# The State Of Application Security, 2021

## Applications Remain A Key Attack Vector, But Signs Of Hope Emerge

by Sandy Carielli

March 23, 2021

## Why Read This Report

Applications remain a top cause of external breaches, and the prevalence of open source, API, and containers only adds complexity to the security team. Happily, organizations have started to recognize the importance of application security and are embedding security more tightly into the development phase. As application development continues to evolve, security pros will need to stay on top of emerging security tools to ensure that they don't get caught unaware. Security pros should use this report to benchmark themselves for the efforts in 2021 and beyond.

# The State Of Application Security, 2021

**Applications Remain A Key Attack Vector, But Signs Of Hope Emerge**

by Sandy Carielli
with Amy DeMartine, Melissa Bongarzone, and Diane Lynch
March 23, 2021

## Applications Remain A Top Attack Vector, But Firms Are Paying Attention

Applications have long been a crucial way for firms to engage with their customers, but in 2020, as the pandemic sent people home and closed physical business locations, applications often became the only way to engage with customers. With so many firms forced to quickly build or upgrade applications to reach their customers, it's not surprising that web applications are the most common form of external attack, with software vulnerabilities not far behind (see Figure 1). Every indication is that applications will remain the top form of external attack because:

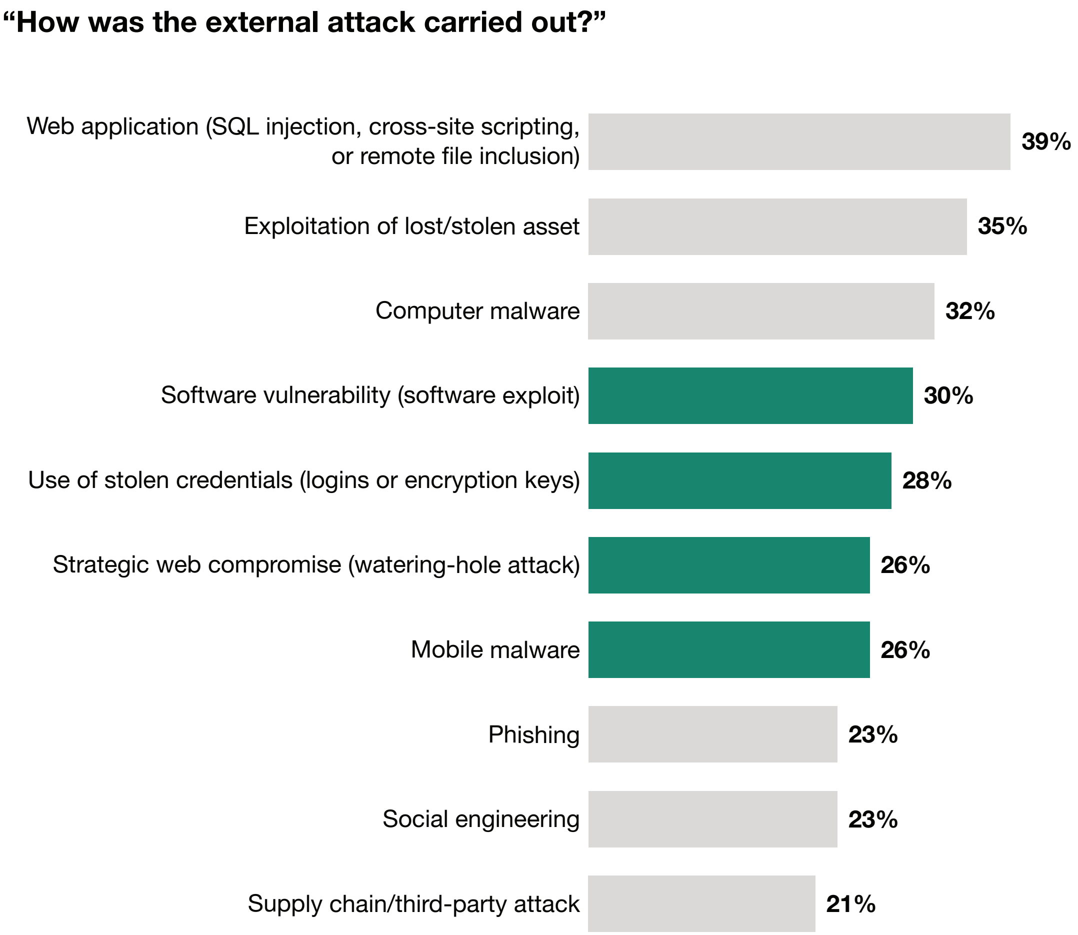
- **Open source usage continues to grow, and security hygiene as-is can't keep up.** Open source usage has only accelerated as development teams strive to produce high-quality applications quickly. Almost 99% of audited codebases contain some amount of open source, and the average percentage of open source in those code bases has almost doubled — from 36% in 2015 to 70% in 2019 (see Figure 2). Unfortunately, open source vulnerabilities continue to be pervasive, and firms are unable to react quickly enough to remediate the issues, with over 50% of survey respondents reporting that it took a week or longer to remediate known OSS vulnerabilities in their code (see Figure 3).
- **Researchers are finding more security flaws, and not just in monolithic web apps.** 2020 saw a jump in bug bounty submissions, with a 50% increase over submissions in 2019. One can speculate that the pandemic had an impact because more security researchers had extra time at home and because of the rapid development of web applications to meet changing customer needs. Vulnerabilities weren't limited to traditional web applications — the number of submissions for API vulnerabilities doubled, with broken access control (a common cause of API-related breaches) becoming the top reported issue. With so many organizations exposing a high percentage of applications to the internet or to third parties through APIs, APIs have become a prime target for attackers (see Figure 4).

