CyberRes

Shifting DAST Left

Fortify WebInspect & ScanCentral DAST

Stan Wisseman, CyberRes GTM Chief Technologist, NA

Securing digital transformation across the value chain

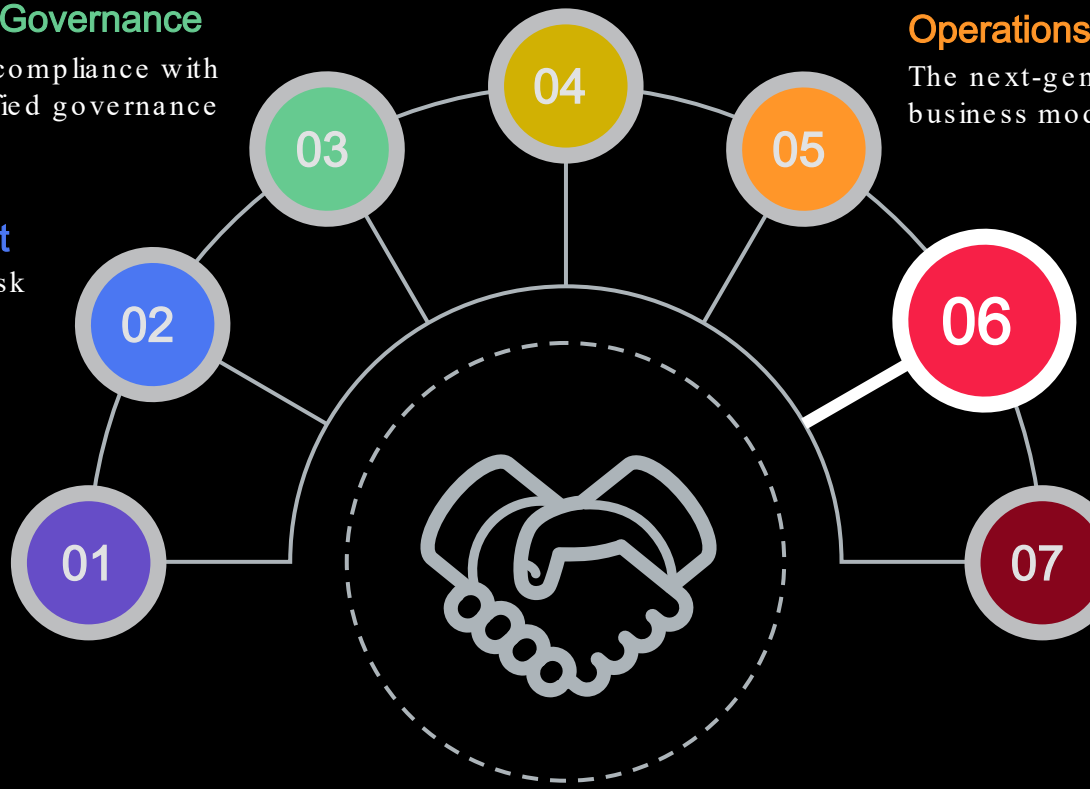
The road ahead will depend on cyber resilience like never before

Privacy and Compliance
Accelerate trust and compliance in data privacy and security

Data, Access, and Identity Governance
Reduce risk and enable compliance with unified governance

Business -Aligned Security Operations
The next-generation SOC enables business modernization

Cyber Exposure Assessment
Assessing exposure to minimize risk



Secure Development and Testing
Embracing DevSecOps to deliver secure software fast

Augmented Detect and Response
Human and machine partnership

Zero Trust
Take a proactive approach of continually verifying devices, services, and individuals rather than trusting them

CyberRes

Fortify Portfolio

Holistic application security to build secure software fast

Fortify

Interfaces & Integrations

IDE | Repo | CI/CD | Web | API | Collab

Enterprise AppSec Program Management – On Prem, SaaS, Hybrid

Scan Control | Scan Results | Policy & Prioritization | Audit & Triage | Analytics & Reporting | Licensing & Entitlements | Identity & Access

Scanning Technology

Static (SAST)	Dynamic (DAST)	Mobile (MAST)
Software Composition Analysis (SCA)	API Security	Infrastructure -as-Code Security (IaC)

