The State Of Application Security, 2018

Application Security Is Worsening, But Automation Offers Hope

by Amy DeMartine

January 23, 2018

Why Read This Report

In 2017, applications rolled out the welcome mat to malicious hackers, topping the list of successful external attack targets. Why? Developers continue transitioning from perfect to fast to provide unique customer experiences, and there aren't enough security pros to maintain manual application security review processes. Before slowing down development and causing customers to revolt, security and risk pros should read this report to understand the current state of application security and how emerging techniques support the speed your business needs.

Key Takeaways

Security Pros Struggle To Adapt To Speedy Releases

Open source vulnerabilities continue to plague enterprises as developers rely more on these building blocks to help speed development and delivery. Security pros have no choice but to embrace application security automation and protection technologies.

App Security Challenges Vary Greatly By Industry

Retail and wholesale companies are bracing for malicious bots, while utilities and telecoms are trying to shore up open source security and prevention technologies. Meanwhile, financial services firms are facing regulatory pressure and falling back on penetration testing services for compliance.

To Increase Prerelease Testing, Make Integrations Easy

Today's method of integration by plug-in or do-it-yourself creation is fraught with potential for inconsistent application of policies and additional work to create, maintain, and version-control. In the future, integrations will become interactive between developer tools and security tools, and policies will be set inside the security tools themselves to remove the current integration workload on security pros.

The State Of Application Security, 2018

Application Security Is Worsening, But Automation Offers Hope

by Amy DeMartine
with Christopher McClean, Trevor Lyness, and Peggy Dostie

January 23, 2018

Table Of Contents

Related Research Documents

The State Of Application Security: 2016 And Beyond

Vendor Landscape: Application Security Testing

Vendor Landscape: Software Composition Analysis

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

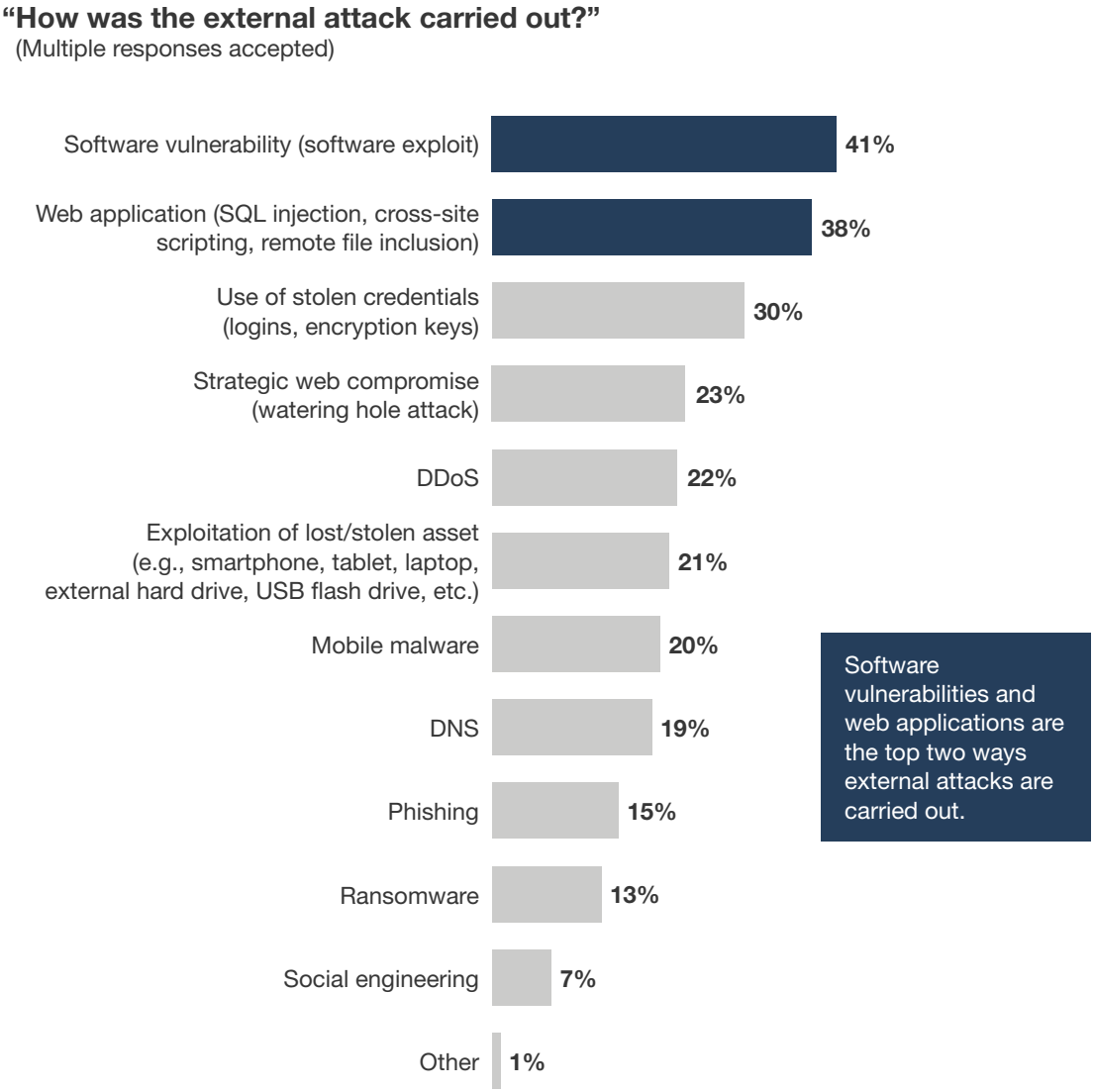
Apps Are Growing As A Revenue Source And As An Attack Plane

