NTT | Application Security

WHITE PAPER

A Modern Approach to Application Security

A Modern Approach to Application Security

The events of the past two years have accelerated a near complete digital transformation for today's enterprise organizations. The COVID-19 pandemic caused a seismic economic shift. Organizations recognized that in order to stay in business, they needed to quickly pivot almost every aspect of their business online, evolving processes and adopting new technology, so that they could succeed in the "new norm." With a new remote workforce and the coming evolution to a hybrid work model, savvy leaders recognize a competitive advantage in being proactive about application security.

However, this accelerated digital transformation has not been without its challenges. As businesses moved quickly to adopt new paradigms and deliver new applications, the security of these applications, once deployed, has continued to elude even the most mature organizations. The biggest names in business today are seeing their application window of exposure, a key metric that indicates the exposure to cyber breaches for software applications, in months, not days. According to NTT Application Security's May 2021, Volume 5 edition of the AppSec Stats Flash,

> **"63% of all manufacturing apps and 52% of all healthcare apps have at least 1 serious exploitable vulnerability open throughout the year."**
>
> **- NTT Application Security AppSec Stats Flash - Volume 5, May 2021**

Organizations need to deliver new applications and API's, fast. Unfortunately, this "need for speed" requirement can lead to vulnerabilities in software code. While 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 released applications. To not do so could open their organization up to the myriad of threats that these vulnerabilities expose.

While there has been more focus on enabling security earlier in development, as well as static testing, *the truth is that applications are compromised in production, not in development.*

SecOps and DevOps teams continue to throw up roadblocks as each functional group operates with their own processes, tools and KPI's. For an organization to truly achieve a process for developing and deploying secure applications, they need to move beyond traditional methodologies and adopt a new approach – one that bridges the gap between security operations and development.

The Modern AppSec Framework delivers a functional plan with which organizations can use to develop and deliver secure applications, regardless of where they are in their security or application development journey. The framework collapses traditional models into four components that focus on business outcomes and correlates those business outcomes with tactical measures and products that can be adopted cross-functionally. The end result is a smoothly running application security program that empowers both security and development teams to develop and deliver secure applications and API's – Fast.

Outcomes and Considerations

As organizations have focused on the unprecedented shift to an online business model and remote workforce, they have also quickly adopted and developed new applications to meet the demands of an online marketplace and workforce. Unfortunately, the focus on speed has exacerbated the risk of deploying untested applications to meet demand. In our paper, DAST to the Future, we expose the risks associated with siloed programs as well as the fundamental problems connected with increased exposure due to lack of visibility and testing:

> **"...It does not matter if developers ship flawless proprietary code and apply the latest security patches to each open source component—which in 2020, netted-out to an average of 528 per application. Many vulnerabilities found in a production application do not exist in its source code and only arise once deployed into production..."**

While these challenges and statistics may seem daunting, it is important to remember that the breakdown exists because old models were being used to solve very modern problems. As with all things in cyber security, there is no "silver bullet." It is only by unlocking the full potential of a comprehensive appsec program, that organizations can develop and deploy truly secure applications. So where is an organization to start if they desire a "digital future that is free from breaches?" Why, at the beginning, of course!

Whether starting an application security program from scratch or maturing their current program, organizations should first establish their goals and business outcomes for the program. The first step is to take a strategic look at why they want to implement an application security program, and where their limitations exist.

- **Sales/Competitive Differentiation:** As today's organizations face the realities of third-party compromises such as the recent SolarWinds attack, more customers and businesses are realizing that they are only as secure as the businesses with which they connect. These customers and partners may wish to discuss application security processes before agreeing to do business. Additionally, as more organizations adopt formal application security programs, the ability to secure software may become a competitive differentiator.
- **Compliance:** There are many compliance regulations that may include application security components, including PCI, HIPAA and GDPR. Additionally, an executive order signed by the United States White House outlined a number of standards and requirements that will be adopted to protect federal agencies and their software infrastructure. Click here to learn more.
- **Risk of Attack:** When determining goals for an AppSec program, it is important to remember that breaches exist not only because of vulnerabilities in code. Developers may create completely secure code only to see the application compromised because of how it interacts with other systems. Testing should be planned accordingly.