Software Security Research

Supporting Offerings

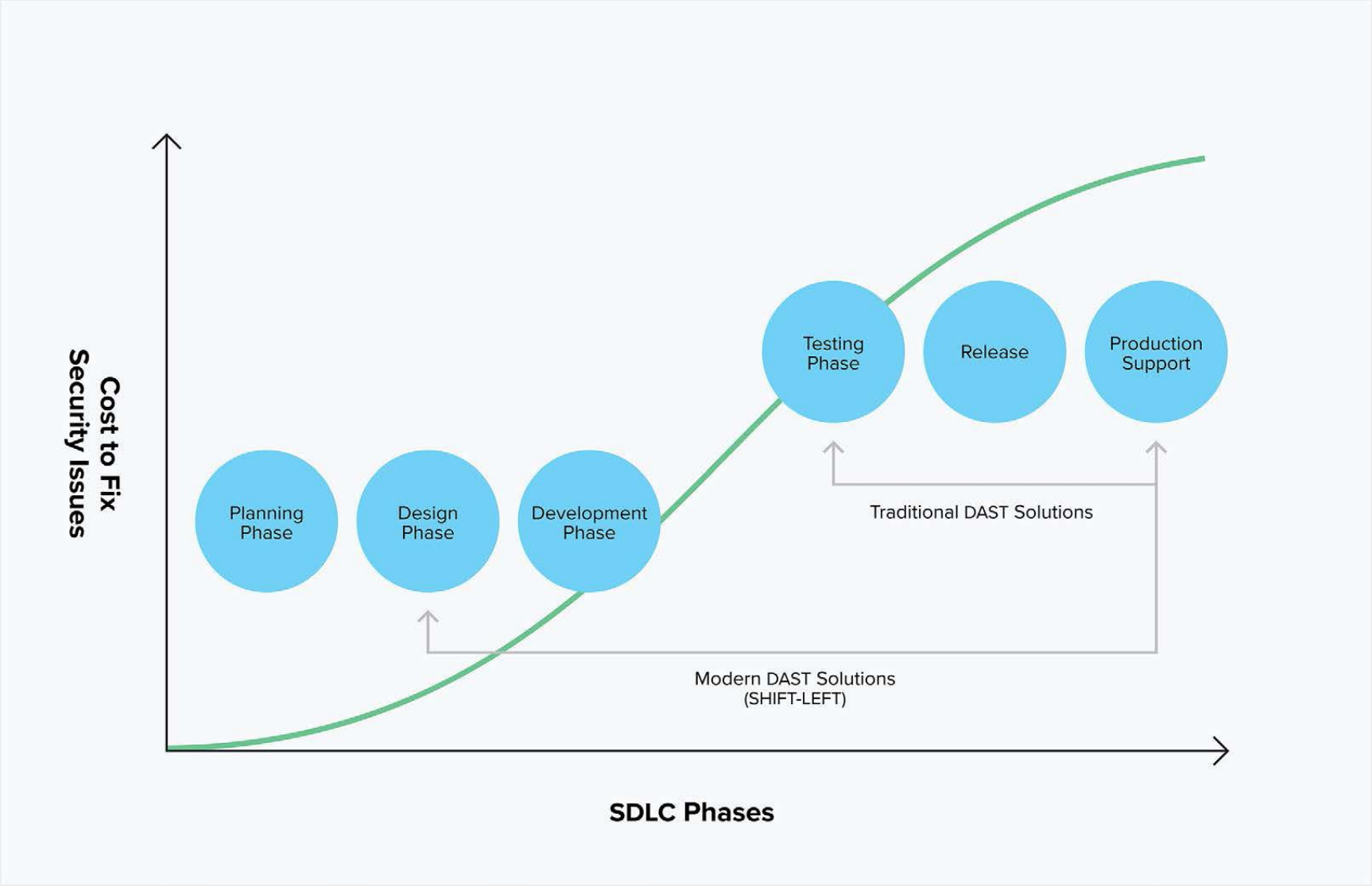
- Managed Services (FoD)
- Machine Learning / AI
- Secure Developer Training
- Professional Services
- Premium Support

Why Shift DAST Left?

Dynamic Application Security Testing (DAST)

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

DAST Timing in the SDLC



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'*

The Need to Scan at Scale

Average Enterprise runs 788 Applications

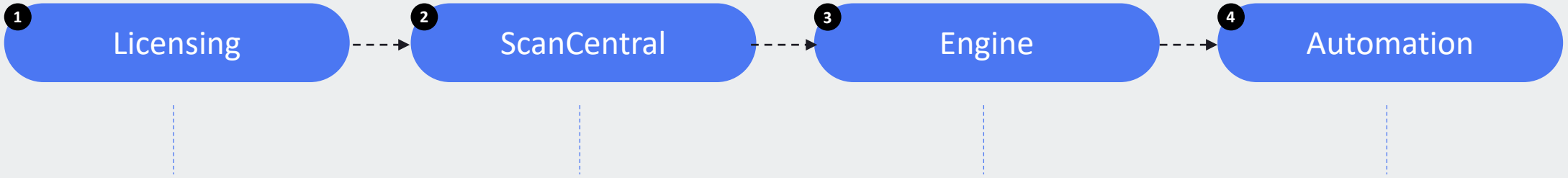
45% of Applications are developed in house

