Contrast SECURITY

Advanced Threat Landscape and Legacy Application Security Ratchet Up Risk

Executive Overview

Today, software vulnerabilities continue to be the prime target of cyberattacks.[1] One of the foremost reasons is the acceleration of application development due to the adoption of Agile and DevOps. More applications and application programming interfaces (APIs) create a much larger attack surface. Cyber criminals recognize the opportunities to exploit a broader number of vulnerabilities, and the volume, velocity, and sophistication of attacks are increasing.

But legacy AppSec tools cannot keep pace with the speed of modern software development and the advanced threat landscape. As a result, successful exploits of application vulnerabilities skyrocketed over the past year, and there is no indication of an abatement.

Applications are Under Attack

To remain competitive in the race to digital transformation (DX), organizations are quickly accelerating application development. Agile and DevOps enable them to hasten release cycles—going from once a month to as many as several per day. This greater agility and velocity creates significant business advantages. Applications are critical in transforming customer experiences, lowering costs, and creating new revenue opportunities. And as enterprises emerge from COVID-19 lockdowns, all signs indicate budgets and resources around DX initiatives are increasing while most other business areas are being slashed or at least reduced.[3]

> “43% of all breaches are now the result of an application vulnerability.[2]

All of this focus on application development increases the application attack surface. More applications, more connections and transactions, more data, and more APIs provide cyber criminals with an attack surface with a growing number of vulnerabilities to exploit. It thus is no surprise that Verizon reported a doubling of data breaches over the past year that are tied to application vulnerabilities—representing 43% of all data breaches.[4]

Why are applications being targeted? When attackers exploit a web application vulnerability, they have potentially unlimited access. Malicious attackers who exploit an application through a

Contrast SECURITY

vulnerability or weakness will also have access to the data to which the application has access, no matter what data security or network protections are in place.[5] Much of the data contained in many applications is valuable—often personally identifiable information (PII) linked to employees, partners, and customers. They also provide a gateway for cyber criminals to gain access to other data sources within the network—product details, marketing strategies, and other critical repositories of intellectual property (IP).

> 61% of organizations plan to accelerate their digital transformation spending because of Covid-19, with 64% planning agile IT delivery and DevOps projects.[6]

Application Attack Methods Increase in Volume, Velocity, and Sophistication

Cyber criminals are increasing the sophistication of their attack techniques and methodologies. Many target the expanded application attack surface—areas such as unsecured API endpoints, invalidated API payloads, and client-side malware injection into unprotected scripts.[7]

Following are some of the more prevalent examples of attack advancements that cyber criminals are using today:

BOTS INSTIGATE AN ARRAY OF NEW ATTACKS

Today's security teams find it difficult to distinguish between real users and fraudulent ones. Cyber criminals know this is the case, and they are employing sophisticated bots to mimic human behavior. On average, bots comprise about 62% of traffic hitting websites and web applications, 24% of which would be deemed safe, while the other 38% are hostile. In other words, more than one-third of average traffic across a website or web application typically consists of harmful bots.[8]

Malicious bots frequently carry out automated attacks against the public-facing APIs and web applications. They hijack and create fake accounts, perform web scraping and distributed denial-of-service (DDoS) attacks. A recent report finds that 60% believe their organization's web-based applications are the primary target of automated attacks.[9]

BRUTE-FORCE ATTACKS BREAK OPEN DOORS TO ORGANIZATIONS

Cyber criminals are becoming increasingly sophisticated in how they use brute-force attacks on applications. The intention is to target authentication protocols to gain access to an application, which is then used to discover hidden content and/or pages within the application.

The attack starts with the identification of the target. Afterwards, the attacker uses several repetitive trial-and-error attempts to break into an application. As an example, an application can be attacked via brute force by taking a word list of known pages from a popular content management system. Then, the attacker uses the list to request each known page, and by analyzing the HTTP response code, is able to determine if the page exists on the target server.[10]

As quarantines spread across the globe due to Covid-19, the number of brute-force attacks on remote desktop protocol (RDP) rose dramatically.[11]

Speed of Exploits Surpasses Legacy Application Security

The use of bots, brute force, and other advanced attack techniques makes it increasingly difficult to protect application vulnerabilities. Over the past year, individual applications averaged more than 13,000 attacks each month.[12] This is an increase over the past year, with one report pegging a spike of 52%.[13] The growing volume and velocity of attacks places more pressure on development and security teams to remediate vulnerabilities in development, and operations teams to quickly diagnose, triage, and remediate vulnerabilities found in production.

