WHITEPAPER

NTT | Application Security

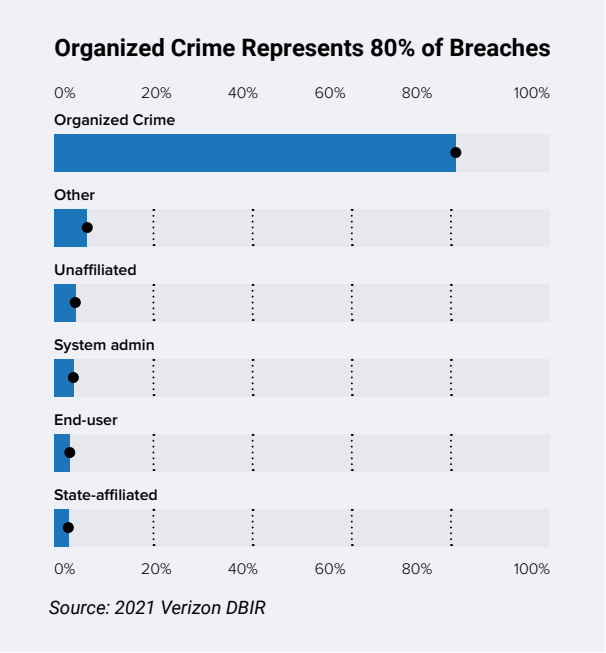
The Modern Approach to Application Security – Layered Security

The past three years brought forth a tremendous transformation in how we live and work. While the digital age has seen technological advancements in almost every area of business, the COVID-19 pandemic introduced a seismic economic shift. In response, organizations acted quickly to migrate almost every aspect of their business online, accelerating an almost complete digital transformation, seemingly overnight. Fundamental to this shift has been the adoption of critical technologies, namely web applications. Organizations that were able to innovate and invest in applications saw a competitive advantage as they adapted to the "new norm."

While business leaders heralded their successes in maintaining workforce productivity, operational agility and business profitability, they came face-to-face with the realities of organized cybercrime.

Almost immediately, these threat actors began attacking the very applications fueling those successes. Capitalizing on the global crisis and expanded attack surfaces, threat actors worked tirelessly to attack application vulnerabilities and evade traditional security measures.

Now that the pandemic has started to release its grip and organizations begin to adopt hybrid work models, one thing has remained top of mind for business leaders: getting proactive about their application security strategy, and the risk to their business by not doing so.

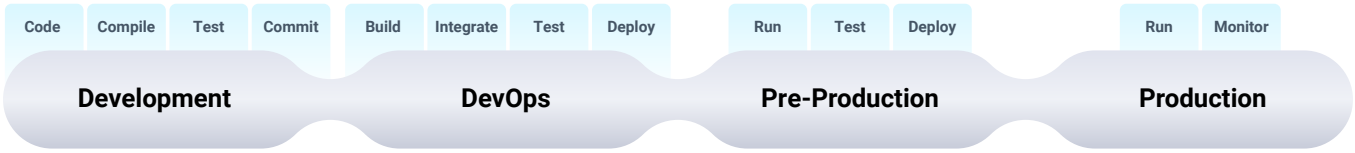


Source: 2021 Verizon DBIR

Current State of AppSec

In the post pandemic economy, organizations need to accelerate their application security to the speed of modern software development. Unfortunately, this "need for speed" requirement can often lead to vulnerabilities getting released. Once these vulnerabilities can be identified once in production, so begins the process by which developers must stop working on new projects to fix the vulnerabilities in live applications. Referred to as "context switching", this constant shift between projects impacts productivity by slowing workflows, reducing efficiency and can ultimately hinder overall system performance.

While there is an increased focus on enabling security earlier in development, organizations continue to face collaborative struggles between SecOps and DevOps teams and the functional roadblocks that result from each group operating within their respective processes, tools and KPIs. With each team owning a stage of software development, identifying and remediating security vulnerabilities can become obstacles to productivity and innovation.



In this traditional model, security is designated to a specific, isolated team in the final stages of development. And while this worked when development cycles operated under a monolithic application architecture, it is no longer viable following the wider adoption of Agile methodologies and development cycles. Now, teams can deliver software updates more often and in much shorter timeframes — sometimes multiple times per day.