Many Large Enterprises have 1000’s of Applications

Source: McAfee, 2018, **Every Company is a Software Company**

NextGen DAST

NexGen DAST



Enable Flexibility

DAST/SAST

Concurrent based

All Capabilities

Shift DAST Left

ScanCentral DAST

WebInspect

CI/CD Plugins

Scan All the Apps

Single Page & Classic

SOAP & REST APIs

Mobile

Deliver Scalability

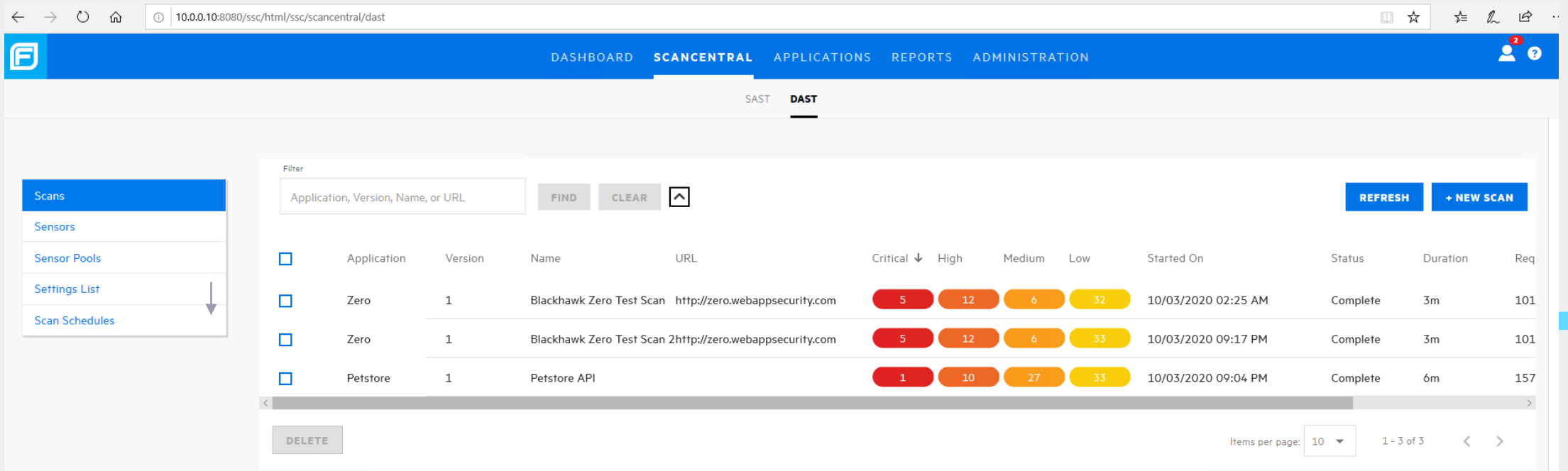
Dockerized Scanners

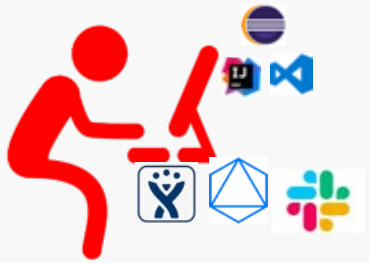
Automatic Scan Tuning

Speed

Fortify ScanCentral

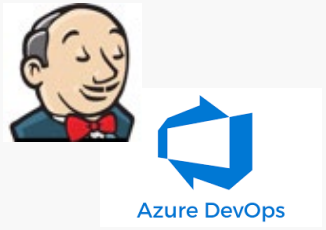
On Premises, SaaS, Fortify on Demand





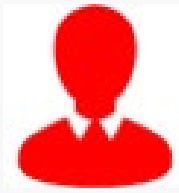
Dev 1st with real - time IDE results

Automated commit level scanning



CI/CD Integration for DAST, SAST, OSS…

DevOps friendly audit & delivery



Actionable results for AppSec pros

Evolving to NexGen DAST Years in the Making

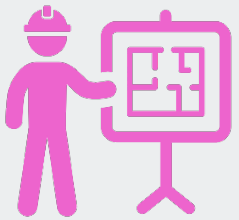
SSC Scan Central DAST

Shift Left (Enable Dev)	Manageability	Shift Right (Enable Scale)
API Scan	Dockerization	Incremental
Postman	Scan Central DAST	Macro Validation
Validate Fix	License Simplification	Auto Tuning
Macro AutoGen/Validate	Azure/Jenkins Plugins	Hybrid Burst Deployment
VS Code Remote Scan	OpenSSL (Platform indep.)	Func. Test Scan + Merge
VS Code Local Scan	Hybrid SaaS	Scanner Scaling
Synthetic Policies	Improved Alerting	Enterprise Incremental