For applications in production, the time from successful exploitation to compromise takes a matter of minutes in three-quarters of cases.[14] However, for most security operations teams, response can take hours, days, or even weeks. Successful exploits can wreak havoc until this window is closed and the breach is remediated.

On average, it takes an organization 15x longer to close a vulnerability than it does for attackers to weaponize and exploit one—seven days to weaponize versus 102 days to patch.[15]

TOP VULNERABILITY ATTACK VECTORS FOR WEB APPLICATIONS:[16]

65%	–	SQL Injection	62%	–	Broken Access Control
54%	–	Cross-site Scripting	51%	–	Command Injection

ZERO-DAY ATTACKS CHALLENGE LEGACY SECURITY SCANNING APPROACHES

Zero-day attacks target previously unknown vulnerabilities. They comprise upwards of 50% of all malware today—a number that continues to rise.[17] The problem is that legacy application security scanning models use signatures to identify vulnerabilities. As a result, they miss unknown vulnerabilities, or false negatives. This exposes applications to risk when they are deployed into production. They also increase the amount of security debt carried by the application.

One-half of attacks today are zero day, targeting previously unknown vulnerabilities.

Legacy Application Security Approaches Cannot Keep Pace

The underlying technology core for legacy application security solutions was built two decades ago, and as a result, they simply cannot scale to support modern software. The data corroborates this claim: The number of vulnerabilities per application is the same today as it was in 2000 at 26.7 vulnerabilities.[18]

Following are some of the most predominant reasons legacy application security is failing when it comes to protecting applications from advanced attacks.

The number of vulnerabilities per application is the same today as it was in 2000 at 26.7 vulnerabilities.

FALSE POSITIVES CREATE HIGHER APPLICATION RISK

Because application scanning and vulnerability management processes reside outside of software, they must often guess at whether a suspected vulnerability poses risk. This results in huge numbers of false positives—in both development and production environments.

In development, developers and security specialists are inundated with alerts that—after triaged and diagnosed—turn out to be false positives. In addition to delaying digital innovation and release cycles and impacting efficiencies, these false positives create alert fatigue. This, in turn, leads to higher risk, as developers and security specialists can ignore alerts they believe to be false positives that are actually real threats. With attack volumes and velocity at higher levels, this results in greater risk.

In production, security operations teams face similar circumstances. Traditional perimeter defenses such as web application firewalls sit outside of the application and must guess at whether attacks can connect with a vulnerability. This produces significant volumes of false positives that consume valuable time triaging and diagnosing—an undertaking that is dramatically more time-consuming and arduous once an application is in development.

Over one-third of development, operations, and security teams indicate that between 25% and 50% of vulnerability alerts are false positives.[19]

ACCUMULATION OF SECURITY DEBT INCREASES RISK

The time it takes organizations to remediate application vulnerabilities in development and production is directly tied to the amount of risk that applications pose. For legacy application security approaches, vulnerabilities can fester for months—research from one static application security testing (SAST) provider locates the median time to remediate at 121 days.[20] This accumulation of security debt—namely, the longer a vulnerability exists—increases the likelihood that a vulnerability will not be fixed and slip into production. Accordingly, research by Contrast Labs shows that organizations with below average security debt have a 1.7x better risk posture than organizations in general.[21]

MANUAL VULNERABILITY MANAGEMENT RESULTS IN GREATER RISK

Manual vulnerability management is a significant problem for many organizations. Time-consuming vulnerability scanning and remediation processes burn valuable development cycles. Couple this with alert fatigue from the overload of false positives, and many developers reach a breaking point.

As a result, when faced with meeting release cycle deadlines or remediating every vulnerability, many developers opt for the former. For example, almost 50% of security professionals report that they struggle to get developers to make vulnerability remediation a priority.[22] But this can create serious security gaps, especially because attacks are on the rise and cyber criminals are becoming increasingly more sophisticated in their attack techniques.