FORRESTER®

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

- **Containers aren't locked down.** According to the Forrester Analytics Business Technographics® Security Survey, 2020, almost one-quarter of global infrastructure decision-makers use containers for both new and existing projects, and half have a container infrastructure service in their data center or are building it. Unfortunately, containers remain rife with code and configuration vulnerabilities — one assessment found that over half of scanned images had at least one high or critical severity vulnerability and that 58% of scanned containers were running as root. Users also struggle to lock down container images and ensure image integrity.

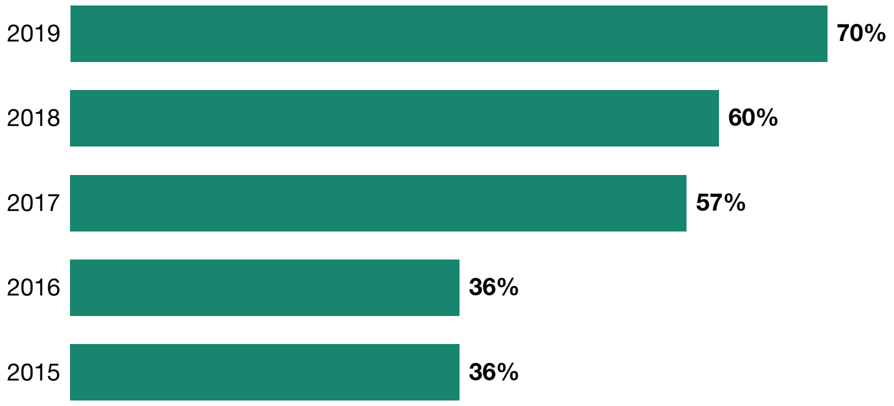
**FIGURE 1** Web Application Exploits Are The Most Common Form Of External Attack



Base: 480 global security decision-makers with network, data center, app security, or security ops responsibilities who experienced an external attack when their company was breached
Source: Forrester Analytics Business Technographics® Security Survey, 2020

