You Can't Secure What You Don't Know About

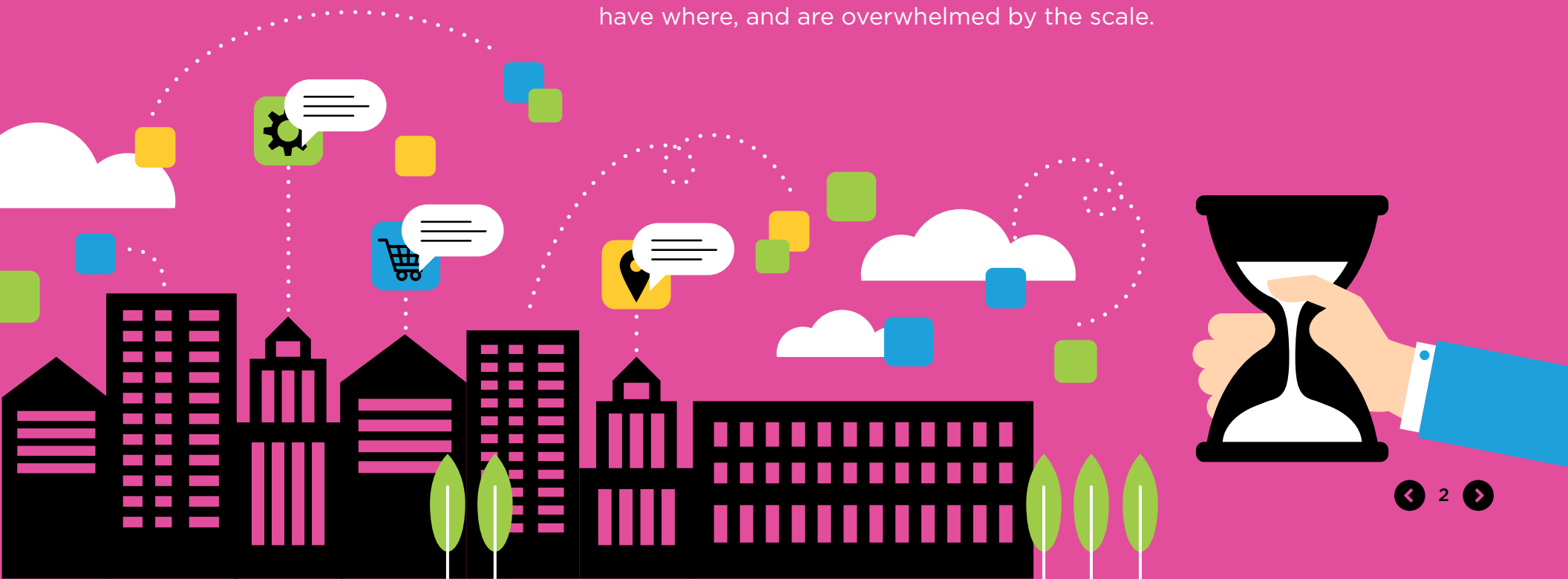
# How to Get a Handle on Your App Landscape

# YOUR APP LANDSCAPE

The advent of digital business has dramatically changed the way organizations operate.

With software playing a critical role in meeting business objectives, software development faces new pressures and expectations. Today, most development organizations don't have the time or the resources to create every application from scratch, and are therefore purchasing more software and integrating more open source code into internally developed software.

But this explosion of software and reliance on third parties have serious security implications. **One of the biggest challenges and barriers to application security is that organizations can't get a handle on their app landscapes.** They don't know what apps they have where, and are overwhelmed by the scale.



To get the visibility application security requires, you need to:

# GET A HANDLE ON YOUR WEB PERIMETER

**Part of the reason for the huge percentage of breaches involving web applications is a lack of visibility into the web perimeter — most enterprises don't even know how many public-facing applications they have.**

Web application perimeters are constantly expanding as enterprises:

1. Spin up new websites for new marketing campaigns or geographies.
2. Create web portals for customers and partners.
3. Acquire companies.

