



Beagle Security

The hacker friend for your organization





Our Vision

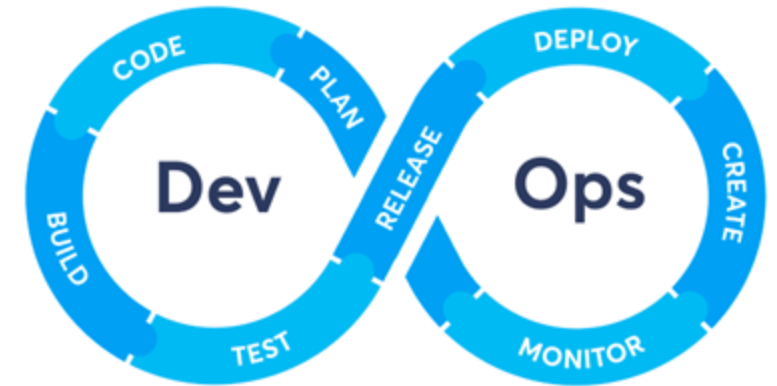
To be the de facto automated, human-like vulnerability assessment and penetration testing SaaS platform that protects our customers' businesses from a third-party perspective while creating a new category of Intelligent Beyond AppSec Platform.

The Beagle Security platform:

- Enables shift-left security
- Assists with compliance needs
- Helps in reducing cost associated with appsec