As companies try to provide unique customer experiences using emerging technologies like internet-of-things (IoT) devices and virtual assistants, along with now traditional mobile and web applications, these emerging technologies are changing the way we conduct our business and personal lives.[1] Forrester forecasts that US online retail sales will comprise approximately 14% of total US sales in 2018; however, digital touchpoints will in some way impact more than half of total US retail sales.[2] And the backbone of all of this interaction is software.

The downside of applications becoming so much more important in commerce is that they are vulnerable, creating liabilities in addition to creating value. When asked how external attackers carried out successful attacks, security pros whose companies had been breached in the previous 12 months said the top two attack targets were vulnerable software and web applications (see Figure 1). Security pros must focus on securing applications because:

- **Applications should be welcome mats for customers, not attackers.** Web applications continue to show vulnerability to attacks such as SQL injection and cross-site scripting, with little relief in sight. The challenge is that development teams are buried under mountains of requirements to make apps more user friendly and engaging within a shrinking period of time, which leaves essentially no room to strengthen and assure application security.
- **Company size does not protect you or your customers.** Forty-one percent of network security decision makers whose enterprise firms have had an external security breach in the past 12 months told us they've suffered from software vulnerability attacks, and 40% of respondents at small and medium-size companies reported the same. For web applications attacks, the numbers were 42% for small and 30% for medium-size companies. While the reported figures suggest that small and medium-size companies may experience these types of attacks less frequently, successful attacks can cause more than just a disruption in business; they can be the reason a company fails.[3]

FIGURE 1 Software And Apps Were Top Targets In Successful Breaches



Base: 404 network security decision makers whose firms have had an external security breach in the past 12 months
Source: Forrester Data Global Business Technographics® Security Survey, 2017

