WEB APPLICATIONS AND APPLICATION PROGRAMMING INTERFACES (APIS) PLAY A PIVOTAL ROLE IN MODERNIZING THE DELIVERY OF SERVICES AND COMMUNICATION BETWEEN CITIZENS AND GOVERNMENT AGENCIES. HOWEVER, ACCORDING TO VERIZON’S ANNUAL DATA BREACH STUDY, WEB APPLICATIONS HAVE BECOME A PRIMARY POINT OF ATTACK BY HACKERS.

FOR PUBLIC SECTOR ORGANIZATIONS THAT HAVE MODERNIZED USING WEB APPLICATIONS, IT HAS BECOME CRITICAL TO MOVE BEYOND PERIODIC OR POINT-IN-TIME VULNERABILITY REVIEWS AND IMPLEMENT AUTOMATED APPLICATION SECURITY PROGRAMS TO BOLSTER THE DEFENSE AGAINST RISING CYBER INCIDENTS.

GOVERNMENT ORGANIZATIONS FACE UNIQUE CHALLENGES THAT SET THEM APART FROM THE PRIVATE SECTOR. LONG-LIVED LEGACY SYSTEMS WITH WEB INTERFACES AND APIs OF VARYING VINTAGE WOVEN IN CREATE HURDLES WHEN IMPLEMENTING TIMELY UPDATES AND PATCHES TO ENHANCE SECURITY. UNLIKE COMMERCIAL SECTORS THAT CAN ADOPT TECHNOLOGY IMPROVEMENTS RELATIVELY QUICKLY, GOVERNMENT AGENCIES OFTEN STRUGGLE TO KEEP PACE DUE TO THEIR RELIANCE ON OLDER APPLICATIONS OR SYSTEMS. HOWEVER, AGENCIES CAN BEGIN TO ADDRESS NEW AND EMERGING THREATS BY SEEKING A MORE THOROUGH UNDERSTANDING OF THE ATTACK LANDSCAPE AND ACQUIRING AVAILABLE TOOLS ESSENTIAL TO NAVIGATE THESE CHALLENGES.

“WE NEED A COMPREHENSIVE UNDERSTANDING OF ANY POTENTIAL ATTACK SCENARIOS AT PLAY; WE NEED TO UNDERSTAND WHO HAS ACCESS TO THESE APPLICATIONS, THE NATURE OF THESE APPLICATIONS THEMSELVES AND THEIR SENSITIVITY LEVELS, AND THEN TAILOR OUR DECISIONS ACCORDINGLY. THE CHALLENGE MAGNIFIES WHEN DEALING WITH LEGACY SYSTEMS, AS THEY RESIST EASY MODIFICATIONS OR SWIFT UPDATES,” SAYS INVICTI SECURITY CHIEF TECHNOLOGY OFFICER FRANK CATUCCI.

“IDENTIFYING ALL THE POTENTIAL VULNERABILITIES IS CRITICAL AS MORE AND MORE APPLICATIONS MOVE TO THE WEB AND INTO A MUCH MORE EXPOSED STATE.”

SYNCHING SECURITY WITH DEVELOPMENT

BECAUSE APIs ACT AS GATEWAYS TO VALUABLE DATA, THEY’VE EVOLVED INTO SIGNIFICANT ATTACK SURFACES. DEVELOPERS INCREASINGLY RELY ON APIs IN THEIR APPLICATIONS, SO THE NEED FOR SOLUTIONS THAT EFFICIENTLY IDENTIFY VULNERABILITIES WITHIN APIs HAS BECOME CRUCIAL.

THE AVERAGE DATA BREACH COST IN 2023 IS $4.45 MILLION; TO STAY AHEAD OF THOSE POTENTIAL COSTS, PERIODIC SCANNING OF WEB APPLICATIONS AND APIs IS INSUFFICIENT. MODERN WEB APPLICATION DEVELOPMENT REQUIRES A STRATEGY THAT BALANCES SPEED, ACCURACY AND INCREASED TESTING FREQUENCY.

“We need a comprehensive understanding of any potential attack scenarios at play; we need to understand who has access to these applications, the nature of these applications themselves and their sensitivity levels, and then tailor our decisions accordingly. The challenge magnifies when dealing with legacy systems, as they resist easy modifications or swift updates.”

Frank Catucci
Chief Technology Officer
Invicti Security
The average data breach cost in 2023 is $4.45 million.

To stay ahead of those potential costs, periodic scanning of web applications and APIs is insufficient. Modern web application development requires a strategy that balances speed, accuracy and increased testing frequency.

“The deliveries of modern applications are moving at a much greater, more frequent cadence, meaning that we’re not releasing the software once a quarter or once a year, like our more legacy applications. We’re releasing multiple times a day for the more modern types of applications and APIs. So, with that, we really need to look at this from a different perspective,” explains Catucci.

“Modern applications are going to have a different threshold, meaning that things are changing multiple times a day in a rapid fashion. We cannot wait for those point-in-time scans. To accommodate this rapid pace of change, there needs to be a shift in perspective towards integrating security practices into DevOps processes,” he adds.

