SYNOPSYS®

DevSecOps Explained

Neil Pathare
Security Consultant, Synopsys

What keeps security and development teams up at night?

Software Security

You need to ensure the software you deliver is secure and can be trusted

Why?

Software is the #1 attack surface for cybercriminals

Development Velocity

You need to ensure security testing doesn't impede the pace of development

Why?

Developers will reject tools & processes that slow them down

Business Risk

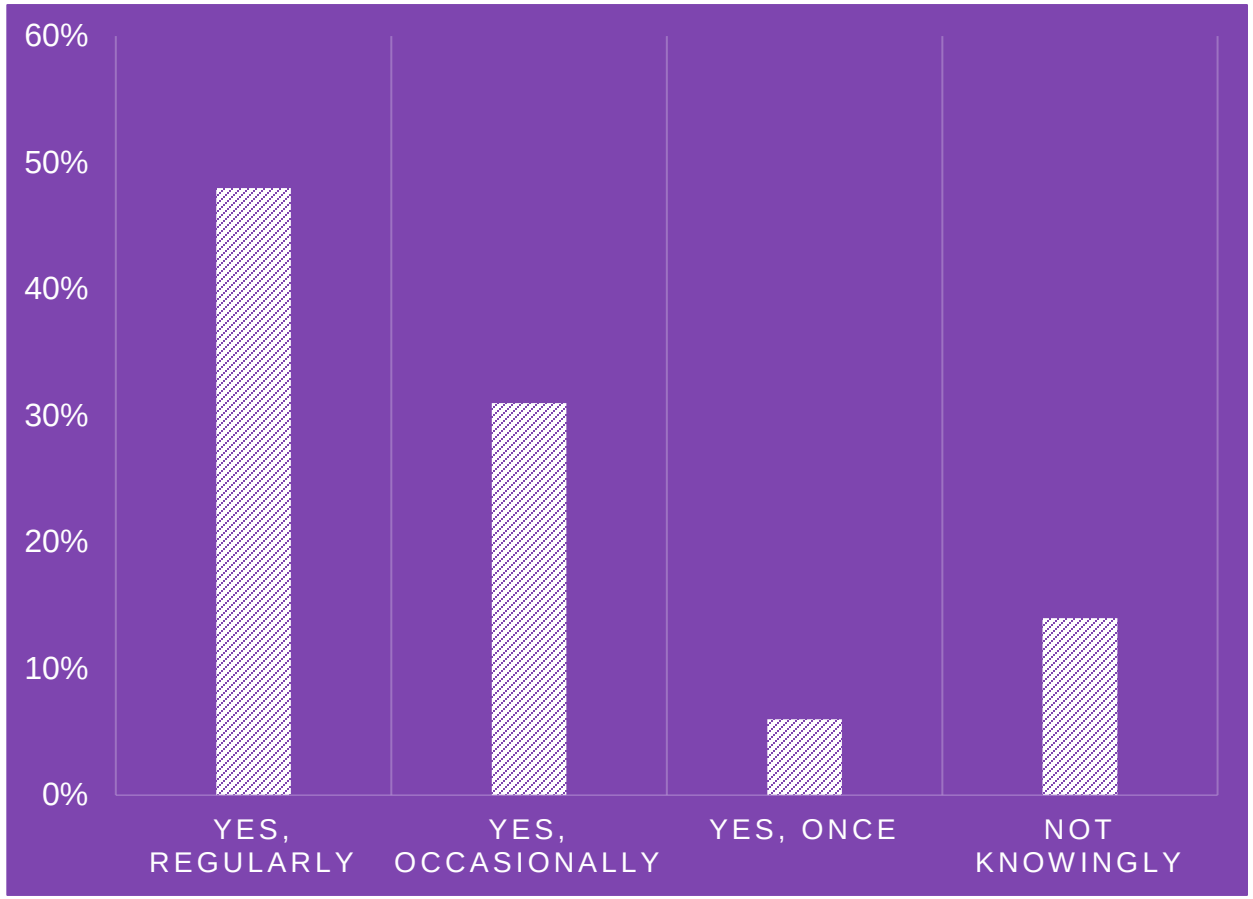
You need to identify and focus the true business risks buried in the sea of findings

Why?