Macro and Scan Engine 6.x

19.1 -20.1

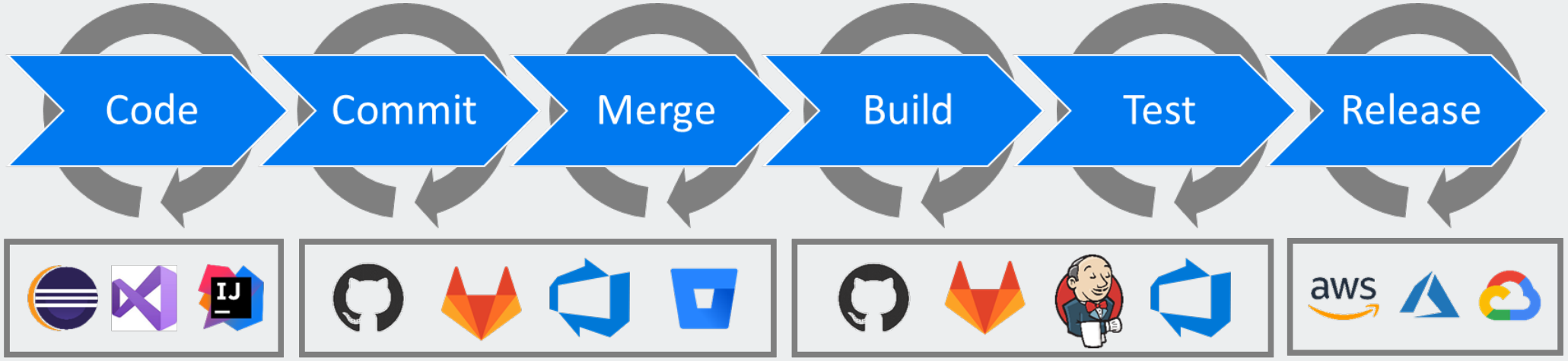
20.2



21.x

Shifting DAST Left

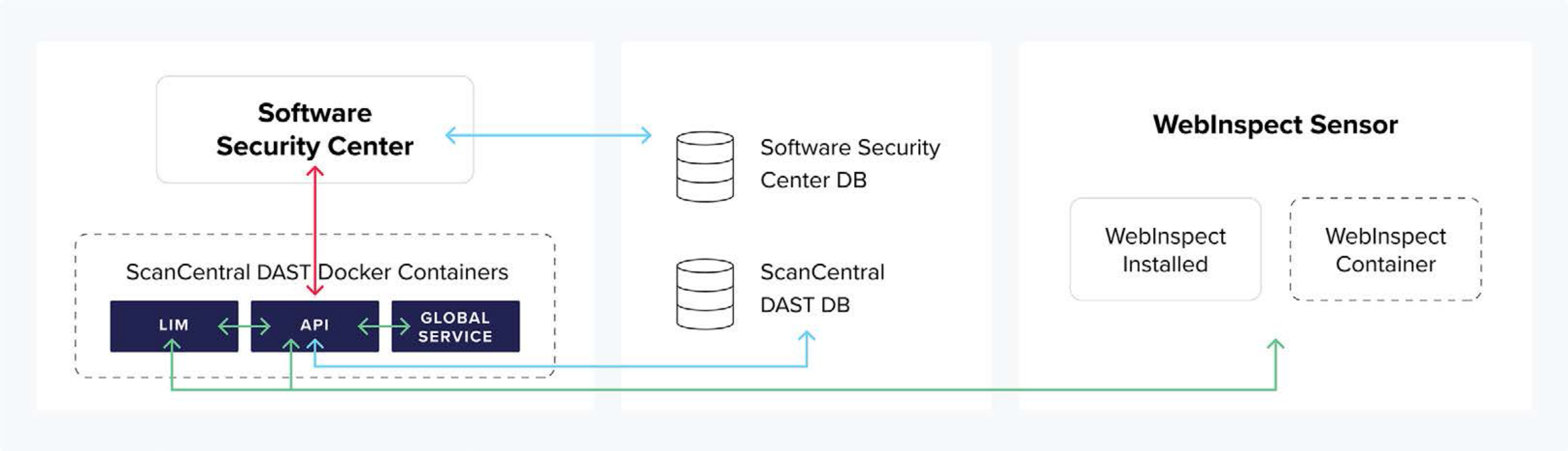
Where no solution has gone before



ScanCentral DAST = DevOps Friendly CICD Integration And FAST Proxy + Containerized Automation and Orchestration at Scale + Simplified Scanning Macro AutoGen API/Postman