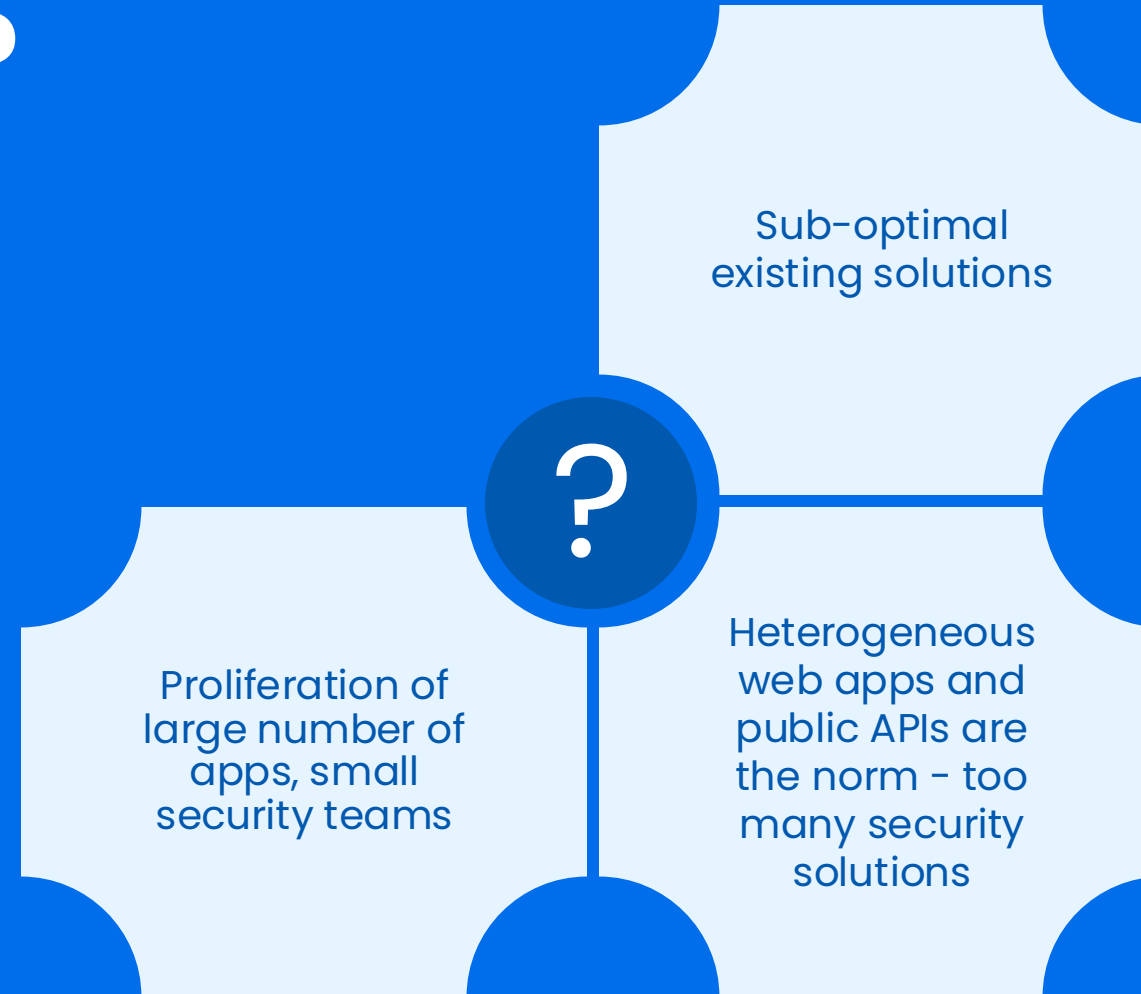


Sec

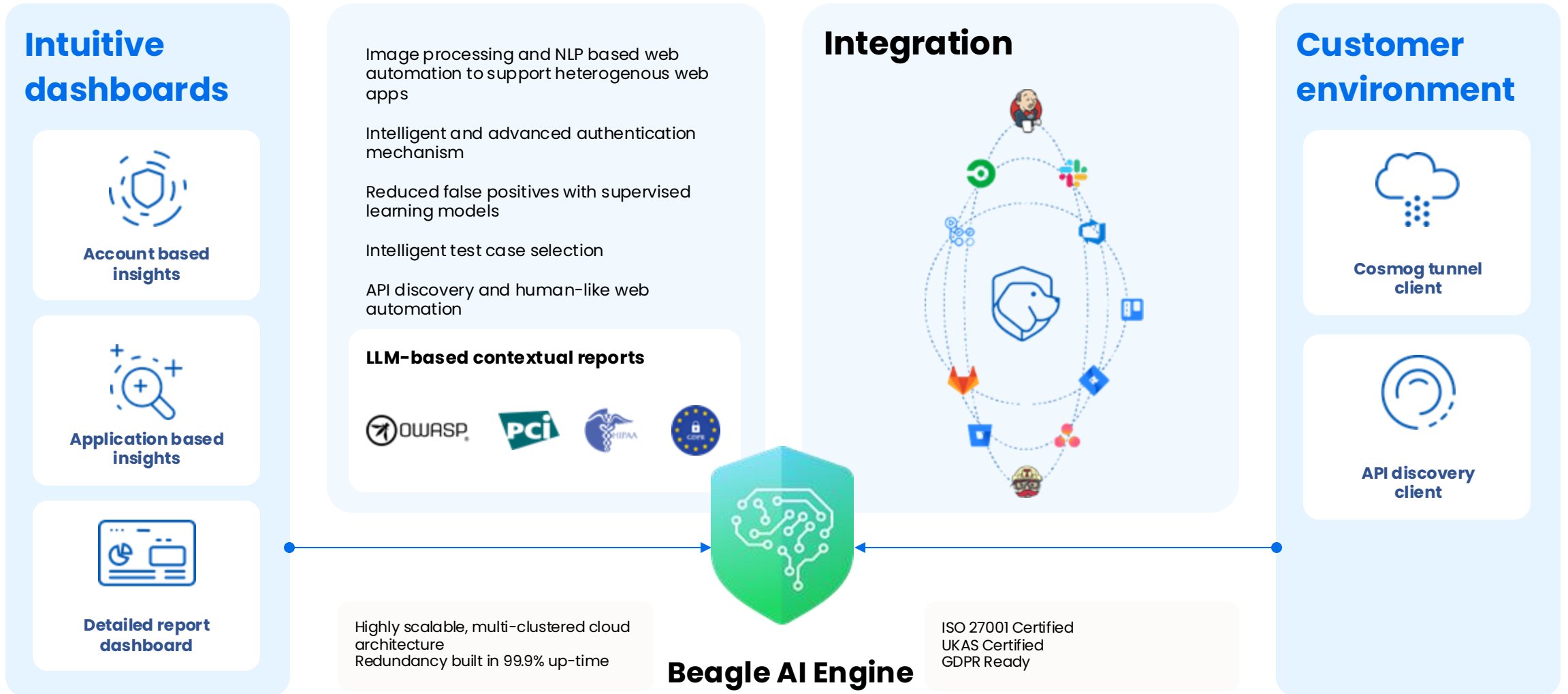


