Architecture Analysis

SecAppDev March 2016

by Jim DelGrosso

whoami

- Run Cigital's Architecture Analysis practice
- 30+ years in software development in many different domains
- 15+ years focusing on software security

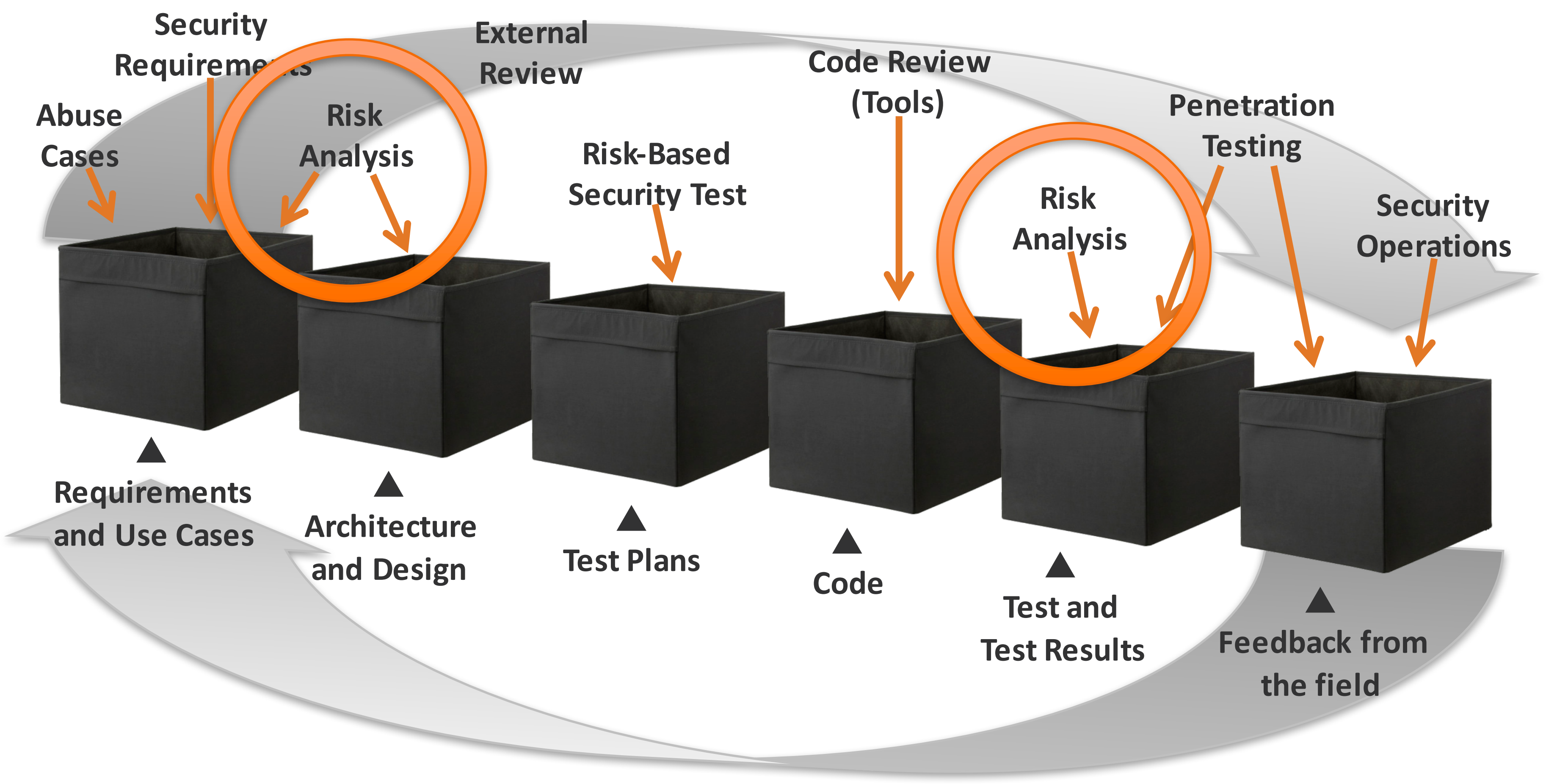
@jimdelgrosso

- Executive Director of IEEE Computer Society CSD initiative

http://cybersecurity.ieee.org/center-for-secure-design/

Cigital

Software Security In The SDLC



Cigital

BUGS VS. FLAW COMPARISON

Defects – Bugs And Flaws

Cross Site Scripting

Buffer Overflow

Weak/Missing/Wrong Security Control

(Implementation) BUGS

(Design) FLAWS

Code Review

Penetration Testing

Architecture Analysis

Cigital

Defect Examples

- No CSRF protection – flaw
- CSRF protection with username as CSRF token – bug
- Not enabling CSRF protection built into framework – bug