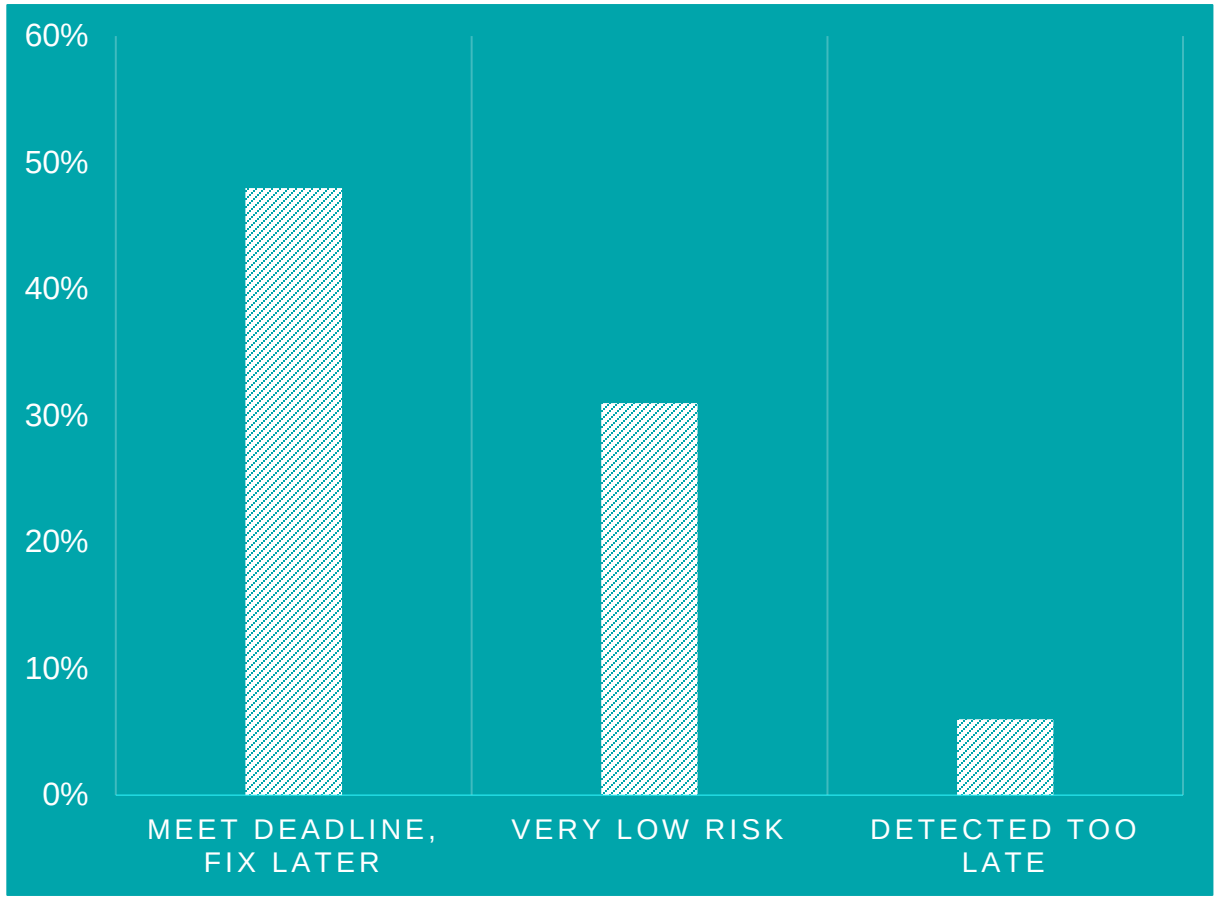
Teams are overwhelmed by vulnerability remediation

Organizations are pushing vulnerable code

Do organization push vulnerable code?



