CyberRes

Next Generation DAST

Fortify WebInspect & ScanCentral DAST

FY21 Sales Play

Agenda

- Why DAST?
- Why Fortify DAST?
- Why DAST complements SAST
- Shifting DAST left/the evolution of DAST
- What's new in 20.2?

Why DAST is Important

- Independent of the application
- Immediately finds vulnerabilities that could be exploited
- Does not require access to the source code

Fortify DAST-WebInspect delivers comprehensive coverage

Dynamic application testing
Comprehensive dynamic web application testing with the breadth of coverage needed to support modern applications.

Security compliance standards
Pre-configured policies and reports for major compliance regulations, including PCI DSS, DISA STIG, NIST 800-53, ISO 27K, OWASP, & HIPAA.

Crawl modern frameworks and APIs
Powerful scanning integrations that enable API and single-page application testing at scale.

Manage AppSec risk at scale
Automation and workflow integrations help meet the needs of DevOps. Monitor trends and use dynamic analysis to take action on vulnerabilities

Shift DAST left
Drive fast and highly focused results earlier in the SDLC with custom scan policies and incremental analysis support.

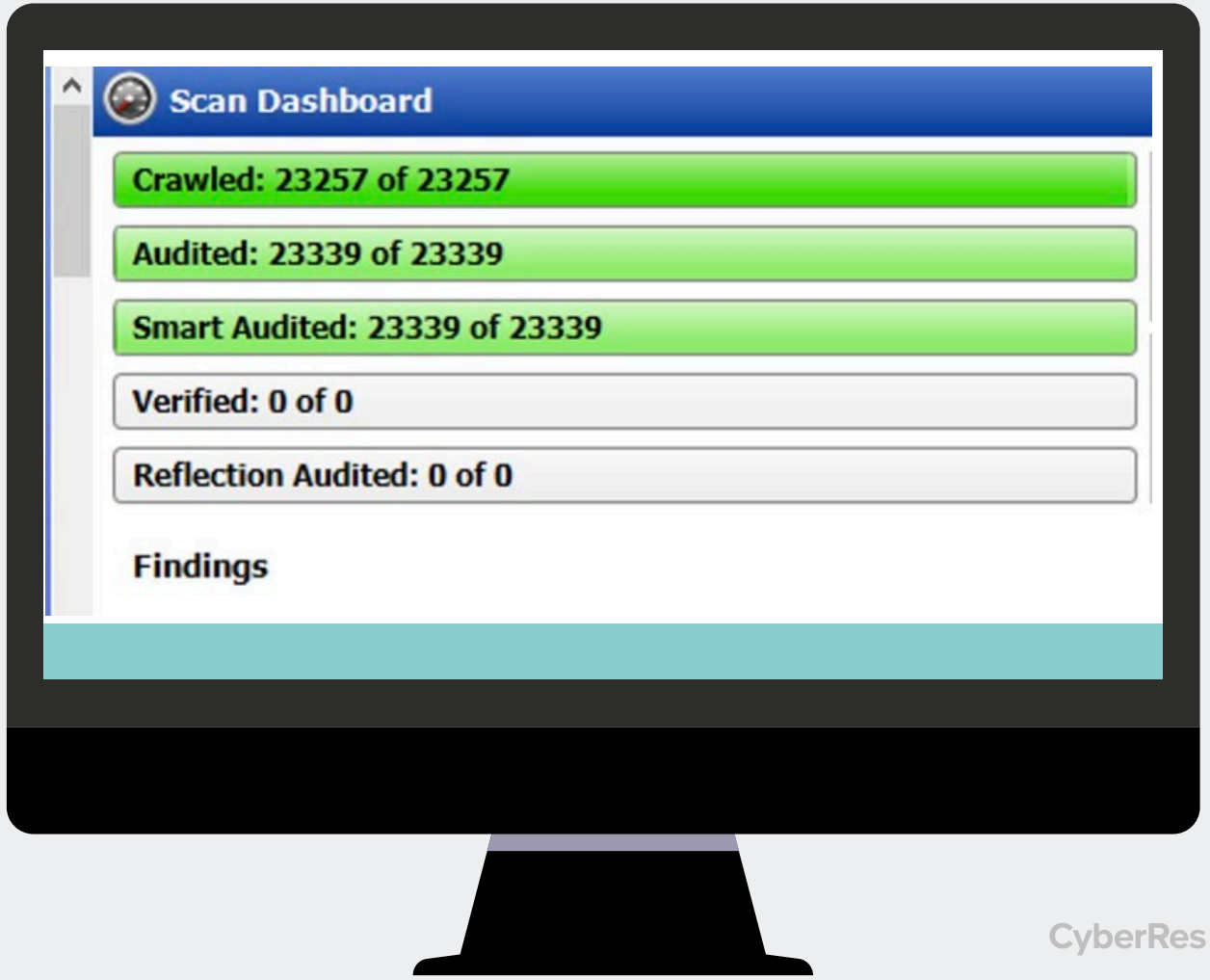
ScanCentral DAST
Centralized platform that allows you to run hundreds of thousands of scans, which gives dev teams the ability to run dynamic scans on their own. By using ScanCentral DAST as an orchestration platform, a small team of AppSec professionals can support an entire organization.

