5 BEST PRACTICES FOR APPLICATION SECURITY

A HOW-TO GUIDE

Cybersecurity INSIDERS

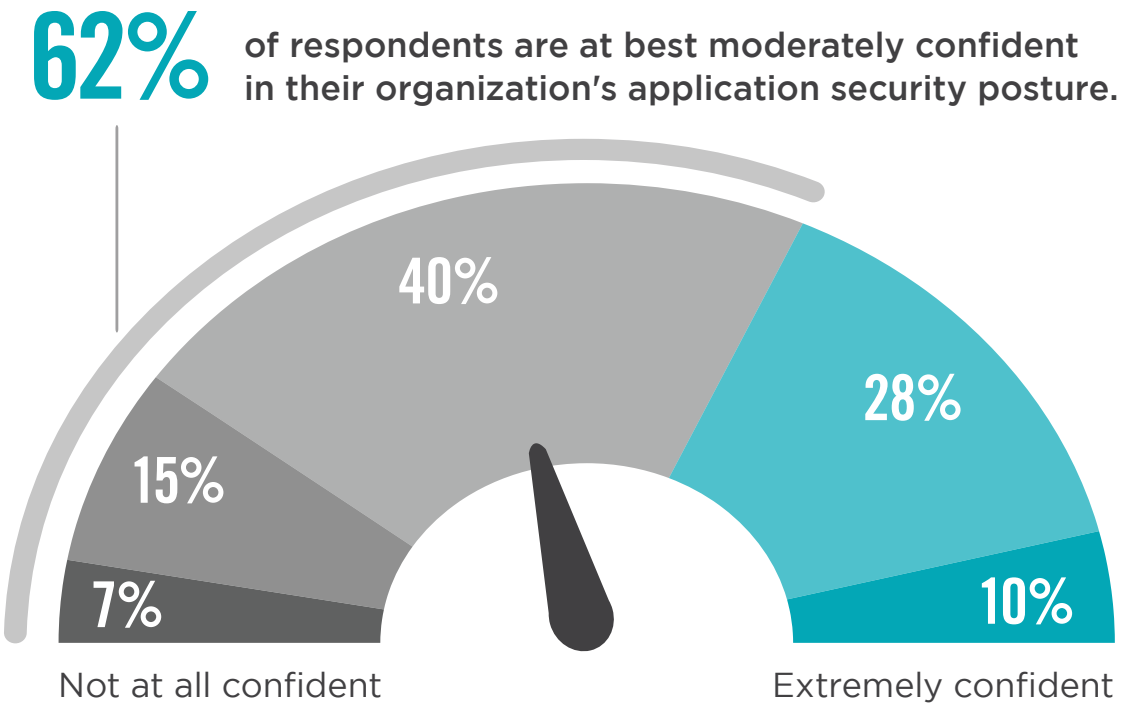
tenable®

INTRODUCTION

Applications play a critical role in supporting key business processes, but organizations are struggling to keep them safe.

The 2018 Cybersecurity Insiders Application Security Report reveals that 62% of cybersecurity professionals are at best moderately confident in their organization's application security posture. Not surprisingly, about the same number consider their application security strategies immature.
.

How confident are you in your organization's AppSec position?

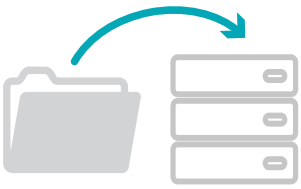


Customer-facing web applications present the highest security risk to businesses, according to 41% of those surveyed. Nearly every single web application today has at least one vulnerability, according to a recent TechRepublic article[1]. Most alarming to security leaders is the time needed to remediate critical application vulnerabilities is often measured in months, not in days or even weeks.

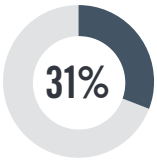
1 TechRepublic, "Report: 99.7% of web apps have at least one vulnerability," June 20, 2017

Which types of apps present the highest security risk?

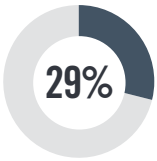
41%
Customer-facing web applications



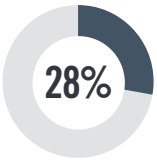
41%
Legacy applications



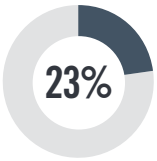
Mobile applications



Desktop (client applications)



Business Applications (ERP, SCM, MES, HR SRM, etc.)