- Sensitive information not protected at rest – flaw
- Sensitive information sent back to client as part of a JSON object – bug

- Creating your own encryption algorithm – flaw (likely)
- Misusing a well-know encryption algorithm – bug

Defect Examples

- Failure to associate a host with their expected x509 certificate or public key (certificate pinning) – flaw
- Improper verification of an x509 certificate (e.g., failure to verify date) – bug

- Missing audit control to track support team member actions – flaw
- “Hidden” debug endpoints used by support team is publicly accessible – bug

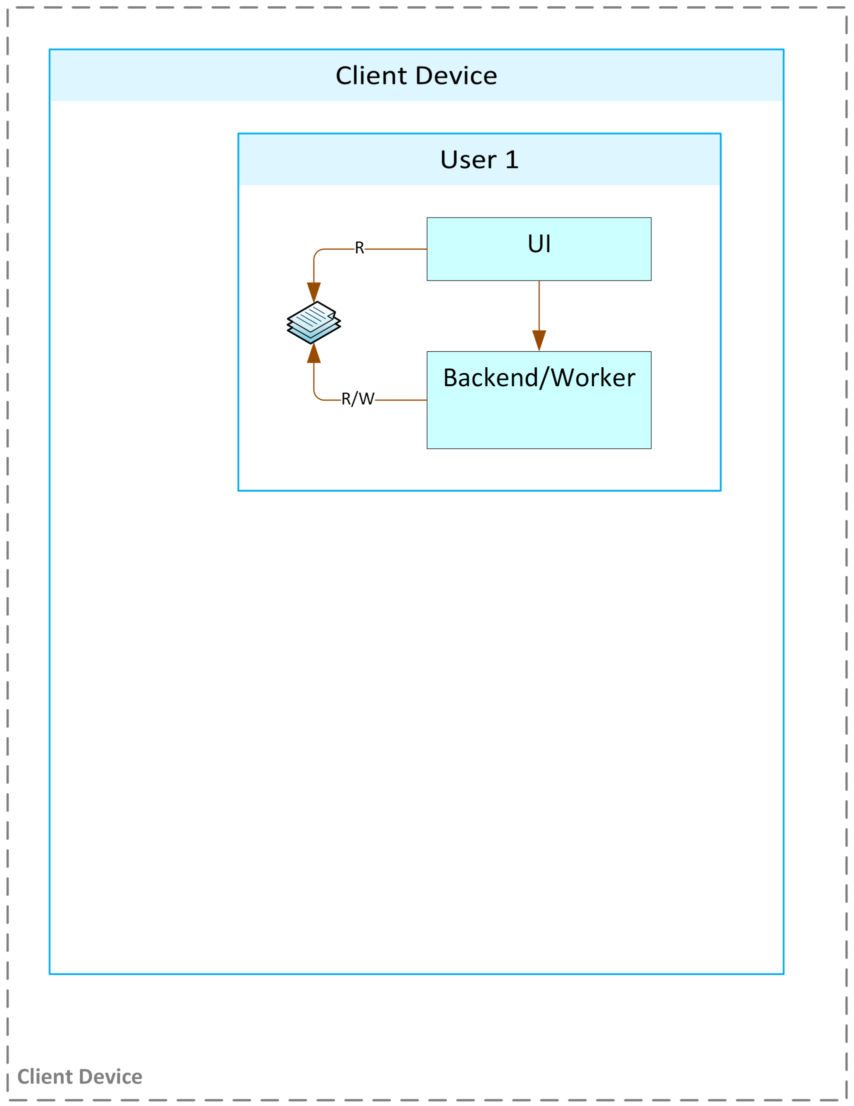
Defect Examples

- Using a confidentiality control when an integrity control is required – flaw
- Using 3rd-party software with known vulnerabilities – flaw in how you build software
- No tamper-detection for files exchanged with business partners – flaw