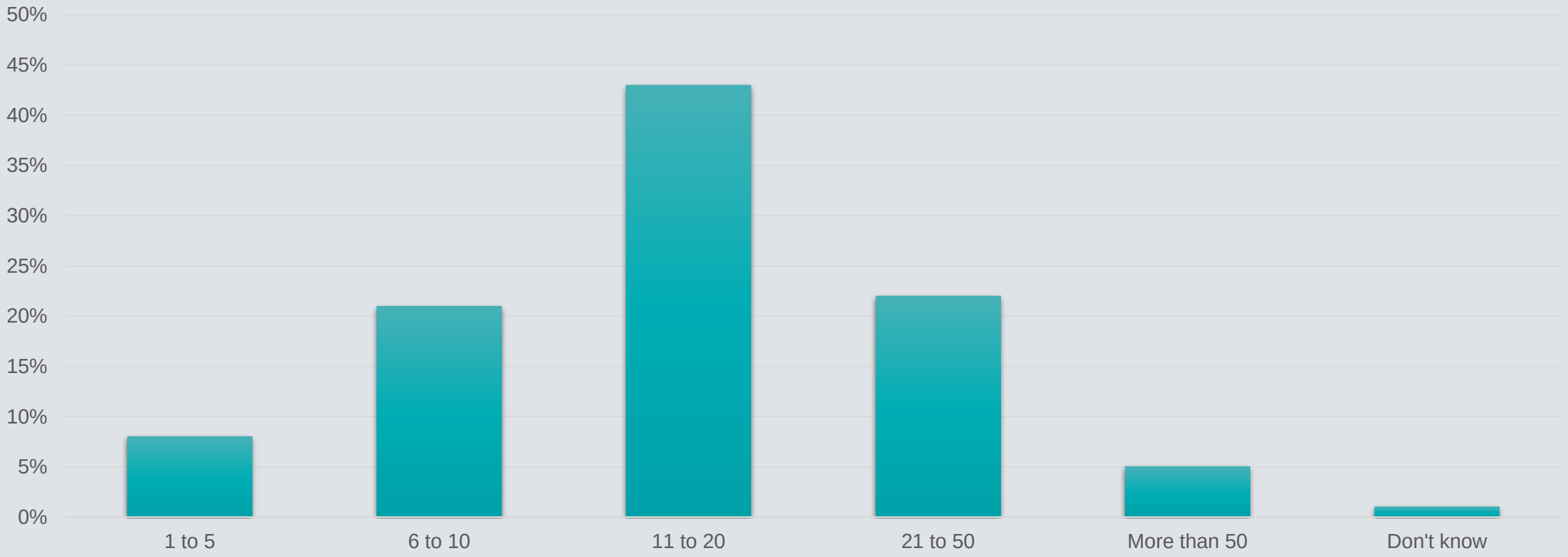
Why organizations push vulnerable code



Source: Enterprise Strategy Group

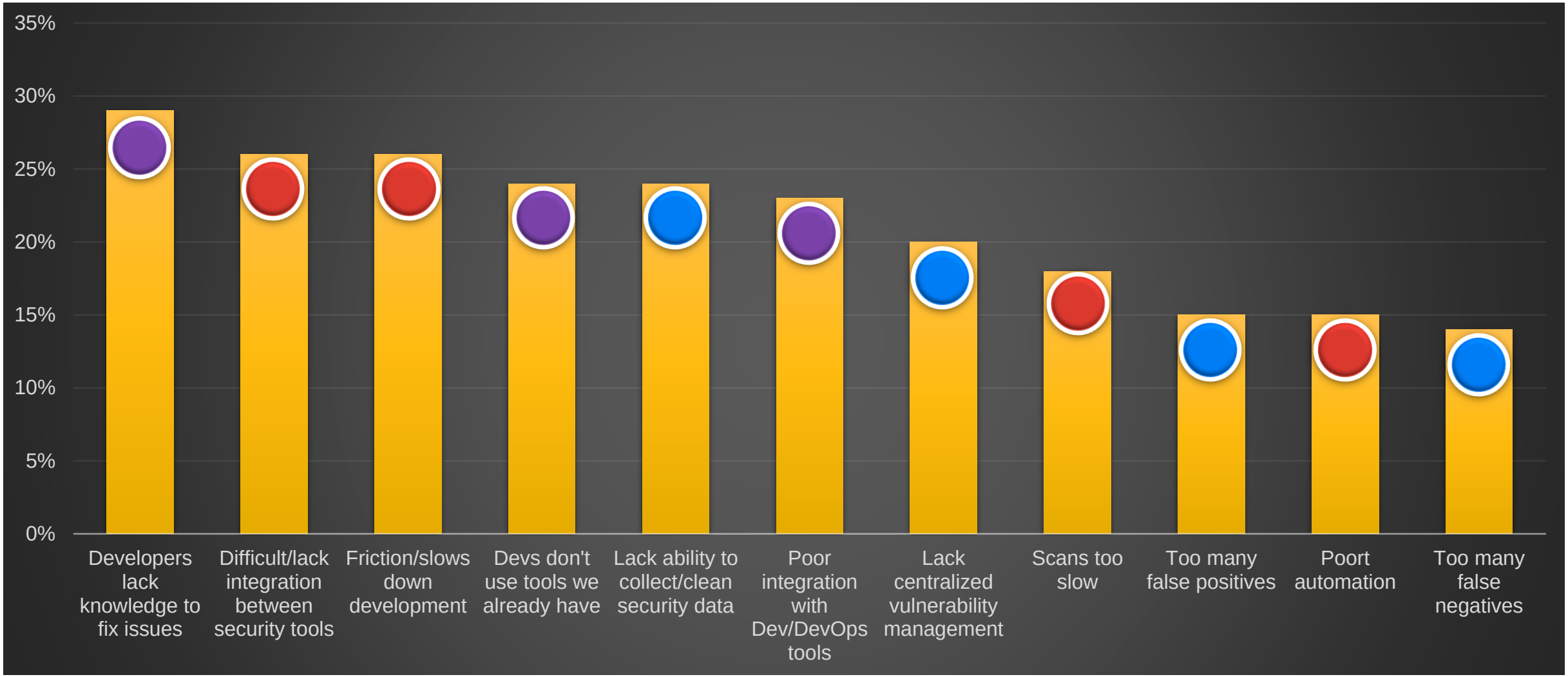
The reality is that organizations have lots of AST tools

How many individual application security testing tools is your organization currently using?



Source: Enterprise Strategy Group

Challenges impacting implementation of AST tools and processes



Source: Enterprise Strategy Group

Application security is evolving to meet the needs of DevOps

AppSec staff are being deployed into DevOps teams

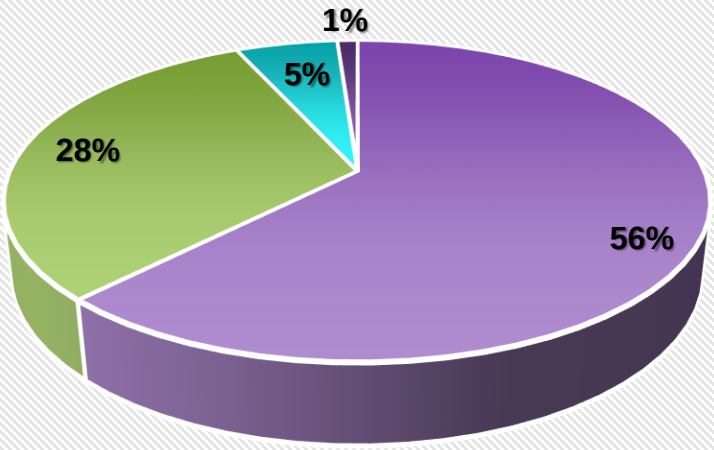
Teams are increasing use of ”policy as code”

Continuous testing is on the rise

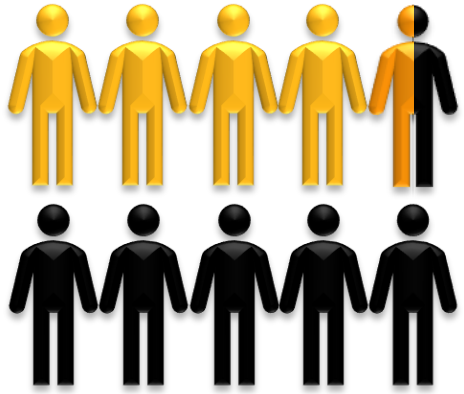
Tests becoming smaller, timely, more frequent

