Scan **Every App**
Secure **Every Layer**
Synthesize **Every Insight**

CHALLENGES

In 81% of organizations, application reviews take more than one business day, and in 35% they extend beyond three days, typically involving around 10 team members.
Automated vulnerability scans can take up from 3 to over 8 hours of this process.
Traditional scanners often treat speed as an afterthought, offering few options to keep pace with modern development practices and the urgency with which updates are deployed.

(sources: CrowdStrike, 2024 State of Application Security Report, 2024;

Contrast Security, The State of DevSecOps Report, 2024)

Security teams often operate with **limited staff**, making it crucial to maximize manual review insights. Many scanners **lack adaptability to incorporate in-house expertise**, leading to repeated or overlooked vulnerabilities.

Traditional DAST tools usually focus **solely** on the **application itself, neglecting** the **broader infrastructure** and **peripheral attack surfaces**, leaving teams to manually cover these gaps or use separate tools.

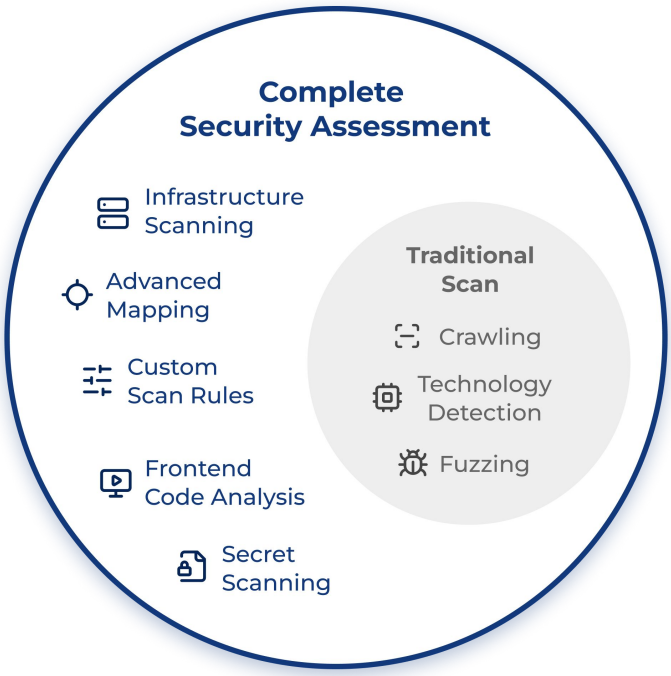
Scanners that charge **per scan** or **per application** force teams to **limit parallel** scans and application slots, causing 55% of organizations to skip security scans due to deadlines or budget constraints, **leaving potential vulnerabilities unaddressed**. (source: Contrast Security, The State of DevSecOps Report, 2024)

SOLUTION

Trickest DAST integrates with existing workflows and **leverages in-house expertise** through highly customizable and scalable scanning methodologies tailored for diverse scenarios.

This solution maximizes the value of manual reviews, reducing the time spent on regressions and variations of known vulnerabilities and enabling **unlimited parallel scans without budget constraints**, in a scalable and cost-effective approach.

Trickest DAST assessments go **beyond traditional** scanning methods, capturing broader infrastructure and peripheral attack surfaces, significantly **decreasing manual effort**.



BENEFITS

Maximize Security Efficiency with Unlimited, Comprehensive Scanning

Break the Cost Barrier

- **Scalable Coverage**: Scan as many applications as many times as needed with no artificial limits.
- **Flexible Resource Management**: Control resource allocation, adjust scan schedules, and fine-tune workflows to accommodate more apps, speed up scans, or create tailored scanning methodologies that fit different applications.

Full Assessment in One Solution

- **Holistic Risk Assessments**: Scanning modules powered by expert-driven methodologies that encompass complete discovery, precise technology fingerprinting, content enumeration, advanced JavaScript analysis, and more.
- **Integrated Capabilities**: Integrate capabilities typically found in separate solutions, including infrastructure analysis, CVE scanning, secret detection, and static analysis.