ScanCentral DAST - Architecture

Built upon Fortify WebInspect and Fortify SSC Server



FAST – Functional Application Security Testing

Reuse functional tests during security testing

Anything sent through the proxy is audited

API

Manual

Mobile

Scripts

API Security Testing

API Security

Unified API Scanning for the modern application attack surface

Support for modern and legacy APIs

Postman Collections

REST, GraphQL, RAML

Swagger / OpenAPI

Swagger 1.0, 2.0 OpenAPI 3.0

Soap

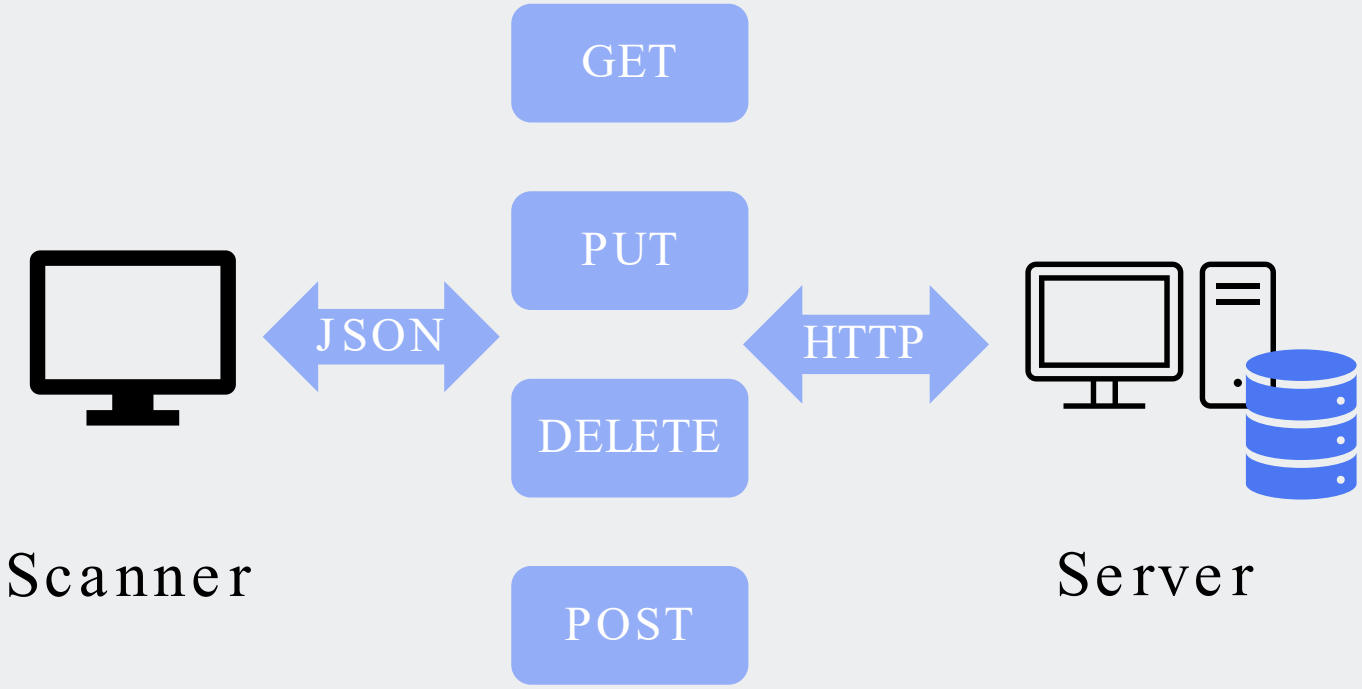
WSDL, Service Test Designer

API Policy

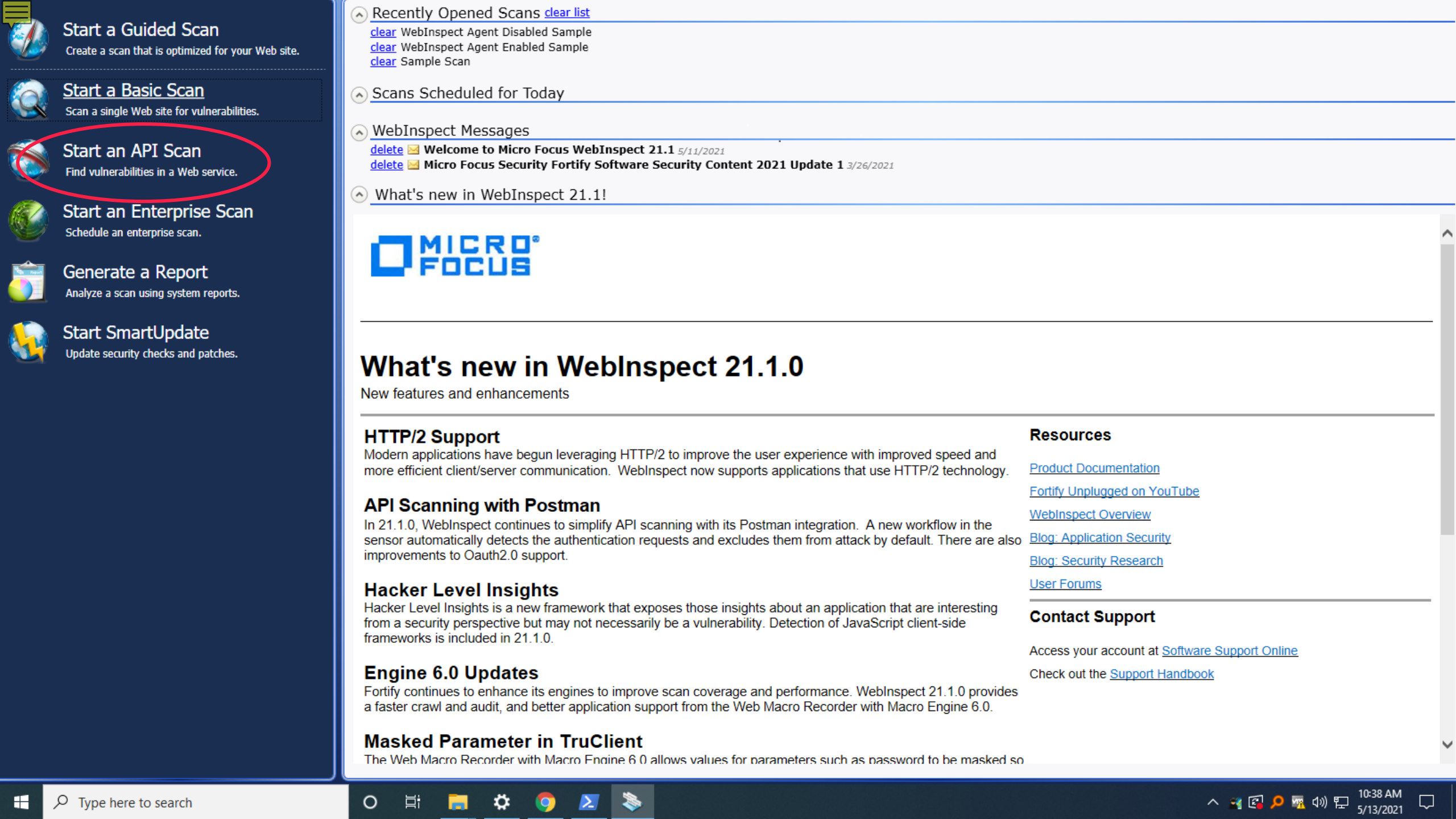
API Specific Checks

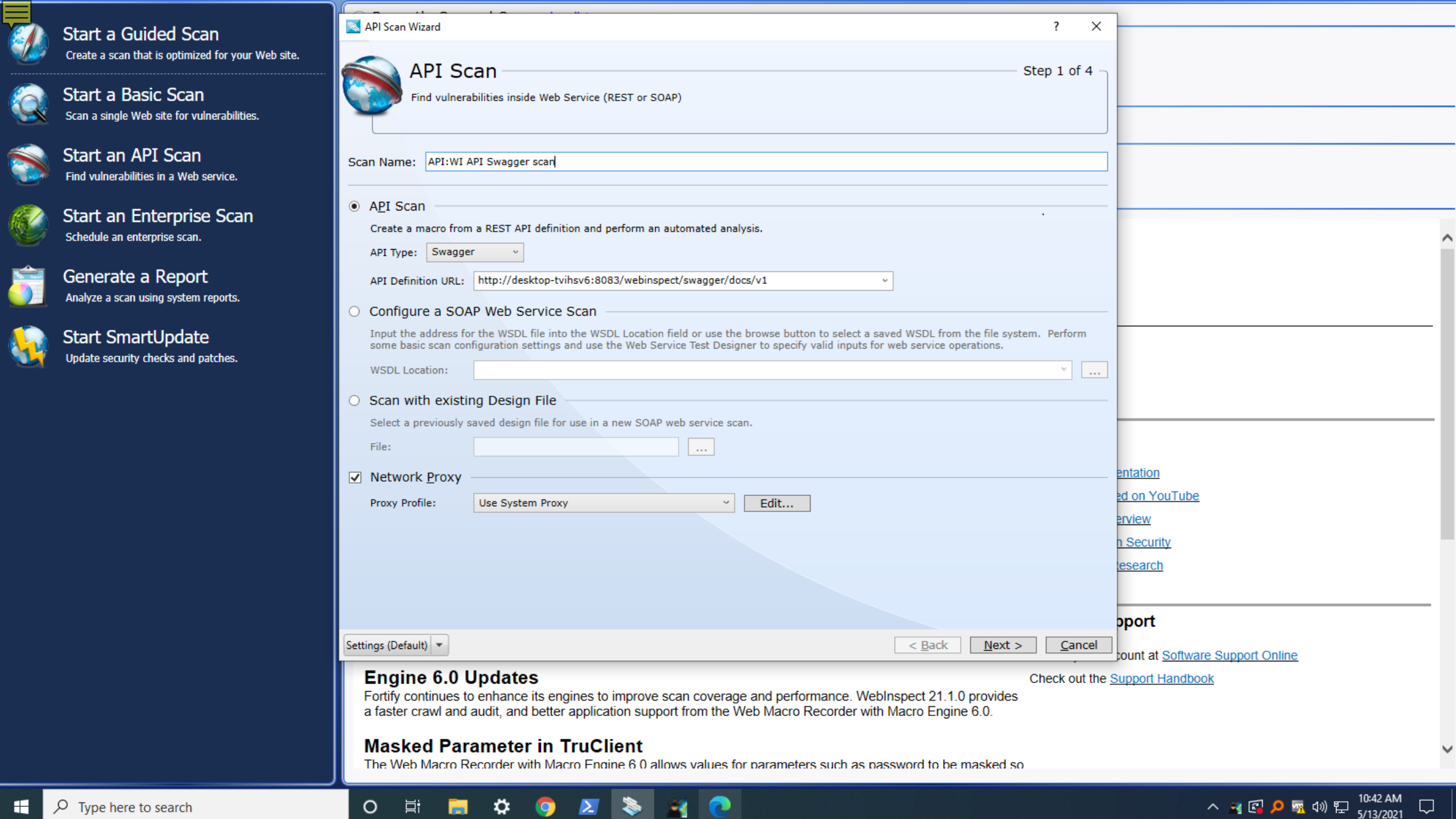
Authenticated

Oauth 2.0 supported



Resource: Advanced API Scanning


Start a Guided Scan
Create a scan that is optimized for your Web site.
Start a Basic Scan
Scan a single Web site for vulnerabilities.
Start an API Scan
Find vulnerabilities in a Web service.
Start an Enterprise Scan
Schedule an enterprise scan.
Generate a Report
Analyze a scan using system reports.
Start SmartUpdate
Update security checks and patches.
Recently Opened Scans clear list
clear WebInspect Agent Disabled Sample
clear WebInspect Agent Enabled Sample
clear Sample Scan
Scans Scheduled for Today
WebInspect Messages
delete Welcome to Micro Focus WebInspect 21.1 5/11/2021
delete Micro Focus Security Fortify Software Security Content 2021 Update 1 3/26/2021
What's new in WebInspect 21.1!
MICRO FOCUS
What's new in WebInspect 21.1.0
New features and enhancements
HTTP/2 Support