DevOps integration is important to AppSec programs

Level of DevOps and AppSec Integration



- We use a highly integrated set of security controls throughout our DevOps process
- We use selective controls, but continue to invest in integrating additional controls
- Our application security tools are not well integrated into our processes
- We are pushing security as far left as possible in our processes



43%

Believe **DevOps integration** is most important to improving AppSec programs

Source: Enterprise Strategy Group

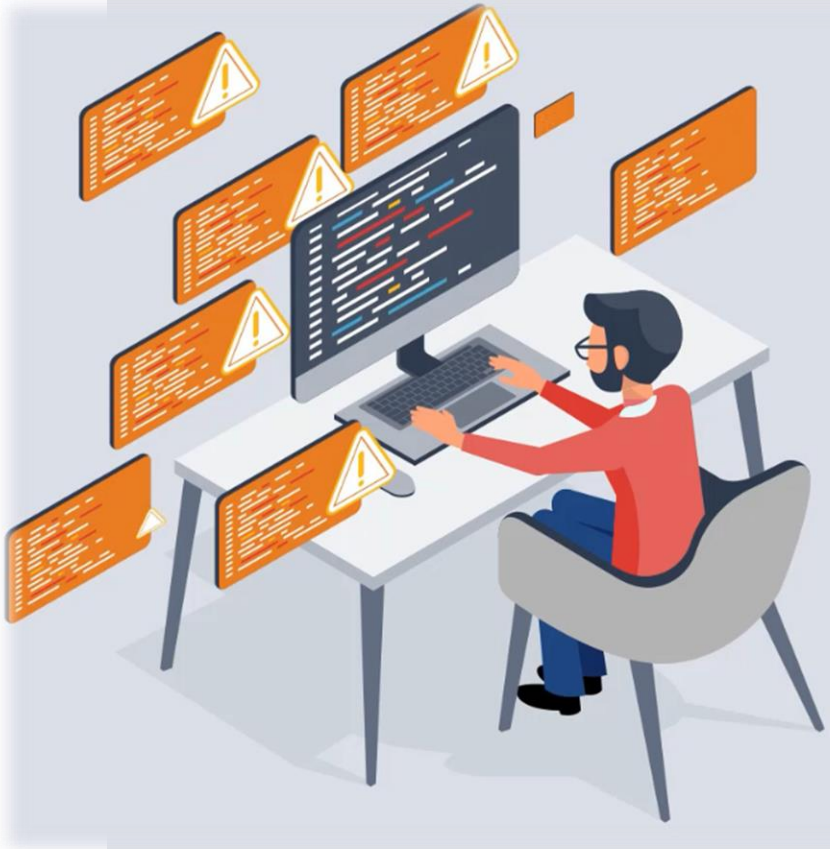
Building trust in software is not simply about installing tools

It's about ensuring your people, processes, and technology are aligned to address security risks at all stages of the application lifecycle.