**FIGURE 2** Open Source Usage Has Exploded

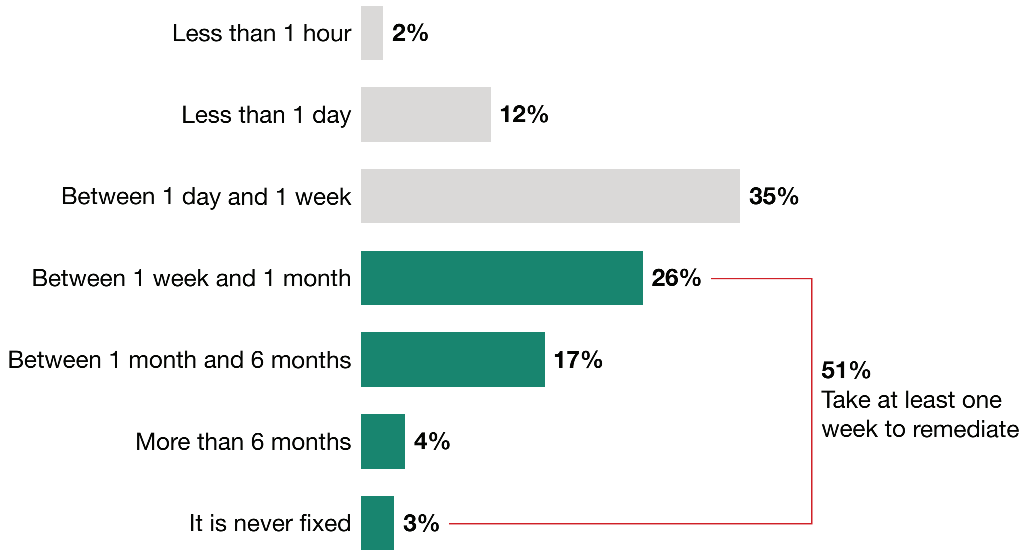
### The percentage of code base that is open source has almost doubled in 5 years



Source: Synopsys OSSRA reports, 2017, 2018, 2019, and 2020

**FIGURE 3** Developers Struggle To Remediate Open Source Software Vulnerabilities

### Time to remediate known OSS vulnerabilities after detection

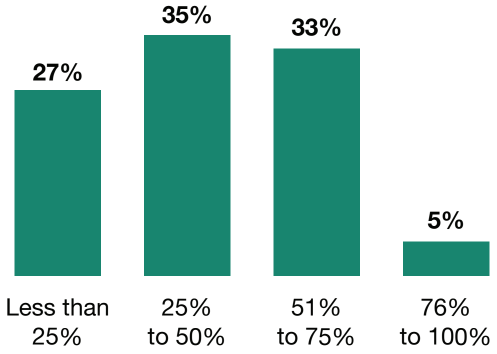


Note: Percentages do not total 100 due to rounding.