Cost savings

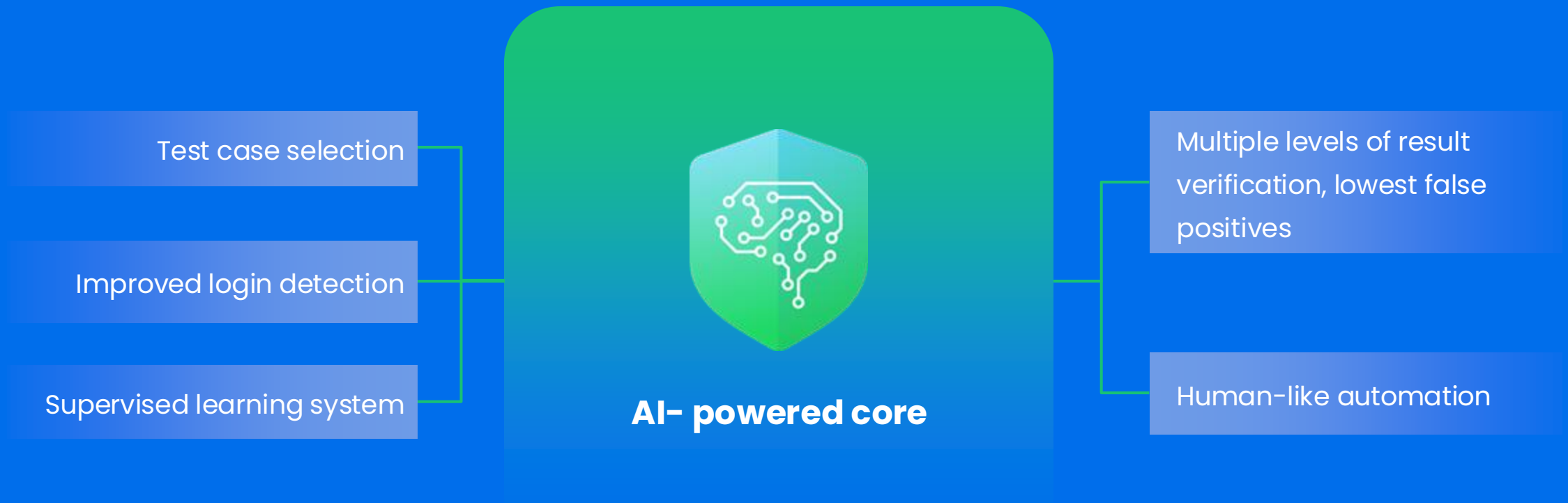
What are the basic problems?



