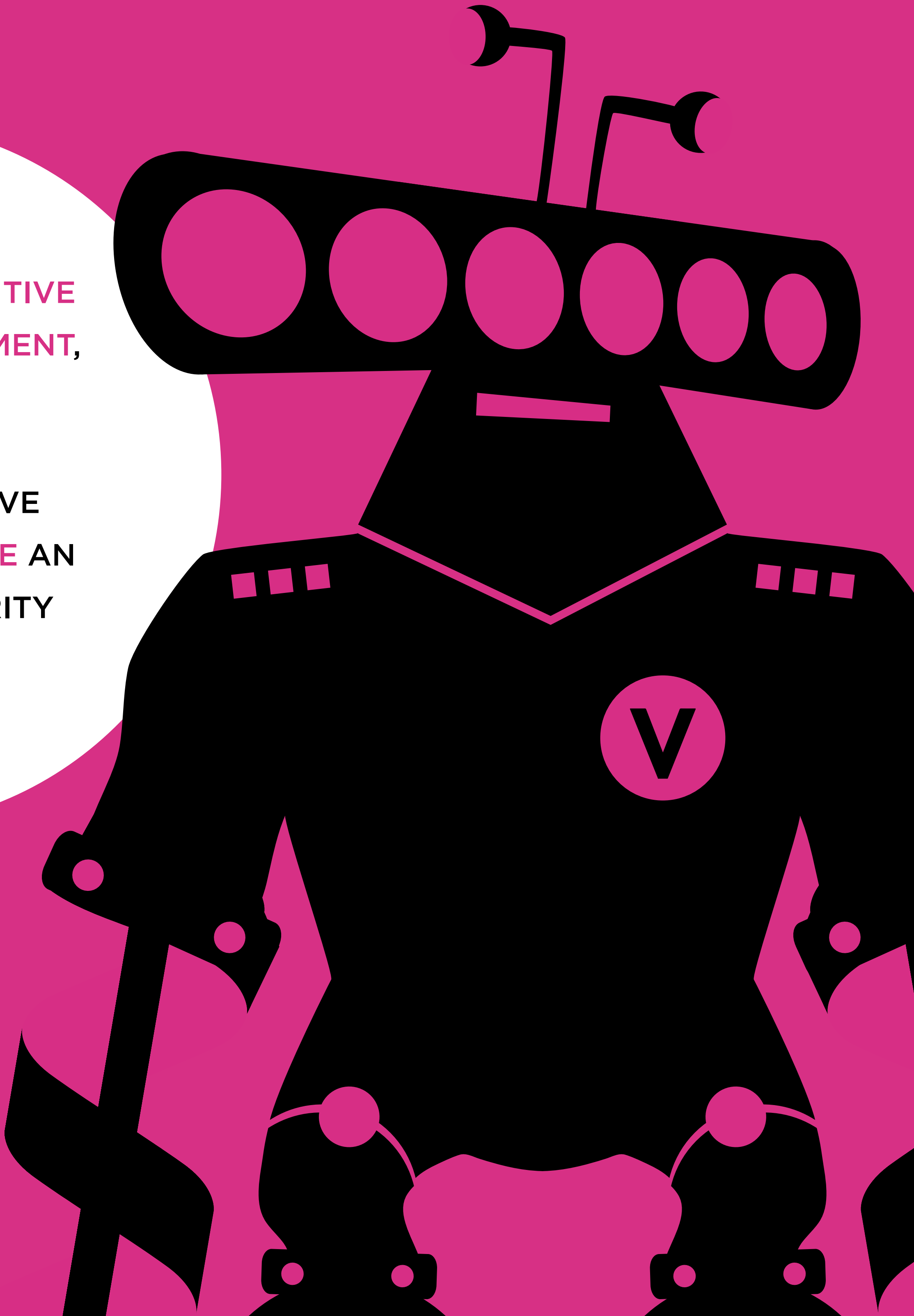
QUICK WINS:

Why You Must Get Defensive About Application Security



IN TODAY'S COMPETITIVE BUSINESS ENVIRONMENT, DEMONSTRATING IMMEDIATE PAYOFFS WILL HELP YOU PROVE JUST HOW VALUABLE AN APPLICATION SECURITY PROGRAM CAN BE.