Source: "2020 State of the Software Supply Chain report," Sonatype

**FIGURE 4** APIs Are A Critical Exposure Point

**Percentage of apps organizations exposed to the internet or to third-party services via APIs**



Source: "The State Of Web Application And API Protection," Radware

## Application Security Tooling Helps Shatter The Silos

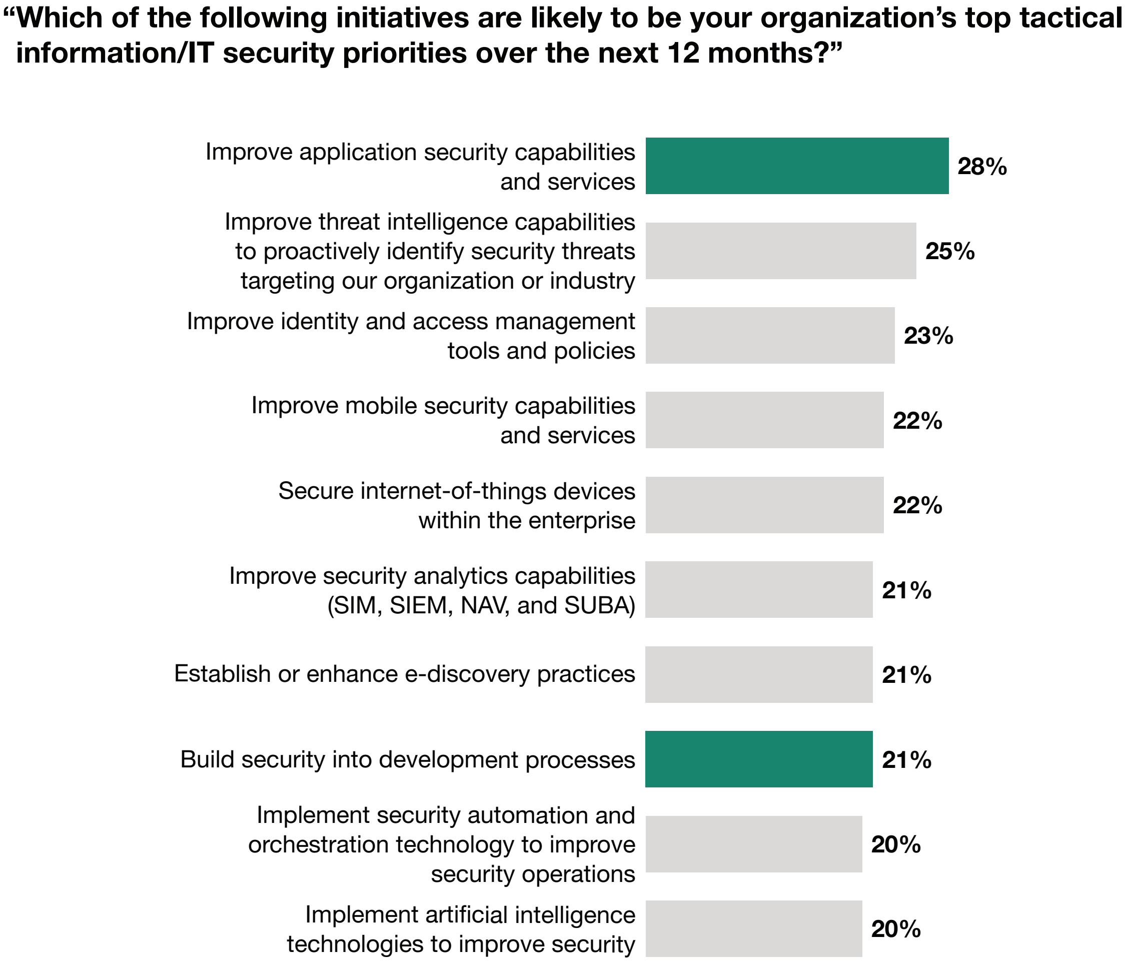
While application security flaws are prolific, management has at least acknowledged the problem, and organizations have started to realize that the solution lies not just with security teams but with developers as well. Among security decision-makers, 28% indicated that improving application security is a top tactical IT security priority in the coming year; this was the most commonly cited initiative (see Figure 5). Twenty-one percent said their firm will prioritize building security into development processes. Well-implemented application security tooling can narrow the gulf between developers and security pros, enabling developers to seamlessly address security issues without leaving their own development pipelines. When building out an application security strategy, security pros must:

- **Integrate into the DevOps toolchain as a standard practice.** The good news about trying to include automated security testing into the DevOps toolchain: The hooks are already there, with top prerelease testing products offering deep integrations with core development tools like Azure DevOps, GitHub, Jenkins, and Jira. Those that consider their DevOps practices mature are more likely both to use prerelease testing tools and to integrate them into their development pipeline.

- **Combine scans to improve visibility and get prioritization right.** Aggregating the results of prerelease testing tools provides a deeper view of security flaws and helps validate and prioritize findings. Combining static application security testing (SAST) and dynamic application security testing (DAST) scans results in findings remediated 24.5 days faster than the average, while combining SAST and SCA scans results in remediations taking place six days faster. Several top

SAST vendors natively integrate with other scanning tools — either their own or other vendors' offerings — to contextualize findings, while others at least display the results of multiple scan types within the same UI.

**FIGURE 5** Firms Have Prioritized Application Security



Base: 2,426 global security technology decision-makers

Source: Forrester Analytics Business Technographics® Security Survey, 2020

## Shift-Left Continues, But Firms Adopt New App-Sec Tools Inconsistently

It's a hopeful sign that organizations will be more focused on building security into the development phase of the software development lifecycle (SDLC), better matching developer speed and enabling faster flaw remediation. Further, the rush to embrace API security at all stages of the SDLC indicates that security pros are quickly responding to the rash of API-driven security breaches. New development approaches call for new tooling, and firms must keep up with the evolving protections to protect emerging application architectures. Consider that:

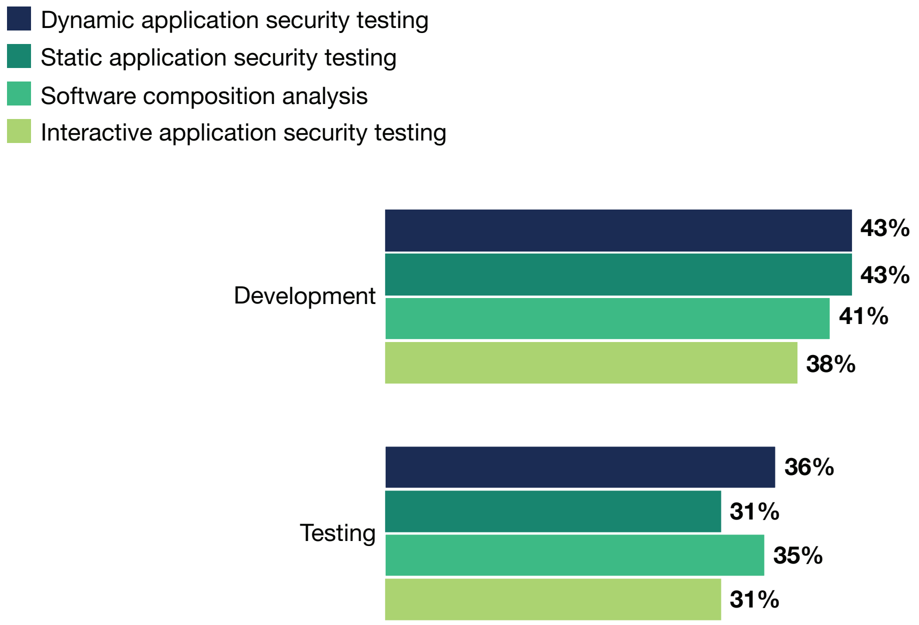
- **Security pros are moving to implement prerelease test tools in development.** The leftward shift continues. As more firms see the value of early remediation and core prerelease testing tools integrate more easily with the continuous integration/continuous delivery (CI/CD) toolchain, plans to implement those tools are weighted more toward the development phase than the testing phase of the SDLC. SAST is experiencing the most dramatic shift, with 43% planning to implement in development, versus only 31% in testing (see Figure 6). More security decision-makers also say that their firms plan to adopt interactive application security testing (IAST), software composition analysis (SCA), and DAST in development than in testing.

- **API security is taking off.** Firms have embraced the business opportunities associated with APIs, and they've started to recognize the security risks. Forty percent of security decision-makers say their firms have implemented API security in production or are in the process of doing so, and 41% are implementing it in testing (see Figure 7). In the coming year, firms will continue to adopt API security in testing and to extend into development and design.

- **Container security implementations are lagging.** Despite growing container adoption, firms focus much of their container security investment on testing, to the detriment of both development and production phase container security controls. Forty-two percent of security decision-makers say their firms have implemented or are implementing container security in testing; a further 48% plan to do so in the next 12 months (see Figure 8). Unfortunately, only 21% say their firms plan to implement necessary runtime container security protections in production, and only 30% in development, in the coming year.

**FIGURE 6** Firms Move To Implement Prerelease Tools In Development

**“In what phase of the application development lifecycle are you implementing or planning to implement the following technologies?”**
(Planning to adopt)