Comprehensive scanning finds more vulnerabilities

WebInspect has the broadest DAST coverage and detects new types of vulnerabilities that may go undetected by traditional black-box security testing technologies.

Scan basic APIs in seconds with support for OpenAPI (Swagger).

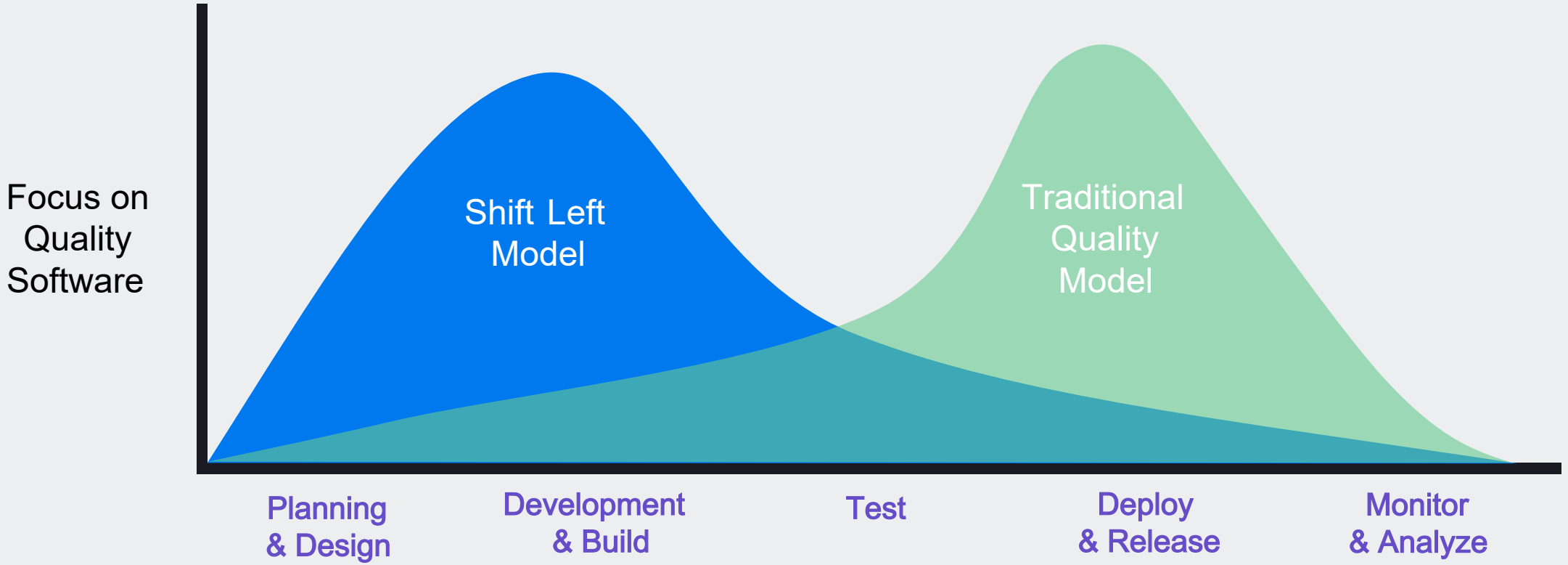
For more advanced API scanning scenarios, use WebInspect's Postman integration to support unique workflows, complicated authentication, and custom parameter requirements.



