Contrast SECURITY

Why Lack of Application Security Skills and Experts Hamstrings Digital Transformation Initiatives

Executive Overview

Software developers face pressure from all sides. While their organizations demand faster delivery cycles, they are concurrently seeing a rising number of successful application exploits—from data breaches to operational disruptions and outages. Traditional scan-based application security tools are largely to blame. These outdated tools complicate Agile and DevOps workflows, relying on human security experts to run tests, analyze results, and triage potential vulnerabilities in software code. At the same time, organizations face an ever-increasing shortage of skilled application security labor as well as problems retaining their existing staff due to burnout and offers from other companies seeking to lure them away with better offers.

Demand for Applications Explodes, Vulnerabilities and Breaches Leap

Developers are under ever-increasing pressure to evolve existing applications and to deliver new ones faster. This is a main contributing factor on why nearly all applications today have at least one vulnerability—and more than one-quarter have at least one serious vulnerability that could lead to a breach or operational disruption or outage.[1] With the average application enduring more than 13,000 attacks per month last year,[2] the odds of successful exploitation are extremely high.

According to Verizon, nearly half (43%) of all successful data breaches can be traced back to an application vulnerability—a share that more than doubled year over year.[3] Similarly, Forrester data shows that 42% of global security decision-makers whose firms experienced an external attack said it was carried out by exploiting a software vulnerability; 35% said it was through a web application with an almost 50% increase in reported vulnerabilities over the prior year.[4]

It stands to reason that the longer a vulnerability exists, the greater the risk that it will be exploited. One study finds that it takes organizations, which rely on static application security testing (SAST) tools for vulnerability management, 121 days to achieve median remediation (50%)—and that 29% of vulnerabilities remain unresolved after a year.[5] This is a huge window of opportunity for cyber criminals to exploit, and one that remains open for a lengthy period of time.

At the same time, cyber criminals are not slow to develop exploits for newly discovered vulnerabilities. A study by Rand Corporation finds that 71% of exploits are developed within a month, with only 10% taking three months or more.[6] FireEye uncovers that the average time between disclosure and patch availability is nine days and that 42% of vulnerabilities are exploited after a patch is released.[7]

To address this heightened risk and manage the tool soup of application security pieces, organizations rely on professionals with specialized skill sets. But in addition to the cost of these resources, they are hard to recruit and retain due to the fact that their skill sets are in high demand. Application security jobs have jumped by 74% over the last five years—yet the number of searches for such jobs (one proxy measure of supply) has risen by only 13%.[8]

> Over the past year, 73% of organizations had at least one intrusion or breach that can be attributed in part to a gap in cybersecurity skills; 47% had three or more such events.[9]

Traditional Application Security Requires Human Experts

Traditional application security approaches that leverage SAST and dynamic application security testing (DAST) require security expertise—both to run the scans and testing and to triage, diagnose, and remediate. Historically, developers were tasked with doing so, but research shows that three-fourths of them are inadequately prepared to address those needs.[10] And as threats grow in volume and velocity as well as sophistication, the need for security expertise will only intensify.

> 70% of CIOS report their teams spend more than half their time finding the cause before they're able to fix system problems.[11]

But even when an organization is properly staffed, scan-based security tools bog down Agile and DevOps processes. Security specialists need to set up and run scanning tests. Analysts then need to interpret the results, before passing results back to developers to locate and remediate vulnerabilities in the code. This complexity disrupts the flow of development and depends on human intervention at a time when there is a historic shortage of skilled security staff available to make this convoluted system even passably functional. Even if they are able to find and recruit these specialized staff members, organizations face higher security and development staffing costs.[12]

> The global cybersecurity workforce needs to grow by 145% to meet the current demand for skilled cybersecurity talent.[13]

Contrast SECURITY

Hiring Difficulties: A Scarcity of Skilled Staff

Over the past year, the cybersecurity skills gap continued to expand. The global workforce shortfall is now an estimated 4.07 million with 65% of companies currently reporting needs for skilled staff in critical areas.[14]

A lack of trained security staff on development teams can lead to release delays and product degradation—analyst investigations may take longer, remediation steps may get missed, and incidents may be handled inconsistently from day to day. In a recent survey of cybersecurity professionals, more than half of the respondents reported that their organizations are at moderate or extreme risk due to security staff shortages, with application security specifically named as an area where the gaps were most glaring.[15]

Another survey of developers shows similar issues when it comes to their current security expertise:

- 62% say their cybersecurity team is understaffed
- 57% currently have unfilled cybersecurity positions
- 32% indicate it takes six months or more to fill an open cybersecurity position
- 70% say fewer than half of cybersecurity applicants are well-qualified for the job[16]

