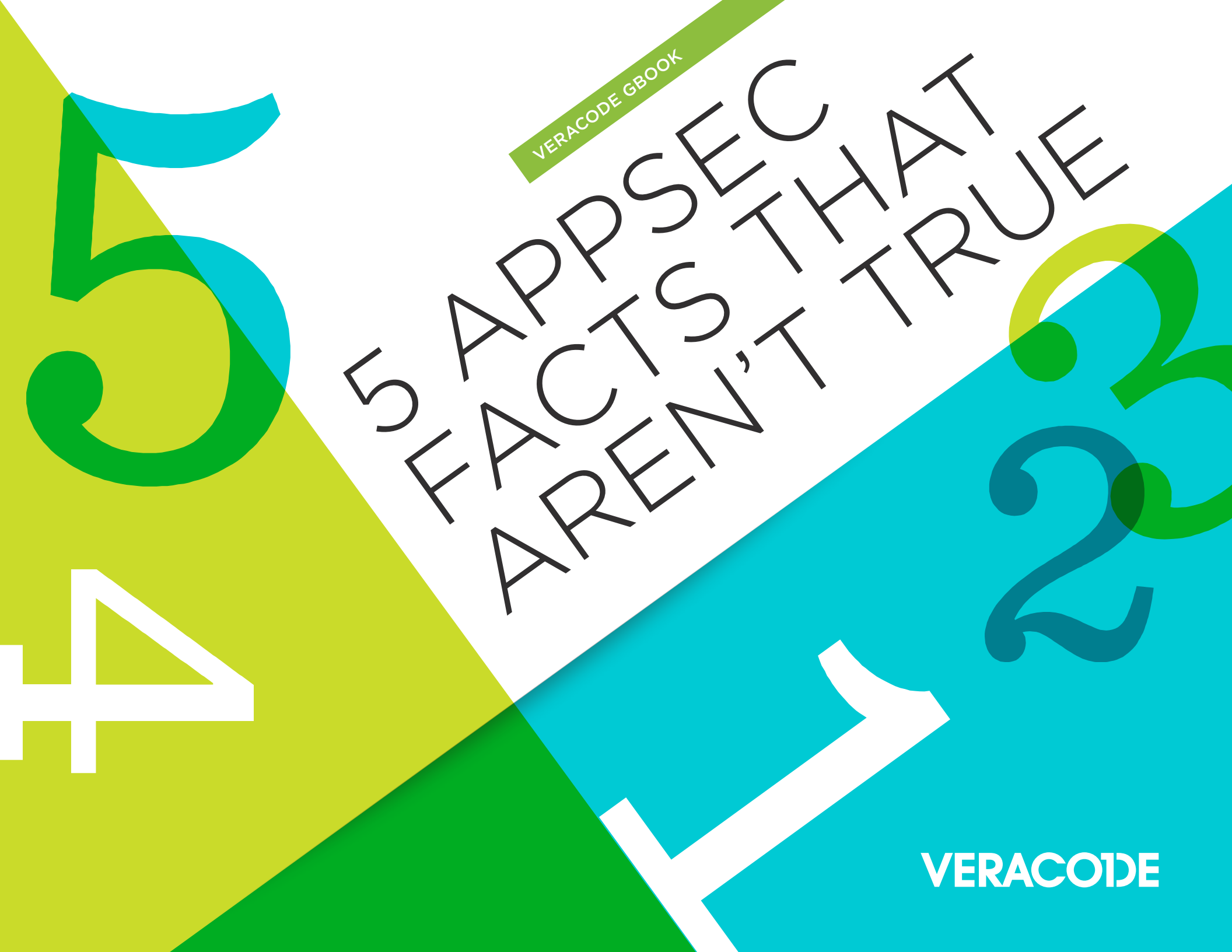
VERACODE GBOOK

5 APPSEC FACTS THAT AREN'T TRUE

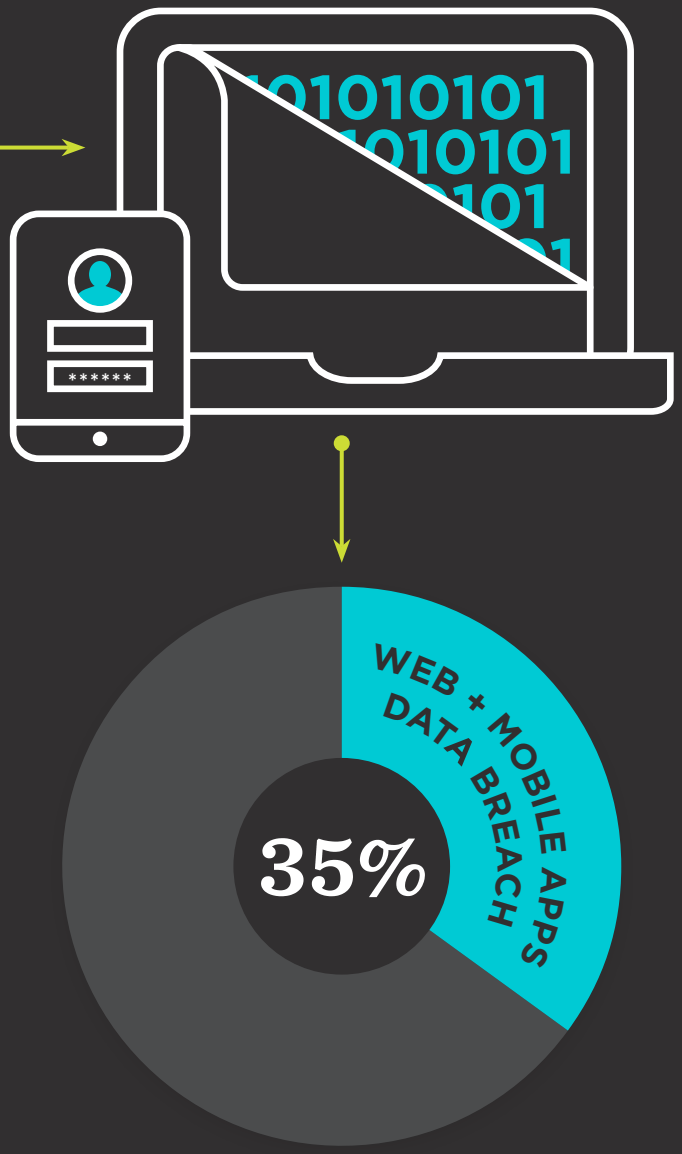


VERACODE

INTRODUCTION

Congratulations. You broke into IT (I mean, into the frustrating world of being underappreciated by most, yet paid enough to gain some satisfaction from the irony). You are no longer naïve enough to think that "stolen cookies" is what happens on Christmas Eve. But, despite being an IT genius, a few common (yet dangerous) misconceptions about application security may be preventing you from taking critical and simple steps to protect your system.

Web and mobile apps account for more than a third of data breaches, yet I'd bet your time, money and thoughts are focused on a security approach that is, at its best, incomplete. Don't let assumptions about your applications' security put you in the headlines for the wrong reasons. Here are some of the common misconceptions about application security and the realities that are often overlooked.



According to the Verizon Data Breach Investigation Report, web and mobile application attacks account for up to 35% of breaches in some industries

APPSEC FACTS THAT AREN'T

But ... implementing an application security program is cost prohibitive. Right? 1

Application security will slip through my fingers like sand. My brain hurts before I've even started. 2

I don't need to worry about security for applications that are not business-critical. 3