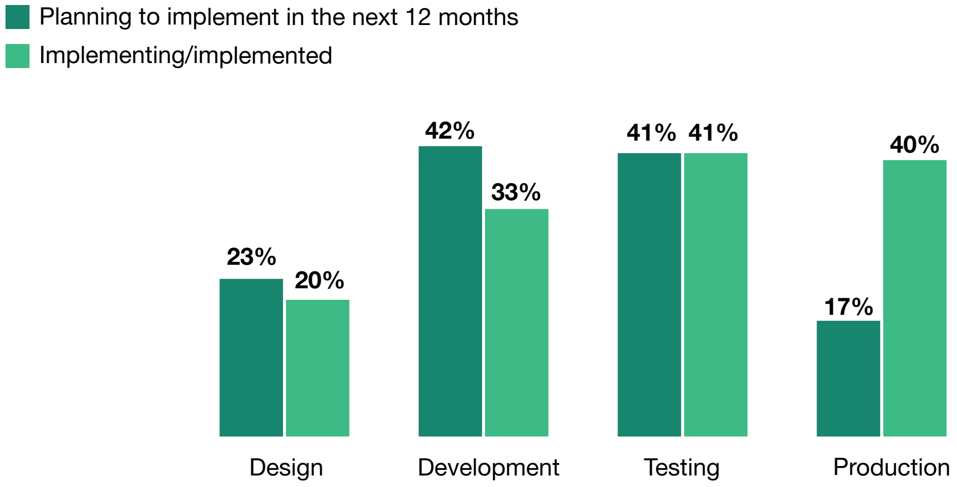


Base: 127 to 136 global security decision-makers with network, data center, app security, or security ops responsibilities whose firms plan to adopt the indicated technologies in the next 12 months

Source: Forrester Analytics Business Technographics® Security Survey, 2020

**FIGURE 7** Firms Are Aggressively Adopting API Security

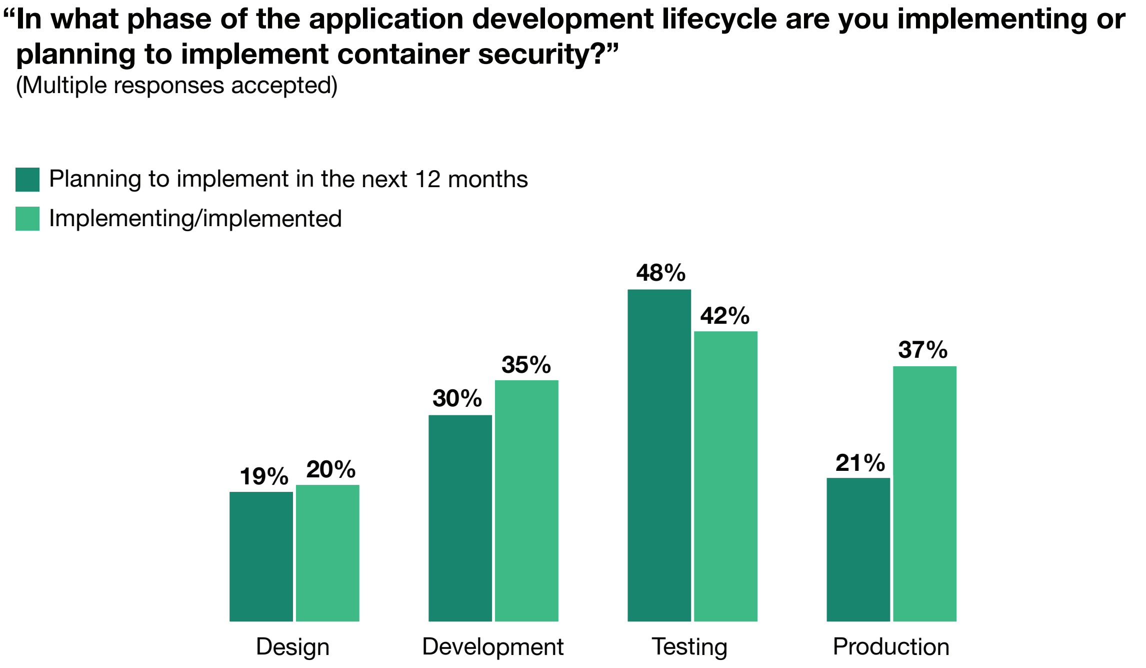
**"In what phase of the application development lifecycle are you implementing or planning to implement API security?"**
(Multiple responses accepted)



Base: 133 to 784 global security decision-makers with network, data center, app security, or security ops responsibilities whose firms are adopting or planning to adopt API security

Source: Forrester Analytics Business Technographics® Security Survey, 2020

**FIGURE 8** Firms Are Lagging In Container Security Implementations



Base: 132 to 763 global security decision-makers with network, data center, app security, or security ops responsibilities whose firms are adopting or planning to adopt container security

Source: Forrester Analytics Business Technographics® Security Survey, 2020

## Planned App Sec Adoption Is Spotty Cross-Industry, But There Are Bright Spots

One might hope that the pandemic and the spate of application-related breaches hammered home the importance of application security across all sectors. Sadly, planned adoption is inconsistent; retail and wholesale have the most aggressive adoption plans in the coming year, while public sector and healthcare lag furthest behind. Multiple industries are interested in SCA, runtime application self-protection (RASP), and DAST. With cautious optimism for the future, we find that:

- **Retail and wholesale are planning to invest aggressively.** In the early days of the pandemic, a retailer's ability to digitally transform was the difference between staying in business and collapsing. As this industry rapidly developed and upgraded applications, it's unsurprising to see it leading in planned application security investments. Retail and wholesale accounts for four of the top nine areas of planned investment: 19% of security decision-makers in retail say their firms plan to adopt RASP, 18% to adopt SCA, 18% to adopt client-side code protections, and 17% to adopt IAST (see Figure 9).

