Contrast
SECURITY

EXECUTIVE SUMMARY

2021 State of Application Security in Financial Services

A Challenge to Both Application Security and Development Teams

Contrast Security's 2021 State of Application Security in Financial Services Report is based on a comprehensive survey of development, operations, and security professionals and technology executives at enterprise-level financial services institutions. It explores the state of application security at 250 organizations, and the findings indicate it is a work in progress at most of them—for both application security and development teams.

This state of affairs comes at a time when banks, insurance companies, and investment firms are in the crosshairs of increasingly sophisticated attacks by adversaries. Bad actors now deliver ransomware that not only locks up systems but also exfiltrates data for sale on the dark web. They steal data for financial fraud against the institutions themselves, the government, and other players. Many of these attacks—including 39% of data breaches according to the latest Verizon Data Breach Investigations Report—now target the application layer as digital services become a growing part of every business's bottom line.

Six Application Security Trends in Financial Services

Based on analysis of the survey data, Contrast Labs identified six insights about application security at financial services institutions:

1. DEVOPS IS MATURING

Organizations represented in the survey have at least 5,000 employees, and their software development operations are highly streamlined. More than 7 in 10 (71%) say that more than three-quarters of their applications in development use Agile or DevOps methodologies. Nearly two-thirds (65%) indicate they release code into production multiple times per day.

Most respondents are cognizant of the application security risk brought to their organizations due to the breakneck speed at which developers crank out new code and release it. Three-quarters report that their application security budget increased for 2021, and 24% said that the increase was more than 25%.

71%

use Agile/DevOps for at least three-quarters of applications in development

65%

release code into production multiple times per day

75%

saw an application security budget increase in 2021

2. APPLICATION SECURITY IS LESS MATURE

The speed and efficiency of DevOps have unfortunately not been replicated when it comes to application security. It is concerning that only one-quarter of organizations are capable of reviewing all alerts in scan reports and returning guidance for remediation to the development team—a fairly basic function that presents significant risk when it is not fulfilled.

One likely reason for this is that only 15% report their application security and development tools are fully integrated. The result of a disaggregated architecture is a lack of full observability, an inability to automate security processes, and a higher likelihood that serious vulnerabilities will fall through the cracks. Tellingly, only 3% of organizations have full observability across their application programming interfaces (APIs), and only 24% can prioritize vulnerability remediation according to the risk posed every time. Just as concerning, only 5% have full visibility into licensing risk for open-source libraries and frameworks.

25%

Only 25% can review all alerts and pass them back to the development team

15%

Only 15% have application security tools fully integrated with development tools

5%

Only 5% always have continuous knowledge of open-source licensing risk

3. APPLICATION SECURITY PROCESSES SLOW DEVELOPMENT CYCLES

These inefficiencies create bottlenecks for the development process. More than 6 in 10 (64%) respondents say that application security processes slow release cycles at least some of the time. Scans by static application security testing (SAST) and dynamic application security testing (DAST) tools are done at least twice a week at most organizations, and 79% of respondents say that more than half of SAST alerts are false positives. False positives continue into production, with a majority of respondents seeing more than six per application per year.

64%

say application security processes slow release cycles at least sometimes

79%

say more than half of SAST alerts are false positives

4. STAFF TIME IS WASTED WITH APPLICATION SECURITY

These inefficiencies also burn staff time at an alarming rate—for both security and development teams. Each true vulnerability found in various tests takes more than 16 hours of staff time for a large majority of respondents—six or more hours for the security team and 10 or more for developers. A vast majority of respondents (81%) say that each false positive consumes at least three hours for the security team. These hours add up quickly, as a single scan may contain hundreds of alerts.

The time sinks do not stop once an application is in production. A majority of respondents say that the security operations team spends at least 20 hours, and the development team spends at least 15 hours, to remediate each vulnerability found in production. Compliance reporting adds to these wasted hours: 87% of respondents say that each report consumes at least 40 hours of staff time, and 68% of organizations have more than 10 compliance reports per year.

52%

say application security professionals spend 3+ hours per false positive

72%

say that true vulnerabilities consume 6+ hours of application security team time

68%

say that true vulnerabilities consume 10+ hours of development team time

72%

say that vulnerabilities found in production consume 15+ hours of developer time

5. APPLICATIONS STILL HAVE TOO MANY VULNERABILITIES

Despite this huge time investment in application security, outcomes at these enterprises leave much to be desired. More than two-thirds (67%) of organizations have 20 or more serious vulnerabilities per application in development, and 48% have 10 or more serious vulnerabilities per application in production. The problem gets worse for larger organizations—even those that have a larger than average application security staff. APIs present similar risks: 44% said that more than one-quarter of their APIs have serious vulnerabilities.

67%

have 20+ serious vulnerabilities per application in development

48%

have 10+ serious vulnerabilities per application in production

6. APPLICATION ATTACKS REGULARLY OCCUR

Given these realities, it is concerning—but perhaps not surprising—that 98% of financial services institutions experienced at least three successful application exploits in the past year. More than half (52%) withstood 10 or more successful attacks. These attacks were more common at organizations with a higher number of serious vulnerabilities per application.

The cost of these attacks was significant. More than three-quarters of respondents (76%) revealed that each attack caused $1 million or more in damage on average. And 83% of respondents said each exploit consumed more than 100 hours of time by employees and outsourced personnel—with 41% putting that figure over 250 hours.

98%

had 3+ successful application exploits in 12 months

76%

suffered $1+ million in losses per exploit

Takeaways

Findings in the report paint a picture of an industry with significant room to grow regarding application security—both in practices and in outcomes. As attackers increasingly favor applications as an attack vector, organizations need true observability into vulnerabilities and attacks. They need to establish an infrastructure that enables them to have continuous visibility into application security across an entire portfolio of applications throughout the software development life cycle (SDLC) and into operations. Instrumentation enables this by providing insight from inside the application rather than outside. This virtually eliminates security-related coding delays while providing more complete protection against vulnerabilities and attacks.

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

Contrast
SECURITY

contrastsecurity.com