Additionally, organizations also have legacy and old websites they're not even aware of.


**Web application attacks are now the most frequent pattern in confirmed breaches.**

2016 Verizon Data Breach Investigations Report

# How Veracode Can Help

**Veracode Web Application Scanning (WAS) offers a unified solution to find, secure and monitor all of your web applications — not just the ones you know about.**

Veracode first discovers and inventories all of your external web applications, using:

- ✓ Web-application-layer crawling
- ✓ Domain brute forcing
- ✓ Integrated web searches
- ✓ Other unique approaches to identify more applications than network-based scanning

At this point, our customers typically shut down old and unused websites to save costs. Veracode WAS then performs a lightweight scan on thousands of sites in parallel to find critical vulnerabilities and help you prioritize your biggest risks. You can then further run an authenticated deep scan on your most critical applications.

**Veracode WAS typically finds:**

30%–40%

**more websites than customers thought they had.**


**A telecommunications firm shut down 20% of its web applications that were no longer needed,**

**breaking even on the cost of Veracode WAS within the first year.**

To get the visibility application security requires, you need to:

# GET A HANDLE ON THIRD-PARTY APPLICATIONS

**Organizations are increasingly relying on third-party applications, yet also struggling to keep track of them and ensure their security.**

Our *State of Software Security* (SoSS) reports, based on our Platform data, consistently reveal a high level of vulnerabilities in commercial software. In fact, our 2016 SoSS report found that **75% of third-party scanned applications were not compliant with the OWASP Top 10 policy for security vulnerabilities.**


This stat reaffirms the need for organizations to demand better proof of software security from their vendors and to perform due diligence around all applications, including commercial software.

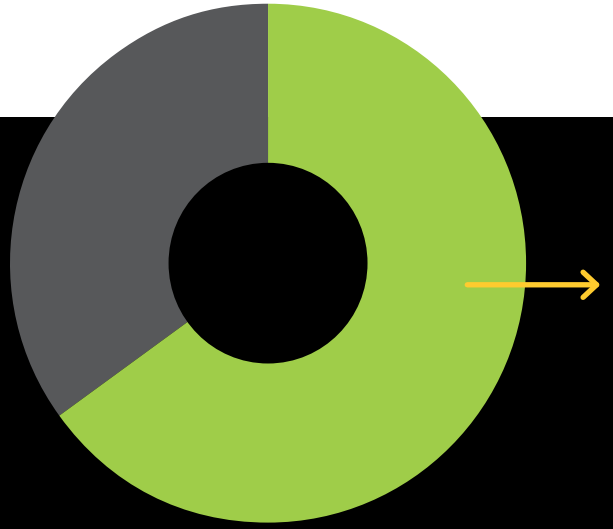
# How Veracode Can Help

**Veracode Vendor Application Security Testing (VAST) provides a scalable program for managing third-party software risk.**

We work with you to formulate a strategy for:

- ✓ Contacting your independent software vendors (ISVs).
- ✓ Defining policies for compliance that can include a mix of automated and manual testing methods.
- ✓ Getting your vendors into compliance.

In addition, because Veracode scans binaries rather than source code, vendors will be more comfortable with the assessments because they don't have to disclose their intellectual property.



## sixty-five percent

**of a typical enterprise application portfolio comes from third parties.**

Quocirca

To get the visibility application security requires, you need to:

# GET A HANDLE ON OPEN SOURCE COMPONENTS

**Chances are, both your internal and external apps were not created from scratch. With the extreme pressure on developers to get working code delivered quickly, it's a common development practice to use pre-built open source software components and code. And we have historically found open-source components to be overwhelmingly insecure.**

In a recent analysis of more than 5,300 enterprise applications uploaded to our platform over a two-month period, we found that components introduce an average of 24 known vulnerabilities into each web application

Despite the risk components introduce, they are still best practice for any company attempting to rapidly produce and deploy new applications or updates. And in fact, discontinuing their use would put an organization at a serious disadvantage. Component use is not the problem; visibility is.