Current Trends Show Greater App Security Challenges Ahead

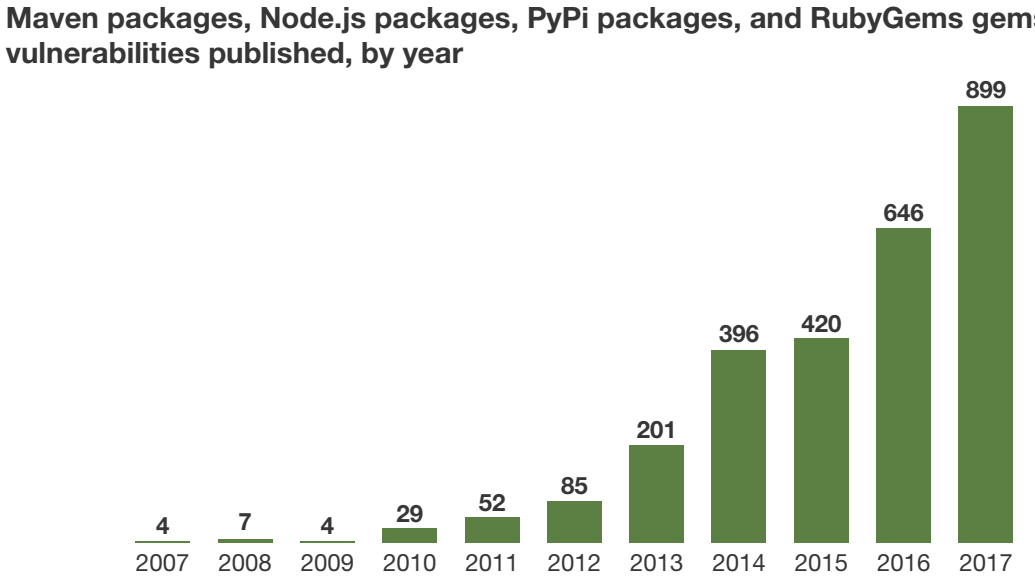
Due to a surge in software's value, growing threats, and a resurgence of the application security market, trends point to things getting worse before they get better. This renewed sense of risk comes as security pros also wrestle with understanding whether their application security risk posture is getting better or worse.

Open Source Is Continuing To Plague Companies That Don't Actively Manage It

Equifax's 2017 breach was notable not only because of the 143 million US consumers affected and the sensitive nature of data stolen, but also because it showed how detrimental open source software can be.[4] Developers are moving from perfect to fast to enable digital transformation, using open source components as vital assets for quickly adding common functionality.[5] To help developers move as quickly as customers demand, security pros must address two fundamental challenges:

- **The time between disclosure and exploit is shrinking.** Today, there is enough information in the common vulnerability and exposures (CVE) description of a vulnerability, including affected software versions and how to execute an attack, for a malicious hacker to immediately create an exploit. Attackers are making use of this information and decreasing the time between disclosure and exploit, as evidenced by Equifax, which had mere days between CVE disclosure and breach.[6]
- **Increasing open source vulnerabilities spur companies to act.** Newly identified open source component vulnerabilities listed in the National Vulnerability Database (NVD) increased by 10% from 2015 to 2016, and 2017 looks to have followed a similar increase.[7] For example, in components from Maven packages, Node.js packages, PyPi packages, and RubyGems gems, published vulnerabilities have more than doubled in the past two years (see Figure 2). Security pros should assume that open source developers are not executing prelease vulnerability scans, so software composition analysis (SCA) and frequent updates to open source components will be the responsibility of the enterprise.[8]

FIGURE 2 Disclosed Maven, Node.js, PyPi, And RubyGems Vulnerabilities Have Increased Drasticallyy



