Contrast SECURITY

Lack of Security Observability Thwarts Application Security

A Lack Of Timely, Actionable Information Impedes Decision Making

Executive Overview

As applications become more important to almost every company, real-time, actionable data about an organization's application security posture—including information about vulnerabilities and attacks—is increasingly critical. Unfortunately, organizations using multiple legacy application security tools must do extensive manual work to generate such information. This lack of observability creates a number of problems. Organizations are unable to define granular metrics by which to measure the success of their application security efforts, and therefore are not aware of areas where they could be improved. This results in incomplete information for strategic planning and investment decisions.

It also impacts compliance, with staff members spending hours compiling audit reports and organizations deriving fewer business benefits from technical achievement of standards. Additionally, it hampers internal and external communications about application security—especially in a crisis situation such as an attack. Finally, it creates significant operational inefficiencies that pull security team members away from more strategic efforts.

As long as organizations lack security observability, they will continue to struggle with application security. The cycle of late identification of vulnerabilities, slow remediation, and mounting security debt will continue, and organizations will have trouble preventing intrusions that impact operations, brand reputation, and the bottom line.

As the economy becomes more digital, software has become increasingly important to the bottom line in virtually every industry. This trend was well underway before the COVID-19 pandemic began, and has accelerated since then.[1] Despite global economic decline and uncertainty because of public health-related shutdowns and travel restrictions, software engineers are nevertheless in even greater demand, at least in many parts of the economy.[2] Methodologies like Agile and DevOps and a growing use of open-source code[3] have helped software engineers work more efficiently in recent years. But despite these great strides, the fast-changing marketplace means that they face intense pressure to crank out software even more quickly.[4]

Unfortunately, this pressure for speed can create cybersecurity risk for organizations. One report found that 43% of data breaches this past year were the result of a web application vulnerability—a figure that more than doubled over the previous year.[5] Similarly, another study found that 42% of companies that suffered a breach attributed the cause to a known but unpatched software vulnerability.[6]

THE NEED FOR TANGIBLE DATA

As they scramble to bolster their application security, what organizations need more than anything else is real-time information—a comprehensive view of the current application security posture and how it can be improved. This is sometimes called security observability. Unfortunately, reports from most legacy application security tools are so complex that they require application security experts to interpret them. Furthermore, organizations that use multiple application security tools must aggregate the data between those tools—often manually—in order to create a comprehensive report. Even if a workable report template can be developed, it may not be possible to populate it with real-time information. In addition, critical details may be missing, or its graphical format may work against the principle of observability. This lack of a single source of timely, actionable information about application security vulnerabilities creates struggles in several areas:

> "Because legacy SAST, DAST, and pen testing only provide a snapshot in time, they can't keep up with today's agile software development life cycle processes." [7]

Organizations do not Know What is Working—and What is not

As the old business adage goes, "What gets measured gets improved." A lack of observability inhibits accurate measurement of current application security practices, both in the short term and over time. The result can be that organizations often have no idea which tools and practices are successful—and which are not. The CISO has no way to justify which application security investments are most effective, and security and development teams have no insight into changes in practice that could improve security.

REDUCING SECURITY DEBT IS DIFFICULT

The inability to accurately measure an organization's application security efforts also makes it more difficult to reduce security debt. Every organization should have the goal of eliminating their backlog of unaddressed vulnerabilities, but many do not even have an inventory of what needs to be done. Recent research indicates that organizations with above-average security debt tend to have more new vulnerabilities in applications in development—183 vulnerabilities per month, compared with 68 for those with below-average security debt.[8]

The result is that even if vulnerabilities are still discovered before an application is released into production, they are discovered later in the process—lengthening the time required for remediation. At the same time, higher mean time to remediation (MTTR) keeps security debt high and increases the chance that vulnerabilities slip into production and/or late-stage remediations delay the launch of applications.