But AppSec falls to software vendors. 4

One single technology can secure all applications. 5

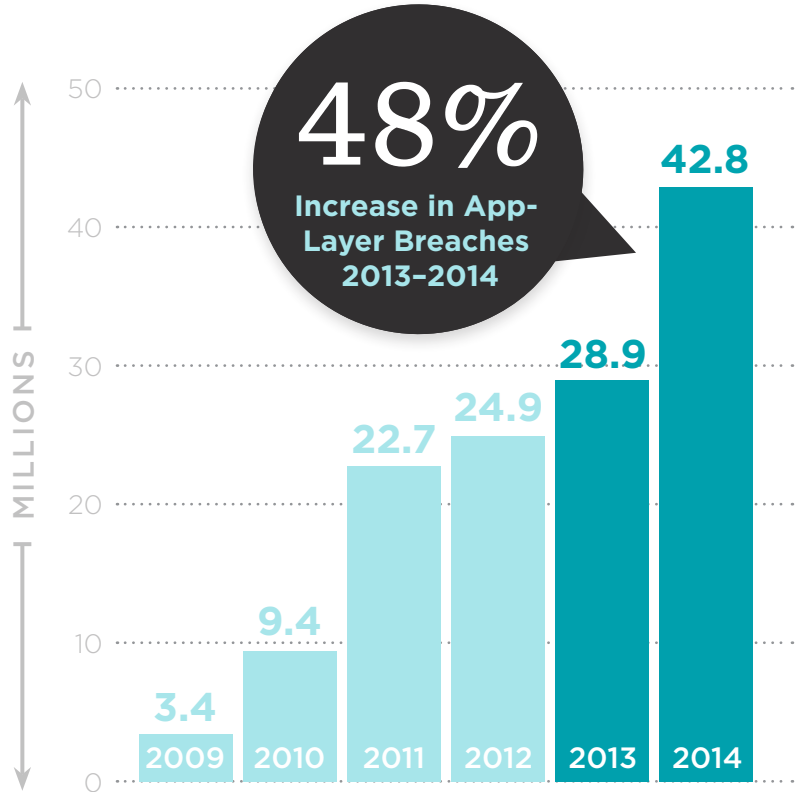
1

But... implementing an application security program is cost prohibitive. **Right?**

THE REALITY

We'll give it to you straight. Considering that, by the end of 2015, Forrester estimates at least **60 percent of organizations will have suffered a security breach,** best not to make your app the weakest link.

Significant damages and financial losses are caused by vulnerabilities in the application layer every day, and this disturbing trend isn't slowing down. In fact, there was a **48 percent increase in app-layer breaches** reported from 2013 to 2014 alone.



The costs incurred by ineffective or nonexistent app security can add up.

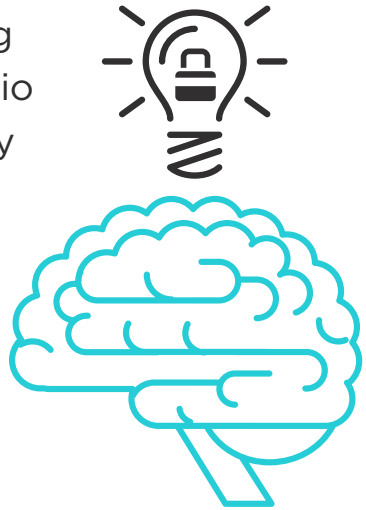
From lost revenue (stolen corporate data, lowered sales volumes or falling stock) to money spent on investigation and cleanup, not to mention downtime **(costs that can average $100,000 an hour)** and intangible yet resonating **brand loyalty damage,** which would you rather pay for?

Luckily for you, the movement toward cloud-based security solutions has reduced many of the costs of application security. The likelihood and cost of a breach clearly outweigh the costs of cloud-based protection. Spend your weekends with your family and friends, rather than with your warm computer at work after a breach.

Application security will slip through my fingers like sand. My brain hurts before I've even started.

THE REALITY

Application landscapes are complex, but securing them doesn't have to be. Your application portfolio wasn't built in a day, and your application security program won't be either. Just K.I.S.S. for now by implementing procedures to assess the most critical apps, then scale further security over time. With the right game plan, application security goes from feeling very overwhelming to becoming very doable.