Source: "The State of Open Source Security," Snyk, 2017

Vendor Consolidation Is Not Showing Value For Security Pros

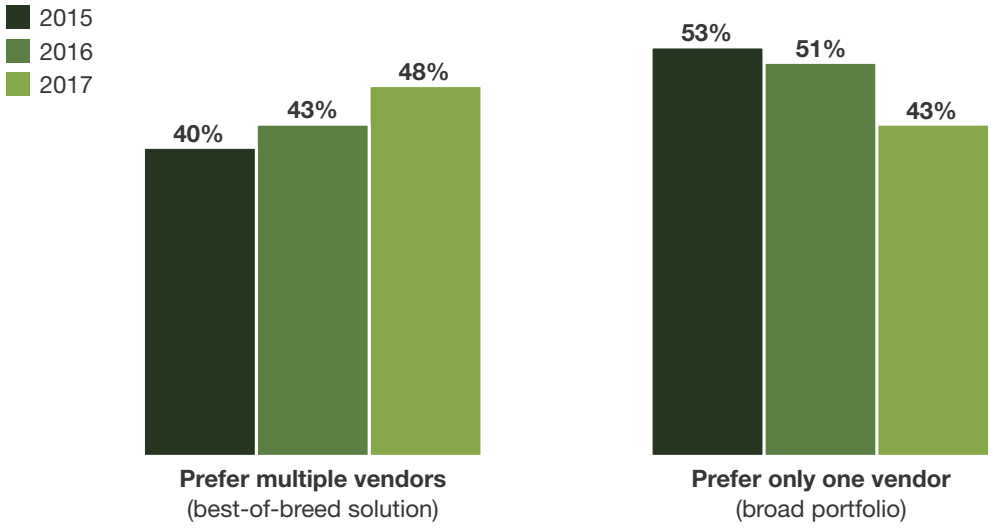
Tech vendors have been expanding their application security portfolios through build-and-buy strategies for years. The industry saw curious mergers and acquisitions in 2017, such as CA Technologies acquiring Veracode, Hewlett Packard Enterprise (HPE) spinning off its software portfolio (including its application security assets) to Micro Focus, and Synopsys (which already had two SCA products) acquiring Black Duck Software.[9] These vendor moves aim to offer security pros comprehensive solutions from a single vendor; however:

- **Portfolio vendors have long promised consolidation benefits with mixed results.** In addition to easing contract negotiations, portfolio vendors should provide differentiated product value, through either integration or consolidated reporting. For example, application security testing tools such as SAST, DAST, MAST, IAST, and SCA could contribute to a single application security score to show CISOs whether applications and portfolios of applications are improving their security posture.[10] Unfortunately, portfolio vendors struggle to create cohesive reporting and scoring for a single product, let alone across their entire portfolios, and correlation remains a road map item for many of them.[11]
- **Security pros increasingly prefer best-of-breed tools.** In 2015, 53% of security decision makers said they prefer to purchase their application security testing tools from a single vendor, while 40% said they prefer multiple best-of-breed solutions. In 2017, this trend reversed, with only 43%

preferring a single vendor and 48% opting for best-of-breed (see Figure 3). Until portfolio vendors show true value from product integration and focused development or acquisition to remove any portfolio weak links, security pros will continue to value best-of-breed functionality, even if it means developing their own integration or using correlation tools such as ThreadFix.

FIGURE 3 Security Pros Favor Best-Of-Breed Application Security Tools

"How does your firm prefer to source application security technologies or managed/SaaS security services?"



Base: 2,121 to 2,168 security technology decision makers
Source: Forrester Data Global Business Technographics® Security Survey, 2015 To 2017

App Sec Adoption Varies, Pushing Earlier Testing And Better Protection

CISOs have come to realize that there are just not enough bodies to throw at security to make the improvements they need. In most cases, the only way to secure applications is using tools that will automate previously manual workflows, helping achieve both faster scanning and stronger protection levels that were unattainable before.[12] Today, adoption of prerelease and production security tools varies from 25% to 64%, depending on the tool and industry (see Figure 4):