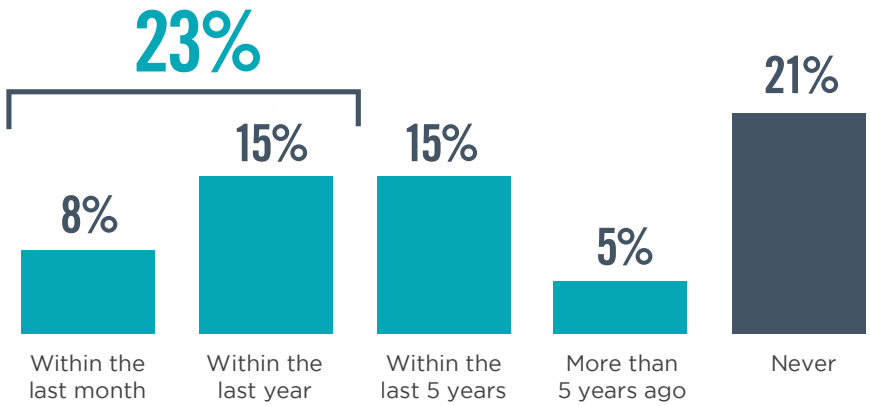


Internal-facing web application

Application security must be a high priority for all organizations to ensure their company's brand and top executives stay out of newspaper headlines. The Application Security Report also shows that 23% of organizations have experienced application breaches or compromises in the past 12 months, with 8% having been attacked just within the previous month. More troubling, more than one-third of respondents couldn't even report whether or not they had sustained a breach or compromise over the past five years.

Clearly, organizations have to make improvements in how they protect business applications, especially as more applications are being designed and hosted on the web for external access. This guide presents five key areas where you should focus to better protect applications against the latest cybersecurity threats.

When was the last time that one of your company's applications was breached/compromised?



Don't know/unsure 36%

CHALLENGE #1: **VISIBILITY**

Due to the emergence of "shadow IT," in which departments, groups, and individual users deploy business applications without the authority or knowledge of central IT management, many security teams have little visibility into what applications are used throughout the organization.

For example, 89% of survey respondents say their organizations are not confident that they know all the applications in use. Only 11% say they are confident about knowing all the applications.

Furthermore, 17% of the organizations cannot even provide an estimated range of how many applications they have in their environment.

Poor web application visibility is a significant problem among security teams today. One recent Symantec study[2] quantified the gap between perceived and actual cloud applications in use to be more than a factor of 20.

BEST PRACTICE #1:
Automate Discovery of Web Applications

Automatic discovery of applications deployed in your organization removes costly manual guesswork and dangerous security blind spots. Fueled by new DevOps practices, web applications are being created and deployed by more teams faster than ever, and it's very difficult to keep up with manual lists of IP addresses and domain names. Take advantage of solutions that can identify web applications through IP ranges, domain names and HTTP port scans.

2 Cloud Threat Labs & Symantec, "2H 2016 Shadow Data Report," May 2017

CHALLENGE #2: **RESOURCES**

It's a common complaint of cybersecurity executives: a lack of resources to defend against the latest attacks. Indeed, the Application Security Report confirms that a lack of skilled personnel (37%) and a lack of budgets (35%) are among the top barriers inhibiting defense against cyber threats.

Skills and budgets are also the top two challenges inhibiting application penetration testing at organizations. To underscore the scarcity of resources, application security teams are often outnumbered by developers by a factor of 100 to 1.

Because of skills, resource, and budget limitations, most organizations are only able to assess and secure their most critical web applications—less than 10% of their total web application estate—via manual penetration testing. This means that the other 90% of mainstream applications are underprotected and need to be assessed for risks.

BEST PRACTICE #2:
Automate Web App Scanning

Given that demand for security skills continues to exceed the supply, automation is critical for reducing costs of both technology and personnel. Organizations need web application scanning solutions that can quickly, accurately, and automatically assess all web applications. Investigate solutions that enable you to "set it and forget it" by scheduling frequent and repeatable web application scans to secure your constantly changing environment.

CHALLENGE #3: **COMPLEXITY**

Organizations are dealing with a growing amount of complexity in their IT environments, including the number and variety of business applications in use. There's also complexity in terms of security tools and services.

Not surprisingly, more than half (54%) of the survey respondents say ease of integration is the most important criteria when selecting an application security solution.

Disconnected point solutions designed for specific asset types create siloed visibility and excessive management overhead. Therefore, web application scanning needs to be part of a broader, integrated Cyber Exposure platform to help security teams manage and measure cyber risk across the entire attack surface.

BEST PRACTICE #3:
Make Application Security Part of Your Overall Cyber Exposure Practice

Deploy easy-to-use and intuitive web application scanning products that are integrated into a broader Cyber Exposure platform. This reduces the need for highly specialized application security personnel to configure, deploy, and manage these systems. And it also enables you to assess applications for cyber risk and prioritize vulnerability remediation alongside other assets across your attack surface. Gain broader security coverage while saving time and money and redeploy personnel to other higher-value endeavors.

CHALLENGE #4: **PRIORITIZATION**

With so many threat vectors and vulnerabilities emerging, it's difficult to know what to focus on. Organizations, on average, need to address upward of 800 vulnerabilities per day across nearly 1,000 assets[3]. About two-thirds of these vulnerabilities have a CVSS score of 7.0 or higher, which means security teams are continuously responding to an unrelenting barrage of new cyber risks.[4]

Nearly half of survey respondents (45%) confirm that keeping up with the rising number of vulnerabilities is their biggest application security concern.