- **Expertise:** All of the models and strategies in the world won't matter if an organization doesn't have the expertise to put it into practice. A successful application security program requires having the right talent and resources, along with the right solutions to run the program. Each functional team will have dedicated resources and business specific metrics and KPI's. A successful application security program requires:
  - Speed and Accuracy - comprehensive testing across the entire application portfolio
  - Access to the right application security talent that can perform high-fidelity, on-demand, manual testing
  - Strong integration with development processes and tools so that security vulnerabilities are fixed faster and prevented in the future

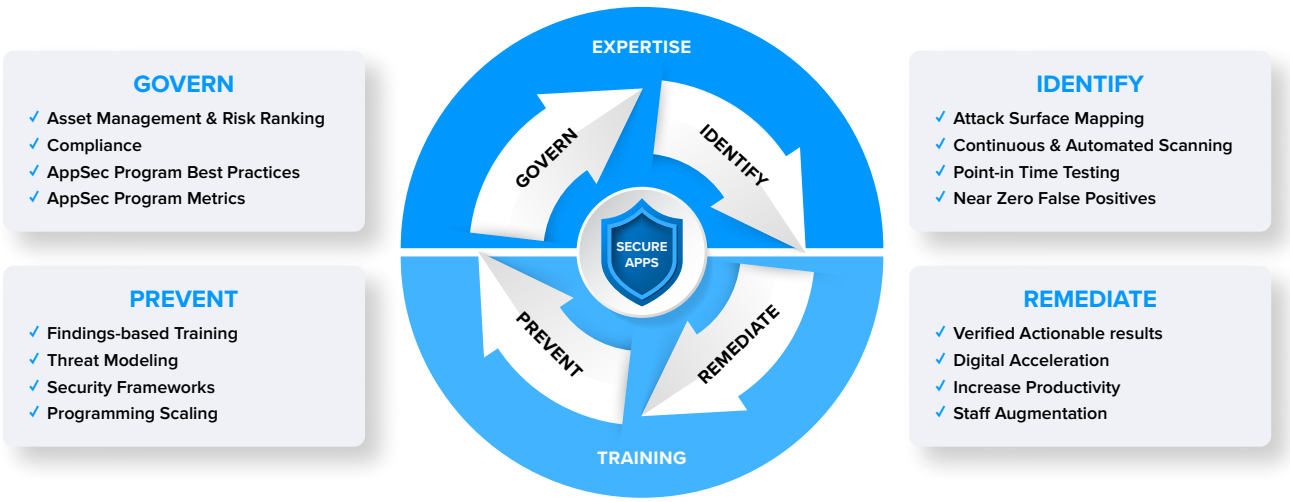
Organizations can take a holistic approach to their AppSec program only when they are able to fully understand their desired business outcomes - and their limitations.

NTT Application Security offers a modern approach to application security, where security, strategy and processes are embedded throughout the Software Development Lifecycle (SDLC) in a programmatic framework for success that encompasses people, processes and solutions, and results in business outcomes.

The Modern AppSec Framework

Definitively, application security is about developing, securing and maintaining secure software. Gone are the days where this was the job of the security team alone. Nor is it the job of the development team alone. Today's organizations need to take a holistic and programmatic approach where application security empowers all teams to work cohesively and is not siloed by job function.

To achieve this, organizations need to evolve past the traditional SDLC model and adopt a fresh approach – *The Modern AppSec Framework*



There are four functional components to the *Modern AppSec Framework*. They are Govern, Identify, Prevent and Remediate. Each component focuses on outcomes of that function. Once each component is complete, the organization then moves to the next functional component, operating in a cyclical process that leverages training and expertise as the organization evolves, matches the right solutions to the goals of the component and empowers all teams to work collectively.

GOVERN: To achieve application security, organizations must be able to govern the application security program. Overarching factors to consider include application asset management and risk ranking, regulatory compliance, best practices across the AppSec program and defining program metrics proactively to demonstrate program success over time.

Asset Management and Risk Rating: It's difficult to secure software if you don't know it exists. Organizations can start by identifying all of their web applications, mobile applications, APIs and cloud applications. Additionally, capture an up-to-date, comprehensive list of various software components, their dependencies, software versions, and open source. Next, assign a risk ranking to each piece of software. Include criteria such as business criticality, data type, and accessibility to group your applications. Important and high-risk applications should have more (and perhaps different) security activities applied to them than less important and/or low risk applications.

Compliance: Many organizations are subject to security requirements because of an application's business function (ex. payments), type of data stored or processed (ex. healthcare data), or geographical location (ex. regional requirements for data privacy and protection). Others may be required to perform specific security activities due to contractual obligations. Due to compliance requirements, certain security controls may not be optional. Organizations should determine what these are and make sure they are meeting the appropriate standards.

AppSec Program Best Practices and Metrics: Best practices in application security are not a one size fits all scenario. Standards and controls are built on years of practical security experience in real organizations. Organizations need to know how to optimize their unique program utilizing defined and measurable metrics. For example, security metrics can help organizations by identifying decision support for optimizing future application security processes. This data can help to answer questions regarding a particular area, such as penetration testing, using evidence-based information instead of opinion or anecdotes.

