The State Of Application Security, 2020

Applications Remain The Top External Attack Method; Don't Get Complacent

by Sandy Carielli
May 4, 2020

Why Read This Report

Application weaknesses and software vulnerabilities continue to be the most common external attack method. Now is not the time to backslide on your application security efforts. Instead, follow the path of many other firms that focus their efforts on pushing security testing early in software development, implement autoremediation, and shore up production protections. Security leaders should read this report to help guide improvements in their own programs.

Key Takeaways

Prerelease Scans Continue To Further Align With Software Delivery Methods

Increasingly, firms move software composition analysis (SCA) and container security into the development phase of the lifecycle. Interactive application security testing (IAST) is also taking hold in the development phase. These shifts help dev teams address security risks with lower friction while still meeting release objectives.

Industries Take Dramatically Different Approaches To App Security

Disturbingly, financial services and retail industries scaled back their application security investments in key areas, and the public sector and utilities focus on basics like web application firewalls (WAFs) and dynamic application security testing (DAST). These industries must increase their investments in tooling that enables security automation.

Get Ready For Autoremediation

SCA tools lead the way for prerelease scanning tools by recommending remediations and allowing developers to automatically implement the recommended fix with the click of a button. Expect this to expand, and create corporate policies and culture that support developers using autoremediation features.

The State Of Application Security, 2020

Applications Remain The Top External Attack Method; Don't Get Complacent

by Sandy Carielli
with Amy DeMartine, Melissa Bongarzone, and Peggy Dostie
May 4, 2020

Table Of Contents

Related Research Documents

Show, Don't Tell, Your Developers How To Write Secure Code

The State Of Government Application Security, 2020

Top Cybersecurity Threats In 2020

FORRESTER®

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

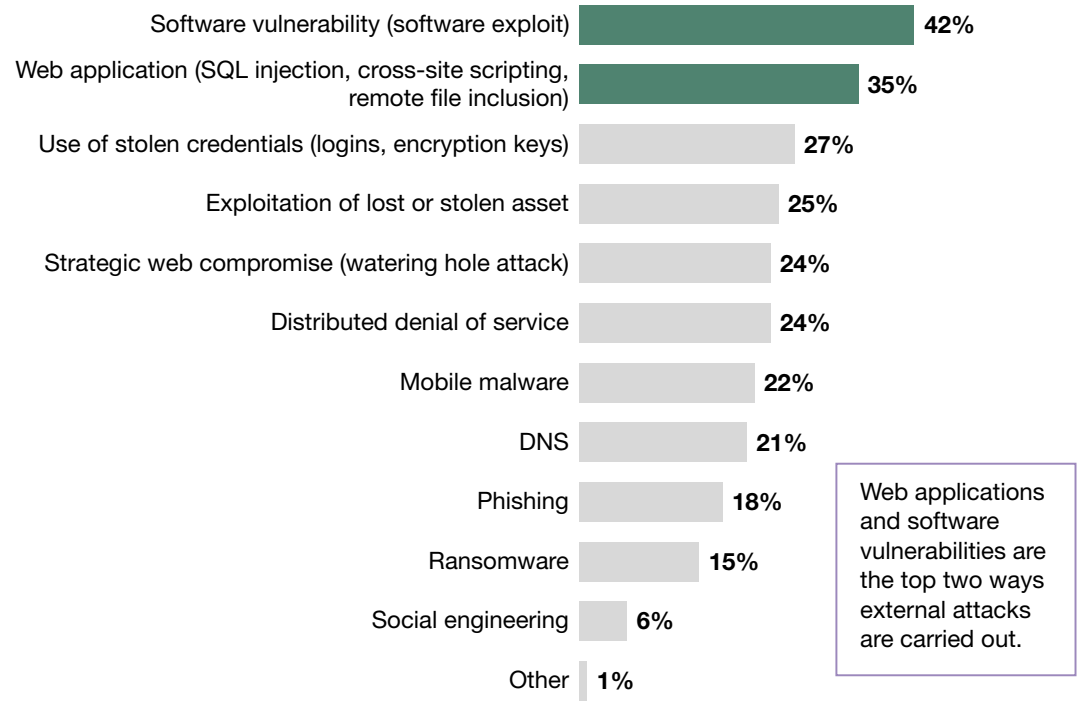
Applications Are The Weakest Link — Again