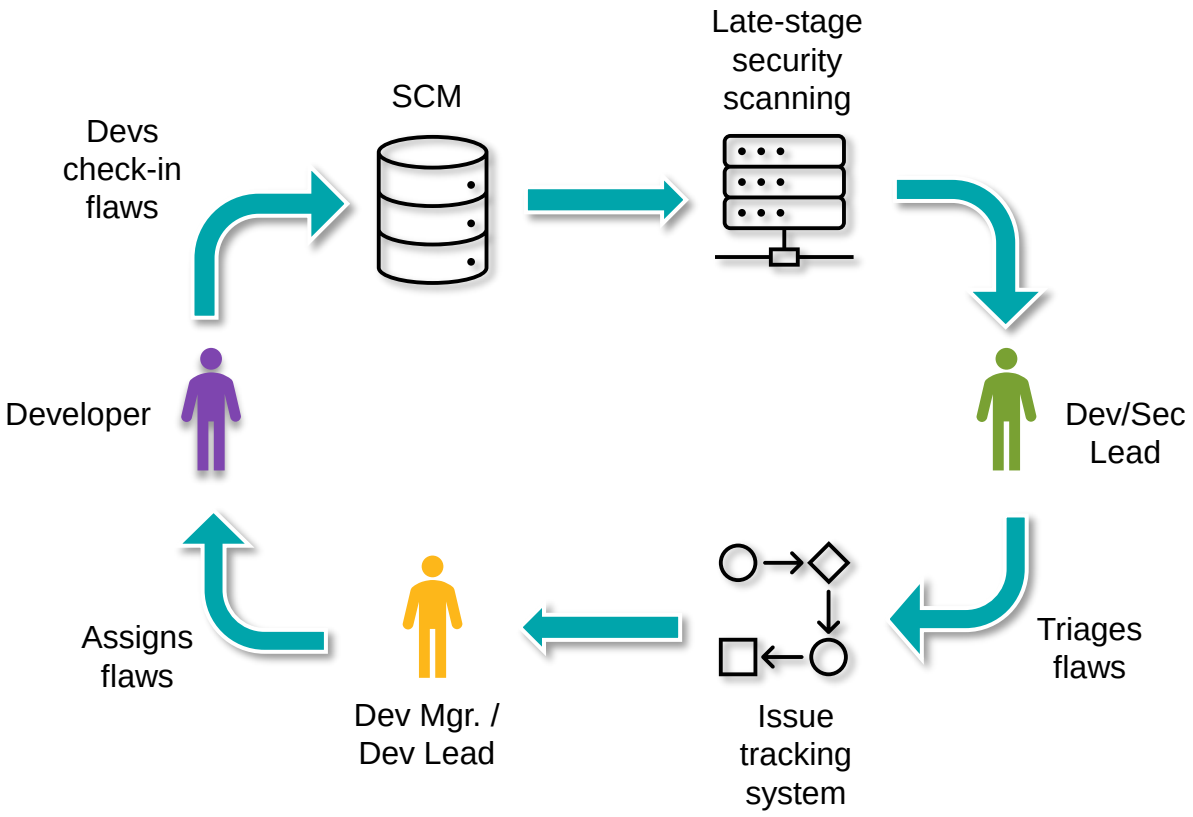
What many teams do today

Bolt-on DevSecOps

- Isolated manual and automated AppSec activities
- Complex, brittle, and slower build / release pipelines
- Lots of noise within the findings
- Difficult to identify the highest-priority software risks
- AST performance not aligned with build and release SLAs



Devs face their own challenges: *DevOps* + *Security*



- Tool fatigue and impediment
- Speed vs Quality conflict
- Pipelines vary based on tech stacks
- SDLC varies between apps
- No uniform way to provide continuous feedback
- Scaling remains a challenge

Pipeline congestion

Vulnerability Overload

DevSecOps is not simply about integrating and automating AST tools.

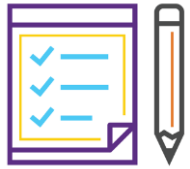
*It's about maximizing velocity by **intelligently running the right tests at the right time** and giving teams the ability to focus on issues that matter most to the business.*

Defining a path toward DevSecOps

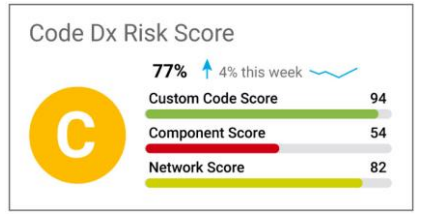
- **Velocity**
  Run just enough tests to meet security and risk needs without bogging down your pipelines or developers.
- **Efficient Efficacy**
  Accelerate testing, close DevOps feedback loops quickly, and address what matters most first.
- **Security Enablement**
  Establish standards and foster risk awareness across the pipeline and functional roles.
- **Scale**
  Simplify the integration into pipelines to facilitate rapid deployment, with modular AST for contextual testing.

Consider this: *Intelligent, policy-driven DevSecOps (NIST 800-53)*

AppSec Program Objectives & Metrics



Policies



Actionable insights into software risk

Policy Management

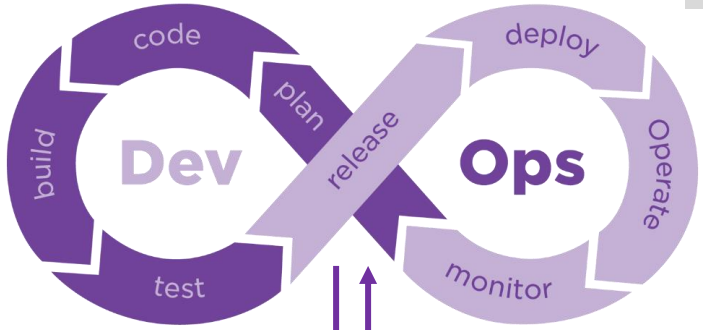
Executes the right tests, at the right time, at the right level; triggers manual tests

Insight Management

Correlates, prioritizes, and tracks remediation. Centralizes risk visibility

Secure Development

Deliver actionable risk insight and remediation guidance to developers in their workflow