Unless developers carefully keep track of each open source component they use, companies do not have a list of components and versions. This lack of visibility makes it very challenging for security professionals to understand the risk associated with their applications and increases their risk of breach.

**IN A RECENT ANALYSIS**

**5,300+**
**enterprise applications**

↓

**2**
**month period**

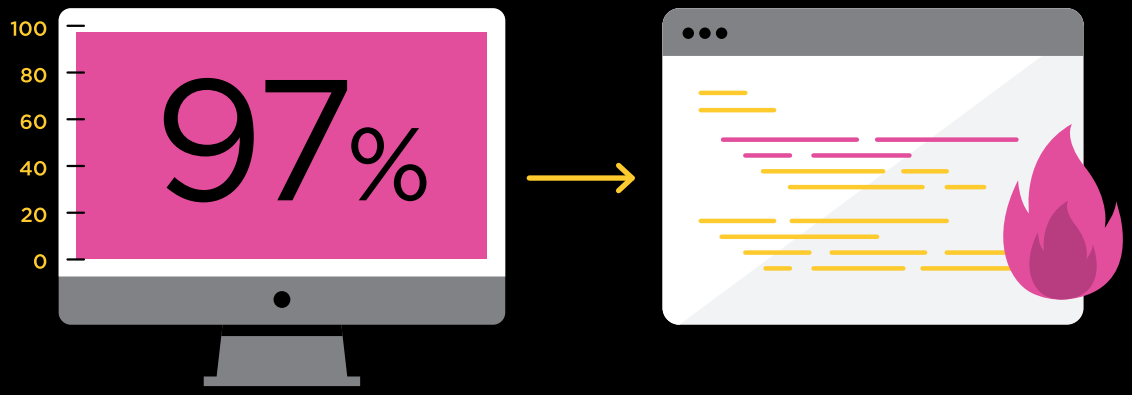
↓

**24**
**known vulnerabilities**

# How Veracode Can Help

**Veracode Software Composition Analysis (SCA) helps you build an inventory of your open source components to identify vulnerabilities.**

The Veracode Application Security Platform analyzes your open source components to find vulnerabilities with the same scan you've already set up for static binary scanning — without having to rescan the applications. When a big component vulnerability hits the news, Veracode helps you quickly identify which applications in your organization are vulnerable.