Modern applications have begun leveraging HTTP/2 to improve the user experience with improved speed and more efficient client/server communication. WebInspect now supports applications that use HTTP/2 technology.
API Scanning with Postman
In 21.1.0, WebInspect continues to simplify API scanning with its Postman integration. A new workflow in the sensor automatically detects the authentication requests and excludes them from attack by default. There are also improvements to Oauth2.0 support.
Hacker Level Insights
Hacker Level Insights is a new framework that exposes those insights about an application that are interesting from a security perspective but may not necessarily be a vulnerability. Detection of JavaScript client-side frameworks is included in 21.1.0.
Engine 6.0 Updates
Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.0.
Masked Parameter in TruClient
The Web Macro Recorder with Macro Engine 6.0 allows values for parameters such as password to be masked so
Resources
Product Documentation
Fortify Unplugged on YouTube
WebInspect Overview
Blog: Application Security
Blog: Security Research
User Forums
Contact Support
Access your account at Software Support Online
Check out the Support Handbook
Type here to search
10:38 AM
5/13/2021


Start a Guided Scan
Create a scan that is optimized for your Web site.
Start a Basic Scan
Scan a single Web site for vulnerabilities.
Start an API Scan
Find vulnerabilities in a Web service.
Start an Enterprise Scan
Schedule an enterprise scan.
Generate a Report
Analyze a scan using system reports.
Start SmartUpdate
Update security checks and patches.
API Scan Wizard
API Scan
Step 1 of 4
