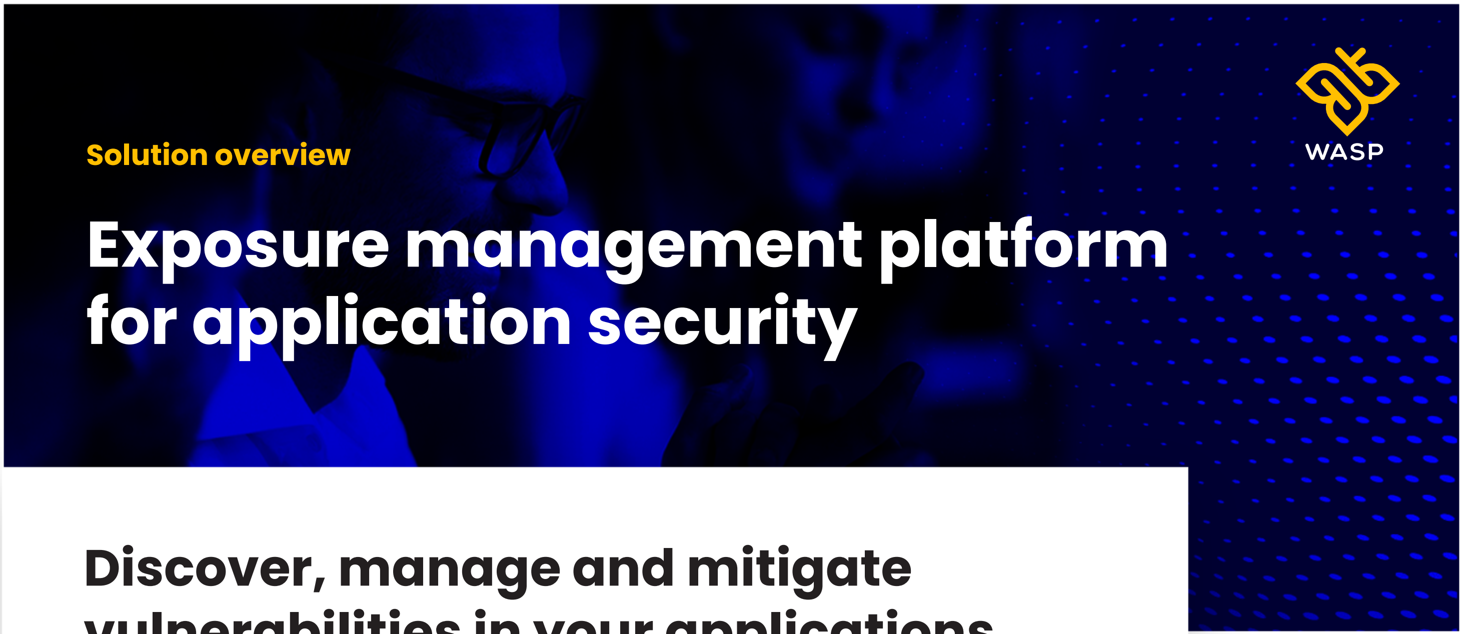


WASP

Solution overview

Exposure management platform for application security

Discover, manage and mitigate vulnerabilities in your applications faster and efficiently

Wasp is transforming exposure management by enabling application security professionals to efficiently test, discover, assess, and manage their internal and external exposure.

Tailored for app security, Wasp combines penetration testing, attack surface mapping, code analysis and risk-based vulnerability triage, with remediation solutions that integrate with your development workflow to deliver full lifecycle visibility and control.

Benefits

Continuously monitor your organization's attack surface and application security posture - Expose vulnerabilities in every asset and application.

Proactively identify risks - Determine exposure resulting from new technologies, and from the known and unknown expansion of the digital attack surface.

Focus your attention - Minimize false-positives and triage findings.

Reduce MTTR by up to 75% - Integrate with your workflow ticketing and communicate effectively with security research experts.

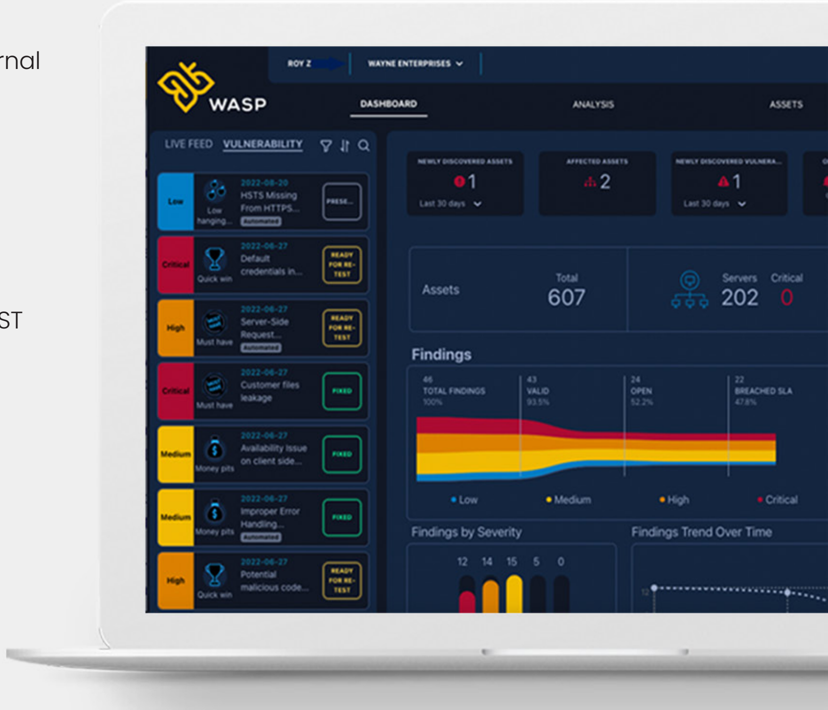
Effectively manage your code security posture - triage, deduplicate, and present SAST, DAST and SCA findings, so you can focus on the prioritized issues.