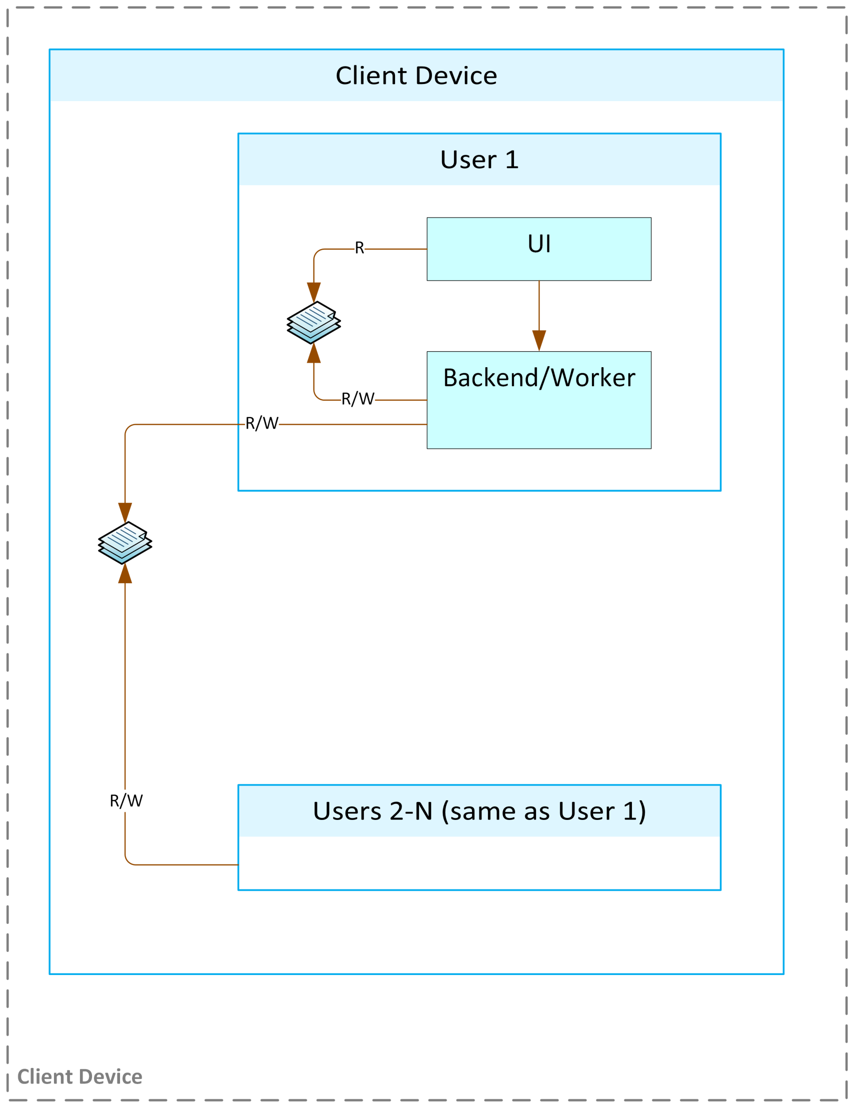
Cigital

WHY PERSPECTIVE MATTERS

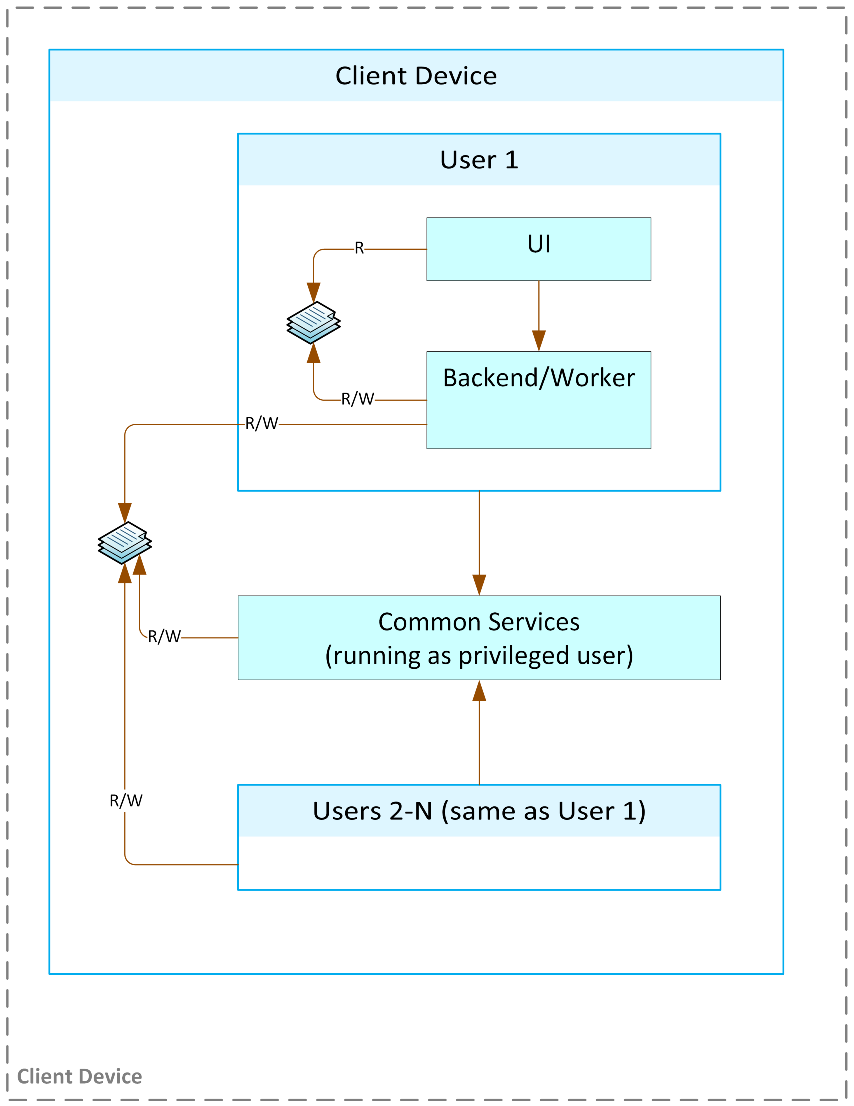
Any Concerns?