Scale Team Efficiency

- **Flexible Integration**: Integrate into your existing CI/CD pipelines, asset inventories, and reporting systems through multiple integration methods—including a versatile CLI, APIs, or direct in-workflow connections.
- **Bridge Expertise and Automation**: Enable your security experts to innovate, formalize repeatable methodologies and convert manual findings into automated scanning rules using widely-adopted formats, templates, automation plans, custom wordlists, and seamlessly integrated open-source or proprietary tools.
- **Enhanced Resource Efficiency**: Reliably automate vulnerability scans for routine applications and initial assessments, freeing your security analysts to focus on strategic tasks. Unlike rigid scanners, this solution continuously evolves through adaptive scanning methods, ensuring comprehensive coverage without additional manual effort.
- **Flexible Deployment Options**: Select self-hosting to achieve maximum control, ensure compliance, and simplify scan configurations; leverage our managed cloud infrastructure (with dedicated IP addresses) for automatic scalability and streamlined deployment; or adopt a hybrid approach that combines the advantages of both models.

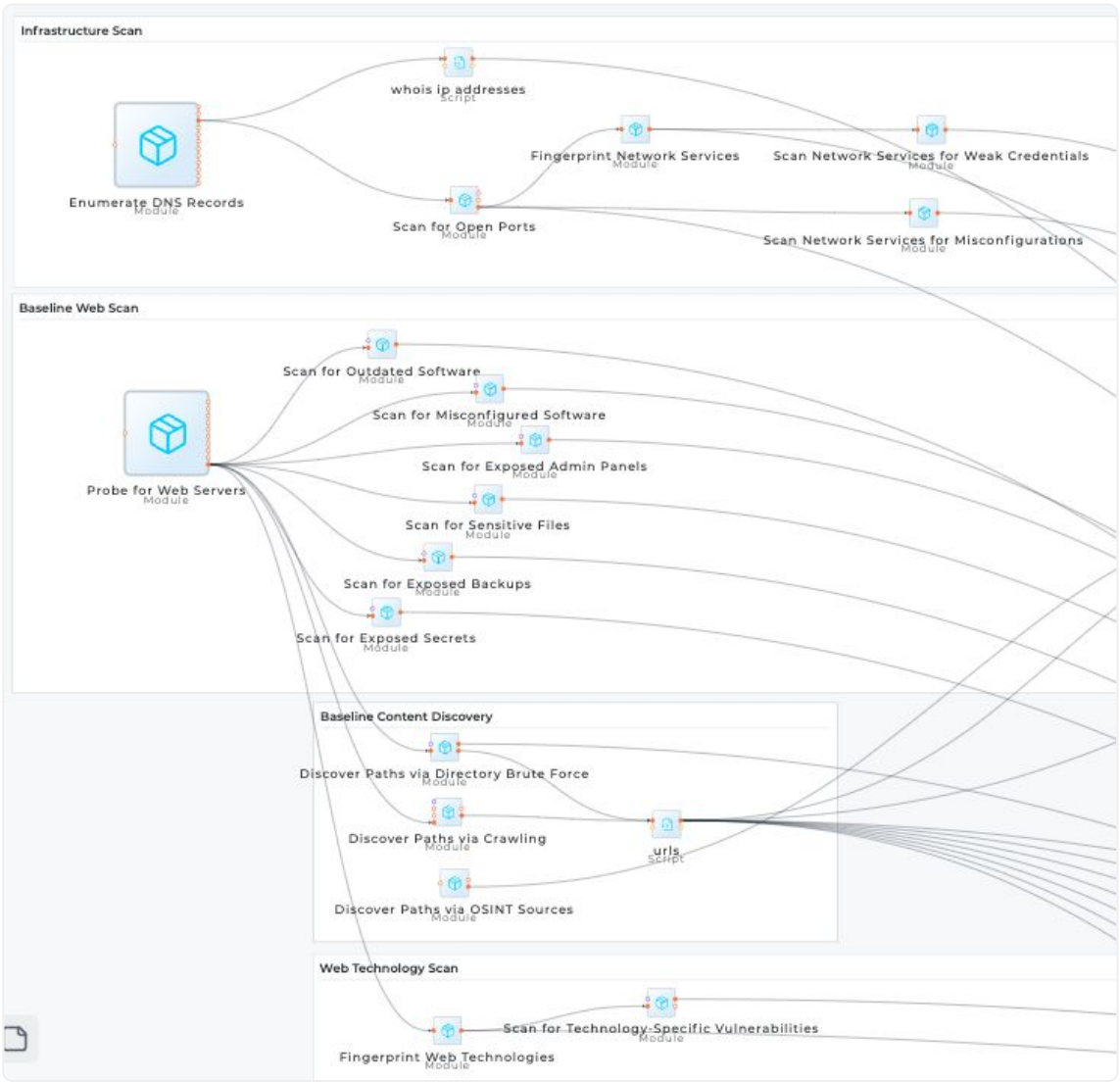
Missing Capabilities in Your Current Solution?

