WHAT'S INSIDE

2 FALLOACY NO. 1
Implementing an application security program is cost prohibitive

4 FALLOASY NO. 2
Application security is highly complex

5 FALLOASY NO. 3
Covering only business-critical applications is the key to success

6 FALLOASY NO. 4
Application security is only for software vendors

7 FALLOASY NO. 5
Developers won’t change their agile processes to incorporate application security

8 FALLOASY NO. 6
One single technology can secure all applications

9 FALLOASY NO. 7
Firewalls, anti-virus and network security cover applications by default

10 FALLOASY NO. 8
Purchased software doesn’t require application security testing
INTRODUCTION

The news headlines have been filled with stories about security breaches in recent months. And most of these high-profile breaches originated with a vulnerability in an application. In fact, web and mobile applications account for more than a third of data breaches (source: 2014 Verizon Data Breach Investigations Report). Yet, most organizations are not spending time or money on application security. So why the disconnect? One reason is that fallacies abound when it comes to application security. Many of these fallacies stem from the traditional, on-premises tools-based approach to application security, which has fostered the misconception that application security programs are expensive and difficult to manage. But as breaches continue to make headlines, organizations are realizing the serious risk posed by applications.

Now is the time for organizations of all sizes to understand the fallacies, and the truths, of application security.

AppSec Fallacy No. 1
IMPLEMENTING AN APPLICATION SECURITY PROGRAM IS COST PROHIBITIVE

The reality
Cyberattackers are increasingly exploiting vulnerabilities in the application layer, leaving companies with significant damage and financial loss. At the same time, the movement toward cloud-based security solutions has reduced the cost of application security. With the odds of a costly breach going up, the expense of application security should no longer act as a barrier to implementing a program, as the cost of a breach outweighs the cost of the program.

The details
With the dramatic shift from on-premises application security to cloud-based, the financial picture has changed. You no longer need to hire more security experts, or install more servers or tools, to start or scale an application security program — leading to substantial cost savings in installation and maintenance compared to traditional on-premises solutions.
In addition, Forrester estimates that in 2015 at least 60 percent of organizations will suffer a security breach. And most of the recent big breaches in the news stemmed from application vulnerabilities. The financial implications of these breaches are substantial. In fact, the Verizon 2015 Data Breach Investigations Report found that data breaches cost businesses around the world $400 million. The cost of a breach is felt in:

- **Lost revenue:** This might result from stolen corporate data, lowered sales volumes (if consumers get scared) or falling stock prices.

- **Money spent on investigation and cleanup:** After suffering a breach, organizations must spend time and money to identify the source of the breach (which can be a lengthy and expensive process), repair the damage and then re-secure (and possibly re-certify) the breached system. A recent joint Veracode/Centre for Economics and Business Research (Cebr) report found that cyberattacks cost UK firms £34 billion in revenue losses and subsequent increased IT spending.

- **Cost of downtime:** When systems are down due to an application flaw, or shut down in response to a breach, the costs can soar. A recent Information Age article estimated that every hour of downtime costs businesses $100,000. In addition, time spent fixing a breach means time diverted away from development and innovation.

- **Brand damage:** The long-term reputation damage associated with security breaches can be substantial and lead to intangible costs or loss of business.

Simply put, spending on proactive application security today reduces the chance of a massive financial loss tomorrow.

---

**Tweet these stats**

“Cyberattacks cost UK firms £34 billion in revenue losses and subsequent increased IT spending.”

According to joint research by Veracode and the Centre for Economics and Business Research (Cebr)

“In 2015 at least 60 percent of organizations will suffer a security breach.”

According to Forrester
AppSec Fallacy No. 2

APPLICATION SECURITY IS HIGHLY COMPLEX

The reality
Application landscapes are complex, but securing them doesn’t have to be. Rome wasn’t built in a day, and your application security program won’t be either. The keys are to start small, keep things simple, prove the value and then mature the program over time. The most successful companies we’ve worked with have started by securing a few apps at a time.

The details
You don’t have to secure every app on day one. Reduce the complexity of application security by working with a trusted partner with AppSec expertise to build the program in stages. You can start by implementing procedures to assess the most business-critical applications, and then scale your program from there.

With the right solution and the right game plan, application security goes from feeling very overwhelming to becoming very doable.
AppSec Fallacy No. 3

COVERING ONLY BUSINESS-CRITICAL APPLICATIONS IS THE KEY TO SUCCESS

The reality
Securing your most critical apps is a good place to start — not a good place to stop. Cyberattacker are increasingly targeting less-critical and third-party applications, meaning the entire application landscape needs to be secured.