Reduce operational costs - Replace costly services and consolidate solutions.

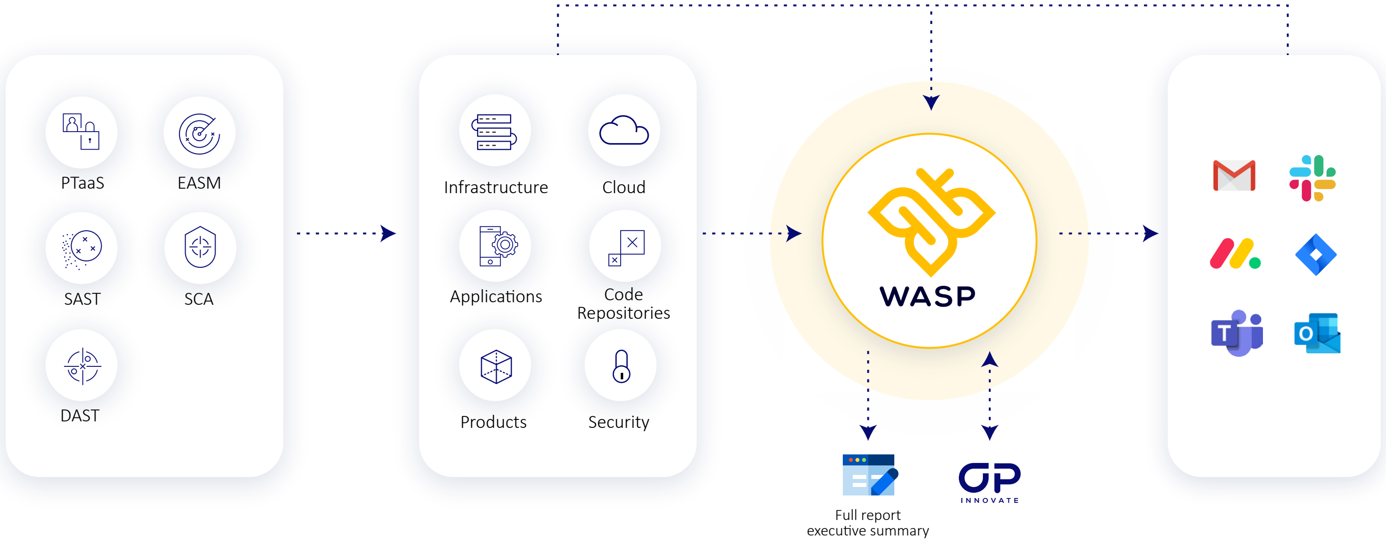
waspcyber.com | info@waspcyber.com

Features and functionality

- ✓ Leverage top notch expertise to get a continuous and comprehensive understanding of your external and internal attack surface and most burning, real security issues
- ✓ Get a bird's eye view on the security posture of your applications and your most urgent action items
- ✓ Benchmark between different products and get insights -such as most vulnerable products, overdue issues
- ✓ Leverage code scanning tools such as SCA, SAST and DAST to build secure code by design
- ✓ Track progress over time and create tasks for your development team that will integrate with their workflow
- ✓ Get executive reports to understand and communicate testing and remediation impact
- ✓ Communicate with the Wasp team to deliver immediate feedback and dive deep into security findings



How it works



Wasp continuously monitors your external attack surface, providing observability to the application's security posture. It proactively identifies the risks resulting from the exposure of new technologies as well as known and unknown expansion of the digital attack surface. The solution manages your code security posture by mapping your code repositories and assesses each and every one of them for vulnerabilities and risk. It de-dupes, scores, and presents SAST, DAST and SCA findings, so you can focus your resources on the most contextually important issues. Seamless integration into your ticketing system while tracking your remediation process and your SLA promotes a paradigm shift from project-based security orchestration to one of continuous testing enabling you to plan and budget over time.

Use cases

Posture Management	Remediation Workflow Optimization	Application Vulnerability Remediation	Compliance
• Leverage continuous discovery of digital assets, combined with periodic testing. • Customize your scanning and alert policy according to your own requirements. • Take advantage of a clean, focused presentation of findings, combined with actionable insights and a prioritized action plan.	Wasp's triaging capabilities allows you to prioritize your team's efforts by pinpointing vulnerabilities and their owner, and providing them with detailed guidance for swift resolution and future mitigation.	• Supercharge remediation management with advanced ticketing, prioritization, SLA management. • Create a direct line of communication between developers and penetration testers.	Deploy measures across your organization required to achieve compliance with data security regulations including HIPAA and the EU's GDPR, among other government and industry regulations.

Our team of experts

The WASP's research team holds extensive expertise in cyber research, penetration testing, incident response, training and forensics. As veterans of prestigious military intelligence units, these accredited professionals are certified on a variety of sought-after qualifications, delivering unparalleled cyber expertise and dedication to deliver high quality findings in all areas examined.