NTT Security

UK Technical Insight

Secure Application Services

For many commercial and operational reasons, security remains a 'bolt on' within the Software Delivery Lifecycle (SDLC). This approach can be problematic and we recommend building in security from the outset. By not doing so, organisations usually end up having to use more resources, to identify, assess and mitigate against vulnerabilities at a later stage, all the while leaving web applications more vulnerable to compromise and exploit than they need to be.

Aware of this growing risk, organisations are seeking practical ways to transform the maturity of their web application security. Organisations are looking for a service that integrates application assessment and control implementation to reduce risk, whilst being agile enough to adapt to an organisation's existing application delivery framework and release timescales.

How mature are your web application security processes?

NTT Security understands that organisations have different levels of maturity, when it comes to application security, and for application owners to keep on top of this is challenging. Frameworks such as the Building Security In Maturity Model (BSIMM) and OWASP's Software Assurance Maturity Model (OpenSAMM), can assist organisations with this onerous task and one of their recommendations is to perform thorough application assessment and testing. Moreover, OWASP's web application testing guide[1] recommends "a balanced approach" to testing, which combines different forms of assessment techniques based on where the application is in its software delivery lifecycle (SDLC).

A business with less developed security processes, and a limited view of the known risks, would require more integrated application testing earlier on in the SDLC. This would use a combination of automated tools and processes to identify the breadth of vulnerabilities, so they can be prioritised, addressed and mitigated sooner rather than later.

An organisation with more mature application security processes, and a fuller understanding of their risk profile, would be looking for the final validation that only manual penetration testing can provide, just prior to the new application going to market.

Key questions to assess the application security maturity of your organisation:

- Are the risks to your application known and understood?
- Do you proactively embed security into the SDLC?
- Do you have security testing integrated into your application lifecycle?
- Are automated security testing tools used?
- Are penetration tests used to assess security prior to release?

NTT Security's Secure Application Services (SAS) can help you access the skills, processes and technology experience you need to reduce web application risk. SAS has combined elements of application testing and technical consulting into a set of services – designed to help organisations incrementally improve the maturity of the SDLC and improve their application security posture, in the most cost-effective way and without impacting go–to-market timelines.

1. https://www.owasp.org/index.php/Testing_Guide_Introduction

The four phases of Secure Application Services

NTT Security's SAS offering is a set of complementary services, all built around a four-phase process. These phases have been designed to provide our customers with an adaptive approach that integrates application assessment with the design and implementation of controls and, finally, provides validation that the vulnerabilities have been mitigated.

1. Assessment – identify vulnerabilities

Having run a workshop where you agree the scope of the assessment, we use a range of techniques including penetration tests, vulnerability scans and a bespoke application security questionnaire, to identify vulnerabilities. These are captured in a tailored, comprehensive assessment report which is used to drive the next phase.

2. Analysis – evaluate risk

In the analysis phase, we use our understanding of your business to review vulnerabilities in context, to assess risks and make practical, prioritised recommendations illustrating the benefits of relevant security controls. Once this report is reviewed we move into the Action phase.

3. Action – implement, tune and stabilise controls

Whatever the right controls are for your organisation – from creating new, or updating current, security policies on an existing Web Application Firewall (WAF), to amending or reconfiguring an application delivery controller (ADC) – a specialist NTT Security consultant will work with you to design and implement these controls seamlessly in your environment.

4. Approval – demonstrate value

We want to give you evidence that the new controls are working, so at this stage our consultants will apply the assessment phase tools once again to demonstrate successful mitigation.

Integrated Web Application Protection Service (IWAP)

NTT Security's Integrated Web Application Protection (IWAP) service is a combination of automated web application risk assessment and mitigation processes that seamlessly integrate with your software release lifecycle to ensure every application is effectively secured against known threats.

IWAP will work across your application release lifecycles to incrementally assess and remediate vulnerabilities as the application moves through the SDLC process. This enables you to be proactive around vulnerability remediation and ensures that security is embedded into the whole development process. IWAP mitigates known vulnerabilities by implementing virtual patching into your SDLC, and gives developers time to remediate application code, in the knowledge that the application is still being protected.

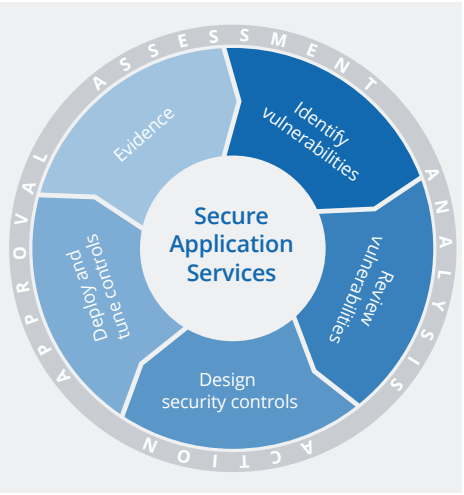
At a glance – Benefits of IWAP

- Light touch engagement, providing protection from known application vulnerabilities
- Embeds security into the SDLC
- Fast deployment
- Takes advantage of automated processes
- Application focused
- On demand
- Can be deployed across release lifecycles
- Completes the SDLC process by providing the full range of security testing techniques (IWAP+)

Secure the lifecycle

NTT Security can also offer IWAP+, as an add-on, once an application has gone through the IWAP process over multiple release cycles. IWAP+ focuses on the 'end-of-lifecycle' phase of your SDLC, and includes a manual penetration test. This validates the web application's correct security posture by ensuring that the application can withstand targeted, goal-specific attacks and, when combined with automated security testing, provides the extra assurance needed that the breadth and depth of vulnerabilities have been discovered and mitigated.