VERACODE

INTRODUCTION

It's no secret that modern enterprises face enormous cybersecurity risks — hackers and attackers are growing more sophisticated and opportunistic by the day. According to IT consulting firm Gartner, worldwide information security spending reached a record $76.9 billion in 2015. By 2020, the figure is expected to reach an astounding $170 billion.[1]

Unfortunately, conventional tools and technologies that take aim at such issues as network security, endpoint security, malware and digital rights management (DRM) don't sufficiently address the reality of how companies are attacked today, which often happens through the application layer. Today, it's critical for IT staff to think and act in a broader, more comprehensive way when addressing security breaches.

This includes a greater focus on application security and how software code impacts the organization, particularly the vulnerabilities it can introduce through web sites, online applications and their connected systems. **According to the *Verizon 2015 Data Breach Investigations Report*, web app attacks are now more common than highly publicized denial of service (DoS) assaults, cyber espionage and cyber intrusions.**[2]

TWEET THIS

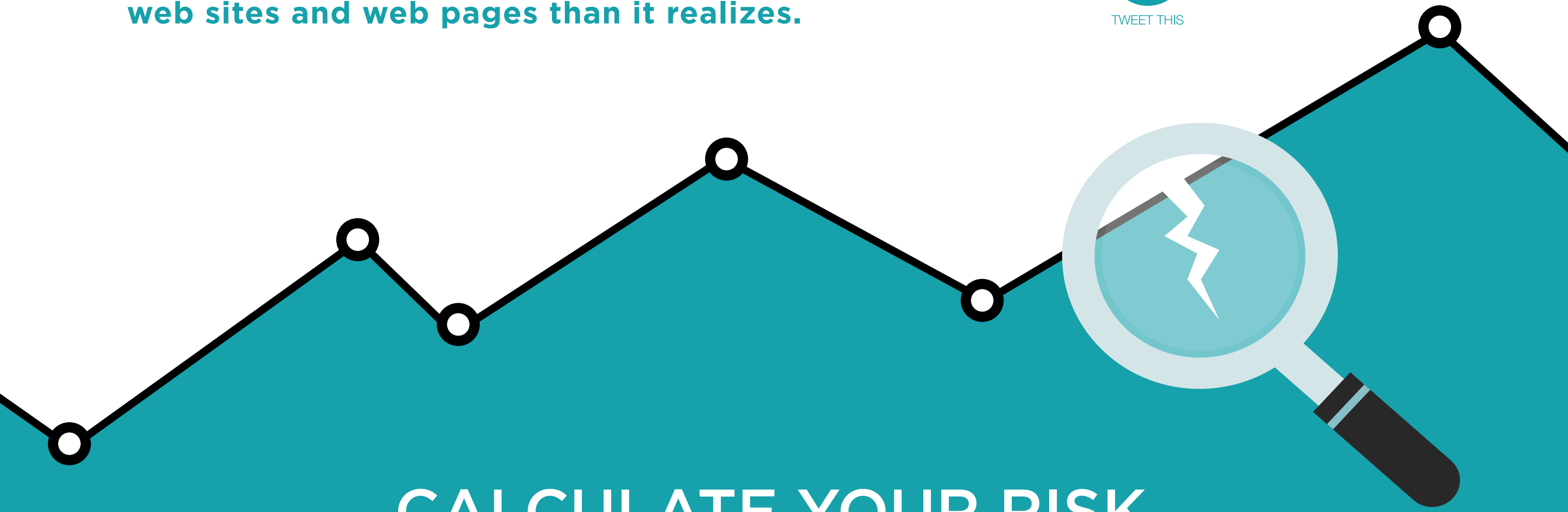
In fact, web application security is a smart first choice for security teams because of the critical vulnerabilities it addresses — issues that can be tackled quickly and effectively to show rapid improvement in your application security initiative. Achieving quick and effective wins can help you gain the upper hand in the cybersecurity war, and build support and funding for a broader and deeper approach to your enterprise's application security program.