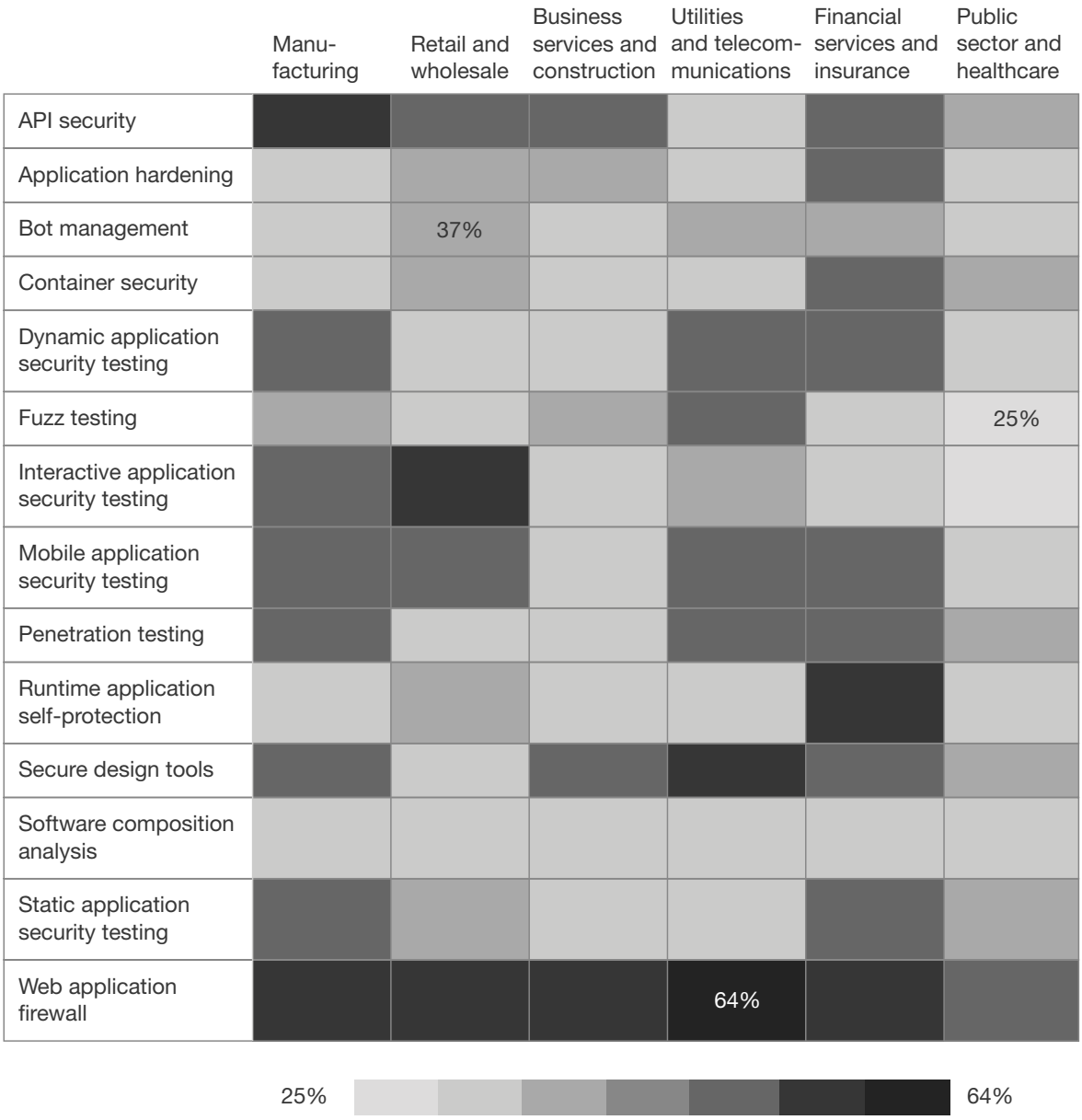
› **Public sector and healthcare are unsurprisingly the furthest behind.** Historically, government agencies and healthcare firms have had much smaller security budgets than firms in other industries.[13] While the size of their security budgets has increased slightly, actual and planned

implementations across all application security technologies remain noticeably behind every other industry (see Figure 5).[14] Low rates of planning for WAF, RASP, and bot management technologies is especially worrisome, considering that the majority of hospitals have given patients access to online portals to view, download, transmit, and discuss their health data.[15]