Applications are the lifeblood of business. Organizations develop applications to meet customer, partner, and employee needs, but even after decades we still have not figured out how to secure applications. Once again, applications are the leading attack vector in security breaches: 42% of global security decision makers whose firms experienced an external attack said it was carried out by exploiting a software vulnerability and 35% said it was through a web application (see Figure 1). It's no surprise that these are the top two causes of external breaches; as applications become more complex, rely on internal and third-party components, and evolve to support new frameworks, security professionals must keep up and understand that:

- **Open source continues to infect everything.** Open source software is a necessary element of modern development, enabling teams to move faster and focusing development on their core expertise and value proposition. Unfortunately, open source is as vulnerable as it is pervasive — open source vulnerabilities had another record year in 2019, with an almost 50% increase in reported vulnerabilities over 2018 (see Figure 2). Open source vulnerabilities impact container security too. Consider that the top Docker images all have vulnerabilities — not just one or two vulnerabilities, but tens or even hundreds (see Figure 3).
- **As applications take on new forms, attackers adapt.** If you still think of applications as monolithic client/server behemoths, then you aren't protecting against current application threats. Attackers compromise modern applications through unsecured API endpoints, unvalidated API payloads, and client-side attacks injecting malware into unprotected scripts.[1] The rise of new architectures and frameworks offers new attack surfaces, and security professionals must be concerned about image integrity, vulnerabilities in common container images, and changes to containers and functions in production.
- **Developers aren't stopping — security can't either.** Development teams continue to move faster. In 2018, 27% of global developers indicated that they released monthly or faster; in 2019, the number jumped to 38%.[2] That speed applies to development frameworks, too — over 50% of containers live 5 minutes or less (see Figure 4). Security tools and processes that can't work at development speeds will be tossed aside.

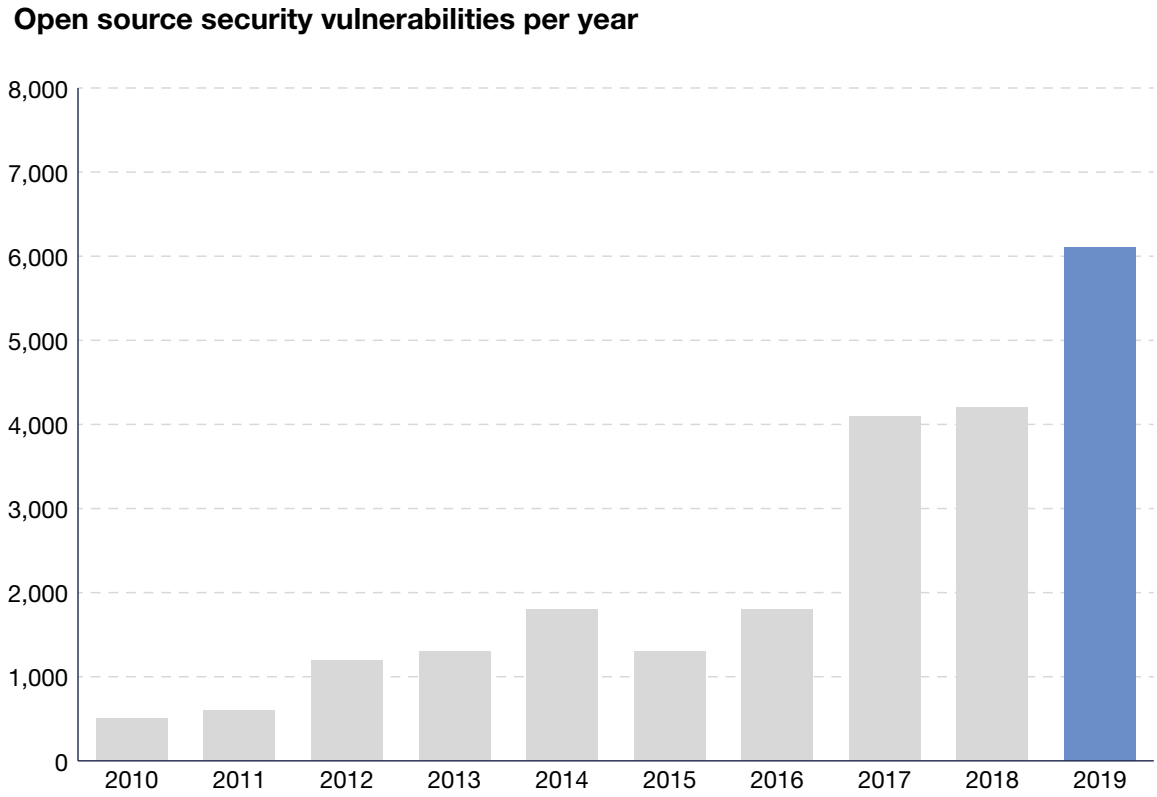
FIGURE 1 Applications Remain The Most Common Attack Vector