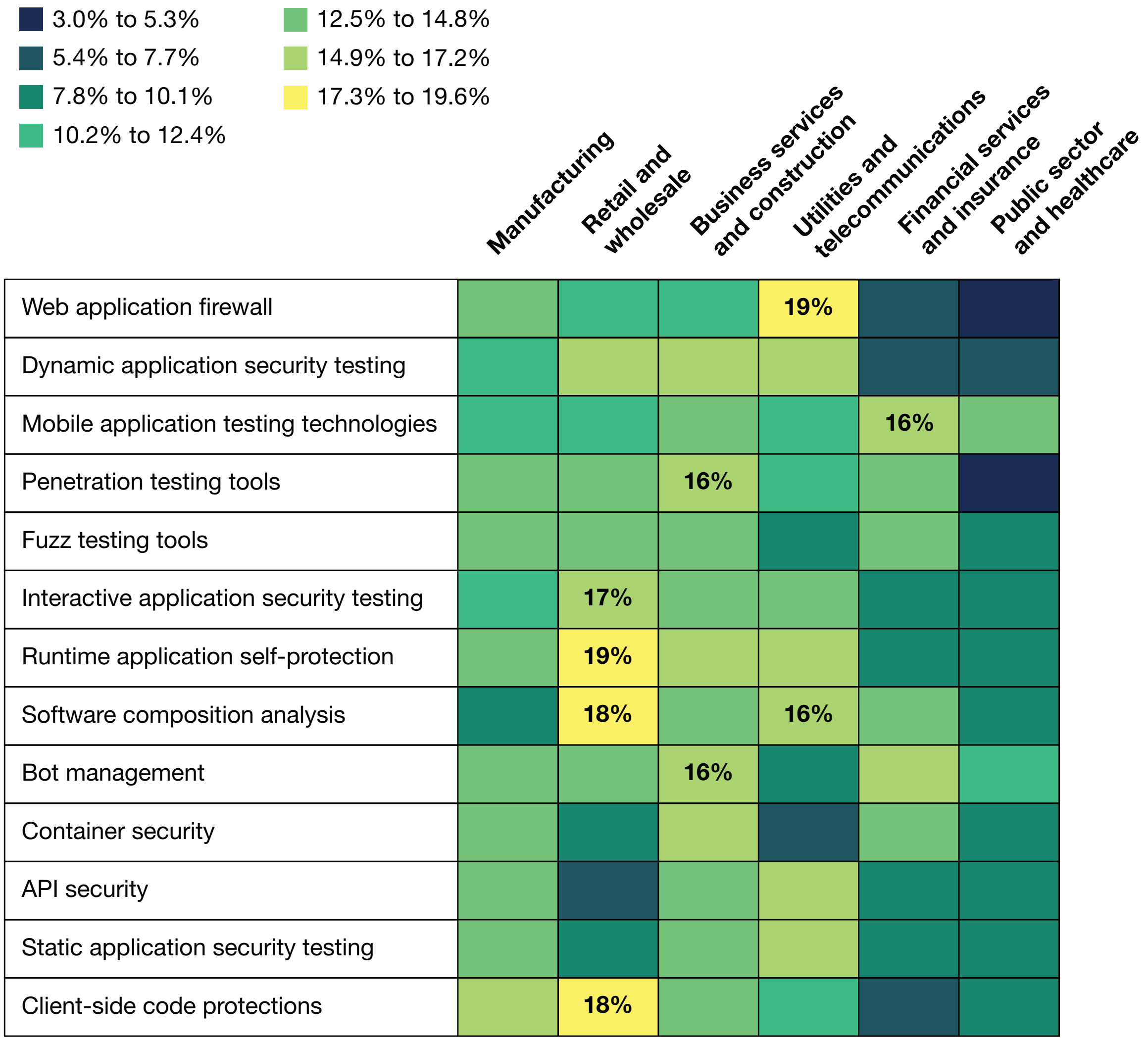
- **Utilities and telecom are focusing on WAF and SCA.** Nineteen percent of security decision-makers in the utilities and telecommunications space say their firms plan to adopt web application firewalls (WAF) in the next 12 months, an indication that many are still paying attention to core application protection requirements. The 16% looking to adopt SCA was another high mark and could belie a growing acceptance of open source in the space.