How Does This Addition Change Our Thinking?

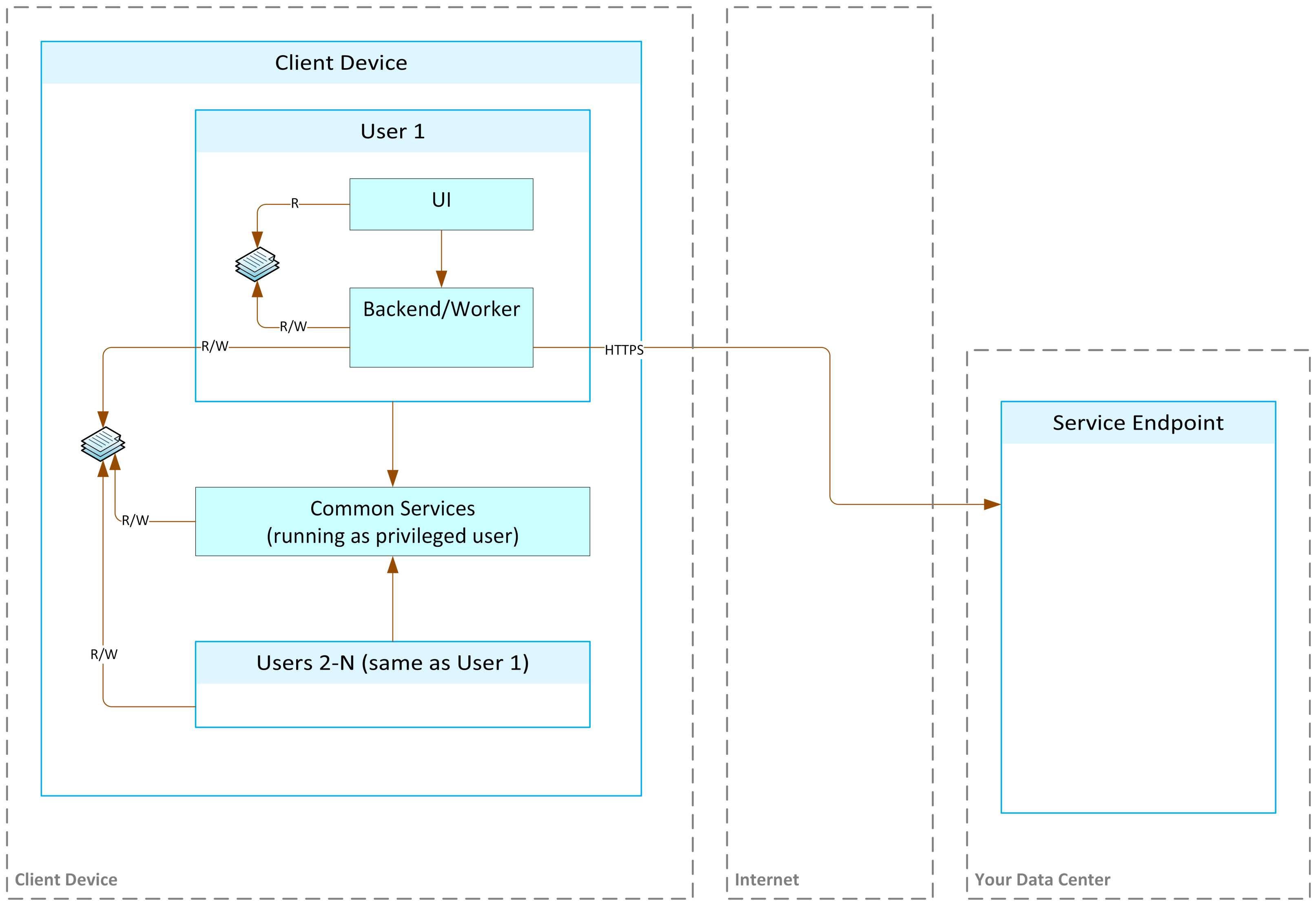


How Does This Addition Change Our Thinking?