The details
If your entire application landscape is not secured, cyberattacker have a way to access your systems and their critical information. Securing all your applications — including those you’ve built, bought or pieced together with in-house and open source components — is critical. Why? Because cyberattacker are looking for the path of least resistance into your organization, and that path is increasingly through less-critical and third-party applications.

Recent high-profile breaches prove this point. JPMorgan was recently breached through a website for its annual charity road race — hardly a business-critical application. Hackers found a vulnerability in this third-party website and used it to access the enterprise’s network.

However, most organizations are not currently securing their entire application landscape and, in fact, don’t even know how many applications they have. Application security starts with knowing what needs to be secured. You need a global inventory of all your public-facing web applications such as corporate sites, temporary marketing sites, related sites (.mail, .info, etc.), international domains and sites obtained via M&A. The security of third-party apps and components shouldn’t be neglected either, as evidenced by the JPMorgan example above. Known vulnerabilities (CVEs) in third-party components and applications are a blind spot for organizations; according to the 2015 Verizon Data Breach Investigations Report, 99.9 percent of all CVEs used by attackers in 2014 breaches were more than a year old when exploited.

You should find an application security solution that can assess all your apps — whether they are built, bought or assembled.
AppSec Fallacy No. 4

APPLICATION SECURITY IS ONLY FOR SOFTWARE VENDORS

The reality
Every company today is reliant on applications and uses them to provide access to its critical information. Therefore, every company must also ensure its applications are secure.

The details
Mobile and cloud computing are dramatically changing the way we deliver business innovation. The world now runs on applications, and users typically interact with enterprises through applications. As a result, every company is becoming a software company — regardless of what its primary business is. Even GE now considers itself a software company. And most companies today are rapidly producing web, mobile and cloud applications in order to keep up with the pace of innovation. To innovate even faster, organizations are using Agile development processes as well as augmenting their own internal development programs by purchasing software from third-party providers and integrating open source libraries and components.

Ideally every piece of software would be assessed for security, but that isn’t the reality. Research done by IDG revealed that almost two-thirds of applications are not assessed for security.

Every company, in every industry, now runs on software and needs to make application security a priority.

LEARN MORE

IDG WHITEPAPER
Why Application Security Is a Business Imperative

WEBINAR
8 Practical Tips to Link Risk and Security to Corporate Performance
AppSec Fallacy No. 5

DEVELOPERS WON'T CHANGE THEIR AGILE PROCESSES TO INCORPORATE APPLICATION SECURITY

The reality
Security assessments do fit into Agile, provided they adapt to the Agile process.

The details
It is true that Agile and security had a strained relationship in the past. This is because the standard ways of assessing code for security didn’t mesh with the Agile methods of software development. For instance, the waterfall development process has very distinct phases, and each security activity is completed before moving on to the next phase. Agile, on the other hand, doesn’t have such distinct phases. And it was assumed that security assessments would slow down the constant flow of development. However, security assessments can fit within Agile processes as long as security practitioners realize that security must adapt to Agile, not the other way around.

For instance, developers should pull security “left” into development processes and the “definition of done” rather than tacking it on at the end. Finding vulnerabilities during the coding phase instead of during a separate security hardening sprint saves time and increases velocity, while at the same time ensuring the security of the software being developed, tested and shipped.

In addition, some security solutions are better suited to working in Agile than others. For example, static analysis, or SAST, which can scan code for potential vulnerabilities when the software is in a non-running state, lends itself to the Agile process. This assessment technique enables developers to assess their software for issues without waiting for a running, testable application. A solution that integrates with developers’ existing processes and tools is also key to coding securely with Agile. By adding APIs to the development tools already being used by the programming teams (JIRA, Jenkins, Team Foundation Server), security can become so integrated into the development processes that it is seamless.

“The Agile methodology will enable those leading development teams to have first-hand insight into security of the code being built, and be able to reconcile these assessments with timelines around product testing and release dates. This ability begins to reduce the gap between the goals of the security side of an organization and those of the development teams. Neither innovation nor security is sacrificed.”

PETE CHESTNA, VERACODE’S DIRECTOR OF PLATFORM ENGINEERING, @PETECHESTNA

LEARN MORE

SECUROSIS WHITEPAPER
Secure Agile Development

WHITEPAPER
8 Patterns of Secure Agile Teams

WEBINAR
Secure Agile & DevOps: How It Gets Done
AppSec Fallacy No. 6
ONE SINGLE TECHNOLOGY CAN SECURE ALL APPLICATIONS

The reality
There is no AppSec silver bullet, and a truly effective application security program uses the strengths of multiple testing techniques.