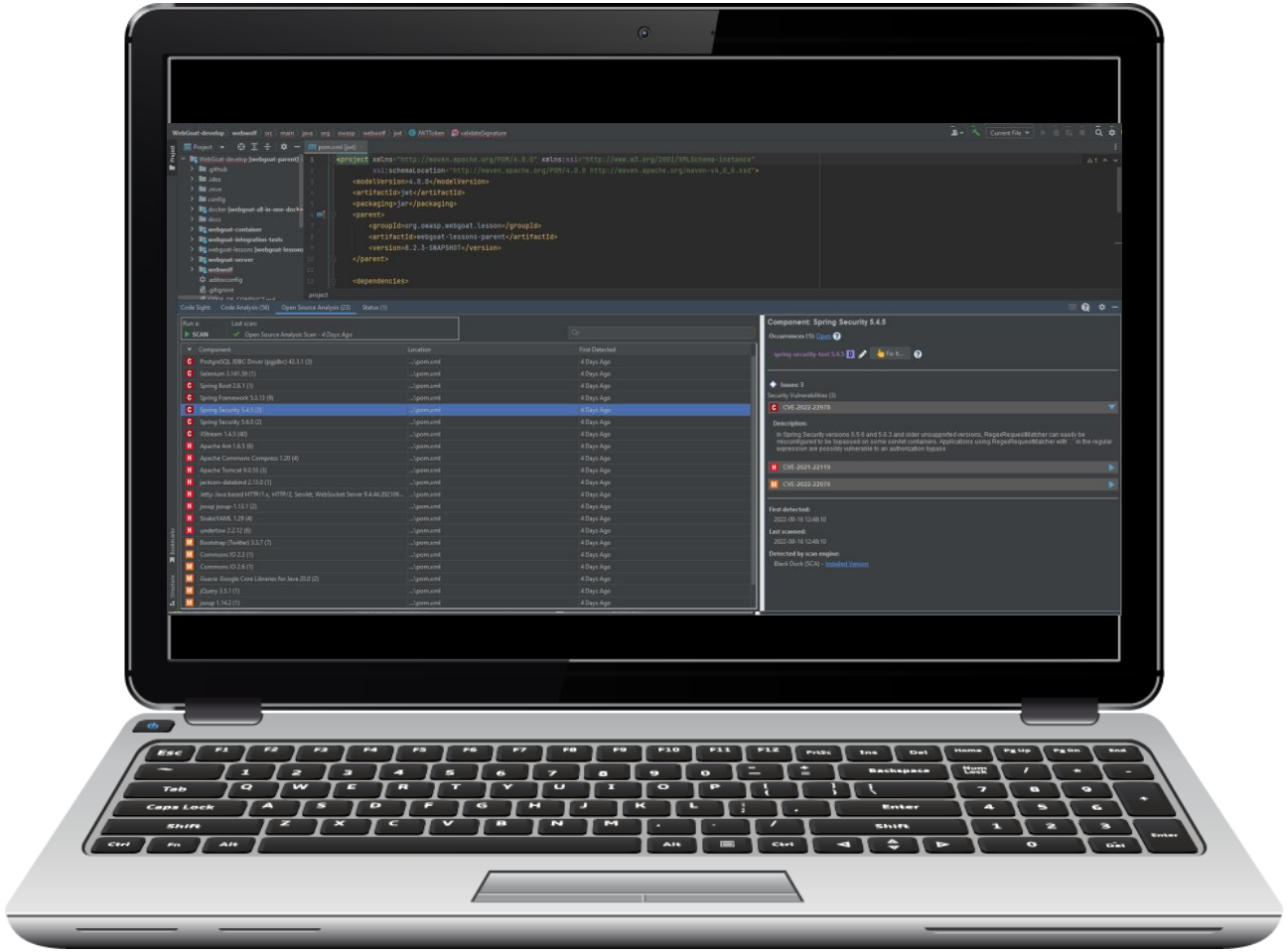
Prioritized tickets for remediation

Jira

Threat Model | Code Review | SAST | SCA | IAST | DAST | Pen Test | Risk Analysis

Secure Development

IDE-based rapid security testing (*e.g., Synopsys Code Sight – SAST, SCA*)



Secure code as it's being written

- Analyze source code, open source, and IaC
- Real-time alerts to new risks as devs code them

Maintain development velocity

- IDE plugin suits existing dev workflows
- Flexible, rapid, automatic or on-demand scans

Write better code

- Detailed remediation guidance minimizes time to fix and raises developer security standards
- Find and fix security and quality defects.

Functional Security Tests

Get more “testing” without running more tests (*e.g., Synopsys Seeker – IAST*)

Analyze running apps in pre-production

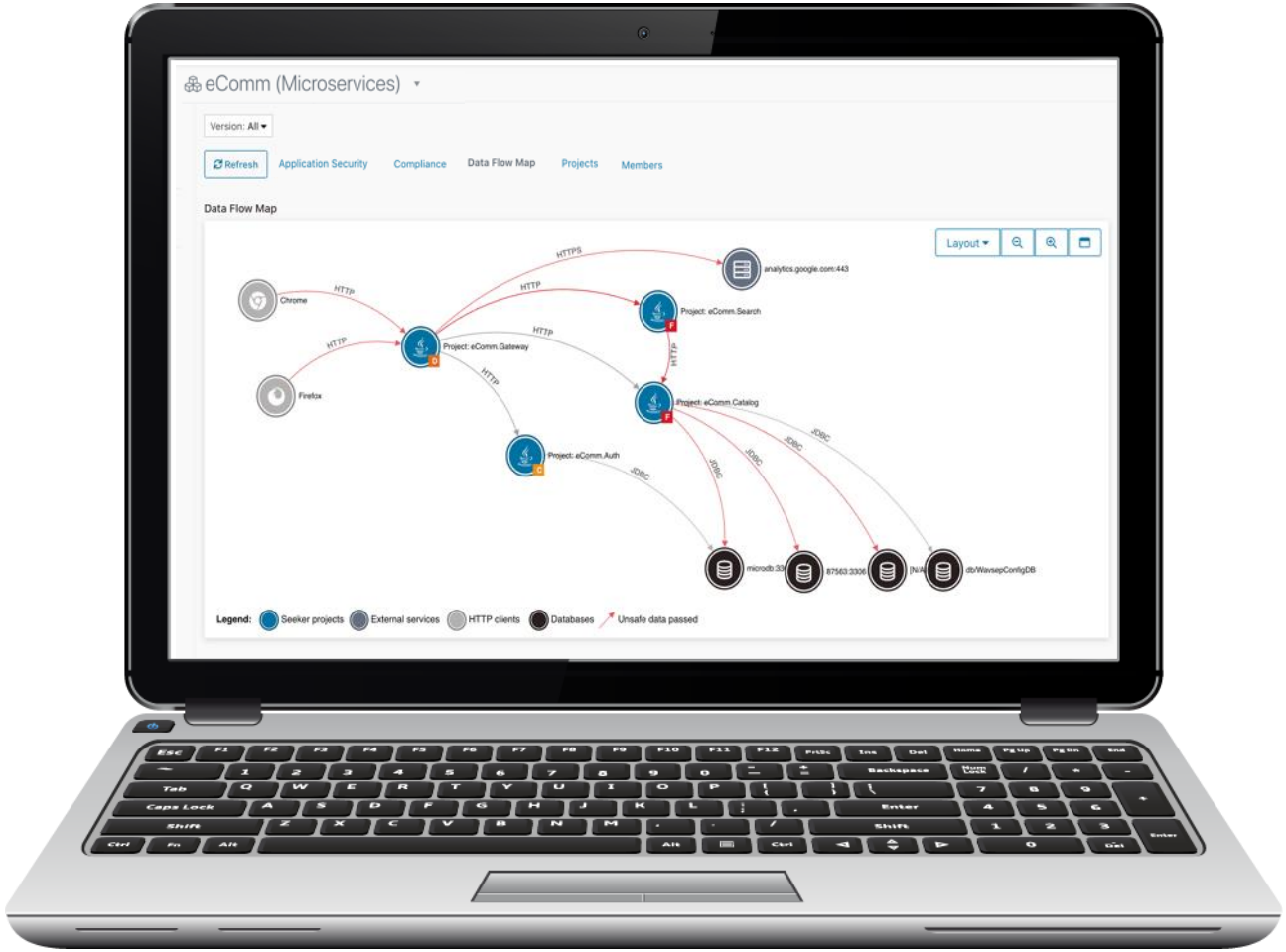
- Visibility into executed code and runtime data
- Continuous testing, real-time results, and automatic vulnerability verification
- Data protection compliance and leakage tracking