Adopting solutions that integrate into the software development cycle (SDLC) — like dynamic application security testing (DAST), interactive application security testing (IAST), or software composition analysis (SCA) — provides comprehensive coverage for applications in development and production, yielding accurate results and reducing manual work.

And these testing solutions are not a one-and-done effort. As code changes or evolves, new vulnerabilities can appear, and old ones re-emerge, making regular and automated testing a necessity. According to Invicti’s AppSec Indicator, “Scanning has been steadily increasing year-over-year since 2019. There was a 50% increase in scan frequency per account over the last four years, showing a trend of companies scanning more internal and external web apps and APIs at a greater frequency as they expand security testing left (in development) and right (in production testing).”

Additionally, the report found that while the scanning increased, there was a decrease in the percentage of severe vulnerabilities, dropping nearly 20% in 2022. The data indicates that dedicating resources to enhance application security programs that incorporate scanning or testing at various stages of the SDLC is yielding positive results. The uptick in scan frequency led to a decline in scans revealing critical vulnerabilities, according to the report. Consequently, this lowers the risk of exposure for organizations. And as the pace of software development accelerates, application security initiatives should embrace a dual approach — expanding security measures to both earlier and later stages of the development cycle to mitigate the potential of data breaches.

Advantages of scalable security testing tools

DAST, a technology-agnostic testing method that doesn’t require source code access, is particularly important for securing web environments encompassing both legacy and modern applications. This is valuable for government organizations, where application lifecycles tend to stretch longer than in commercial contexts, and where systems and processes can be siloed to the point that it’s hard even to start a conversation about a standard security solution.

By incorporating testing with proof-based assessments into the development pipeline, organizations can improve security over time, detecting vulnerabilities before they impact production. The proof is in the numbers: According to Invicti’s research, proof-based scanning can confirm 94% of major exploitable vulnerabilities with 99.98% accuracy. Proof-based scanning cuts through this uncertainty by showing which issues are real and exploitable and cannot be false positives. This eliminates guesswork and manual work, enabling the move to fact-based web application security at any scale.

Additionally, agencies should look at solutions offering flexible deployment options across diverse environments — whether on Windows or Linux systems; containerized deployment using tools like Docker and Kubernetes or software-as-a-service (SaaS) in the cloud; and hybrid configurations in between. This enables time-strapped teams to incorporate security into their existing environments and workflows, ensuring effective, consistent testing and centralized visibility.

Alleviating pain points from top to bottom

When equipped with the right modern solutions, AppSec engineers can conduct scans and share their findings with the DevOps team without having to directly engage in the more intensive tasks of validating and addressing those vulnerabilities. The value of these findings lies in their ability to determine whether a quick and standard solution suffices or if a more prolonged phase of investigation and iterative communication is necessary, spanning weeks or even months. Integrating this process seamlessly into the DevOps workflow yields cost savings by highlighting security concerns at their earliest stages. This proactive approach prevents the potentially expensive need to define, implement and retest fixes during later project phases.

Frank Catucci
Chief Technology Officer
Invicti Security
Converging traditional and cloud security
Another development Catucci is starting to see is the convergence between traditional application security and cloud security.

Many agencies are adopting cloud and containerized environments to gain scalable and on-demand bandwidth benefits over traditional on-premises networks. This has resulted in exponential migration to and development of web applications that are more easily supported in these types of environments. Consequently, ensuring their security requires web application and API security testing in pre-production and production settings.

Addressing this expansive landscape requires a holistic approach, encompassing people and processes. “AppSec is not new, cloud security is not necessarily new; leaders need to understand the convergence of bringing them together. You can’t have these two siloed groups working (apart) anymore,” says Catucci.

He explains that adapting security practices for agile, cloud-centric modern application development involves integrating security throughout the process, embracing zero trust principles and ensuring that people and processes are integral components of a comprehensive security journey.

Strategies for building a successful AppSec program
Securing application workloads calls for orchestration, automation and governance that can only be provided by modern web application security testing solutions. To accelerate those efforts, Catucci recommends that agencies:

- Partner with renowned commercial cybersecurity vendors to work with mature security solutions and ensure vendor support for smooth implementation, integration and customization.
- Embrace a DevSecOps approach with automated security testing and consider testing solutions like Invicti’s to effectively secure numerous websites, applications, and APIs.
- Understand attack surfaces by mapping cloud-based data, open-source components, and online resources, including maintaining a software bill of materials, to identify potential vulnerabilities and access points.
- Regularly update, test and maintain your incident response plan to identify and address gaps, ensuring cyber resiliency across various potential scenarios while implementing a comprehensive data backup policy and restoration testing to mitigate the risk of data loss effectively.
- Instill a culture where every employee and contractor recognizes their role as the first line of defense by prioritizing cybersecurity awareness and education as an integral part of your agency’s everyday operations.

Learn more about securing your application security posture in the long run.

This report was produced by Scoop News Group for FedScoop and DefenseScoop and underwritten by Invicti Security.