> "Ideally, our developers work at a high speed, and the security team investigates and analyzes vulnerabilities as they occur. But when we have a rush of work, this is not actually happening." [9]

Strategic Planning is Difficult

Organizations trying to mature their application security efforts typically aim to "shift left" by discovering vulnerabilities earlier in the development process.[10] This is important because the later a vulnerability is discovered, the greater the cost of fixing it. In fact, one analysis found that compared with remediation in the design phase, the cost goes up sixfold if the vulnerability is found during implementation, fifteenfold if it is detected in testing, and hundredfold if identified in production.11 Another less emphasized priority is to "shift right" to identify vulnerabilities and prevent attacks for applications in production.[12]

Accomplishing these priorities is virtually impossible without accurate, timely, and actionable information. If this data is not available, operational improvements like more timely scanning, developer training on avoiding vulnerabilities, and strategic resource allocation are based on mere guesswork. Likewise, decisions on areas of new investment will not benefit from understanding of the "big picture" on the part of decision-makers.

> "[T]here are two tracks to pursue: how to measure risk in a way that informs action, and how to use metrics to train the development staff in ways that prevent the Creation of new vulnerabilities." [13]

Demonstration of Compliance is Complicated

Without a centralized platform and a single source of truth, it is virtually impossible for an organization to know whether it is compliant with the various regulations and standards that touch application security. Demonstrating that compliance to auditors is an even more difficult hurdle. Organizations that use multiple legacy application security tools must find a way to correlate the data and dependencies from the different tools into a single report that contains all the information of interest to auditors. In many cases, this work must be done manually, consuming many hours of staff time.

STRICTER REQUIREMENTS ARE A BURDEN—AND AN OPPORTUNITY

This is a real problem, as organizations with geographic reach must demonstrate compliance with a patchwork of cybersecurity regulations in various jurisdictions, and in many cases, industry-specific and company-mandated standards. And those requirements are getting more stringent. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework recently released new guidelines that directly impact application security.[14] Since that organization has become the default standard for the public and private sectors in the United States, other standards are likely to add these guidelines soon.

While increased compliance mandates can feel burdensome to already overwhelmed security teams, they represent an opportunity to truly make applications safer at an organization—if they are viewed as more than a checkbox. Investments in the name of compliance with a required standard may be looked upon more favorably by the CFO than those with a more amorphous goal.[15]

> "[T]here are many opportunities to leverage compliance requirements to build substantial and mutually beneficial processes and procedures that... [Fill] in security gaps that increase risk." [16]

Timely Communications can be Hampered

Another consequence of a lack of observability is that communications are negatively impacted, both across an organization and with the outside world. The reports that legacy application security tools produce are often difficult for a security team member without application security testing experience to interpret—let alone a rank-and-file employee. And when multiple tools are involved, no one can interpret the overall application security posture without help from multiple experts.

This means that the application security team must "translate" this information to IT leadership, the development team, executive management, and the overall employee base—all of whom need different mixes of information to understand what should be done. In some companies, communicating with the development team specifically may present challenges, as coding delays caused by application security processes often cause the relationship between the two teams to be frayed.

This translation can potentially be done manually for routine status updates, but crisis communication in the event of an intrusion may not allow for that much time. Without continuous observability, compiling the data necessary to keep the company informed in a crisis might result in the communication being out of date by the time it is sent out. And providing outdated information to the general public via the media and social media channels can degrade brand value.

44% Of companies have delayed moving an application into production due to security concerns. [17]

ORGANIZATIONS STRUGGLE WITH OPERATIONAL INEFFICIENCY

Legacy application security testing practices bring myriad inefficiencies to both developers and security team members.[18] A lack of observability adds to that friction by slowing every phase of the development process. The length of time required for scans to be completed—and interpreted by application security team members—means that significant additional coding has occurred by the time earlier vulnerabilities are identified. And as developers move into the testing phase of a project, they may not even know how many vulnerabilities still need to be addressed, and how risky they are, because of these delays.

