WhiteHat Vantage Platform

Collapsing Paradigms: Building AST from the Ground Up

In today's evolving digital economy, applications have become the backbone of modern business. From delivering goods and services to customers to greater data efficiencies within the organization, applications play a crucial role in ensuring sustainability and profitability in a modern, global marketplace.

Recognizing this, organizations have pushed their digital teams to accelerate the development of applications throughout the organization. As businesses have adopted more modern methodologies and technologies to build and deploy applications faster, traditional application security approaches and solutions have fallen short as they do not meet the current needs of application development.

According to NTT AppSec Stats Flash Report, **85% of vulnerabilities that organizations find this year will never be remediated**. This is alarming when one considers the sophistication of organized threat actors and the vulnerability of an organization's data when left unfixed. Primarily due to COVID-19 and the mass influx of remote and hybrid work, the speed of application development has increased, with security often falling to the wayside. Now, two years into the pandemic, it is critical for organizations to shift their focus to a holistic application security model that includes less high-priority items that were passed over to focus on more obvious threats. The reality is that while a nation-state campaign or ransomware attack is the flashier avenue for attackers to take, many companies are more likely to experience an attack caused by a smaller exposure point or hidden vulnerability within their network of applications or that of a third party.

> ***Digital transformation has led to an inflection point in how we approach application security testing.***

Simply put, traditional application security platforms and tools have put many organizations' risk management programs in a continuous reactive state that cannot keep up with development requirements and abstraction layers.

NTT Application Security believes that the only way to solve today's modern application security testing challenges is to start completely fresh, leverage 20+ years of application security experience to deliver an entirely new approach with differentiated, innovative products. In doing so, we can help our customers build and release modern applications without sacrificing speed, accuracy, or security.

Overcoming Modern Application Security Challenges

To begin, we must confront three main challenges to modern AppSec:

1. **Historically, application security has been purpose-built for application security teams** and therefore lacks the intelligent context and holistic visibility of application security throughout the Software Development Lifecycle (SDLC).
2. **Traditional application security tools are designed and built for use in post-detection remediation workflows**, instead of focusing where it is most effective— predictive pre-production testing that aligns quality with security and naturally adapts with modern development and deployment practices.

3. **Current application security approaches enable DevSecOps to be a bridge between Development and SecOps**. While revolutionary in concept when it was first introduced, the role of DevSecOps has been plagued with obstacles that have ultimately led to its stumbling to gain solid footing in many organizations.

These challenges are not new and yet most organizations are stagnant in their approach to solve them.

Quite simply, we collapse the current paradigms and assumptions around application security and start brand new.

NTT Application Security is pioneering the next wave of application security and delivering exciting, fresh approaches to securing modern applications at the speed of modern development.

Step 1: Reinvent Application Security Testing to fit Modern Solutions

Whether implementing a traditional static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA) or application programming interfaces (API) solution, there are both pros and cons to their testing approaches and methodologies. Now more than ever, these solutions need to be reimagined and reinvented to fit a modern environment:

- **Traditional SAST** tools can analyze large codebases within a matter of minutes, they can't detect most access control issues. If the codebase is large, there is a greater opportunity for false positives that will require expertise to validate. Since SAST analyzes the codebase without executing it, the tool cannot detect runtime issues (e.g., authentication issues or server misconfigurations). Finally, while SAST does allow a developer to produce more secure code early in the SDLC, once in production, there may be vulnerabilities in code introduced due to integrations with other systems and third party tools.
- **Modern SAST** solutions should help you by aggregating multiple point products such as SAST and SCA into one automated, powerful, easy to use solution. It should analyze code faster with fewer false positives and offer your developers security best practices at their fingertips to become better at writing secure code. It should automatically enable functional testing, decreasing the time to test while increasing accuracy – all delivered from the cloud.
- **Traditional DAST** tools examine running web applications from outside, simulating a real attack, like a penetration test. Like SAST, traditional DAST cannot identify access control issues, or pinpoint the exact location within the code where the vulnerability exists. This requires the developer to search the code by block to identify and fix the vulnerability. This can be a long and laborious exercise, with results taking weeks and requiring human verification for potential false positives.
- **Modern DAST** works in both pre- and post-production environments. This allows for you to test faster and sooner within the SDLC pipeline. Modern DAST also enables more users to utilize application security tools without needing to be security experts. Finally, DAST needs to be a self-service tool that allows your team within the SDLC to test for application vulnerabilities in a fast, automated, accurate and safe way.