Figure 1: Our structured approach to web application security – IWAP helps reduce application risk for your business



Web Application Shield (WAS)

NTT Security's Web Application Shield (WAS) service is the final piece of the SAS jigsaw, combining automated and manual risk assessment, along with mitigation, to ensure that your production-ready applications are both safe and secure for consumers to use with confidence.

By bringing together manual penetration tests with automated testing, WAS offers a greater depth of analysis than a vulnerability assessment alone and will result in a richer set of mitigating controls. Further, as WAS targets production-ready applications, it will also include functional validation testing, to ensure that application functionality remains consistent.

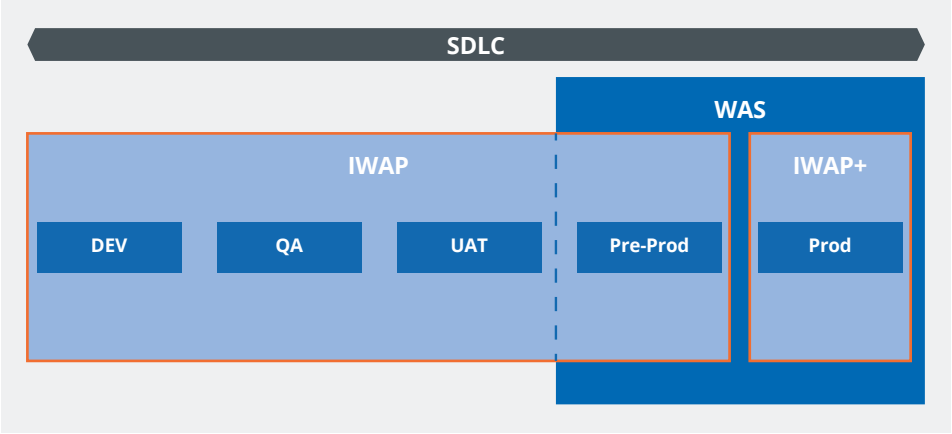
At a glance – Benefits of WAS

- Transforms long-term application security posture for the better
- Application and infrastructure focused
- Deeper and richer assessment, leading to more effective implementation of security controls
- Takes advantage of both automated and manual processes
- Creates a more robust approach to vulnerability/threat awareness
- Action taken in context of the client's known and unknown security risks
- Provides full design documentation

Secure Application Services and SDLC

NTT Security sees SAS working as part of your software development lifecycle to guarantee that security is embedded, rather than bolted on. As shown in Figure 2, the complementary offerings are aimed at different stages of the SDLC and will work together to help you build a mature application security lifecycle.

Figure 2: IWAP, WAS, IWAP+ and SDLC



The value of Secure Application Services – making web applications an asset not a risk.

Increasing the maturity of your web application security will deliver:

- **Reduced attack surface area:** integrating vulnerability assessment, pen testing and controls implementation helps narrow the possible threats to your web application(s).
- **Optimised application security delivery:** establishing comprehensive visibility to your web application assets helps you to prioritise risk and determine the relevant security posture.
- **Faster go-to-market timelines:** by embedding security into all your software lifecycles, applications can be released faster, eliminating post-production security delays that impact go-to-market timelines.
- **Increased level of knowledge and understanding:** improves understanding and awareness of the risks associated with application delivery.
- **Improved compliance:** using industry best practices, IWAP builds compliance into software delivery.
- **Formulate a secure policy framework for applications:** IWAP is a repeatable service that can be embedded into existing software frameworks and work alongside the deployment and release of applications.
- **Brand confidence:** including security in the application development framework gives assurance of embedded security, which increases consumer confidence in live applications.

Secure Application Services: balancing security and innovation

NTT Security has designed Secure Application Services (SAS) to help organisations answer the challenges of digital transformation; such as staying ahead of the competition within aggressive go-to-market timescales whilst ensuring that the applications are secured and safe for customers to use. These competing requirements have often led to security being 'bolted on' as an afterthought, in the hope that any vulnerabilities don't delay release timescales and do not have too costly an impact. By embedding security in to the SDLC at an early stage, SAS can help organisations safeguard the security of their applications, increasing customer confidence. And by giving developers time to remediate vulnerabilities in the most cost effective and speedy manner, build resilience and security maturity.

To speak to a member of the application security team about how our Secure Application Services can help you establish the right testing and application security controls for your business, please speak to your NTT account representative or visit: **nttsecurity.com** for contact information.

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.