- **Manufacturing and business services are investing moderately across the board.** In the manufacturing space, no planned investments stood out, with 10% to 15% of security decision-makers in the industry saying their firms plan to adopt each of the application security technologies listed. In business services and construction, 16% of respondents reported plans to adopt penetration testing tools and bot management; at least 10% said their firms plan to adopt each of the other technologies.

- **Financial services and the public sector are looking to mitigate mobile attacks and bots.** Adoption plans in the financial services and insurance industry and the public sector and healthcare segment were disappointing; for many application security technologies, fewer than 10% of respondents said their firms have plans to adopt in the next year. Mobile application security testing (MAST) and bot management were among the few areas of relatively higher planned investment. While the mobile security focus is promising, particularly given the importance of mobile applications in financial services and healthcare, it's otherwise disconcerting to see so little planned investment.

**FIGURE 9** Adoption Of Specific Application Security Technologies Varies By Industry

**"What are your organization's plans to adopt the following application security technologies?"**
(Planning to adopt)



Note: The top nine percentages are highlighted with text.

Base: 84 to 334 global security decision-makers with network, data center, app security, or security ops responsibilities (sample size varies by industry)

Source: Forrester Analytics Business Technographics® Security Survey, 2020

## Align Your Application Security Strategy To The Changing Nature Of Applications

Security pros must adjust to the reality of more modular and more agile application development. As firms rely on more third-party components and open up more APIs externally, security teams lacking cross-department relationships and automation will be left behind. Here's what you need to do:

- **Remember application security when looking at supply chain risk.** Supply chain risk is on the tip of everyone's tongue after the Solar Winds breach, but you must focus on more than the Solar Winds use case. Existing and new vulnerabilities in your open source libraries and container images also present exploit opportunities — and if you don't regularly identify and remediate those issues, you and your customers are at risk. Educate executive stakeholders on the value and risk of open source, and use software composition analysis and container security tools to protect your applications.

- **Integrate all the tools that developers love.** Today's application security tools are much more developer focused, so work with the dev team to integrate security into their workflow and process. Leverage your tools' out-of-the-box integrations with popular CI/CD tools, or take advantage of vendors' increasingly robust APIs to create custom integrations. Look for deep integrations that assign discovered flaws to the right developer, provide deep context and remediation guidance, and enable automated signoffs for policy creation and exceptions. Remember to integrate your multiple application security tools to help validate and prioritize flaws.

- **Proactively build security into new application development plans.** Match your security tooling to your future application architecture. Whether it's APIs, containers, serverless functions, or low code, new development methodologies mean changes to the traditional security paradigms. Reach out to your development and IT leadership to understand what new development approaches they're looking to adopt in the next six to 12 months — then review your processes and invest in the tooling to support new architectures.

- **Continue with your developer security champions program.** Bridging the gap between security and development is primarily a people problem. Programs like developer security champions, in which developers are trained in security principles raise security issues earlier in the development process, help scale the security team and increase its credibility with development.

## Supplemental Material

### Survey Methodology

The Forrester Analytics Business Technographics® Security Survey, 2020, was fielded from June to August 2020. This online survey included 3,691 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

Forrester Analytics' 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 and in marketing efforts. Dynata fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics' Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

FORRESTER®

forrester.com

## We help business and technology leaders use customer obsession to accelerate growth.

PRODUCTS AND SERVICES

- › Research and tools
- › Analyst engagement
- › Data and analytics
- › Peer collaboration
- › Consulting
- › Events
- › Certification programs

## 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.