Those who take longer to fill positions also report more attacks. Organizations that filled a key cybersecurity position in two weeks or less saw 12% fewer cyberattacks than those who took six months or more to fill the position and 16% fewer than those who didn't fill the position at all.[17]

Staff Retention is Also a Growing Problem

In addition to recruiting qualified candidates, organizations also say they have a hard time hanging on to their existing security team members. Specifically, a whopping 66% of organizations admit they have difficulty retaining cybersecurity talent—and the current situation is poised to get even worse.[18]

> According to indeed, the typical tenure for an application security engineer is less than one year.[19]

One contributing factor to poor retention involves employee fatigue. Many security staff face daily pressure with some of the cited reasons including aggressive delivery schedules, a backlog of tasks, inefficient workflows, and having to cover for other staff vacancies. Because of the high stress and overburdened workloads of most cybersecurity positions, burnout is a very serious factor that impacts staff retention.[20]

Most cybersecurity salaries are also constrained at present.[21] Reduced supply of skilled security staff offers a competitive advantage to companies with deeper pockets (such as those in the banking and financial sectors) that can poach top talent by offering higher salaries and other perks. Companies that cannot compete by increasing financial incentives are at a disadvantage.[22]

> Some larger companies have gone so far as to offer new hires double their previous pay to lure them away from their current employers.[23]

Overcoming Outdated Modes of Application Security

The skills shortage battle is unwinnable if the only approach used is to hire more and more highly trained application security specialists to deal with mounting security problems. There will never be enough "experts" to throw at these kinds of problems. The issues must be approached from many different perspectives,[24] such as decreasing the skill needed to be an expert.

Organizations require an alternative, one that bridges the gap between the available skill sets. Specialized application security specialists are expensive to find and retain. Application security must evolve, just as software development life cycle approaches, accelerating to support Agile and DevOps while delivering the accuracy and speed demanded by digital transformation. Application testing must eliminate the complexities of legacy scanning models—while enabling other people to fill the current cybersecurity expertise gap with the skills that they do have. In doing so, application security becomes a business enabler and not an inhibitor to modern software development life cycles.

[1] "2020 Application Security Observability Report: Connecting Vulnerability and Threat Analysis with Real-World Implications in Applications and APIs," Contrast Security, July 2020.

[2] Ibid.

[3] "2020 Data Breach Investigations Report," Verizon, May 2020.

[4] "The State Of Application Security 2020," Forrester, May 4, 2020.

[5] "2020 Application Security Observability Report: Connecting Vulnerability and Threat Analysis with Real-World Implications in Applications and APIs," Contrast Security, July 2020.

[6] "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," Rand Corporation, accessed June 1, 2020.

[7] "Think Fast: Time Between Disclosure, Patch Release, and Vulnerability Exploitation—Intelligence for Vulnerability Management, Part Two," FireEye, April 13, 2020.

[8] "Application security and your career: 5 key areas to focus on," TechBeacon, January 22, 2020.

[9] "Fortinet Survey Finds Widespread Impact from Cybersecurity Skills Shortage," Fortinet, May 22, 2020.

[10] "AppSec Instrumentation Addresses AppSec Skills Shortage," Security Boulevard, March 9, 2020.

[11] "Survey: CIOs Struggle to Understand Legacy Architecture, Reduce Software Maintenanceand Fix Costs," Globe Newswire, October 2, 2018.

[12] "AppSec Instrumentation Addresses AppSec Skills Shortage," Security Boulevard, March 9, 2020.

[13] "State of Cybersecurity 2020," ISACA, June 2020.

[14] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study 2019," (ISC)2, November 2019.

[15] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study 2019," (ISC)2, November 2019.

[16] "State of Cybersecurity 2020," ISACA, June 2020.

[17] "State of Cybersecurity 2020," ISACA, June 2020.

[18] "State of Cybersecurity 2020," ISACA, June 2020.

[19] "Application Security Engineer Salaries in the United States," Indeed, July 13, 2020.

[20] "Preventing Cybersecurity Employee Burnout and Churn: 6 tips for Managers," Security Boulevard, June 30, 2020.

[21] "Survey Finds Cybersecurity Salaries Constrained," Security Boulevard, January 2, 2020.

[22] "The War for Cyber Talent Will Be Won by Retention not Recruitment," Dark Reading, July 7, 2019.

[23] "Why Competing For New Talent Is a Mistake," Harvard Business Review, February 5, 2020.

[24] "Addressing the Cybersecurity Skills Shortage Through Upskilling and Retention," Security Magazine, December 3, 2019.

Contrast SECURITY

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com