Why SAST + DAST with Fortify makes sense

	Customer Value
Holistic AppSec	▪ Launch both SAST and DAST from Software Security Center (SSC). You don't have to decide between on or the other. Users have the flexibility to run any combination of static and dynamic scans.
Consistent Remediation Guidance	▪ A common vulnerability description allows developers to spend less time researching vulnerabilities, and more time remediating
Prioritization	▪ Overall security is enhanced as the unified taxonomy enables customers to focus on most important findings first
Layered Defense	▪ By leveraging static analysis early in SDLC, and dynamic analysis later in the SDLC and into production, security teams can deliver greater security
Feedback Loops	▪ Organizations that identify vulnerabilities early in SDLC and continue to detect in production can focus resources on addressing systemic problems

What does it mean to Shift DAST Left?



Why shift DAST left?

- 42% of firms that experienced an external attack said it was carried out by exploiting a software vulnerability
- 35% said it was through a web application

Source: Forrester, The State of Application Security 2020

Business Need for Shifting DAST Left

- **Accelerating time** from design to deployment
- **Reducing costs** of rework
- **Greater awareness** amongst developers of quality and testing requirements

Source: Forbes, 2018, *Shift Happens, Why Your Software Needs to 'Shift Left'*

What’s New in 21.2

Release Summary

WebInspect 21.2

API Discovery

- Users aren't aware of all the APIs —they don't always know there is an API in their application. Now WebInspect can detect APIs automatically.

Modern App Support

- Engine updates ensure WebInspect keeps up to date with current trends and is always able to scan applications.

2FA support

- More and more orgs are requiring two -factor authentication (2FA). Many organizations had to work around this, but it's WebInspect supports this automatically so scans can avoid getting paused.

- Engine 6.1 (improved performance and accuracy)
- TruClient
- DOM XSS Engine (test a DOM fragment)
- 2FA Support, once this is configured it is a hands -free scan

* New features to the DAST market

Features & Benefits

WebInspect 21.2

	Pain Point	Main Benefit	Additional Benefits
2FA Support	Couldn't do it before, now we can. More and more orgs are requiring it. It's becoming a standard. Many orgs would have to do a workaround, or having to manually watch a scan to log in. Now it's automated. Now you don't have to turn it off or skip scanning those apps.	Hands-free, set it up through Android app or email.	
Engine 6.1 Updates	Out of date with the latest apps.	TruClient (macro recorder) update. Supporting modern applications. Continue to scan any app anyone writes. ECMAscript , we keep up to date this this to make sure we can scan any app.	DOM XSS Scan Engine. Test a DOM fragment where you couldn't before. DOM fragment is purely client -side code. Client -side fragments are things that don't make a request to the server, but change the page within the browser. We now have the ability to test the things that only exist within the browser itself, not just what goes to the server.
ScanCentral Visualization	Won't need a separate tab.	You'll be able to view the scan results in a new tab within the browser.	
ScanCentral Advanced Prioritization	Having to wait for scans to complete when you have higher priority apps to scan.	If the low -priority one is already running, it will be paused for the higher -priority scan. Pausing of existing scans and moving them around.	

Features & Benefits

WebInspect 21.2

	Pain Point	Main Benefit	Additional Benefits
Automatic State Detection	If you find an API mid -scan, but you don't authenticate against it, that doesn't do a lot of good. You have to always be an authenticated user.	It helps enable the automatic state detection User doesn't need to configure this now. They don't have to onboard applications. We pick up the state and apply it automatically. Automating the authentication for APIs	Complementary with In -scan API discovery. Gives us the ability in APIs to capture the common authentication mechanisms, Oauth , Beaer Token, JWT. We can pick that up and be able to log in automatically without the user being involved.
In-scan API Discovery	Users aren't aware of all the APIs, they don't always know there is an API in their application.	Automatic Swagger definition. We can pick up automatically add the API to the current scan.	

ScanCentral DAST

ScanCentral in Software Security Center (SSC)

Fortify's Centralized Scanning Solution allows small teams of AppSec Developers to deliver scalable, dynamic and static, scanning solutions to large teams of developers.