From the application security team's perspective, the large number of false positives generated by legacy application security tools mean that reports must be reviewed line by line before accurate information can be reported to anyone—a process that consumes an hour of staff time per alert.[19] And application security professionals often must do hours of work to correlate data between different tools to inform executive management as to an organization's application security posture. All of these inefficiencies mean that vulnerability information is not timely, and vulnerabilities are identified too late in the process.

> "While cybersecurity requires the latest technology and solutions, operational efficiency is a key determinant of its overall effectiveness." [20]

Conclusion

Organizations that lack application security observability are positioned to have ongoing struggles. Without real-time, comprehensive visibility into the entire application security architecture, identification of vulnerabilities will be delayed, and dangerous vulnerabilities will slip into production. It is exceedingly difficult to set benchmarks by which application security can be measured and to make strategic plans for improving them. It also complicates compliance and increases the likelihood of noncompliance. It also impedes communications about application security issues with stakeholders across the organization. And it exacerbates operational inefficiencies that already exist with legacy application security tools.

Unfortunately, full observability is impossible for organizations that use multiple legacy application security tools. Even with a sophisticated reporting template that pulls data from the different solutions, extra work must be done to eliminate false positives from the report and make the data digestible for different roles in the organization. But an integrated platform approach with robust reporting capabilities can result in customized, real-time information for application security team members, executive management, and the general employee base—in a format that is clear and actionable.

> "With the software development ground shifting, it's time for application security teams to get a move on—from appsec after the fact to secure code throughout the software development life cycle." [21]

Contrast SECURITY

[1] "COVID-19 Is Accelerating the Rise of the Digital Economy," BDO, May 2020.

[2] Maayan Manela, "COVID-19 cutbacks? No one told the software industry, salaries see a boost despite the pandemic," CTech, September 7, 2020.

[3] Forrester found a 40% increase in the use of open-source code in one year; see Amy DeMartine and Jennifer Adams, et al., "Application Security Market Will Exceed $7 Billion By 2023," Forrester, updated March 29, 2019.

[4] "The State of DevSecOps Report," Contrast Security, December 2020.

[5] "2020 Data Breach Investigations Report," Verizon, April 2020.

[6] "The State of Vulnerability Management in the Cloud and On-Premises," Ponemon Institute and IBM, August 17, 2020.

[7] Jeff Williams, "SAST, DAST, and IAST: Why the Difference Matters," Contrast Security, May 1, 2019.

[8] "Contrast 2020 Application Security Observability Report," Contrast Security, September 2020.

[9] Survey Respondent (cloud architect in the technology industry), cited in "The State of DevSecOps Report," Contrast Security, December 2020.

[10] Jakob Pennington, "Shifting Left: DevSecOps as an Approach to Building Secure Applications," Medium, July 18, 2019.

[11] Mukesh Soni, "Defect Prevention: Reducing Costs and Enhancing Quality," iSixSigma, accessed April 9, 2020.

[12] Alan Shimel, "DevOps Chat: Shifting Security Left and Right, With Contrast Security," Security Boulevard, October 7, 2019.

[13] Rob Lemos, "5 application security metrics that should matter to your team," TechBeacon, accessed November 16, 2020.

[14] Derek Rogerson, "What You Need to Know About the New IAST and RASP Guidelines in NIST 800-53," Contrast Security, March 19, 2020.

[15] Matt Kelly, "The Business Case for Compliance, Even Now," Security Boulevard, May 18, 2020.

[16] "AppSec for the Newly Hired CISO/CSO," Contrast Security, October 2020.

[17] "The State of Container and Kubernetes Security, Winter 2020," StackRox, accessed March 20, 2020.

[18] "A Major Roadblock To Business Innovation," Contrast Security, May 2020.

[19] "The State of DevSecOps Report," Contrast Security, December 2020.

[20] Albert Zhichun Li, "Security Success Is Based On Operational Efficiency," Forbes, October 28, 2020.

[21] John P. Mello Jr., "The state of application security testing: The shift is on to secure code," TechBeacon, May 11, 2020.

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