Find vulnerabilities inside Web Service (REST or SOAP)
Scan Name:
API:WI API Swagger scan
API Scan
Create a macro from a REST API definition and perform an automated analysis.
API Type:
Swagger
API Definition URL:
http://desktop-tvihsv6:8083/webinspect/swagger/docs/v1
Configure a SOAP Web Service Scan
Input the address for the WSDL file into the WSDL Location field or use the browse button to select a saved WSDL from the file system. Perform some basic scan configuration settings and use the Web Service Test Designer to specify valid inputs for web service operations.
WSDL Location:
Scan with existing Design File
Select a previously saved design file for use in a new SOAP web service scan.
File:
Network Proxy
Proxy Profile:
Use System Proxy
Edit...
Settings (Default)
< Back
Next >
Cancel
Engine 6.0 Updates
Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.0.
Masked Parameter in TruClient
The Web Macro Recorder with Macro Engine 6.0 allows values for parameters such as password to be masked so
Check out the Support Handbook
Type here to search
10:42 AM
5/13/2021

Summary

Shifting DAST Scans Left

Examples of how you can shift DAST scans left

CI/CD + Standard Scan: ScanCentral DAST automatically runs fast targeted scans triggered by Agile, Scrum tests in CI/CD pipelines and merges those results with slower, more complete DAST scanning configurations that occur at regular intervals.

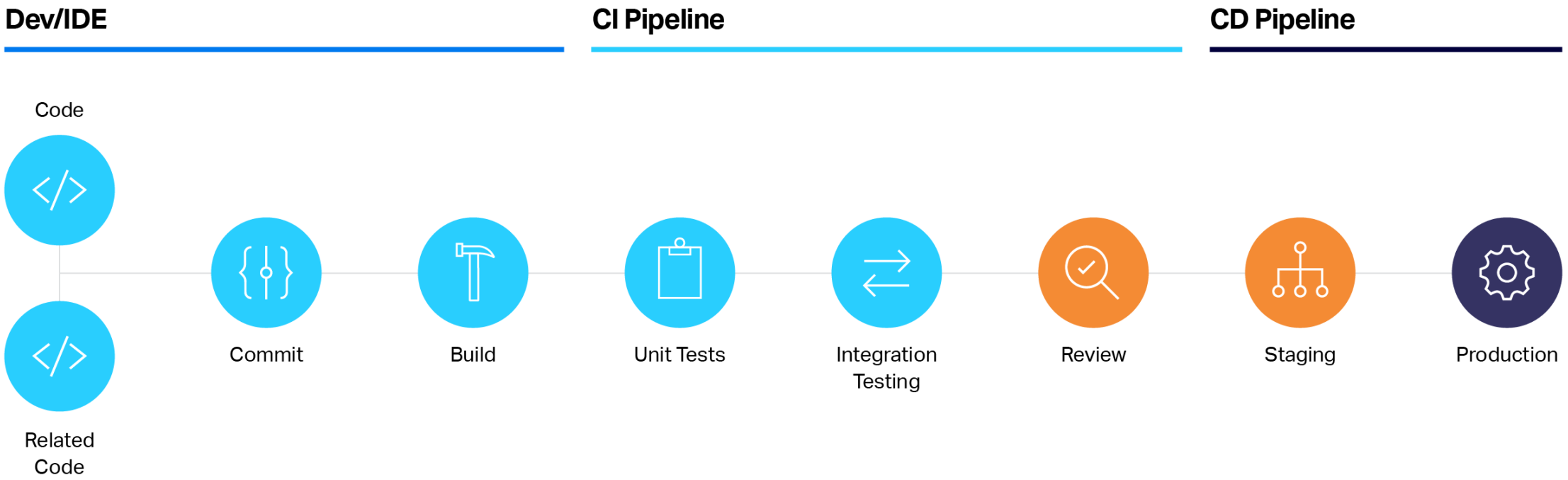
Hotspot + Notspot: The hotspot policy is configured to run at a higher priority and the Notspot (less frequently found checks) with a lower priority as sensors are available.