Test the spectrum of modern applications

- Web Apps, Web APIs, mobile app back-end, serverless functions, containers, or microservices
- Enhance protection against supply chain risks

Integrate for seamless detection and alerts

- Deploy and run via CI/CD
- Automatic ticket creation or pipeline interruption



API Security Tests

Discover and test APIs (*e.g., Synopsys Seeker – API Testing*)

Discover

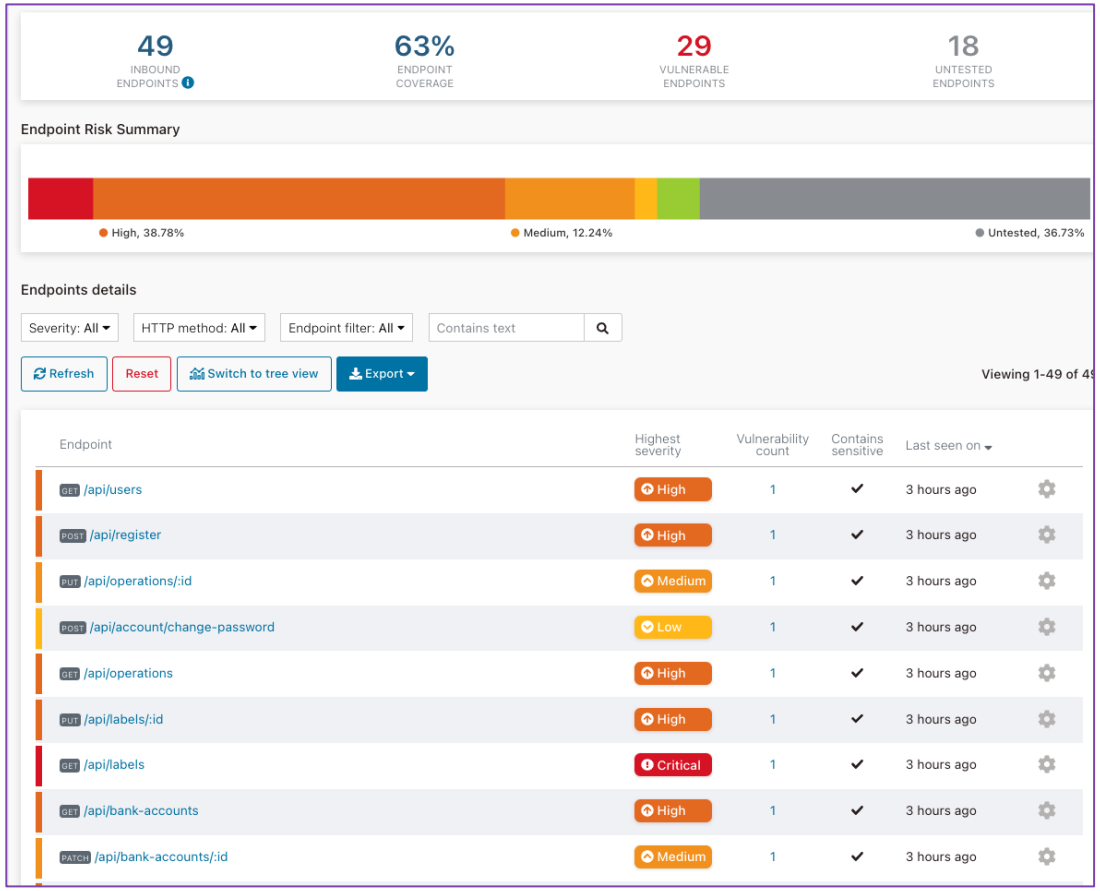
- Automatically discover all endpoints/APIs
- No upfront documentation requirements.

Assess

- Tools should automatically detect outbound endpoints/APIs used by the application.
- Simultaneous vulnerability assessment of APIs and Web interfaces.
- Provide a white/grey box experience.
- Complete inventory of endpoints with vulns and sensitive data.