"How was the external attack carried out?"



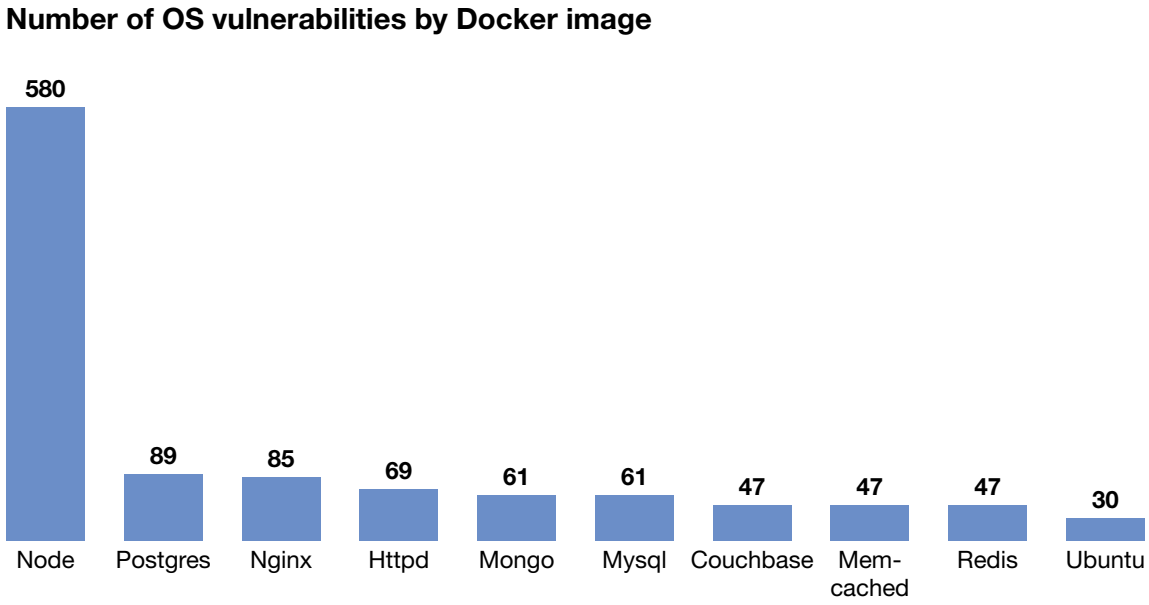
Base: 465 security decision makers with network, data center, app security, or security ops responsibilities who experienced an external attack when their company was breached
Sources: Forrester Analytics Global Business Technographics® Security Survey, 2019

FIGURE 2 Open Source Vulnerabilities Continue To Increase



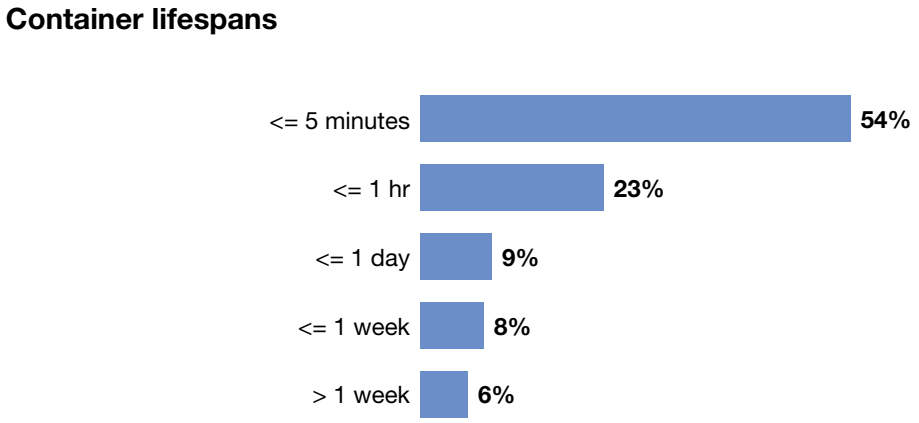
Source: WhiteSource, "The State of Open Source Vulnerabilities Annual Report 2020"