Scalable dynamic analysis farm

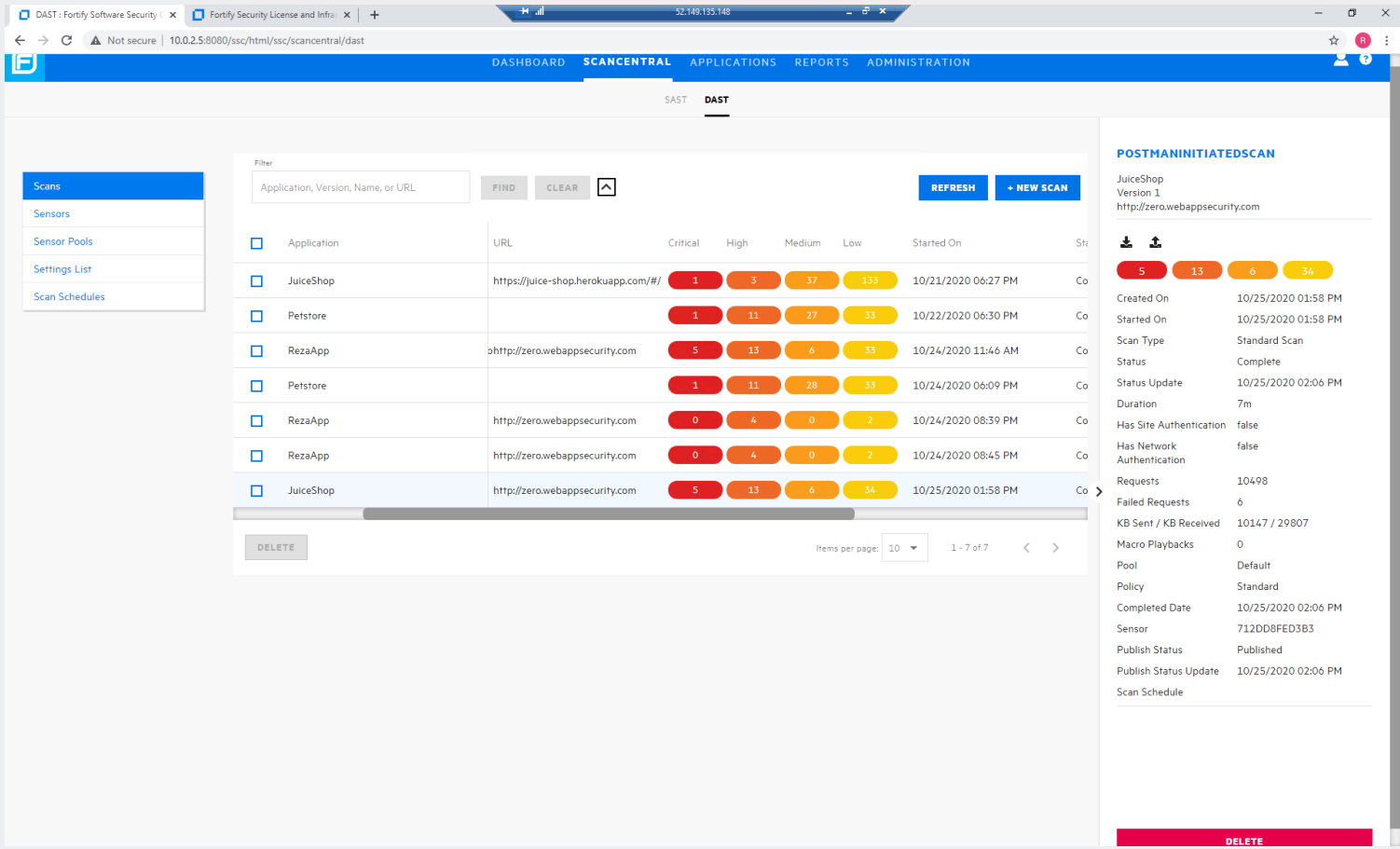
- Dynamically scales up or down to meet the changing demands of the CI/CD pipeline .

DevOps scan solution

- Integrates into popular CI/CD solutions like Azure DevOps.

Flexible licensing

- Flexible licensing allows teams to choose between scanning methodoligies based off need, whether that's CI/CD, ad -hoc, scheduled, etc.