NTT Application Security offers several solutions to help organizations govern their application security programs:

- **Application Security Testing:** NTT Application Security is a complete Application Security and Risk Management platform with integrated secure development, security testing and continuous monitoring. The Software-as-a-Service (SaaS) platform delivers a centralized set of products and services that enables businesses to quickly deploy a scalable application security program across their entire DevOps lifecycle.

- **Pen Test & Business Logic Assessment Services:** The NTT Application Security Pen Test Service is a comprehensive application security testing service that helps organizations find high priority vulnerabilities and meet key compliance requirements.
- **Professional Managed Services:** NTT Application Security empowers application security by continuously assessing the risk of software assets. We help organizations embed security throughout the Modern AppSec Framework. The NTT Application Security platform, supported by our Professional Services team, can bridge the gap between an organizations SecOps and DevOps teams.

IDENTIFY: With the many methodologies employed by organizations, including waterfall, agile, and DevOps, there must be a way to identify security issues as they exist in applications. These security issues will generally fall into two categories - bugs and flaws. Bugs are often identified as code level security issues whereas flaws are often categorized as design level security issues. Regardless of category, or the application type (mobile, API, web application), organizations should be able to know exactly what they have and find security issues – Fast!

Attack Surface Mapping: The cybersecurity maxim rings true for AppSec – "You can't secure what you can't see." One of the most prevalent challenges that today's organizations face is an accurate account of their entire attack surface of exposed assets. Hackers attack applications in production, not development. With today's shadow IT challenges and legacy web applications, it is crucial that before testing their applications, organizations can compile a comprehensive map of their externally facing assets, so that security vulnerabilities in unknown applications do not go unchecked.

Continuous and Automated Scanning: Web application attacks represent one of the greatest risks to an organization. Web applications may not be updated regularly or often and may be attacked, changed or updated with a new feature that was not carefully vetted by security controls.

As web security is always evolving, organizations need to ensure that their scanning and testing evolves along with it. A practice of continuous production site monitoring with regular security scans will provide faster awareness of changes and updates and increase application security measures.

Point-In-Time Testing: While continuous scanning provides automated testing of application vulnerabilities for potential vulnerabilities, Point-in-Time testing assesses application security by emulating a real-world attack. When used in concert, an organization can identify both vulnerabilities that exist in the development code of an application, while also testing the security of that application as it interacts with other systems. By deploying both continuous scanning as well as point-in-time scanning, organizations can reduce the risk of attack from multiple vectors.

Reducing False Positives: The ability to ensure accuracy in vulnerability scanning is crucial for any application security program. Continuous and point-in-time scanning ensures that all of a web application attack surfaces are correctly tested in a reasonable amount of time. However, false positives can break down this process, inhibit productivity and introduce distrust across functional teams. It is therefore crucial that every alerted vulnerability is checked individually to ensure it is not, indeed, a false positive.

NTT Application Security offers several solutions to help organizations compile a complete list of their attack surface and identify vulnerabilities, faster and with unprecedented accuracy.

- **Attack Surface Management:** Delivers a fast, simple, and automated way for organizations to create a comprehensive inventory of their complete attack surface. Leveraging an innovative database of nearly 4.5 billion internet-connected assets, Attack Surface Management discovers, learns, and provides a complete inventory of an organization's internet exposed assets, details about where in the tech stack exposures exist, and alerts when the attack surface changes. Using this information, organizations can more quickly identify and prioritize their security resources.
- **Dynamic Testing:** Enables your business to quickly deploy a scalable web security program. No matter how many websites you have or how often they change, NTT Application Security's Dynamic Application Security Testing (DAST) can scale to meet any demand. We perform vulnerability assessments pit-crew style, which enables unparalleled efficiency and vulnerability coverage. NTT Application Security adopts the perspective of the adversary to find weaknesses and help you remediate them before they can be compromised.
- **Auto API Testing:** Provides highly scalable, accurate and fully automated vulnerability scanning for web service APIs, including public, private and internal facing APIs.
- **Mobile Testing:** This cutting-edge mobile application security testing solution combines dynamic and static automated scanning as well as manual mobile application-layer penetration testing to provide complete Mobile App coverage across the entire DevOps lifecycle.

REMEDIATE: Once an organization has a comprehensive mapping of their attack surface and identified security vulnerabilities, they need to develop a process for keeping track of what has been tested, by what means, and when. This will enable security teams to prioritize what needs to be fixed by using business context to understand what issues matter most. This will also enable development teams to identify and fix prioritized vulnerabilities first.