Unauthenticated + Authenticated: You could scan all your applications without a login macro every month and then run more complete WebInspect scans that are authenticated once per quarter.

Standard + Adhoc Zero Day: In addition to regularly scheduled Standard scans, you might want to merge extremely fast WebInspect scans for very specific zero days.(Apache struts is a great example.)

Functional Test Audit Only + Standard: You could capture functional tests as workflow macros that are automatically uploaded for fast, audit-only WebInspect scans and then merge full, standard WebInspect scans prior to release.

Fortify Simplifies Application Security Testing



SCA
Sonatype Software Composition Analysis
Fortify on Demand

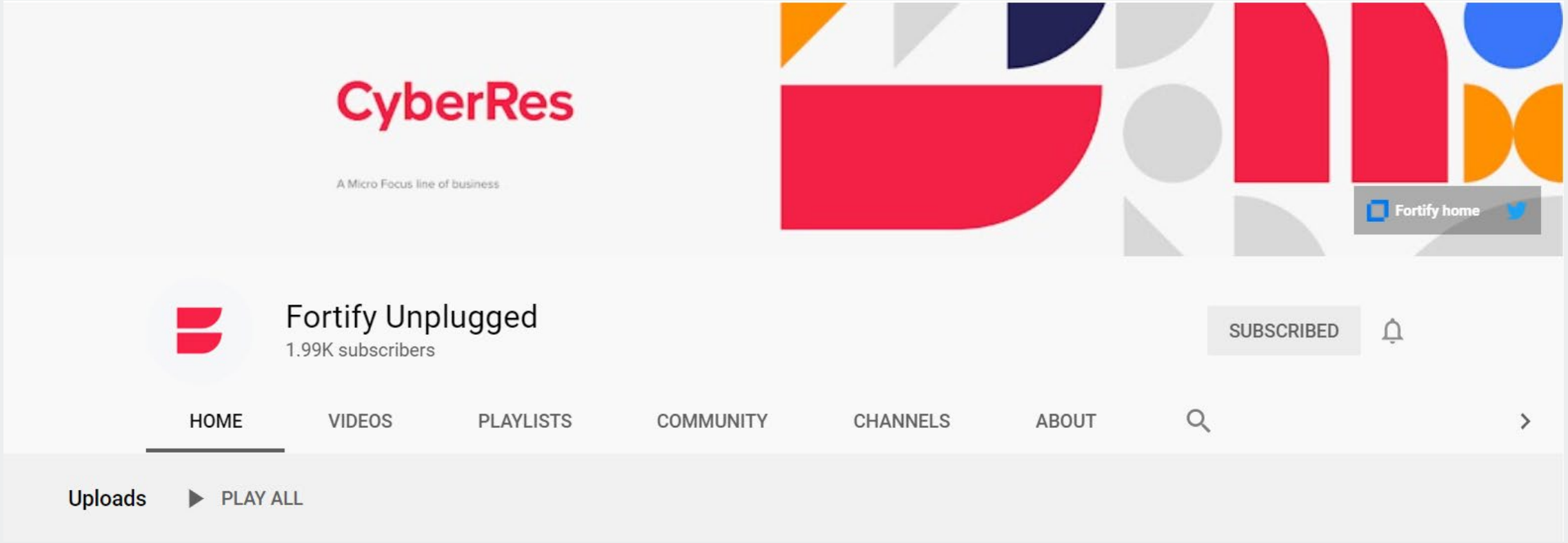
SAST
Fortify Static Code Analyzer
Fortify on Demand

DAST
Fortify WebInspect
Fortify on Demand

RASP
Fortify Application Defender
Fortify on Demand

Demo Videos: Subscribe to Fortify Unplugged

Short demo videos on Fortify products capabilities and how to's



Fortify Unplugged

Questions?

Fortify