Tell us what capabilities you're lacking and discover if we already support them—or find out how quickly (in days, not months) we can deliver

Let's Talk

CAPABILITIES

Tailored Security Operations with Custom Workflows and Collaborative Tools



Customizable Workflows for Any Scenario

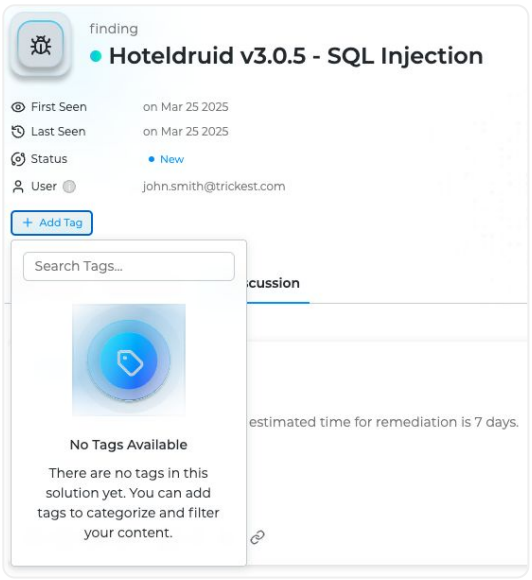
- **Fast scans** for CI/CD pipelines that finish in minutes, not hours.
- **Full scans** to conduct a comprehensive evaluation of the application's attack surface.
- **Pre-pentest assessments** that export all intermediary data to give testers full context from the start.

Flexible Scheduling and Scaling

- **Unlimited scans** at no extra cost.
- **Recurring scans** to automate periodic retests and continuously catch new vulnerabilities as they emerge.
- **No setup required** to run internet-facing scans from our cloud infrastructure.

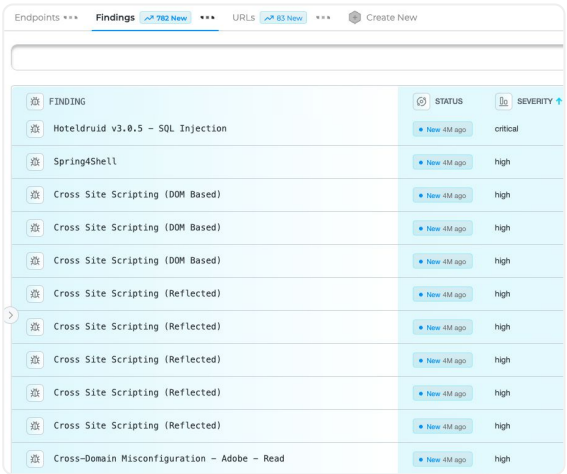
CAPABILITIES

Tailored Security Operations with Custom Workflows and Collaborative Tools



Collaborative Security Operations Workspace

- **Collaborative Dev Environment**: Develop and refine workflows, ensuring synergy and eliminating redundant efforts across security projects.
- **Module Builder**: Enable subject matter experts to create specialized, reusable modules that integrate directly into scanning workflows, leveraging internal expertise at scale.
- **Data Collaboration Tools**: Utilize tagging, commenting, saved queries, and custom exports to streamline team collaboration, accelerate remediation, and simplify reporting processes.