- **Utilities currently rely on WAF and are moving toward prerelease testing and RASP.** Utilities and telecom companies are spearheading WAF and RASP adoption; a full 64% of respondents in those industries say they have implemented WAF, and 28% say they are planning to implement RASP — the highest in both categories. Additionally, utilities and telecoms are highest in having plans to adopt SCA and IAST tools.
- **Retail companies are bracing for malicious bots.** Bot management is not just for preventing large-scale DDoS campaigns like what we saw with the Mirai attack.[16] Bots can also perform business-disrupting actions such as inventory hoarding, user account theft, resource exhaustion, and web content scraping. Today, only 37% of retail respondents say they have implemented bot management; however, another 30% of this group (the highest percentage of any technology by a single industry) say they plan to implement bot management.
- **RASP is taking off in other industries, after financial service firms led past adoption.** To date, financial service firms have outpaced firms in other industries in RASP implementation, but with the lowest number of respondents planning to implement, it seems financial services adoption is plateauing. In the near term, RASP tools will continue to find their sweet spot among companies that can handle additional server loads and applications that don't have developers actively scanning and remediating them, rather than being broadly applicable for firms in all industries.
- **Financial services firms are highest at having plans to increase penetration services.** With the increase in prerelease application security testing, only 20% of respondents overall said they are planning to invest in penetration testing. However, for financial services and insurance respondents, that number is 25%. Requirements from industry and state regulators, such as the New York State Department of Financial Services (NYDFS), will continue to push financial services to temporarily increase their use of penetration testing services until regulations acknowledge automatic testing as an acceptable alternative for application security quality.

FIGURE 4 Application Security Implementations, By Industry

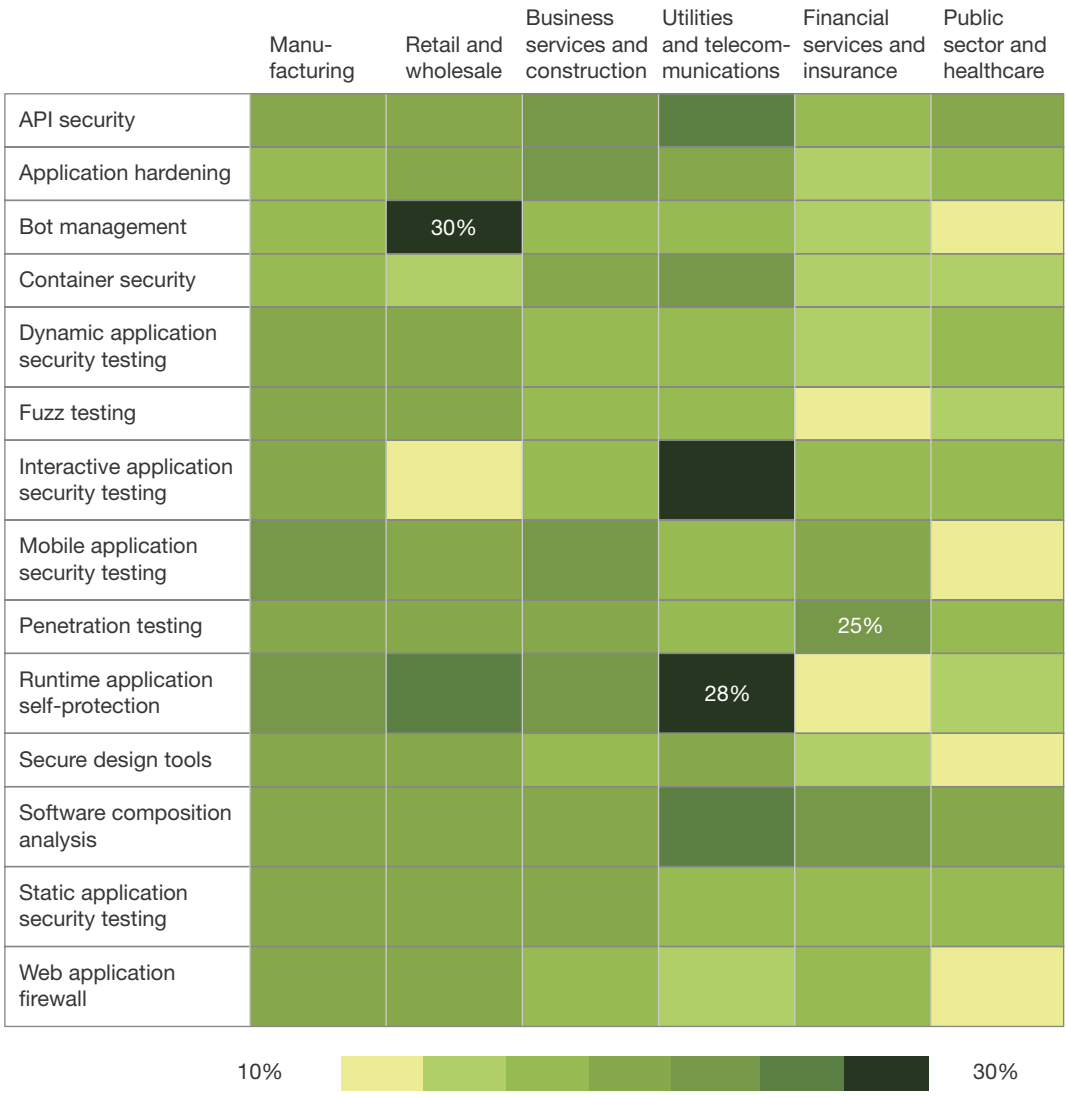
"What are your firm's plans to adopt the following application security technologies?"
(Respondents who replied, "implemented")