FIGURE 3 Top Docker Images Are All Vulnerable



Source: Alyssa Miller, "The State of Open Source Security - 2020," Snyk, March 25, 2020

FIGURE 4 Most Containers Live For A Matter Of Minutes



Source: "Container Lifespans" from the Sysdig 2019 Container Usage Report: New Kubernetes and security insights by Sysdig

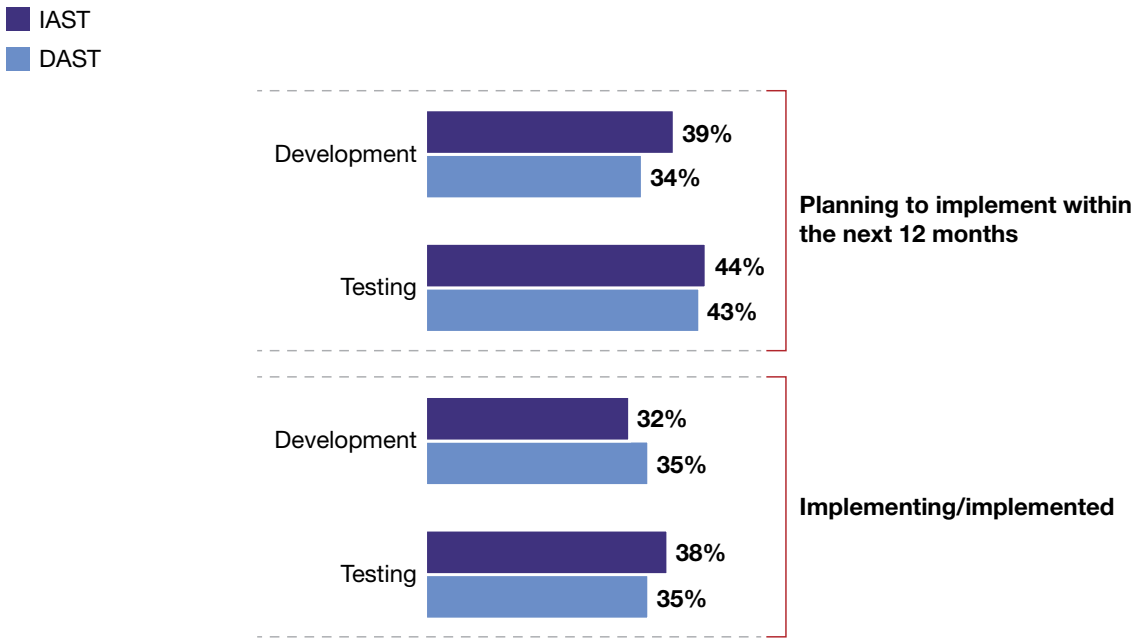
Application Security Is Taking Hold In Prerelease But Not Enough

Only 14% of organizations fully integrate security throughout the software development lifecycle (SDLC), and those just starting to integrate security into the lifecycle usually begin by focusing on the test phase.[3] We continue to see a slow move toward implementing prerelease scanning in development — and a slower move toward implementing security prerelease scanning in design. Getting security to match developer speed demands integration at all phases, and firms must move faster at pushing prerelease testing earlier in the SDLC. However, there's a glimmer of hope that firms are moving in the right direction as:

- **IAST overtakes DAST in the development phase.** Interactive application security testing (IAST) emerged a few years ago as an alternative to dynamic application security testing (DAST), and organizations are finally ready to make the switch.[4] Today, 32% of global security decision makers implement IAST in the development phase, while 35% implement DAST in development (see Figure 5). In the next year, that will get flipped on its head, with 39% planning to implement IAST in development, compared with only 34% planning to implement DAST. These firms will benefit from running IAST in unit testing and will use the added stack trace to make findings more actionable — the move from DAST to IAST helps teams embed security into their existing development processes.
- **Container security efforts move toward the development and design phases.** Container security must be addressed at every stage of the SDLC, but implementation efforts to date lean more toward production and testing.[5] Thankfully, that's changing — in the next 12 months, 37% of security pros plan to implement container security in development, and 20% plan to implement it during design (see Figure 6). Security pros must continue to invest in container security at the early phases of the lifecycle to use trusted images and secrets management.
- **SCA efforts must accelerate their shift toward the development phase.** Savvy firms that use SCA early in the SDLC ensure that open source vulnerabilities and licensing issues don't cascade throughout the application. While 39% of security pros still plan to implement SCA in testing this year, 37% plan to implement SCA in development, compared with 31% that have already done so (see Figure 7). As open source vulnerabilities continue to increase, teams will benefit from SCA implementations that help them prioritize vulnerabilities and remediate them in line with the development process.

FIGURE 5 IAST Begins To Overtake DAST In Prerelease Testing

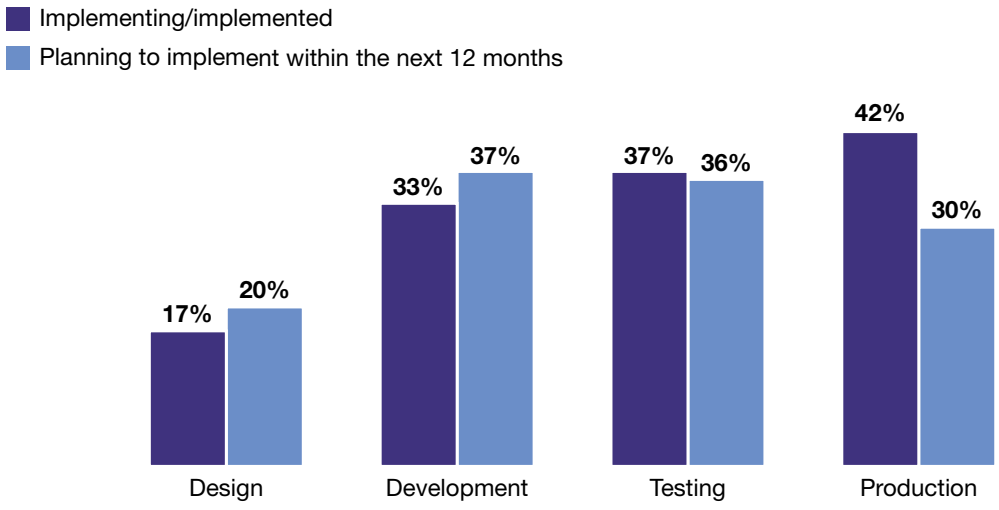
"In what phase of the application development lifecycle do you plan to implement or are you implementing the following technologies?"



Base: 280 to 756 global network path security decision makers whose firms are adopting DAST or IAST
Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

FIGURE 6 Container Security Pushes Left In The SDLC

"In what phase of the application development lifecycle do you plan to implement or are you implementing container security?"