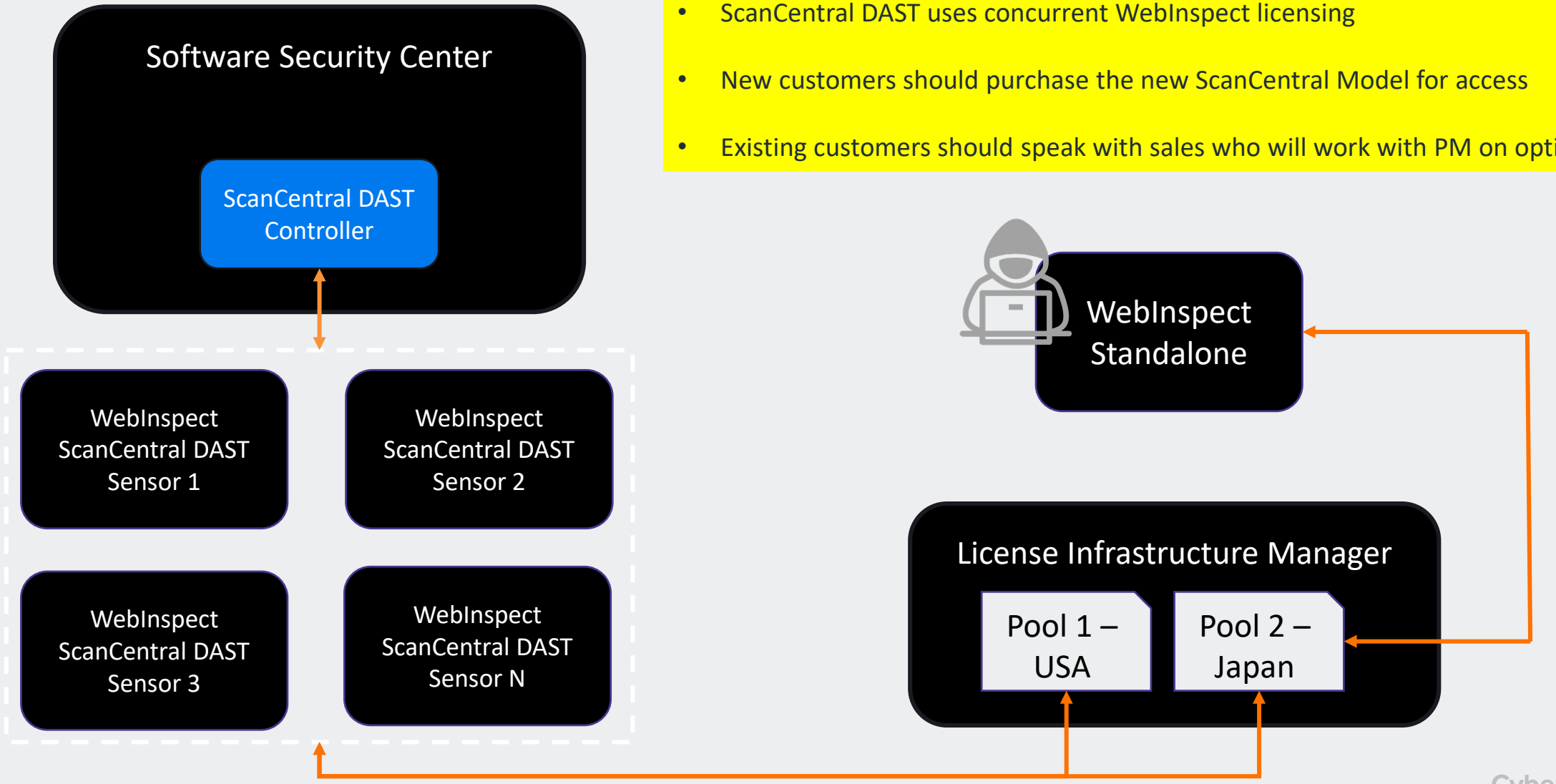


Automation Improvements

- **ScanCentral DAST**
  - Containerized controller, LIM, and scanners
    - Simplified deployment and management via containerization
    - WebInspect sensors used to take 1-2 hours to install, but now it's instant—no installation required.
    - Simplified automation of dynamic scanning whether it's through CI/CD, ad-hoc scans, or setup scans
    - Integration into Azure DevOps
    - Simplified API scanning
    - United static and dynamic platform

ScanCentral DAST - Licensing

- ScanCentral DAST uses concurrent WebInspect licensing
- New customers should purchase the new ScanCentral Model for access
- Existing customers should speak with sales who will work with PM on options