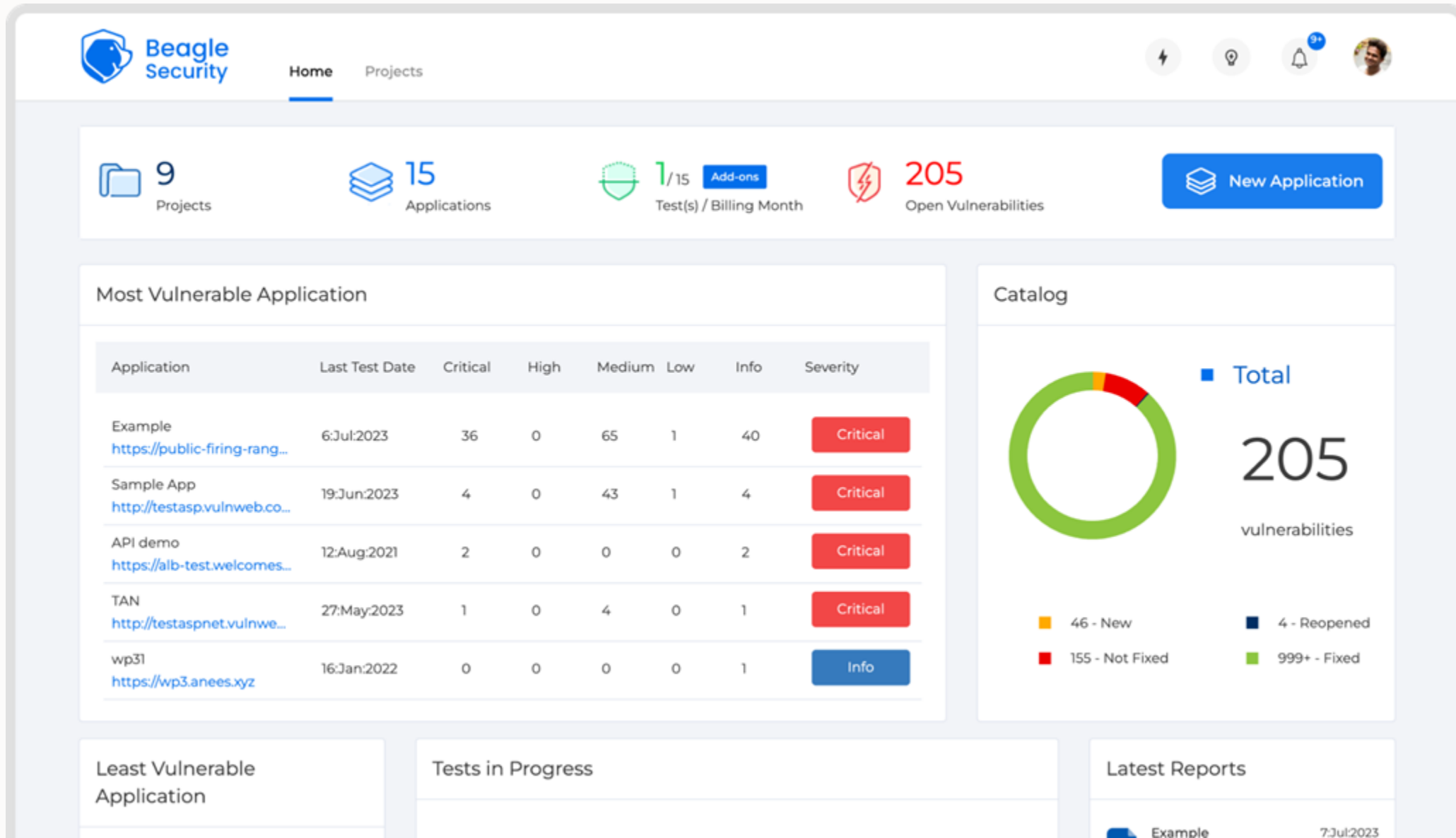
The Beagle Security platform



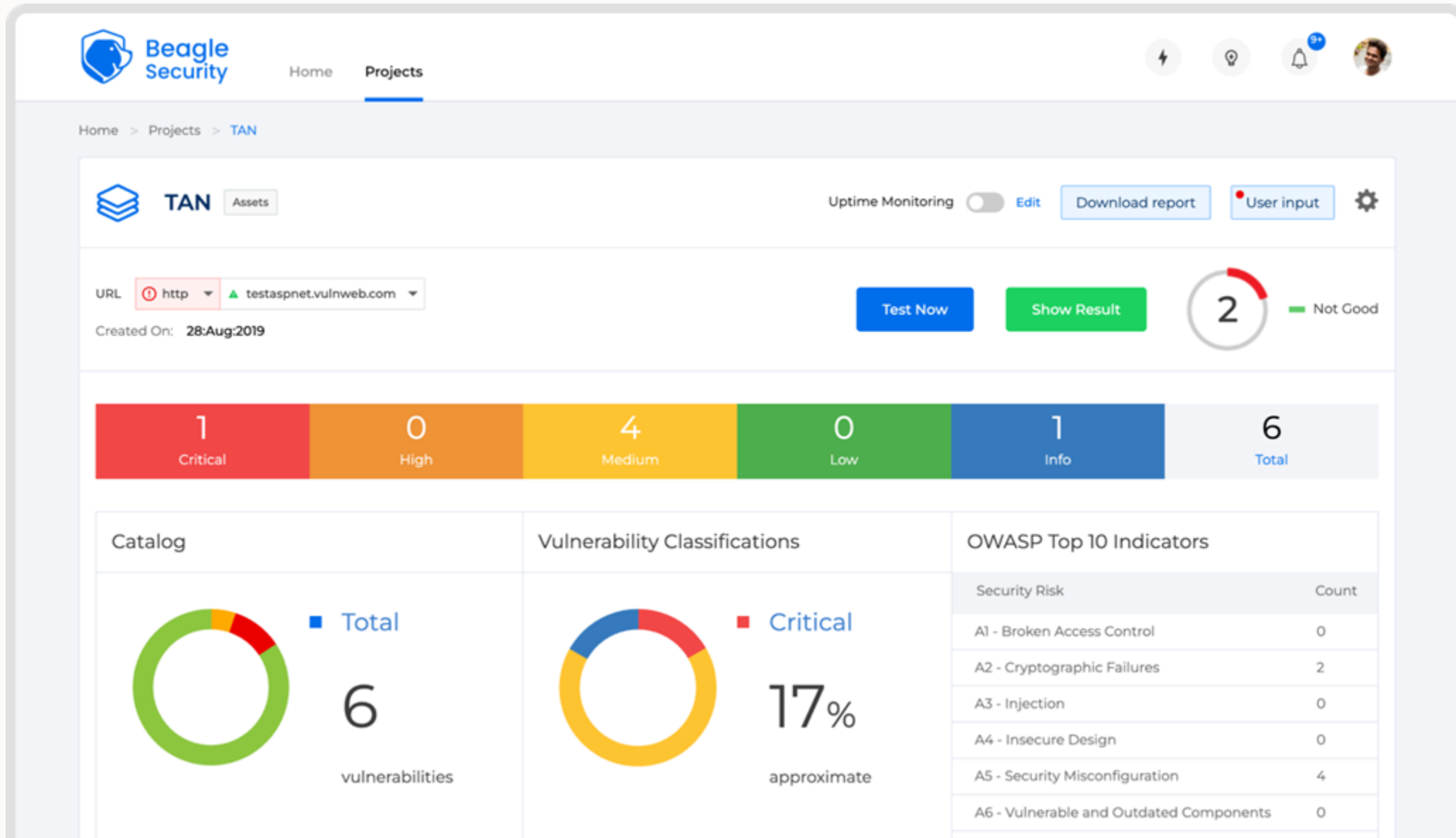
What Differentiates Us?



Intuitive Home Dashboard



Application Dashboards



Contextual, PDF Reports



Beagle Security

Continuous Vulnerability Assessment Platform



API Penetration Test Report

Demo API 2
29 May 2023

Confidential

2. Executive Summary

The executive summary section provides you with charts, tables, and graphs to give you a better understanding of all the vulnerabilities present in the API based on its status and severity. The severity of each vulnerability is calculated based on its occurrence, frequency, and impact on the API.


By examining the graphs generated by Beagle Security, you can know the current level of the API's security and improvement areas.