Base: 1,097 network security technology decision makers
Source: Forrester Data Global Business Technographics® Security Survey, 2017

FIGURE 5 Plans To Implement Application Security Technologies, By Industry

"What are your firm's plans to adopt the following application security technologies?"
(Respondents who replied, "planning to implement")



Base: 1,097 network security technology decision makers
Source: Forrester Data Global Business Technographics® Security Survey, 2017

What It Means

Application Security Won't Really Improve Without Better Integration

If the industry ever wants to truly see application security take off, prerelease testing tools such as SCA or SAST must be embedded into developer tools and processes as another software quality check.[17] Currently, integration into the software delivery life cycle (SDLC) is a do-it-yourself exercise with inconsistent support for continuous integration (CI) tools such as GitLab CI or Jenkins, ticketing tools such as Bugzilla or Jira, and build tools such as Apache Maven and Microsoft Team Foundation Server. Application security efforts are therefore getting left behind rapid advancements in software development and will continue to fall behind unless security pros and vendors make critical changes:

- **Interactive developer tools will have to spawn integrations themselves.** In Forrester's recent evaluation of CI tools, the products demonstrating the best integration capabilities use webhooks.[18] Webhooks are callback methods in an application that eliminate the need for plug-ins or do-it-yourself integrations.[19] For example, when prerelease security tools are hooked to CI or other automation tools, they could automatically receive calls to trigger a scan at check-in before a build.[20] This kind of integration saves security and application pros from having to make complex and nonstandard integrations for each application and each scanning tool based on project specifications.
- **Application tools must support inherent policy setting for consistency.** Today, some integrations between security scanners and developer tools rely on configuration and coding to initiate scans, process results, and take actions such as failing a build. What's worse, requirements might be different depending on whether the application is developed in-house or by a third party or at what point in the SDLC the scan takes place. To make the process scalable, security pros need to be able to set policy within the prerelease security tools, so the timing and type of scans will be based on a consistent consideration of application types, business units, or other company needs.

Supplemental Material

Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2017 was fielded between May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Data Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

The Forrester Data Global Business Technographics Security Survey, 2016 was fielded in March to May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Data Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

The Forrester Data Global Business Technographics Security Survey, 2015 was fielded in June and July of 2015 to 7,267 information workers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Endnotes

[1] For more information on growth of mobile apps, visit the following website. Source: Avery Hartmans, "Here are the 10 fastest-growing smartphone apps," Business Insider, August 31, 2017 (http://www.businessinsider.com/fastest-growing-smartphone-apps-comscore-2017-8/).

For more information on IoT adoption, see the Forrester report "Predictions 2018: IoT Moves From Experimentation To Business Scale." For more information on virtual assistant adoption, see the Forrester report "The Rise Of Intelligent Agents."