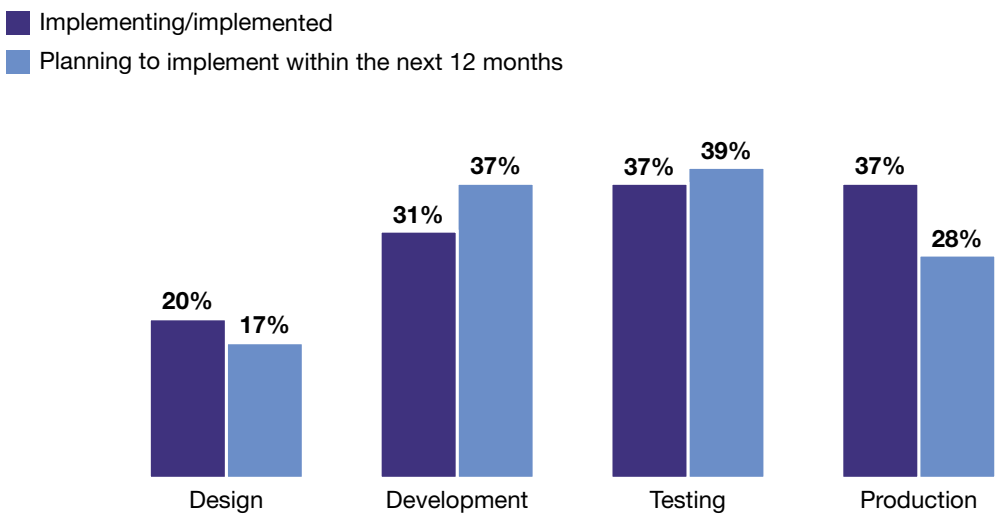


Base: 291 to 794 global network path security decision makers whose firms are adopting container security

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

FIGURE 7 SCA Implementation Moves Closer To Development Phase

"In what phase of the application development lifecycle do you plan to implement or are you implementing software composition analysis?"



Base: 282 to 753 global network path security decision makers whose firms are adopting SCA
Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

It's Time To Embrace Automation In Testing And Remediation

Automation is top of mind for developers: 29% of global development managers say that increasing SDLC automation will be one of their top three priorities for the coming year.[6] To meet developer needs, security pros must integrate application security testing tools into the CI/CD pipeline and enable scans to run automatically on check-in, build, and integration while also enabling autoremediation to make mitigating security flaws quick and painless. Consider that:

- **Automation leads to fewer vulnerabilities and educates developers in real time.** The more you scan, the faster flaws get fixed. For applications scanned over 260 times per year, the median fix time is 19 days, but the median fix time jumps to 68 days for applications scanned less than 12 times per year.[7] Automated scanning within the developer's IDE serves two purposes: It helps identify and remediate vulnerabilities before they progress in the SDLC, and it provides developers an in-the-moment, real-time training, teaching them how to spot and fix vulnerabilities in their own code.
- **Emerging autoremediation features scale dev teams and further reduce time-to-fix.** Leading players in the SCA space not only identify OSS vulnerabilities in their scans but recommend fixes — e.g., upgrade to a specific nonvulnerable version of the library — and allow developers

to implement the fix by simply clicking a button. This level of autoremediation may seem scary at first — it requires trusting the vendor to recommend a fix that will both address the problem and not introduce new functional or security errors. Building that trust will pay off by further scaling your development and security resources by reducing time-to-fix.

