too complex and that they lack the skilled staff to build a proper cloud security framework.

Figure 14: Attack Surfaces in Software Supply Chain



APPLICATION SECURITY VS. THE NEED FOR SPEED IN SOFTWARE DEVELOPMENT

Despite the obvious need for application security, it often competes against the need for developers to quickly develop software. Moreover, factors such as accelerated digital transformation plans, application migration to the cloud, and the growing reliance on agile and DevOps practices further increases the pressure to develop and deliver applications at speed.

This rapid movement to a digital world only ratchets up demand for faster software development. This leaves application security teams in a bind. Just as application security has become both more important and more complex to implement, shrinking development cycles leave less time to do so. How do companies reconcile the need for speed in software innovation with the equally pressing need for effective application security?

In order to adapt and support the constantly evolving threat landscape of today's digital world, IT and security leaders need to build a modern AppSec strategy designed to support demanding development cycles while also ensuring application security. To build holistic and modern AppSec programs that move beyond checking compliance boxes, organizations should follow five key principles.

5 PRINCIPLES OF MODERN APPLICATION SECURITY

1. Meticulous prep and planning
2. Beyond shift left: Shift smart
3. Automation plays a critical role
4. The value of governance
5. DevSecOps demands cultural change

1 METICULOUS PREP AND PLANNING

It might seem obvious, but the reality is that attackers would be much less successful in their endeavors if they had less to attack. The first role of the application security team should be to reduce the attack surface. To that end, a number of questions should be answered, including:

Do you know your application operating environment?

The first step in reducing your attack surface is to know your application operating environment or the environment in which users run the application. Specifically, it's vital to know whether the application communicates with the internet.

Do you know your software?

Knowing your software means you know what's in it, the level of risk it carries, and whether every application has a software bill of materials (SBOM). SBOMs are a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships. As such, when a component is found to contain a critical security vulnerability, security teams can quickly ascertain which applications are affected. The importance of SBOMs has increased significantly over the past two years as both public- and private-sector organizations grapple with the fallout from incidents like Log4j. Indeed, both the May 2021 presidential Executive Order on improving cybersecurity and the Department of Homeland Security (DHS) Software Supply Chain Risk Management Act of 2021 include directives on SBOMs. But the onus for creating accurate SBOMs falls on enterprise security teams, and many struggle to do so. Only 27 percent of IT and security professionals say their organizations currently generate and review SBOMs, and 90 percent say it's increasingly difficult to do so. Almost half say their current SBOM processes involve manual steps, and 44 percent say they lack expertise to create SBOMs.

What potential impact does it have?

To understand the impact that an application has on your organization, a few questions should be answered:

- Does the application interact with sensitive data?
- Is it critical to the business?
- Do you have full visibility into all applications and data assets, including the ability to quickly see and understand application dependencies?
- Are you keeping application dependencies updated through proper software hygiene?

- Do you have the ability to continually assess vulnerabilities and rapidly patch any issues that arise?
- Do you have a process for breaking systems to test cyber resilience? The reality is that if IT and security teams aren't doing so, attackers certainly will.
- Do you deploy red teams made up of seasoned security professionals and/or independent ethical hackers to act as adversaries to overcome cybersecurity controls?
- Do you perform third-party penetration testing?

2 BEYOND SHIFT LEFT: SHIFT SMART

Shift left security aims to streamline and improve application security by embedding it earlier in the software development lifecycle (SDLC) rather than as a separate process at the end. However, many companies struggle to find AppSec tools that are easy enough for developers to use. Because, if truth be told, application developers will not use tools that slow them down or cause them to go through much of a learning curve. AppSec-resilient companies focus instead on shifting smart, which means making the security tool as invisible and as automated as possible.

Shifting smart starts with the following tactics:

- **Match security to the speed and automation of your DevOps environments** with an eye toward fast results and automating as much as possible. Throughout all phases, automated detection, prioritization, and remediation tools can be integrated with your team's development environments, code repositories, build servers, and bug-tracking tools to address potential risks as soon as they arise.
- **Widen the scope of design** and move away from project-by-project processes. This means looking at multiple languages, every project under development, and everything running in production, containers, and Kubernetes.
- **Make it easy for developers to fix their code.** Don't force developers to leave their development environment. Adapt your security testing tools and processes to the developers – not the other way around. Likewise, don't force them to become security experts. While every person on the DevOps team should have security training, they shouldn't be expected to become security experts. For instance, make it a priority to train all developers in the basics of secure coding and the ways applications can be attacked.

- **Watch out for false positives.** Almost half of all security alerts are false positives, which tends to sour developers on using security testing tools. Your goal shouldn't be to achieve perfect security and zero risk – that's simply impossible. Instead, apply what Gartner refers to as CARTA – a continuous, risk- and trust-based assessment. This strategic approach prioritizes application vulnerabilities without trying to remove all possible vulnerabilities from applications, in essence acknowledging the trade-off between the speed of testing, wasting developer time with false positives, and increasing risk from false negatives.