Custom Reporting & Logs

- **Advanced Search of Vulnerabilities, Endpoint Logs, and APIs**: Quickly query and review the found vulnerabilities and endpoints.
- **Historical Records**: Track new and recurring vulnerabilities with precise timelines, including first detection, latest occurrence, and identifying scans.
- **Tailored Scan Reports:** Generate custom reports aligned precisely with your specifications—without relying on rigid, predefined templates.

USE CASES

Optimizing Security Strategies with Trickest

Automated Recurring Scans: Enhancing Security for Multinational Enterprises Managing Multiple Web Applications per Division/Brand

For enterprises managing numerous web applications across various brands and regions, implementing automated recurring scans is essential to maintain a robust security posture.

- **Continuous Vulnerability Detection:** Regular automated scans ensure that vulnerabilities are identified promptly, reducing the window of opportunity for potential exploits.
- **Efficient Resource Allocation:** Automating routine security assessments allows security teams to focus on strategic initiatives, optimizing the use of skilled personnel.
- **Regulatory Compliance:** Consistent scanning supports adherence to industry regulations and standards, demonstrating a commitment to data protection and security best practices.

Pre-Penetration Testing Application Attack Surface Mapping: Accelerating Penetration Testing with Tailored Automation

Integration of DAST into penetration testing workflows improves ability to identify and address vulnerabilities efficiently. By automating the initial discovery phase, DAST enables our security analysts to focus on more complex threats, enhancing the overall effectiveness of our security assessments.

- **Comprehensive Discovery**: Automated scans identify all accessible components of an application, including APIs, subdomains, and hidden endpoints, ensuring no part of the application remains unassessed.
- **Identification of Low-Hanging Vulnerabilities**: Early detection of easily exploitable vulnerabilities, such as misconfigurations or outdated components, allows for prompt remediation before deeper manual testing.
- **Pattern Recognition**: Analyzing recurring vulnerability patterns across applications aids in understanding common security gaps, informing both immediate remediation and long-term security strategies.

MORE RESOURCES

- Platform Overview - A quick introduction to Trickest's Platform core features.
- Modules - Speed up your offensive security workflows with reusable building blocks that cut down on manual effort.
- Trickest Attack Surface Management (ASM) - Achieve unparalleled visibility and control over your attack surface with Trickest's superior, customizable, and hyper-scalable ASM solution.
- Trickest Vulnerability Scanning - Identify vulnerabilities across your entire attack surface—regardless on how many assets you manage.
- Trickest Dynamic Application Security Testing (DAST) - Continuously uncover security gaps in real time with automated DAST workflows.
- Trickest Query Language - Dive into advanced filtering, custom views and integrations with out-of-the-box API.
- Trickest ASM Solution Brief - Read about Trickest ASM Solution in the dedicated Solution Brief

ABOUT TRICKEST

Trickest specializes in automating offensive security operations at scale. Our platform empowers organizations to uncover attack surface, vulnerabilities, streamline security workflows, and fortify their digital ecosystems against real-world threats.

Built for large enterprises, Trickest handles complex infrastructures with unmatched scalability. Unlike rigid traditional solutions, our automation-driven approach adapts to unique needs, enabling security teams to integrate custom tools, iterate rapidly, and manage their attack surface—without vendor delays or asset-based pricing constraints.

See it for yourself

Trickest doesn't just discover and secure your assets—it transforms how your organization manages risk.

Let's Talk

TRICKEST

Trickest, Inc.
1111B S Governors Ave STE 6511
Dover, DE 19904, US

https://trickest.com

Information Security Management System certification ISO/IEC 27001