97%

**of all Java applications assessed had at least one component with a known vulnerability.**

*Veracode State of Software Security, Volume 7*

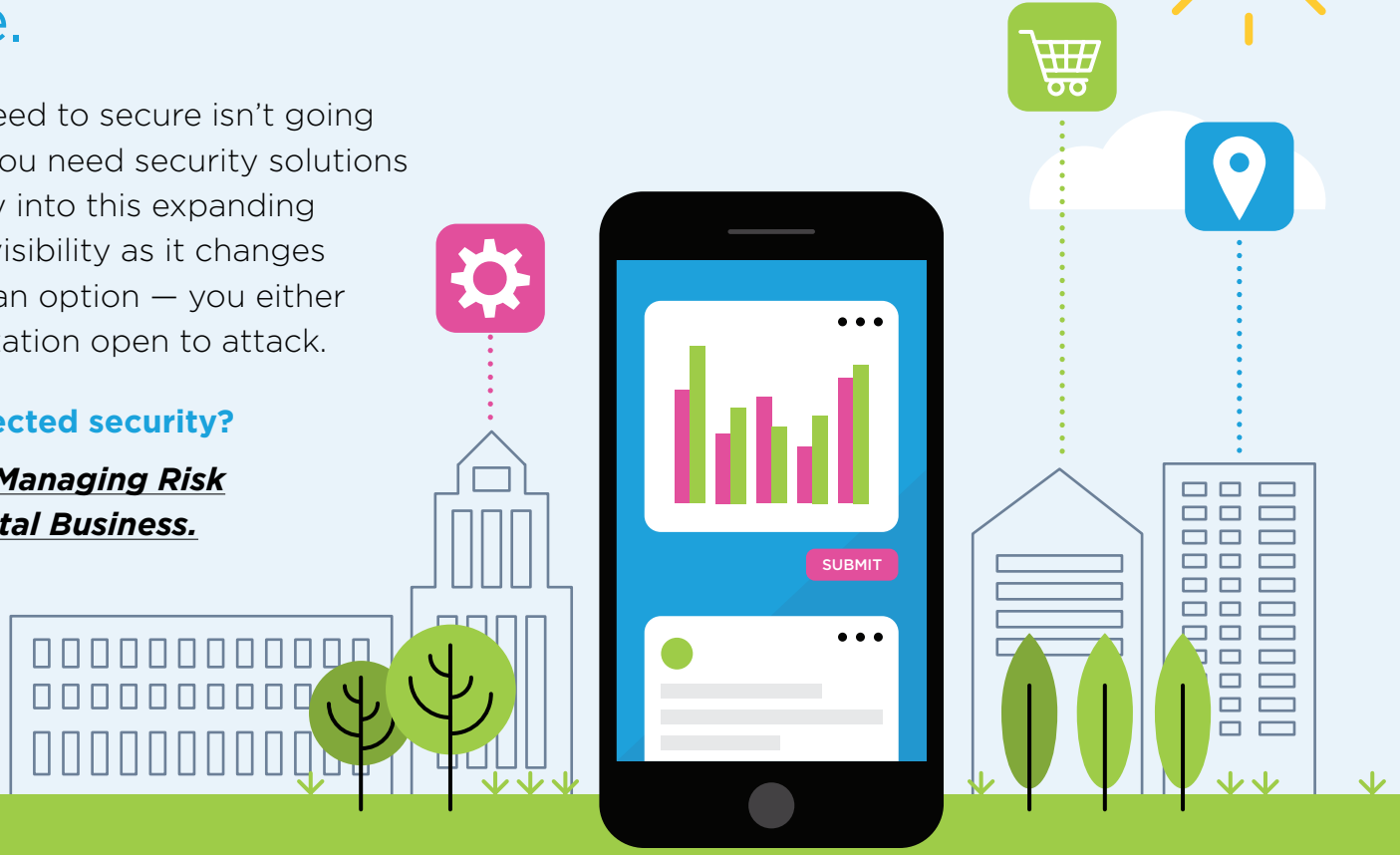
# SECURITY GAME CHANGER

## Digital business changed the security game.

The number of applications you need to secure isn't going to get smaller or less complex — you need security solutions that will allow you to have visibility into this expanding landscape, and that will maintain visibility as it changes and grows. Not keeping up is not an option — you either keep up, or you leave your organization open to attack.

**How else has digital business affected security?**

**Check out Gartner's new report, *Managing Risk and Security at the Speed of Digital Business.***



VERACODE

**SECURING THE SOFTWARE THAT POWERS YOUR WORLD.**

Veracode delivers the application security solutions and services today's software-driven world requires. Veracode's unified platform assesses and improves the security of applications from inception through production so that businesses can confidently innovate with the web and mobile applications they build, buy and assemble as well as the components they integrate into their environments.

With its powerful combination of automation, process and speed, Veracode seamlessly integrates application security into the software lifecycle, effectively eliminating vulnerabilities during the lowest-cost point in the development/deployment chain, and blocking threats while in production. By protecting each and every application throughout its entire lifecycle, Veracode not only prevents cyberthreats, but also responds to them — delivering application security unmatched in coverage and effectiveness.

Veracode serves hundreds of customers across a wide range of industries, including nearly one-third of the Fortune 500, three of the top four U.S. commercial banks and more than 20 of Forbes' 100 Most Valuable Brands.

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