Bright

+ Case Study

How a Global Software Company Scaled Authenticated Security Testing With Bright DAST

How a central application security team moved beyond periodic penetration tests and built continuous, authenticated testing of web applications and APIs across multiple product brands.

- Enterprise Software
- Authenticated Testing
- APIs
- Application Security

Company Overview

Company
A global software company

Industry
Enterprise software

Team
Central AppSec team supporting multiple product brands

Use Case
Authenticated web application and API testing

Solution
Bright DAST by Bright Security

Context

Company Overview

The company operates multiple product brands, each with its own authentication mechanisms, deployment practices, staging environments, and security controls. A central application security team supports development teams across the organization, coordinating penetration tests, validating web application and API security, triaging vulnerabilities, and working with engineers on remediation.

As the portfolio grew, periodic manual penetration testing could no longer keep pace. Many relevant risks sat behind login screens, inside protected workflows, authorization boundaries, business logic, and API endpoints that basic unauthenticated scans cannot reach.

The Challenge

What the Team Needed to Solve

The team needed a consistent way to test authenticated applications across product teams, without forcing every application into the same configuration.

Expand Authenticated Coverage
Test protected functionality, user workflows, business logic, authorization boundaries, and API endpoints.

Support Different Environments
Handle applications with different development practices, authentication models, and staging setups.

Keep Operational Control
Manage scan scope, authentication, rate limits, and sensitive endpoints so testing runs safely alongside development.

Test Between Pen Tests
Reduce reliance on point-in-time manual assessments as the main way to evaluate application security.

The Solution

Bright DAST: Continuous, Authenticated Testing Across Product Teams

The company selected Bright DAST to test its running web applications and APIs repeatedly, including functionality available only after login. The security team worked with each product's development, QA, and platform stakeholders to configure scans for their own staging environments.

Testing Behind the Login
Authenticated scans reach protected workflows, authorization boundaries, business logic, and API endpoints.

Configured per Product
Central oversight, with scans tuned to each application's authentication and staging environment.

Safe in Shared Staging
Controls for scope, authentication, rate limits, and sensitive endpoints keep testing from disrupting other teams.

Alongside Manual Pen Tests
A repeatable testing capability that complements expert-led penetration tests rather than replacing them.

The Implementation

A Repeatable Authenticated Testing Playbook

Rollout meant solving real-world issues: SSO redirects, short-lived tokens and single-session limits, rate limits and WAF behavior, and dynamic user interfaces. Working closely with Bright, the teams turned these lessons into four onboarding practices.

1. **Establish stable authentication steps**
Reliable login sequences for each application help scans gain authenticated access consistently.

2. **Validate access to protected resources**
Confirming access on the same target host proves the setup works before broader testing.

3. **Simplify browser interactions**
Removing unnecessary browser actions reduces complexity and improves scan reliability.

4. **Start with smaller pilot scans**
Pilots surface authentication and environment constraints before the scope expands.

Impact

The Impact on the Business

The value went beyond running more scans. The company gained a structured application security process that works across multiple product brands, complex authentication, and different development environments.

Before
Periodic Manual Pen Tests
Point-in-time assessments and unauthenticated scans left gaps between engagements.

→

After
Continuous Authenticated Testing
Repeatable scans reach protected workflows and APIs in staging.

→

Result
A Repeatable AppSec Process
A shared onboarding playbook that scales across product teams.

Five improvements stood out: deeper coverage of authenticated applications and APIs, continuous testing between manual assessments, greater control over testing in shared environments, a repeatable process for onboarding new applications, and stronger collaboration between Security and Engineering.

Testimonial

Voices from the Application Security Team

> *"We needed a scalable way to test authenticated web applications and APIs across multiple products without relying only on periodic manual penetration tests."*
>
> GS **Application Security Team**

> *"For us, the value is not only in running scans, but in building a safer and more repeatable application-security testing process with product and engineering teams."*
>
> GS **Application Security Team**

Looking Ahead

The Future with Bright Security

With a repeatable approach to authenticated testing in place, the company is positioned to extend security testing to more web applications and APIs, while keeping manual penetration testing as part of its broader security program.

Bright Security gives the central AppSec team both the technical capabilities and the hands-on support to turn complex testing requirements into a process that security and engineering teams can maintain together.

+ Bright Security

© 2026 Bright Security