RESOURCES

GUIDE

Ultimate Guide to Starting an Application Security Program

WEBINAR

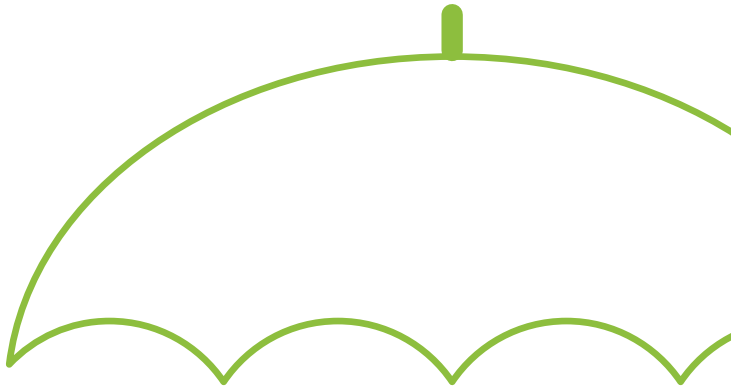
5 Steps for a Winning Application Security Program

WEBINAR

Work Smarter, Not Harder: How You Can Get More From a Mature Security Program

3

I don't need to worry about security for applications that are not business-critical.



THE REALITY

Securing your most critical apps is absolutely a good place to start — but not a good place to stop.

Cyberattackers are increasingly targeting less-critical and third-party applications, because they know those apps are like lost puppies — unprotected and alone. For you, this means the entire application landscape needs to be secured.

Don't forget the apps you've built, bought or pieced together with in-house and open source components. Most organizations are not currently securing their entire application landscape and, in fact, may not even know how many applications they have. Starting with creating a global inventory is not a paranoid step for you to take. Recent high-profile breaches continue to prove this point.

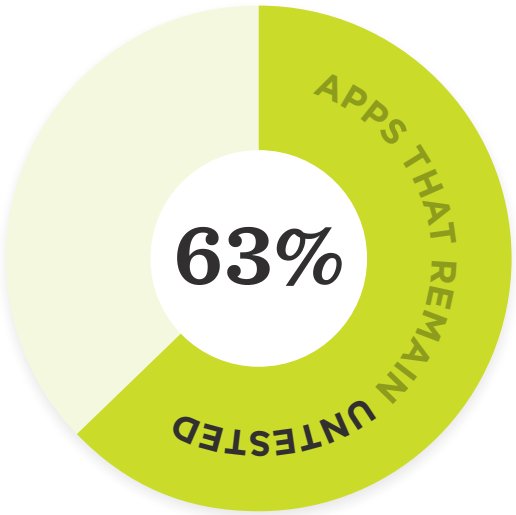
REAL-WORLD EXAMPLE

In Target's case, a sophisticated kill chain exploited a vulnerability in a web app. Though the application was designed to be used by Target's vendors to process payments, it ultimately allowed hackers access to critical customer data.

Most enterprises don't even know how many public-facing applications they have. Web application perimeters are constantly expanding as enterprises spin-up new websites for new marketing campaigns or geographies, create web portals for customers and partners, and acquire companies. Most organizations also have legacy and old marketing sites they're not even aware of. **No wonder your application threat surface is constantly growing.**

Find out the extent of your application threat surface with this Web Application Perimeter Calculator.

4 But AppSec falls to software vendors.



Apps that ARE TESTED for Security Vulnerabilities

38%
MOBILE APPS

38%
WEB APPS

37%
CLIENT/SERVER APPS

33%
TERMINAL APPS

THE REALITY

Guess who is going to be left holding the bag if you don't step up?

Every company is reliant on applications, and uses them to provide access to its critical information. Therefore, every company must also ensure its own applications are secure. Since outside users typically interact with enterprises through applications, every company is becoming a software company, regardless of what its primary business is. To innovate even faster (and complicate your job), organizations are using Agile development and incorporating third-party and open source software — all of which must be checked as well. IDG research revealed that **almost two-thirds of applications are not assessed for security.** Let's be proactive, shall we?

5

One single technology can secure all applications.