WEB APPLICATIONS ARE AMONG THE TOP TARGETS FOR HACKERS AND CYBERTHIEVES, WITH SOME INDUSTRIES EXPERIENCING AS MUCH AS 35 PERCENT OF THEIR BREACHES FROM THE WEB APPLICATION LAYER.[3] INCREDIBLY, ABOUT 80 PERCENT OF APPLICATIONS WRITTEN IN WEB SCRIPTING LANGUAGES ARE VULNERABLE TO AT LEAST ONE THREAT RISK AT AN INITIAL ASSESSMENT.[4] CONSEQUENTLY, AN ORGANIZATION CAN FIND ITSELF FACING A MAJOR BREACH WITH LITTLE OR NO WARNING.

AVOIDING RISKY BUSINESS

A formidable challenge for organizations of all shapes and sizes is coping with the steady addition and growth of web sites and software. Over a period of years and even decades, web sites and software applications swell — often incrementally — to the point where an organization may lose track of old and obsolete web pages, embedded web software and other web assets. In fact, **Veracode has found that a typical organization has about 30 percent more web sites and web pages than it realizes.**

TWEET THIS

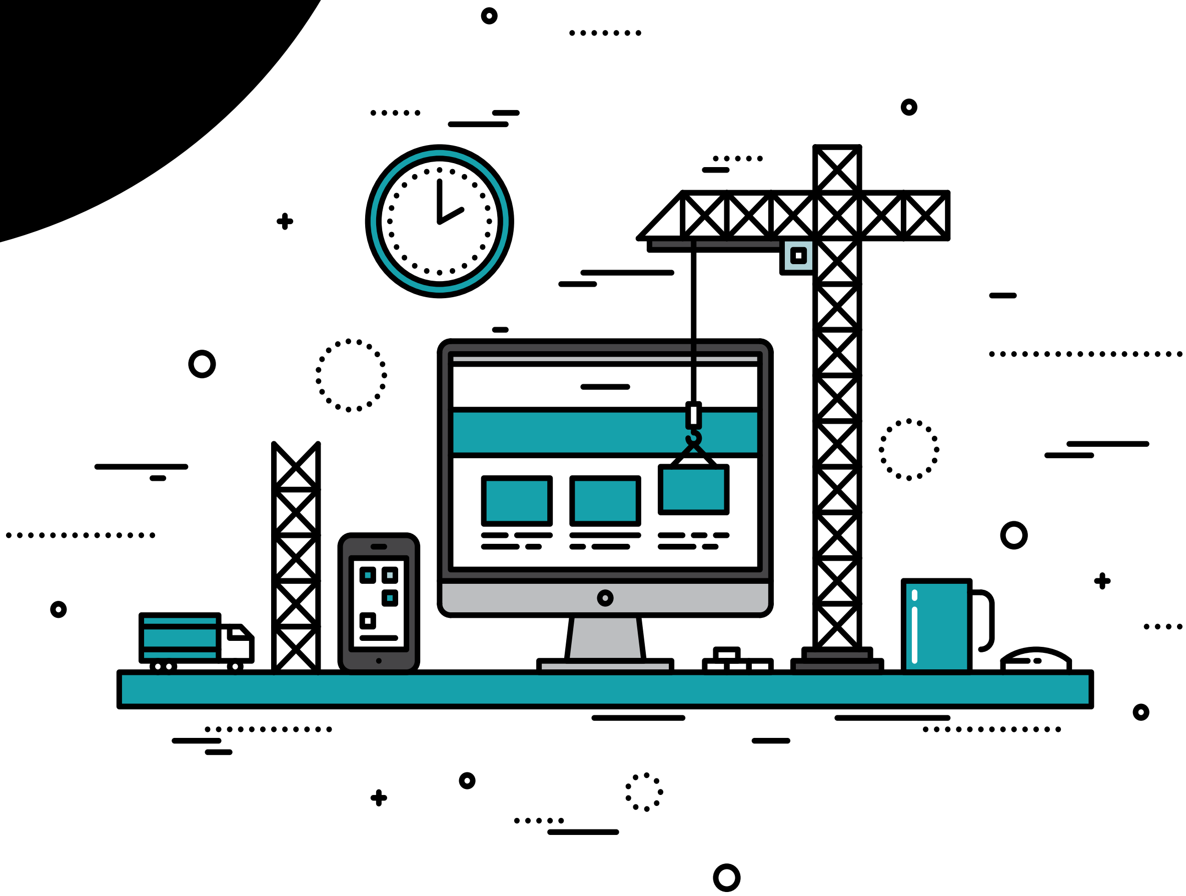


CALCULATE YOUR RISK

A starting point for navigating application security and achieving quick wins is understanding exactly where your organization is at and what risks exist. Veracode, which has assessed thousands of web sites for leading enterprises, offers a free analysis tool that compares how many web sites you think you have in your organization with how many likely exist. After performing a scan, it presents an estimated number of critical vulnerabilities present in your web perimeter, as well as the overall number of vulnerabilities present in your web perimeter. You can download the Veracode APM calculator here.