Key Industries Backslide In Application Protections

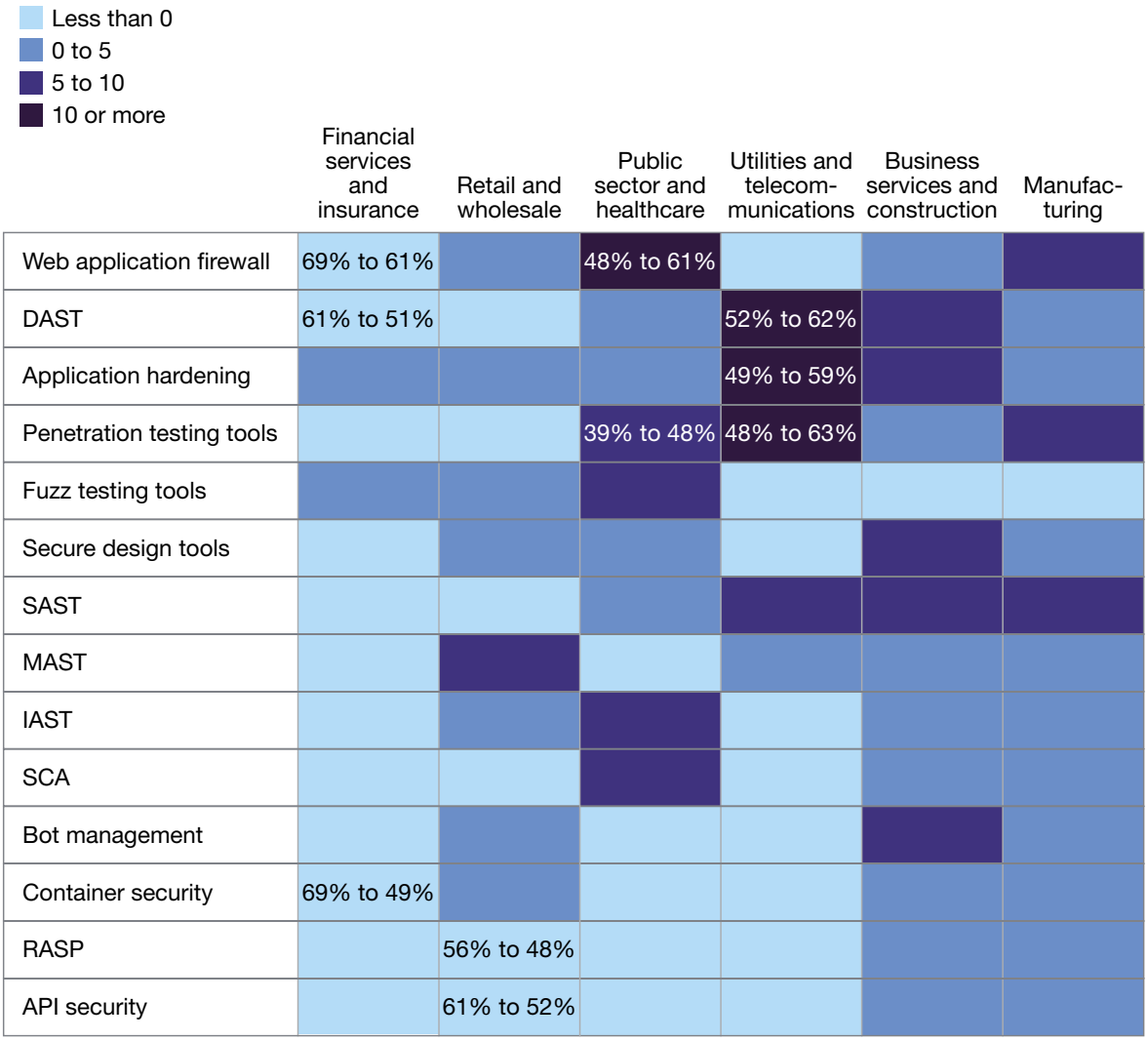
Security pros will struggle to keep up with the new application languages and delivery methods without the heavy use of tools and automation. Unfortunately, some leading industries are scaling back on critical tooling, and other industries are focused on legacy tools that don't fully address agility requirements (see Figure 8). This is exactly the wrong direction — firms must double down on application security prerelease scanning that enables development to address security issues early and seamlessly and on a full stack of production protections. Unfortunately, we find that:

- **Financial services and retail reduced application security almost across the board.** The proportion of global security decision makers at financial services and insurance firms implementing a container security tool went down by 19 percentage points between 2018 and 2019, and the proportion implementing WAF decreased by eight percentage points — a disconcerting development in a year where one of the biggest financial services breaches, Capital One, was traced to a misconfigured WAF.[8] In the retail space, the proportion of global security decision makers implementing API security fell by nine percentage points from 2018 to 2019. Both verticals showed smaller decreases in implementing most other application security protections, and almost no increases.
- **Public sector and utilities have focused on a few basic tools.** Public sector and healthcare organizations are focusing on WAF and penetration testing tools. From 2018 to 2019, the proportion of global security decision makers in those industries who indicated that they were implementing WAF jumped by 13 percentage points, while the proportion who responded that they were implementing pen-testing tools increased by nine percentage points. Penetration testing tools are also popular in utilities and telecommunications, where the proportion of global security decision makers implementing those tools rose by 15 percentage points, as the proportion implementing DAST rose by 10 percentage points. Public sector and utilities' focused investment on slow-innovation security basics like WAF and DAST reflects the slower moving nature of these verticals; however, considering that these firms also collect and store data on large numbers of customers, focus on newer protections is needed.
- **Business services and manufacturing spread their app sec investments thin.** In the business services and manufacturing verticals, there were few decreases from 2018 to 2019 in the proportion of global security decision makers implementing any app sec technology. That's good news. However, the increases in implementations of particular technologies were slight and spread over a multitude of options. These industries are not on the leading edge of security adoption, and the peanut buttering of their application security investments could reflect an uncertainty about where to prioritize.