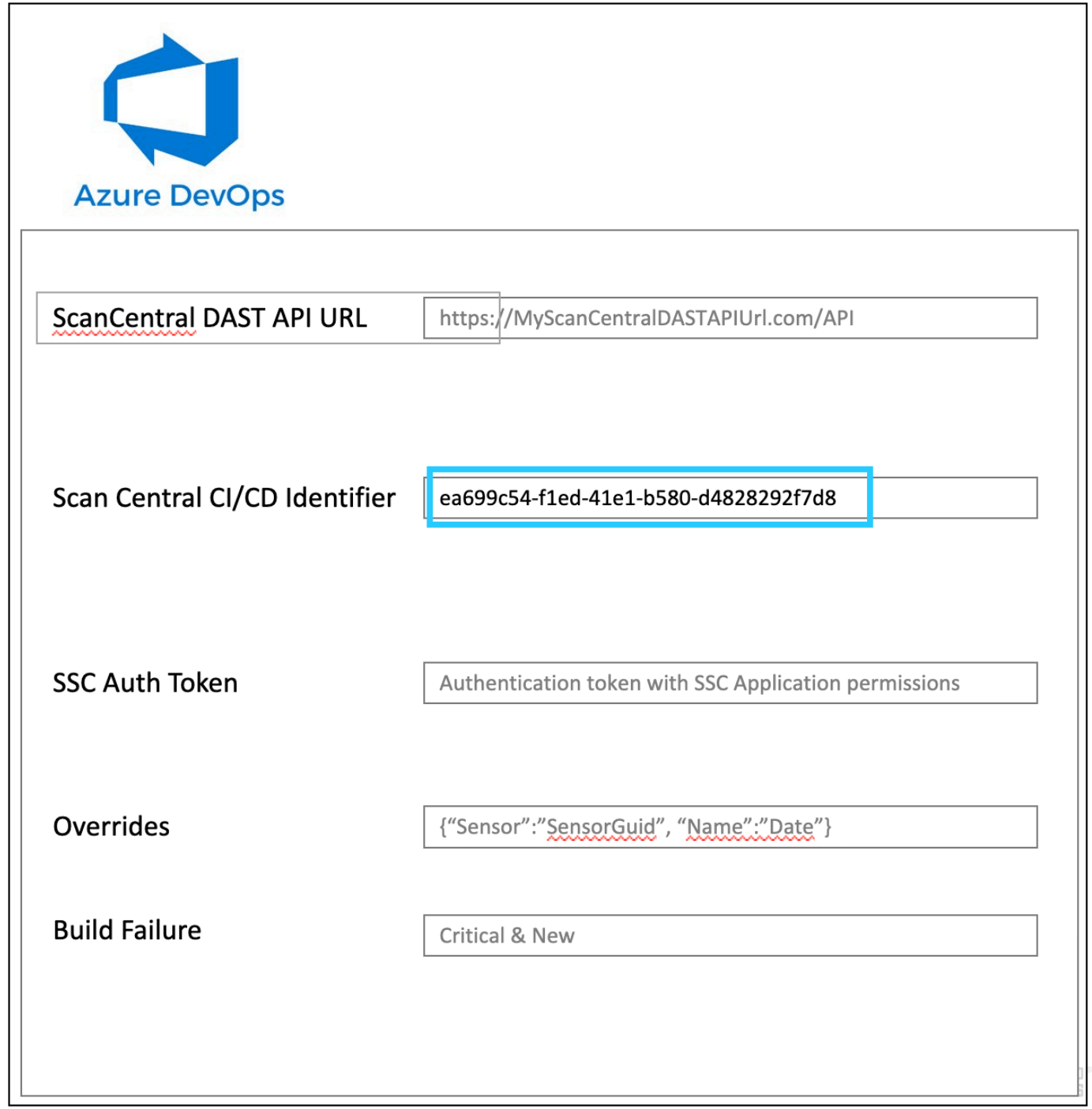
Scan Central DAST

Azure and Jenkins Plugin

Extending the existing Fortify Jenkins and Fortify Azure plugins to support starting a DAST scan from the new Scan Central DAST integration.

Requirements:

1. **Scan Central DAST API URL** – This is the URL which the plugin will need to communicate with to trigger the scan.
2. **Scan Central CI/CD Identifier** – This is the template ID which the user will pass in that references the scan configuration that the plugin should execute
3. **SSC Auth Token** – An authentication token with access to run a scan from the project version associated with CI/CD identifier
4. **Overrides** – A JSON payload which allows for future extensibility
5. Plugin writes a scan start status to the Jenkins or azure log based on response from ScanCentral DAST API.



Fortify