This enormous and growing web perimeter — built in an attempt to achieve a competitive advantage — may represent sites and pages collected through a merger or acquisition, old and often obsolete products, various branding initiatives or specially branded pages, or international pages that are no longer necessary or relevant. Consequently, these unneeded and potentially risky pages may spiral out of control, and an organization may find itself staring down the barrel of a major breach with little or no warning.

ACHIEVING QUICK AND EFFECTIVE WINS CAN HELP YOU GAIN THE UPPER HAND IN THE CYBERSECURITY WAR, AND BUILD SUPPORT AND FUNDING FOR A BROADER AND DEEPER APPROACH TO YOUR ENTERPRISE'S APPLICATION SECURITY PROGRAM.



BRINGING ORDER TO THE CHAOS

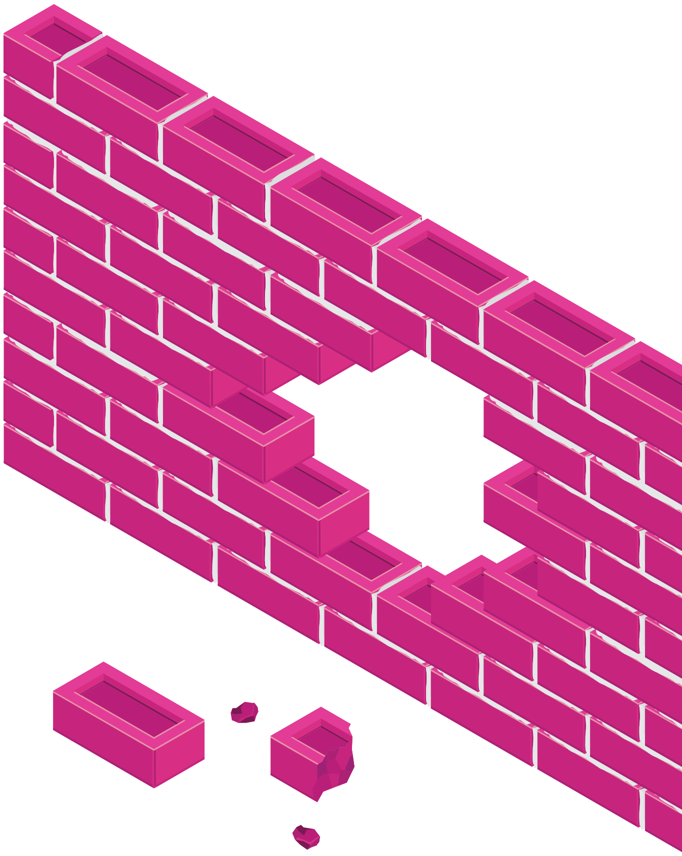
While it's relatively easy to understand how a firewall works or produce metrics and numbers for malware detection software, getting a handle on application security can be a bit more challenging. In many cases, there's no way to know that a fundamental problem exists — until a breach occurs. But, make no mistake, organizations often pay dearly. **Ponemon Institute reports that the cost of a data breach to a typical large organization in the U.S. was about $15.4 million in 2015.**[5]