2.1 Catalog

Status	Count
New	5
Not Fixed	0
Reopened	0
Fixed	4


2.2 Graphical Summary

Vulnerability Distribution



- Critical(80.0%)
- High(20.0%)
- Medium(0.0%)
- Low(0.0%)
- Very Low(0.0%)

Overall Risk score



2
Not good

Confidential

4. Technical Summary

4.1 Detailed Technical Report

4.1.1. SQL injection

OWASP 2019-API8
PCI V3.2-6.3.1
OWASP PC-C3
CAPEC-66
CWE-89

Subpart C, HIPAA-164.306(a)(2)
ISO27001-A14.2.5
WASC-19

CVSS3.1(AV:N/AC:L/PR:L/UR:N/S:U/C:H/I:N/A:H)
WSTG-INPV-05
A12.2.1
PCI v4.0-6.2.4

- Likelihood: High
- Impact: High
- Severity: Critical

Issue Description:

SQL injection is a kind of method used by hackers to access, modify and delete the data from the database. By leveraging SQL Injection hackers will also be able to bypass authentication and access unauthorized data from databases. Potentially allowing an attacker to escalate to more damaging attacks inside the network where the application is hosted.

Recommendations:

1. Use parameterized queries (also known as prepared statements) instead of string concatenation to build queries.
2. Use whitelisting to validate all input data.
3. Escape all user-supplied input data before using it in a query.
4. Use stored procedures to execute database queries.
5. Use the latest version of the database server and configure it securely.

```

$stmt = $db->prepare('SELECT * FROM users WHERE name = ?'); $stmt->bind_param('s', $name); $stmt->execute();

$allowed_inputs = array('first_name', 'last_name', 'email'); $input = $_GET['input']; if (!in_array($input, $allowed_inputs)) { die('Invalid input!'); }

$name = $mysqli->real_escape_string($_POST['name']); $query = "SELECT * FROM users WHERE name = '$name'";

CREATE PROCEDURE get_user_by_name(IN name VARCHAR(255)) BEGIN SELECT * FROM users WHERE name = name; END;

-- Disable information_schema location -- */information_schema { deny all; }
    
```

Confidential

Founders & Team



Rejah Rehim A A

CEO

- 13+ years in cyber security
- Project Lead, OWASP Kerala Chapter
- Commander, Kerala Police, Cyberdome
- Infosec author



<https://www.linkedin.com/in/rejah/>



Prathapachandran V

CTO

- 20+ years in software industry
- Software Architecting & Project Management
- Worked with top players – Hitachi, Toshiba, Schneider Electric, ABB, Daimler AG



<https://www.linkedin.com/in/vprathap/>

Our team strength

30

Our team is a mix of

- Cyber security engineers
- AI engineers
- Product development & support engineers
- Marketing & sales specialists



Our Growth So Far

ARR:

\$293,640

Customers:

1731 (136 recurring)

Countries:

144, >70% from USA

Segments:

72% Small

23% Mid

5% Large



Customer Testimonials



Great DAST tool for a SMB. Easy to use interface with a clear description of the problem and where it should be remediated.



Rick Elder
Director of Cybersecurity at MAXEX



Affordable and easy to use! We are required to complete periodic scanning in order to maintain our accreditation which Beagle Security easily enables.



Roshelle Weir
CEO at Decida

Some of our happy customers:





Achievements



Gartner Peer Insights 4.1/5 star rating overall.

[Check the rating](#)



Highest rated in Web & API security on G2



93% overall customer satisfaction rating on G2 – [check the amazing reviews!](#)



Product Roadmap

Theme	Q1 2025	Q2 2025	Q3 2025	Q4 2025
Advanced API security			<ul style="list-style-type: none">Mobile application security testing	
UX Improvements	<ul style="list-style-type: none">Executive dashboardsMajor platform UI revamp	<ul style="list-style-type: none">Throttling of pentests	<ul style="list-style-type: none">Website improvements	
Enterprise Readiness			<ul style="list-style-type: none">GDPR compliance	<ul style="list-style-type: none">Network asset discovery and PT
Innovation		<ul style="list-style-type: none">AI inferences		<ul style="list-style-type: none">Collective intelligence v1



Funding we are seeking



\$2MM capital raise to reach **\$1.5MM** in ARR by 2025

The fund will be utilized for **marketing & sales** efforts, **product development**, expanding operations in **USA**, and scaling the team

Planning to raise **next round** of fund in **18-24** months for further marketing & sales efforts and product development



Thank You