GROWING USE OF OPEN-SOURCE FRAMEWORKS AND LIBRARIES

Business requirements for more applications and updates to existing applications, along with faster development cycles, is rapidly accelerating the use of open-source software (OSS). For example, Forrester finds that the use of open-source code in applications jumped 40% in the last year.[23] Further, upwards of 80% of applications contain open-source frameworks and libraries, with the average application containing 32 different libraries.[24] Applications might be built from as much as 90% open-source code.[25]

Despite its many advantages, open source contains vulnerabilities (Common Vulnerabilities and Exposures [CVEs]) that can pose serious risk. And with the number of CVEs in open source growing 50% year over year, this expanded attack surface offers cyber criminals greater opportunities for a successful application exploitation.[26]

Summing Up Application Risk

Organizations must heed the warnings when it comes to their application security posture. First, an increased focus on digital transformation and application development exposes a much larger application attack surface. Second, this has not gone unnoticed, with cyber criminals using more advanced attack techniques to exploit application vulnerabilities. Third, legacy application security approaches are not built for modern software and fall short in detecting and remediating vulnerabilities in development and then protecting applications in production.

For each of these reasons, application vulnerabilities can pose a serious risk to organizations. With the number of data breaches doubling this past year and the average cost of a data breach pegged at $3.92 million and increasing—12% over the last five years—the importance of application security has never been more important.[27]

1 Sandy Carielli, et al., "The State Of Application Security, 2020," Forrester, May 4, 2020.

2 "Verizon 2020 Data Breach Investigations Report," Verizon, May 2020.

3 "Thriving in the New Normal: How IT Operations Leaders Can Deliver Business Value in an Economic Slowdown," OpsRamp, May 2020.

4 "Verizon 2020 Data Breach Investigations Report," Verizon, May 2020.

5 Sandy Carielli, et al., "The State Of Application Security, 2020," Forrester, May 4, 2020.

6 "Thriving in the New Normal: How IT Operations Leaders Can Deliver Business Value in an Economic Slowdown," OpsRamp, May 2020.

7 Josh Zelonis, et al., "Top Security Threats In 2020," Forrester, January 24, 2020.

8 Eyal Hayardeny, "The Hidden Dangers of Malicious Bots," CPO Magazine, March 13, 2020.

9 Byron Mühlberg, "Automated Attacks Surge as Malicious Bots Take Center Stage," CPO Magazine, May 22, 2020.

10 "Brute Force Attack," OWASP, accessed June 26, 2020.

11 Jessica Davis, "COVID-19 Remote Work Causes Spike in Brute-Force RDP Cyberattacks," HealthITSecurity, April 30, 2020.

12 "2020 Application Security Observability Report: Connecting Vulnerability and Threat Analysis with Real-world Implications in Applications and APIs," Contrast Security, June 2020.

13 "2020 SonicWall Cyber Threat Report," SonicWall, 2020.

14 "Take the Lead on Cyber Risk," Deloitte, 2017.

15 Richard Melick, "Mean Time to Hardening: The Next-Gen Security Metric," Threatpost, December 30, 2019.

16 "2020 Application Security Observability Report: Connecting Vulnerability and Threat Analysis with Real-world Implications in Applications and APIs," Contrast Security, June 2020.

17 "As malware and network attacks increase in 2019, zero day malware accounts for 50% of detections," Help Net Security, December 13, 2019.

18 "Malware and ransomware attack volume down due to more targeted attacks," Help Net Security, February 5, 2020.

19 "Application Vulnerabilities and False Positives," Contrast Security Webinar Poll, June 2020.

20 "2020 Application Security Observability Report: Connecting Vulnerability and Threat Analysis with Real-world Implications in Applications and APIs," Contrast Security, June 2020.

21 Ibid.

22 Suri Patel, "2019 Global Developer Report: DevSecOps finds security roadblocks divide teams," GitLab, July 15, 2019.

23 Amy DeMartine, et al., "The Application Security Market Will Exceed $7 Billion By 2023," Forrester, updated March 29, 2020.

24 "2020 Application Security Observability Report: Connecting Vulnerability and Threat Analysis with Real-world Implications in Applications and APIs," Contrast Security, June 2020.

25 Ian Folau, "Rethinking your open source use policy," InfoWorld, January 2, 2018.

26 Zeljka Zorz, "Number of open source vulnerabilities surged in 2019," Help Net Security, March 13, 2020.

27 "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, accessed June 26, 2020.

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