TWEET THIS

Avoiding a culture of inertia, indifference or ignorance is paramount. A successful application security initiative focuses on achieving tangible results with quick wins. A best-practice approach that leads to quick wins involves three steps:

1. Monitor your web application perimeter.

It's critical to gain visibility into your company's web perimeter and the vulnerabilities it presents by identifying all the sites and pages that may contain public-facing applications — as well as those used by business partners and others in a supply chain. Unfortunately, you may not even know about many of these pages because they're located on inactive, obsolete or dead sites. What's more, as your enterprise activates new sites and pages based on new marketing, sales, operational, financial or

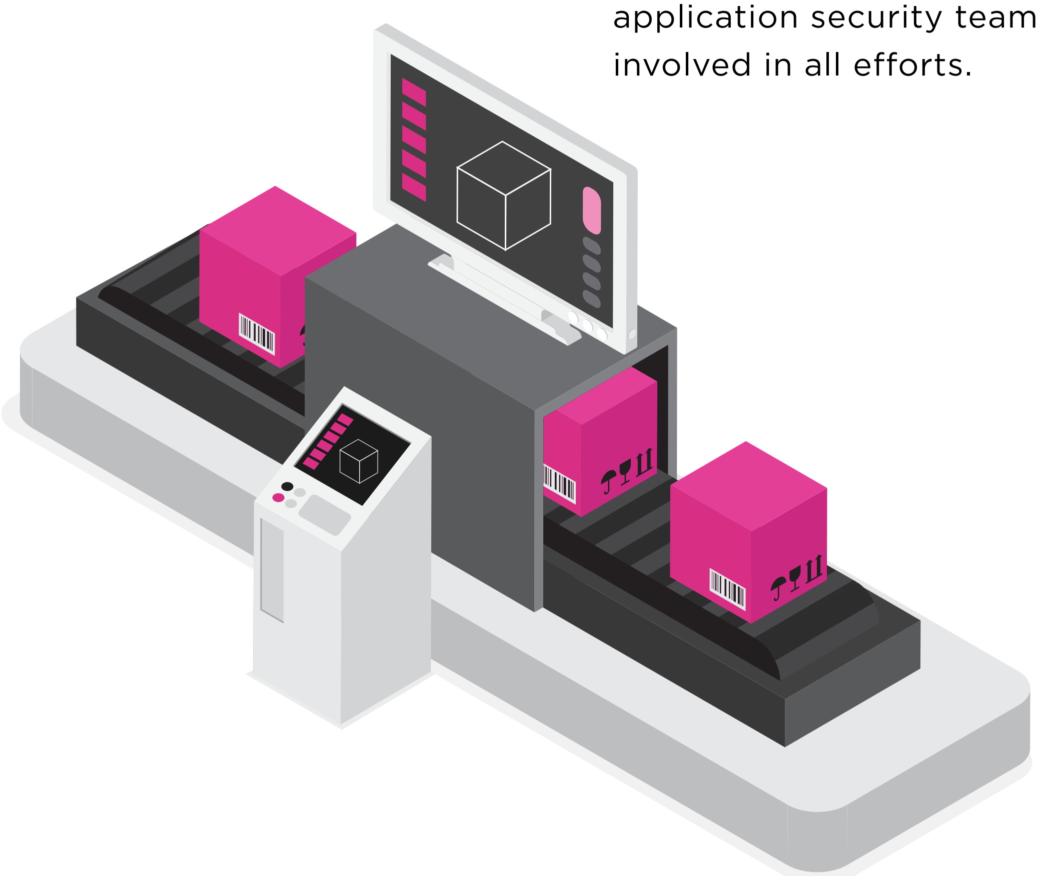


other needs, what seems like a fairly straightforward task can become exponentially more complex — and risky — as the attack surface grows.