The problem is that security teams lack the data and insight they need to prioritize remediation, which means they are unable to address the most critical security issues quickly. As a result, the time it takes to remediate only the high and critical risk vulnerabilities is often measured in months. This exposes the organization to excessive and unnecessary cyber risk.

BEST PRACTICE #4:
Prioritize Based on Risk

Advanced prioritization based on actual cyber risk, combining asset criticality, vulnerability severity and exploit availability, is essential to securing your applications. Filter out lower-risk vulnerabilities, so that you can work on remediating the most business-critical security issues, and focus on vulnerabilities that are being actively exploited by threat actors rather than those that could only theoretically be used.

3 Tenable Research, November 2018
4 Ibid

CHALLENGE #5: **SPEED**

Many organizations are simply too slow in responding to security incidents or are not nearly proactive enough in stopping attacks. Almost half of all organizations surveyed (48%) scan applications quarterly or even less frequently. This lack of speed will not adequately secure applications in today's age of rapid software development.

The rise of DevOps means new web applications are released and existing web applications are updated much more quickly than in the past. Highly mature DevOps organizations, for example, are releasing code multiple times per day, and many organizations (59%) update existing web applications at least monthly[5]. Security has not yet adapted to the new DevOps reality.

BEST PRACTICE #5:
Integrate Security into Your Software Development Lifecycle

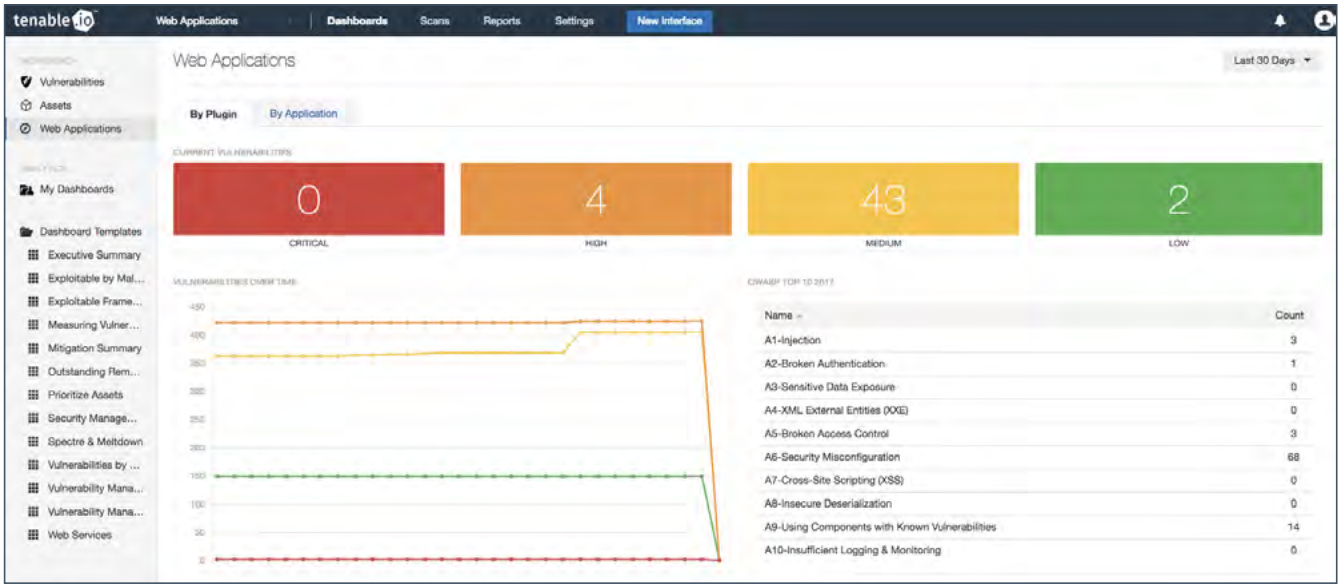
Support high-velocity DevOps processes by integrating web application scans in the DevOps pipeline before application release. The earlier you address security defects in the software development lifecycle, the less costly it is to remediate them. Additionally, scan web applications in production at least monthly to ensure continuous visibility of cyber risk.

5 Forrester Research, "The Rise of Web Technology," May 2015

GET STARTED NOW

Web application attacks are the top source of data breaches today. Tenable can help you secure your web applications as part of a comprehensive Cyber Exposure program.

Tenable.io Web Application Scanning enables automated, safe, and accurate scans of web applications, providing deep visibility into vulnerabilities and valuable context to prioritize remediation. Now you can keep pace with developers and secure your entire web application estate, while ensuring your developers are addressing the most critical cyber risks.



Rely on the world's most widely used web application vulnerability assessment solution to deliver your web application scanning needs.

START YOUR FREE 60-DAY TENABLE.IO WEB APPLICATION SCANNING EVALUATION NOW

For more information, visit: www.tenable.com/products/tenable-io/web-application-scanning.