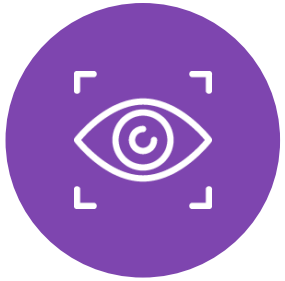
Integrate

- Deploy and run via CI/CD.
- Support all modern infrastructure, including microservices, docker, k8s, cloud native, serverless, etc.



Dynamic Security Tests

Dynamic Application Security Testing (*e.g., Synopsys WhiteHat – DAST*)



Full Visibility

Delivers full visibility and the front line of defense for secure DevSecOps

Intelligent Prioritization

Automates the prioritization of results based on machine learning

Continuous and On-Demand Risk Assessments

Provides continuous and on-demand scanning to automatically check for vulnerabilities

Production-Safe

Scans production servers safely and without causing any downtime - saving valuable time, resources, and cost

Insight Management – Application Security Orchestration & Correlation (ASOC)

Actionable insights into AppSec risks across the organization (*e.g., Synopsys Code Dx*)

Correlation and Prioritization

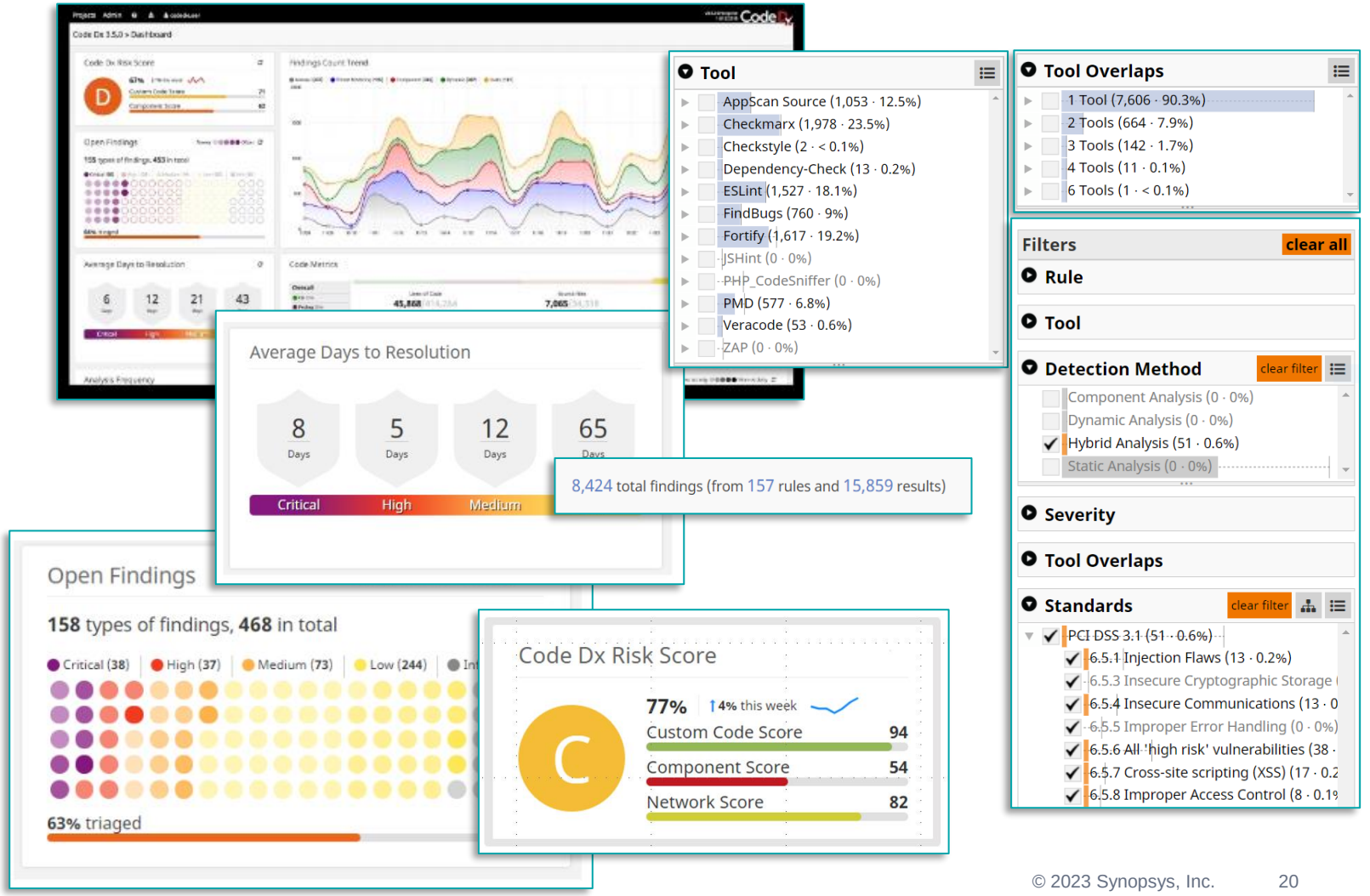
- Identify and focus on issues with the highest business risk

Consolidated Dashboard

- View of AppSec activities and software risks across your entire organization

AppSec System of Record

- Track when software was tested, what was found, and when/if it was fixed



Thank you

Visit **Synopsys.com/Software-Integrity** for more information.

Gartner Magic Quadrant
for Application Security Testing (2023)

Build Trust in Your Software