Many organizations rely on expensive and largely ineffective manual methods. Web Application Perimeter Monitoring introduces an effective way to manage the discovery process, identifying not just standard web sites and applications, but also mail and messaging apps, as well as mobile sites that introduce vulnerabilities. An effective solution performs production-safe application-layer crawling to build an accurate inventory and highlight exploitable vulnerabilities. In addition, it relies on massively parallel, auto-scaling cloud infrastructure to scan thousands of applications simultaneously and, using multiple discovery techniques and application intelligence, produce highly actionable information and reports.

Here are three actions you can take to successfully complete this step:

- ✓ **Conduct** a web application perimeter scan to assess your situation and gauge existing risks.
- ✓ **Ensure** that various groups and departments within the enterprise have access to the results of the scan and any relevant status reports.
- ✓ **Foster** collaboration and cooperation among key groups and ensure that the web application security team is involved in all efforts.

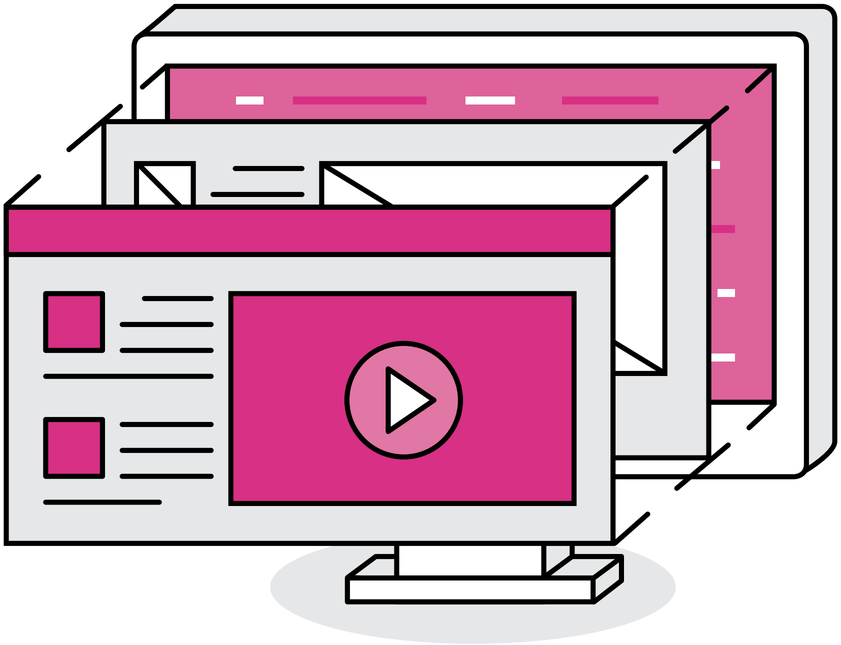


2. Analyze the inventory of your organization's web applications.

A robust application security solution will not only scan sites and pages, it delivers detailed information about exploitable vulnerabilities. This makes it possible for you to prioritize the risks and determine what actions you can take to fix the problems that could result in an intrusion and data breach. This could include removing unnecessary pages and sites or updating protection rules without the need to involve developers — at least in the short-run. For example, Vercacode's DynamicMP identifies SQL injections, cross-scripting and other top vulnerabilities, including Insecure Direct Object References, Cross Site Request Forgery (CSRF) and Sensitive Data Exposure. It also delivers a centralized dashboard that developers, security personnel and others can use to make decisions based on the use of central policy management and other factors and criteria. In addition, it's important to rely on an application security solution that continuously adapts to new and changing attack vectors and methods, and conduct a thorough automated analysis on a regular timetable.

Here are two actions you can take to successfully complete this step:

- ✓ **Quantify and weigh** the risks you've discovered in order to gain mindshare and financial support for a web application security initiative.
- ✓ **Demonstrate** results in high value areas to sell executives and others on the initiative.



3. Implement an action plan for addressing existing vulnerabilities and hardening your protection.

Once your enterprise has produced a comprehensive list of vulnerabilities and risks, it's possible to take action in a strategic and cost-effective way. A security team or other group can view a report and determine which sites require immediate action, what types of temporary fixes are critical until a long-term solution is possible (such as bringing a site or pages behind a firewall), and when it's necessary to bring developers or others into the picture. Organizations that rely on manual methods often find they're mired in spreadsheets, PDF files and other ad hoc data that leads to chaos. By bringing scanning, analysis and security policy management into a unified platform, an enterprise can fix problems quickly, rescan an app or page to verify results and quickly move forward.