The details
Effective application security ultimately includes more than one automated technique, plus manual processes. For example, static analysis (SAST) doesn’t require a fully functional system with test data and automated test suites, and dynamic analysis (DAST) doesn’t require modifying the production environment. Because of these strengths, SAST can be used earlier in the development cycle than both interactive application security testing (IAST) and DAST. DAST can be used more easily than SAST and IAST in production.

Each analysis technology has its own strengths. Static, dynamic, IAST, mobile behavioral, software composition analysis, web perimeter monitoring and manual penetration testing all play a role in a complete application security program.

Ultimately, effective application security is not focused on tools, but rather a systematic approach that leverages multiple technologies that, taken together, reduce application risk.

“Businesses aren’t asking for SAST, IAST, DAST — they’re asking, ‘how do I solve my problem’ and the right answer is, ‘with a little bit of everything, depending on your environment.’”

CHRIS WYSOPAL, VERACODE CO-FOUNDER, CTO AND CISO @WELDPOND

LEARN MORE

BLOG POST
No One Technology Is a Silver Bullet
AppSec Fallacy No. 7

FIREWALLS, ANTI-VIRUS AND NETWORK SECURITY COVER APPLICATIONS BY DEFAULT

The reality
Your organization is not secure if your applications are not. Firewalls, network security and anti-virus are not securing your apps. A dedicated application security strategy reduces risk in the area that is most likely causing the weaknesses in your infrastructure.

The details
One of the reasons that cyberattackers have turned their attention to web-facing applications is that most enterprises are proficient at hardening traditional perimeters with next-generation firewalls, IDS/IPS systems and end-point security solutions. This makes applications an appealing target, because they are:

- Exposed to the Internet, making them easy to probe by attackers from anywhere in the world.
- Replete with common vulnerabilities, such as SQL injection, that can easily be found via free scanning tools.
- Always changing, with short development cycles driven by new methodologies such as Agile and continuous deployment.
- Assembled as hybrid code from a combination of in-house development, outsourced code, third-party libraries and open source components — without visibility into which components contain critical vulnerabilities.
- Even more vulnerable with modern technologies that increase the attack surface by incorporating client-side logic using complex JavaScript or RIA technologies such as Adobe Flash.

Of course, you still need your WAFs and your anti-virus, but application security is another critical part of your security ecosystem, and should be treated as such.
AppSec Fallacy No. 8

PURCHASED SOFTWARE DOESN’T REQUIRE APPLICATION SECURITY TESTING

The reality

You do need to worry about the security of purchased software. Why? Because 65 percent of a typical enterprise application portfolio comes from third parties (source: Quocirca), yet 90 percent of third-party code does not comply with enterprise security standards such as the OWASP Top 10 (source: Veracode State of Software Security Report, Enterprise Testing of Software Supply Chain).

The details

Most enterprises use third-party code, and most third-party code is vulnerable. Yet the enterprise, not the vendor, is held responsible if the code leads to a breach. When customers’ financial data is compromised, they don’t hunt down the third-party vendor that wrote the code, but blame the company they engaged with in the first place. When Target was breached through an HVAC vendor, Target’s name was in the headlines, not the vendor.

In an age where outsourced IT is the norm, and attacks on third-party software are increasing, third-party security can no longer be ignored. In fact, regulatory bodies such as the OCC and industry organizations such as FS-ISAC, OWASP and the PCI Security Standards Council are now placing increased focus on controls required to mitigate the risks introduced by third-party software.

Traditionally, vendor surveys and self-attestations were the extent of third-party security, but this is no longer sufficient.

Engaging an outside application security specialist who can work with you and your third-party vendors to ensure application security is ideal. These specialist organizations understand the most pressing threats to applications and can help vendors and enterprises work together to make the process as seamless as possible.
CONCLUSION

You can no longer afford to ignore application security. Every company now runs on software, and that software introduces risk. Rather than relying on application security assumptions and anecdotal evidence, you need to get the facts, and take steps toward a comprehensive application security program.

KEY TAKE-AWAYS

1. The odds of an expensive breach due to an application vulnerability are going up.
2. Building an application security program in stages is key.
3. Cyberattackers are increasingly targeting third-party and less-critical apps.
4. All companies are reliant on applications, and must ensure the applications are secure.
5. Security assessments do work with Agile, as long as they adapt to Agile processes.
6. There is no AppSec silver bullet—a mix of technologies is needed.
7. Firewalls, anti-virus and network security do not secure your applications.
8. It’s critical to secure third-party software.

LOVE TO LEARN ABOUT APPLICATION SECURITY?
Get all the latest news, tips and articles delivered right to your inbox.
Veracode’s cloud-based service and systematic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world’s largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 20+ of Forbes’ 100 Most Valuable Brands.

LEARN MORE AT WWW.VERACODE.COM, ON THE VERACODE BLOG, AND ON TWITTER.