The traditional approach of relying on a single point-product solution will not meet the modern needs for rapid development and agile security. By using a combination of tools, your organization can benefit from better coverage and lower the risk of vulnerabilities in production applications. Using automated testing tools in all stages of the SDLC can significantly improve security.

Step 2: Enable All of Your Teams – not just SecOps

According to the 2021 Gartner® Magic Quadrant™ for Application Security Testing, "...the major driver for the evolution of the application security testing market is the need to support enterprise DevOps initiatives. Customers require offerings that provide high assurance, high-value findings, while not unnecessarily slowing down development efforts. Clients expect offerings to fit earlier into the development process, with testing often driven by developers rather than security specialists. As a result, this market evaluation focuses more heavily on the buyer's needs when it comes to supporting rapid and accurate testing capable of being integrated in an increasingly automated fashion throughout the software development life cycle (SDLC)."

None of this is earth shattering news. When we look at application security solutions that are currently in the market, they do not meet these requirements as defined by Gartner nor do they address modern market trends.

Modern AppSec Should:

- Allow you to test code as it relates to business functions.
- Enable your teams to test applications without requiring specialized security expertise.
- Be fast – delivering results in minutes, not hours or days.
- Work where your teams work, in modern DevOps platforms such as GitHub or Postman.
- Support cross-community workspaces: work with the tools and within the user experiences that work best for your business and all phases of your SDLC.

Step 3: Fully Realize DevSecOps to Bridge the Gap

DevSecOps arms traditional DevOps with the tools needed to implement security earlier into the SDLC while bridging the gaps between developers, DevOps, and SecOps. DevSecOps allows security integration into modern agile processes by responding to security issues as they arise and acting in a faster, less costly time to resolution. Most of all, DevSecOps introduces the concept of security as being more than just a SecOps concern, but a joint responsibility of all teams throughout the SDLC.

Organizations that can fully deploy DevSecOps will bridge the gap between Development and SecOps. This can be done through both organizational changes and the right solutions.

- **Cultural Shift:** To be successful, your organization as a whole should embrace the concept of DevSecOps. This means security must be communicated as a top priority for the business. This will set the stage for productive security conversations throughout the organization. It will also encourage an open dialog regarding the KPI's and goals of various teams. For example, by understanding the role of DevOps, SecOps can better show value without adding friction to the current release processes.
- **Agile DevOps:** Many traditional application security testing tools were built for waterfall development models. Organizations need modern solutions that can easily be integrated into existing agile processes. This ensures that application security tests can be run in an automated fashion without security expertise and that security policies can be implemented automatically, allowing developers to concentrate on the most critical issues first.

---

[1] Gartner, "Magic Quadrant for Application Security Testing" Dale Gardner, Mark Horvath, Dionisio Zumerle, 20 December, 2021

- **Integration:** Arguably, the most important, modern application security testing solutions must integrate into modern development and operational toolchains. Modern solutions must seamlessly assimilate with current processes and methodologies and work together as one comprehensive solution that bridges the gap between developer, DevOps, DevSecOps, and SecOps.

Traditional application security technologies have reached the point of extinction and organizations that do not evolve will continue to struggle when integrating into modern SDLC pipelines. Very simply, there needs to be a new approach. One that enables an organization's application development goals, works within the tools and environments that developers and security teams use, and operates both independently and holistically throughout the SDLC.

A New Age of Application Security

After 20+ years of delivering market-leading, trusted appsec solutions, NTT Application Security has pioneered a new approach to meet the demands of modern development. We are changing the conversation and delivering purpose-built, lightning-fast application security testing at the most critical inflection points of your SDLC. We are building a brand-new platform with agile, modern products that empower developers, DevOps and security teams with accurate and contextual security insights as they build, run and deploy web applications and APIs.