TO PROTECT YOUR WEB PERIMETER, IT'S IMPORTANT TO RELY ON AN APPLICATION SECURITY SOLUTION THAT CONTINUOUSLY ADAPTS TO NEW AND CHANGING ATTACK VECTORS AND METHODS, AND TO CONDUCT A THOROUGH, AUTOMATED ANALYSIS ON A REGULAR TIMETABLE.

Here are three actions you can take to successfully complete this step:

- ✓ **Address** the biggest threats first and publicize your results to gain further buy-in.
- ✓ **Place** lower risk sites and pages behind a firewall or take other actions that reduce immediate risk, but leave major resources for tackling the biggest vulnerabilities.
- ✓ **Address** other operational and functional changes through different protection rules that can easily be applied throughout the organization. Bring in development teams only when necessary.

30,000 DOMAINS IN 8 DAYS

Putting a solution to work in the real world is the ultimate test of success. For one Global 100 manufacturer, the path to progress has been nothing less than stellar. After migrating to Veracode's cloud-based application perimeter monitoring (APM) platform, it was able to prioritize, assess and ultimately address the risk for 30,000 domains and IP addresses in just eight days, and sort through upwards of 3,000 web applications over the course of three months. The end result? A 79 percent reduction in critical and high vulnerabilities within eight months. Moreover, this manufacturer now has the ability to easily and continuously monitor and address web application issues as they unfold.

This is a huge improvement over the way the business operated in the past. Not only did it lack the ability to identify what risks existed at its external and internal sites around the world, it couldn't even determine how many sites it owned and operated, including those functioning through external cloud-hosted sites and services. Today, nine business units are unified on the Veracode platform, and the company has a comprehensive security program, as well as standardized polices and KPIs in place. What's more, the manufacturer continues to move forward. While it now continuously scans 4,000 sites each month, it is also working with Veracode to tame third-party software — including commercial and outsourced applications, third-party libraries and open-source components — using Veracode's Vendor Application Security Testing (VAST) program.

PUTTING THE PLAN TOGETHER

While there's no simple or easy way to address web application security and the growing risks to organizations in all sectors and industries, an effective application security strategy is vital. Within this security framework, it's necessary to use web application security tools and solutions that identify risks, prioritize threats and deliver a framework for managing enterprise software and web environments.

The ability to reduce necessary exposure goes a long way toward building a more robust and effective cybersecurity framework. According to analysis done by Veracode, organizations that use APM typically open the aperture from detecting 10 percent or less of threats residing on web sites and pages to detecting nearly 100 percent — and moving forward with a clear and cogent plan that addresses the web application perimeter monitoring lifecycle.

WANT TO LEARN MORE ABOUT APPLICATION SECURITY?

Get all the latest news, tips and articles delivered right to your inbox by subscribing to our blog.

info.veracode.com/blog-subscribe.html

[1] "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware," Gartner, August 22, 2014.

[2] *Verizon 2015 Data Breach Investigations Report*, Verizon, April 2015

[3] Ibid.

[4] "Four Out of Five Applications Written in Web Scripting Languages Fail OWASP Top 10 Upon First Assessment," Veracode, December 3, 2015.

[5] *2015 Cost of Cyber Crime Study: Global*, Ponemon Institute, October 2015.

ABOUT VERACODE

Veracode is a leader in securing web, mobile and third-party applications for the world's largest global enterprises. By enabling organizations to rapidly identify and remediate application-layer threats before cyberattackers can exploit them, Veracode helps enterprises speed their innovations to market — without compromising security.

Veracode's powerful cloud-based platform, deep security expertise and systematic, policy-based approach provide enterprises with a simpler and more scalable way to reduce application-layer risk across their global software infrastructures.

Veracode serves hundreds of customers across a wide range of industries, including nearly one-third of the Fortune 100, 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**.