FIGURE 8 Adoption Of Specific App Sec Technologies Varies By Industry

"What are your firm's plans to adopt the following application security technologies?"
(Implementing/implemented/expanding or upgrading implementation)

Change in adoption from 2018 to 2019, in percentage points



	Financial services and insurance	Retail and wholesale	Public sector and healthcare	Utilities and telecom-munications	Business services and construction	Manufac-turing
Web application firewall	69% to 61%		48% to 61%			
DAST	61% to 51%			52% to 62%		
Application hardening				49% to 59%		
Penetration testing tools			39% to 48%	48% to 63%		
Fuzz testing tools						
Secure design tools						
SAST						
MAST						
IAST						
SCA						
Bot management						
Container security	69% to 49%					
RASP		56% to 48%				
API security		61% to 52%				

Base: 114 to 388 (2019) and 65 to 287 (2018) global security decision makers with network, data center, app security, or security ops responsibilities at firms with 20+ employees (sample size differs by industry)
Source: Forrester Analytics Global Business Technographics® Security Surveys, 2018 and 2019

Recommendations

Now Is Not The Time To Get Complacent

Building application security seamlessly into the development process has never been more urgent. With many teams forced into sudden remote work situations, security blockers can't be solved by a walk over to someone's office.[9] This means that you must make security investments that align with the development process and put the right communication channels and support structures in place. Here's how:

- **Incorporate open source and container images in third-party risk assessments.** Firms must simultaneously embrace open source and address its increasing number of vulnerabilities. This may seem like a difficult line to walk, but the key is to catalog and manage the risk. Highlight all open source and container usage when documenting application risk, and use SCA and container tools to maintain an updated inventory of all third-party code and components. Reinforce any corporate policies around open source and container usage through SCA and container security tool policies.
- **Create developer security champions to extend security's reach.** Developer security champions serve as the main security point of contact on a dev team, trusted individuals that other developers can go to for questions and advice. They know when and how to bring in the application security team. Firms need a formal, funded program to identify and train developer security champions — champions need training on secure coding practices and attack trends and regular meetings and events that connect champions with the security team and with each other. To further engage security champions, provide incentives such as career opportunities and unique recognitions.
- **Develop software development policies and training to support autoremediation.** Provide developers clear guidance on when to accept tools' remediation recommendations immediately and when to seek additional approvals — for example, for certain levels of criticality, based upon the scope or likely impact of the fix, and considering the developer's experience. Review these policies periodically and plan to expand autoremediation support as teams get more comfortable with the tools and the tools extend their autoremediation capabilities.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

Survey Methodology

The Forrester Analytics Global Business Technographics® Security Survey, 2019, was fielded between April and June 2019. This online survey included 3,890 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. 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.

Endnotes

[1] See the Forrester report "Top Cybersecurity Threats In 2020."

[2] Source: Forrester Analytics Global Business Technographics Developer Survey, 2018 and 2019.

[3] Source: "2019 State of DevOps Report," Puppet, 2019 (https://puppet.com/resources/report/state-of-devops-report/).

[4] An emerging technology promising to replace cumbersome DAST tools, interactive application security testing (IAST) tools are either agents installed on a web application server or additional libraries that instrument the application binary. See the Forrester report "Construct A Business Case For Interactive Application Security Testing."

[5] See the Forrester report "Ten Basic Steps To Secure Software Containers."

[6] Source: Forrester Analytics Global Business Technographics Developer Survey, 2019.

[7] Source: "Veracode State of Software Security Volume 10," Veracode, 2019 (https://www.veracode.com/sites/default/files/pdf/resources/sossreports/state-of-software-security-volume-10-veracode-report.pdf).

[8] Source: Lily Hay Newman, "Everything We Know About the Capital One Hacking Case So Far," Wired, August 29, 2019 (https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/).

[9] Source: Charles Betz, Sandy Carielli, Christopher Condo, Chris Gardner, Bill Martorelli, Margo Visitacion, William McKeon-White, Tyler Brown, "Agile, DevOps, And COVID-19," Forrester Blogs, March 23, 2020 (https://go.forrester.com/blogs/agile-devops-and-covid-19/).

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that 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.