- **Cut down on tool sprawl.** More than half of companies today have deployed between 21 and 50 separate security tools, and another 36 percent of companies deploy between 10 and 30 separate security tools. Not surprisingly, 37 percent of companies say they have too many security solutions and technologies to achieve cyber resiliency. On top of that, consolidating security tools actually lowers total cost of ownership and improves operational efficiency in the long term, leading to better overall security. A good example of the benefits of tool consolidation can be seen through static application security testing (SAST) and software composition analysis (SCA). SAST is used for testing code that's been developed in-house, while SCA is used to manage open-source components. In an ideal world, application developers use both tools to gain a holistic view of an application's security. Giving developers a single platform from which both can be done increases the likelihood that they'll use both.

3 AUTOMATION PLAYS A CRITICAL ROLE

Automation not only reduces the time that developers spend on security, but it also makes security processes faster and more thorough than any manual approach. Two-thirds of business leaders recognize that automation strengthens cyber resiliency by providing support for IT security teams, as well as by reducing security risks. Likewise, automation addresses the need for speed in detection, triage, and response, while also easing the stress caused by the ongoing shortage of cybersecurity professionals. Automating processes like dependency saves time and reduces risk by ensuring current versions are in use.

And by deploying solutions that automatically detect and remediate vulnerabilities, companies can improve AppSec outcomes and make it simpler and easier to integrate application security into the SDLC. Given all these benefits, it's not surprising that 35 percent of organizations say they will invest in security automation in the coming year.

4 THE VALUE OF GOVERNANCE

While resilient AppSec practitioners know the importance of process and policy, many companies lag. AppSec should be part of a cybersecurity incident response plan (CSIRP); however, only 26% of organizations have a CSIRP that's applied consistently across the entire enterprise, a figure that has remained low over the years.

And even for companies that do have a CSIRP, 74 percent inconsistently apply it. Moreover, the frequency in which companies review and test them is problematic, with seven percent doing so quarterly, six percent doing so semiannually, and 40 percent failing to establish a set time period for doing so. A full 12 percent have no plans to do so at all.

Nevertheless, it's vital for companies to have an incident response plan. Yet less than half of companies say they have specific incident response plans for at least one of the eight types of cyberattacks. For instance, 35 percent lack an incident response plan for distributed denial of service (DDoS) attacks, and 68 percent lack a plan for supply chain attacks. And only 40 percent regularly assess third-party risk.

Yet regularly updating and reviewing an incident response plan has helped 38 percent of companies improve their cyber resiliency. In doing so, these companies improved visibility into applications and data assets (65 percent), and they reported timely assessment of vulnerabilities and patches (39 percent).

5 DEVSECOPS DEMANDS CULTURAL CHANGE

It will likely surprise no one that 65 percent of companies say there is limited or no collaboration between their application development and security teams. And 50 percent say that security isn't adequately emphasized during the development of new applications.

Modern AppSec programs require a collaborative security culture. Ultimately, your attitude toward application security should lean toward more guardrails and fewer speed bumps. In other words, it's important to make sure that developers and DevOps teams are working toward the same goals with the same understanding of what's expected to get there. So, for instance, it's vital for enterprises to develop and apply best practices for application security – as long as those practices don't become so onerous that they're ignored or avoided altogether.

One increasingly popular method for ensuring success is to embed security ambassadors within development teams. Doing so enables an enterprise to leverage the limited resources of security teams into the development organization. As such, security ambassadors should be able to act as readily available experts who can anticipate potential problems early in the development process. They should work to reduce the complexity of securing applications by promoting best practices and explaining to all stakeholders how they benefit from them.

Another increasingly popular option is to make use of security champions. This is a fresh take on a practice that both development and IT teams are familiar with, wherein chapters, guilds, and communities of practice are created and used to benefit all stakeholders. Successful security champions will have time to deliver training and stay abreast of new tools and trends. Likewise, security champions will only be successful if they have the support they need as they work with development teams.

CONCLUSION

There's no question that the world is becoming increasingly digital, which further highlights the critical role of application security. Today's organizations cannot function without applications, which provide them with benefits like improved engagement with customers, better brand awareness, more detailed and actionable data to drive marketing and sales, and so much more.

However, applying outdated methods to ensure the security and resiliency of apps is the equivalent of taking a cutlass to a light saber fight. Meanwhile, there's no question that adversaries are launching attacks using the most modern and nefarious tools possible.

The bottom line is, there is no such thing as absolute application security — attackers are smart, motivated, and never give up. Modern application security strategies built for the constantly evolving threat landscape rely on organizational flexibility and the ability to consistently assess adjust to changing conditions. For that to work, such programs must be resilient.

APPENDIX

[1] **Accenture State of Cybersecurity Resilience 2021**
https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

[2] **Forrester: The State of Application Security 2021**
https://www.forrester.com/report/the-state-of-application-security-2022/RES177413

[3] **Executive Order on Improving the Nation's Cybersecurity**
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[4] **Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23**
https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

[5] **MuleSoft Research 2022 Connectivity Benchmark Report**
https://resources.mulesoft.com/ty-report-connectivity-benchmark.html#loaded

[6] **OpenLogic 2022 State of Open Source Report**
https://www.openlogic.com/resources/2022-open-source-report

[7] **Mend State of Open Source Vulnerability Report**
Gartner https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022