[2] See the Forrester report "Forrester Data: Online Retail Forecast, 2017 To 2022 (US)." For more information about predictions in 2018 for retail, see the Forrester report "Predictions 2018: Customer Obsessed, Data-Driven Retailers Thrive."

[3] For more information on the cost of a breach, see the Forrester report "Calculate The Business Impact And Cost Of A Breach."

[4] See the Forrester report "Equifax Exposed Two Massive Systemic Risks."

[5] For more information on best practice use of open source for developers, see the Forrester report "Best Practices: Adopt Open Source Software To Improve Development Effectiveness." For operations pros, see the Forrester report "Open Source Powers Enterprise Digital Transformation."

[6] For more information about the Equifax timeline, see the Forrester report "Equifax Exposed Two Massive Systemic Risks."

[7] Source: "2017 Open Source Security and Risk Analysis Report," Black Duck Software (https://www.blackducksoftware.com/open-source-security-risk-analysis-2017).

[8] For more information about software composition analysis, see the Forrester report "Vendor Landscape: Software Composition Analysis" and see the Forrester report "The Forrester Wave™: Software Composition Analysis, Q1 2017."

[9] For more information about the CA Technologies acquisition of Veracode, see the Forrester report "Quick Take: CA Technologies Fills Its DevOps Security Gap With Veracode."

For information about both the spin merger of HPE Software to Micro Focus, visit the following website. Source: Shaun Nichols, "HPE wraps up $8.8bn Micro Focus software dump spin-off," The Register, September 1, 2017 (https://www.theregister.co.uk/2017/09/01/hpe_8bn_micro_focus_software_spinoff/). For more information about Synopsys announcing its acquisition of Black Duck Software, read the following article. Source: Charlie Osborne, "Synopsys to acquire security firm Black Duck Software in $565 million deal," ZDNet, November 3, 2017 (http://www.zdnet.com/article/synopsis-to-acquire-security-firm-black-duck-software-in-565m-deal/).

[10] SAST: static application security testing; DAST: dynamic application security testing; MAST: mobile application security testing; IAST: interactive application security testing.

[11] For more information about how vendors have performed for both reporting and creating numeric scores after scanning, see the Forrester report "The Forrester Wave™: Static Application Security Testing, Q4 2017" and see the Forrester report "The Forrester Wave™: Software Composition Analysis, Q1 2017."

[12] For more information about how companies struggle to find the right resources, see the Forrester report "Top Seven Recommendations For Your Security Program In 2017."

[13] For more information about the unique threats, regulations, and financial burdens, see the Forrester report "Brief: Top 10 Security Priorities For US Healthcare Organizations."

[14] For more information about healthcare's security budget, visit the following website. Source: Amy DeMartine, "Grading Forrester's 2016 Cybersecurity Predictions Plus A Sneak Peek Into Our 2017 Predictions," Forrester Blogs, November 1, 2016 (https://go.forrester.com/blogs/16-11-01-grading_forresters_2016_cybersecurity_predictions_plus_a_sneak_peek_into_our_2017_predictions/).

[15] For more information about patient portal adoption and use, visit the following website. Source: "How Patient Portals Improve Patient Engagement," PatientEngagementHIT (https://patientengagementhit.com/features/how-patient-portals-improve-patient-engagement).

WAF: web application firewall; RASP: runtime application self-protection.

[16] Source: Nicky Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, October 26, 2016 (https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet).

[17] For more information on how to be successful with application security by making it hidden, see the Forrester report "The State Of Application Security: 2016 And Beyond."

[18] For more information about Forrester's evaluation of CI tools, see the Forrester report "The Forrester Wave™: Continuous Integration Tools, Q3 2017."

[19] Standard definitions of the data to be transferred could come soon from projects such as grafeas.io, making webhooks even more viable in the future. Source: Grafeas (https://grafeas.io/).

[20] For more information about the difference between and API integration versus webhooks, visit the following website. Source: Roger Jin, "Webhook vs API: What's the Difference?" Hacker Noon, July 10, 2017 (https://hackernoon.com/webhook-vs-api-whats-the-difference-8d41e6661652).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.