Enter DevSecOps

In order to solve the aforementioned challenges to business operations and efficiency, organizations are increasingly adopting a DevSecOps model to address security earlier in the SDLC. . This approach creates a bridge between DevOps and SecOps by expanding collaboration between the two teams to effectively deliver more secure applications, all without affecting the speed and agility of development. Often referred to as "shifting left," this approach moves security testing to software developers and enables them to fix vulnerable code in near real-time, rather than "bolting security" on at the end of the SDLC. DevSecOps offers a holistic approach to security throughout the SDLC — from planning and design to coding, building, testing and release — with continuous, real-time feedback loops and insights.

While the DevSecOps approach is a valiant effort centered around the idea that security is "everyone's job", it is not without obstacles. The implementation of DevSecOps can bring about a variety of challenges across an organization: operationalizing a cultural shift, the realization of sub-par security knowledge and expertise and new, complex tool integrations to name a few.

To aid in the implementation of a successful program, application security vendors have offered various solutions that enable DevSecOps throughout the stages of organizations' CI/CD process. These solutions include Static Analysis Security Testing (SAST) and Software Composition Analysis (SCA) early in the development cycle, Dynamic Application Security Testing (DAST) for pre-production and production stage applications and Interactive Application Security Testing (IAST) for functional testing.

In "Collapsing Paradigms: Building AST from the Ground Up," we highlighted the challenges to modern application security that each of these traditional testing solutions pose, and elaborated on how the traditional approach of relying on a single point-product solution no longer meets the needs driven by agile development and rapid security fixes. Now, even if developers deliver secure code that is tested and validated by DevOps, vulnerabilities can still leave an application exposed after connecting to other third-party applications and APIs after going live in production.

While there are clear, definite challenges to these application security testing methodologies, there is another approach available — one that's already proven to be widely adopted and successful within network security teams.

A "Tried and True" Approach

In network security, the "layered approach" concept has become a widely accepted and successful strategy for reducing the risk of compromise. In the IT context of perimeter security, layered security is defined by deploying several independent layers of security solutions so that it is much harder for a threat actor to penetrate the network. If an attacker breaches one layer of security, there is another layer safeguarding the network and its resources. If this layer is breached, there is yet another that can prevent compromise. Also known as a "defense-in-depth" strategy, a layered approach is also centered around the simple premise that multiple layers of security provides multiple layers of protection.

While there are pros and cons to a layered security strategy on the perimeter, the benefits become clear when applied to application security.

Applying the Defense in Depth approach to AppSec

In applying the concept of a layered perimeter security strategy to application security, the debate over which application security testing method (i.e., SAST vs. DAST) becomes irrelevant. Rather than arguing the merits of one testing method over another, the layered approach stresses that organizations should adopt all methods. By adopting a layered security strategy and applying it to the SDLC, organizations can help improve efficiencies within the CI/CD pipeline, operationally test code where it is being developed and ensure its production applications are secure.

As *Figure 1* shows, the software development lifecycle model is continuous and is represented as an infinite loop. However, when applying application security testing to the model, gaps begin to appear when developers switch context from writing new code to fixing existing code. By implementing DevSecOps and leveraging purpose-built application security testing solutions designed specifically for each functional group, the SDLC is empowered by an infinite loop of security.

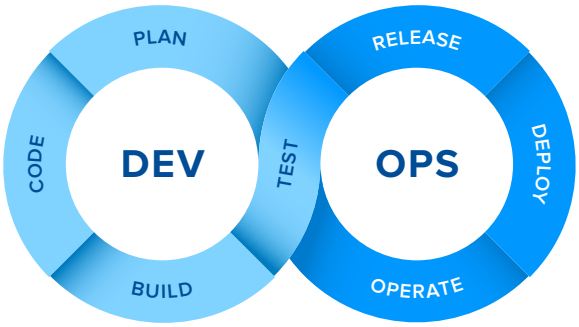


Figure 1: Software Development Lifecycle

When each functional group within the SDLC has the ability to test within their native environments, security vulnerabilities are identified earlier and more efficiently. Additionally, by applying purpose-built testing at the most critical inflection points of the SDLC, developers, DevOps and security teams become empowered with accurate and contextual security insights as they build, run and deploy web applications and APIs.

Whether through a managed security service provider or a self-service SaaS platform, organizations that adopt both DevSecOps and a layered approach to application security can fully realize the power that applications can bring to their business' productivity and bottom line.