For example, many organizations require that findings be fixed within a certain period of time, depending on the criticality of the findings. An e-commerce business might require that critical findings discovered on its customer facing applications be fixed within 48 hours, high severity findings be fixed within 10 days, medium severity findings be fixed within 30 days, and low severity findings be fixed within 90 days.

By tracking what vulnerabilities are open, those that have been addressed, and those that are closed, organizations can ensure clear communication and tracking between functional teams. Additionally, summary information can be reported to relevant stakeholders, so everyone is always in the know about current status. By developing a process for identifying, tracking, and remediating vulnerabilities in production applications, organizations can realize an increase in productivity by fixing vulnerabilities earlier and releasing applications faster.

While identifying and developing a process of remediating attacks may seem straight forward, not all organizations have the expertise, processes, and resources to tackle it on their own. NTT Application Security offers both in-house services and partnerships that help organizations prioritize and remediate application security vulnerabilities, while enabling and developing expertise and best practices.

- **NTT Application Security Professional Services On-Demand and Premium Support:** Includes accelerated and prioritized response times, 24x7 escalation for critical issues and a personalized engagement with a Technical Account Manager to ensure that issues are resolved quickly.
- **Staff Augmentation:** Enables organizations to take application security one step further by augmenting their in-house security teams. Joint customers will have access to hundreds of application development experts that scan the vulnerabilities identified by NTT Application Security and implement the fix, saving time and resources.
- **E-Learning:** Educate your teams through self-paced training on application threat modeling, best coding practices, mitigation, and defensive remediation, all in an easy-to-learn, web-based environment. The information learned in these modules can be used to produce guidelines for consistent secure programming practices throughout your organization.

PREVENT: Once an organization has determined what is important (the Govern component), what needs to be fixed (the Identify component), and how they are going fix it (the Remediation component), The next step is to determine how to scale efforts across the application security program in its entirety. This is achieved by a combination of training, threat modeling, adherence to security frameworks, and operationalization of application security solutions. It is important that the solutions and processes throughout the components of the framework complement one another. For example, when used to detect vulnerabilities in applications, NTT Application Security's DAST can inform both the security and development teams of its findings so that not only is the vulnerability fixed in the current application, but future vulnerabilities can be proactively avoided.

- **Findings Based Training:** The best application security training for developers is based on real security findings, whether these are demonstrated during an actual security incident or found in manual penetration testing. The OWASP Top 10 contains a list of common web application security risks. However, each organization will have its own unique top 10 list. Once determined, an organization can and should use this information to prevent entire categories of security vulnerabilities by implementing focused developer training.

- **Threat Modeling:** There are two types of application security problems: bugs and flaws. Bugs are code-level mistakes, and flaws happen at the design level. Threat modeling is a type of design-level security assessment that is intended to examine the way an application system works in order to identify potential flaws. The process involves analyzing assets, security controls, and threat agents in the context of an application system. When flaws are detected in threat modeling before software implementation, some security problems can be avoided.

- **Security Frameworks and Configuration Standards:** Some security issues can be prevented by using certain security framework and configuration standards. A few examples include CSRF tokens (prevent Cross Site Request Forgery attacks), CSP (whitelist assets that the browser should allow to load and execute in order to minimize the impact of Cross Site Scripting exploits), and HSTS (encrypt data in transit and prevent fallback to non-HTTPS traffic).

  Other kinds of security issues can be avoided by securely configuring the software environment, for example by following the Amazon CIS benchmark to harden AWS accounts and cloud services.

- **Program Scaling:** Due to size, complexity, and available resources, some enterprise organizations are challenged with scaling their application security program. Development teams are not security experts and security teams may lack specialized application security knowledge. Organizations that want to mature their AppSec program may not have the resources required to lay out a roadmap to take them to the next level.

By leveraging resources, best practices, and performing modeling assessments, organizations can programmatically prevent application breaches by identifying and fixing vulnerabilities as they exist across the application security lifecycle – whether they exist in development, or in deployment.

Putting it All Together

The Modern AppSec Framework enables organizations to expand beyond identifying and remediating application security issues in siloes by taking a functional and holistic approach to their application security program. Beginning with identifying the limitations and goals of their current plan, organizations can then assess an inventory of their program based on the four components of the framework. With each component, NTT Application Security offers the right products and expertise to help organizations advance to the next step of the framework. From identifying to remediating, preventing to governing, organizations that adopt the Modern AppSec Framework can develop and deploy applications fast – and succeed in today's rapidly changing marketplace.