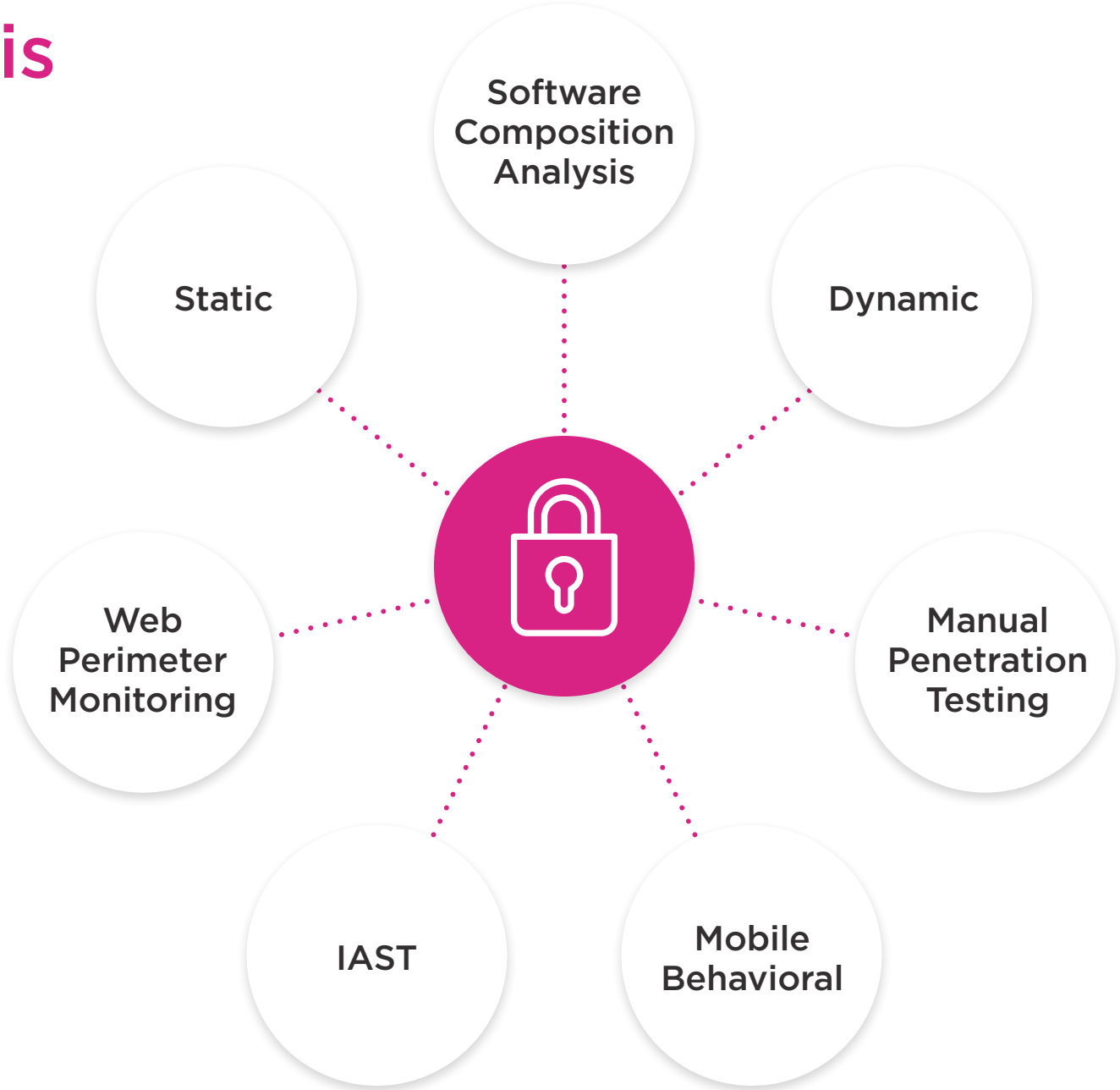
THE REALITY

There is no AppSec panacea. A truly effective program uses the strengths of multiple assessment techniques.

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. And so on.

Each analysis technology has its own strengths.

All play a role in a complete application security program.



CONCLUSION

Hopefully now you've gained a few insights into the best ways to defend your applications. Here's to you checking your own fallacies at the door and developing a robust global security plan that includes every connected app. It's time.

LOVE TO LEARN ABOUT APPLICATION SECURITY?
Get all the latest news, tips and articles delivered right to your inbox.

LEARN MORE

Why You Need an Application Security Program