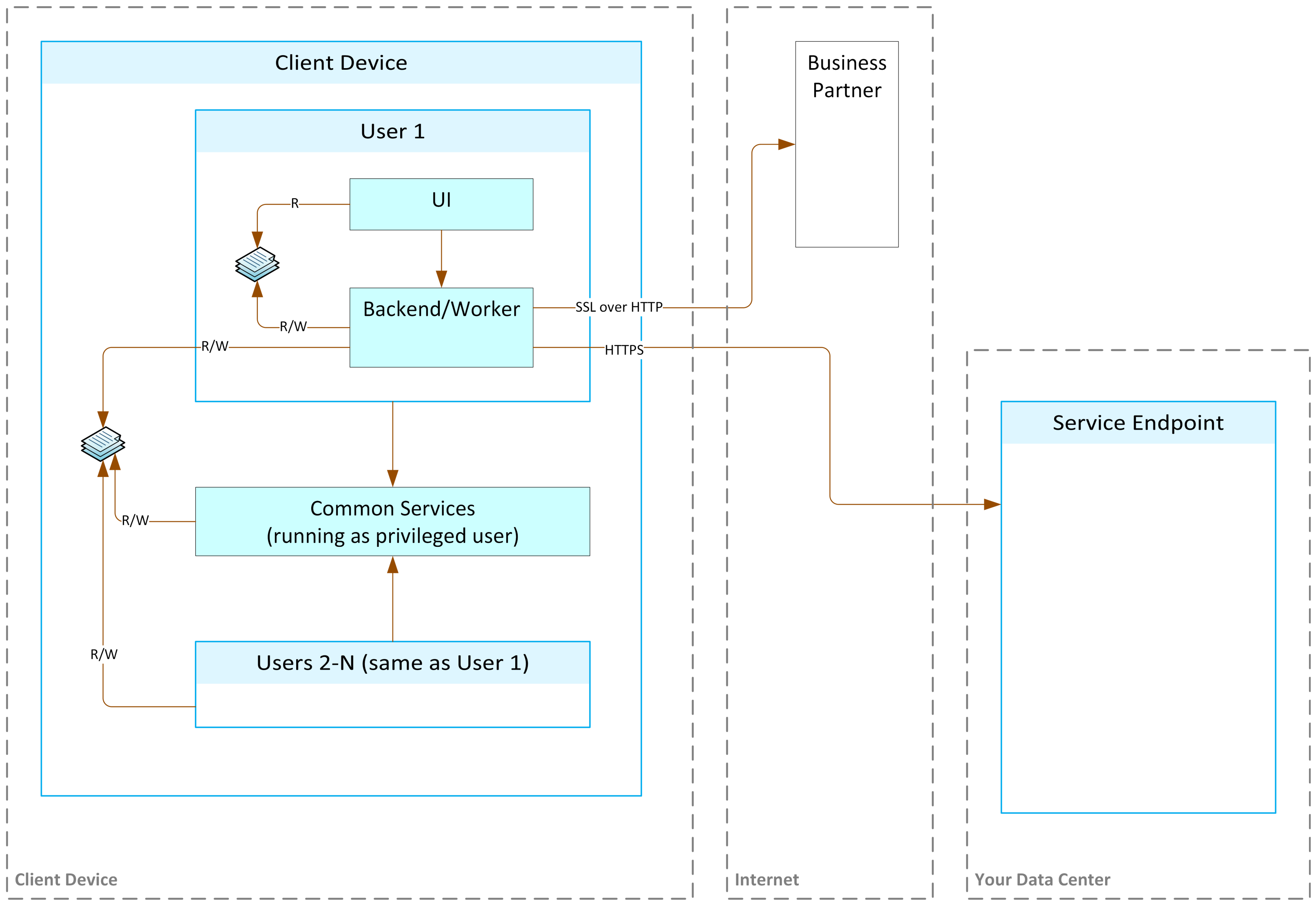

Client Device
User 1
UI
R
Backend/Worker
R/W
R/W
Common Services (running as privileged user)
R/W
R/W
Users 2-N (same as User 1)
Client Device

Cigital

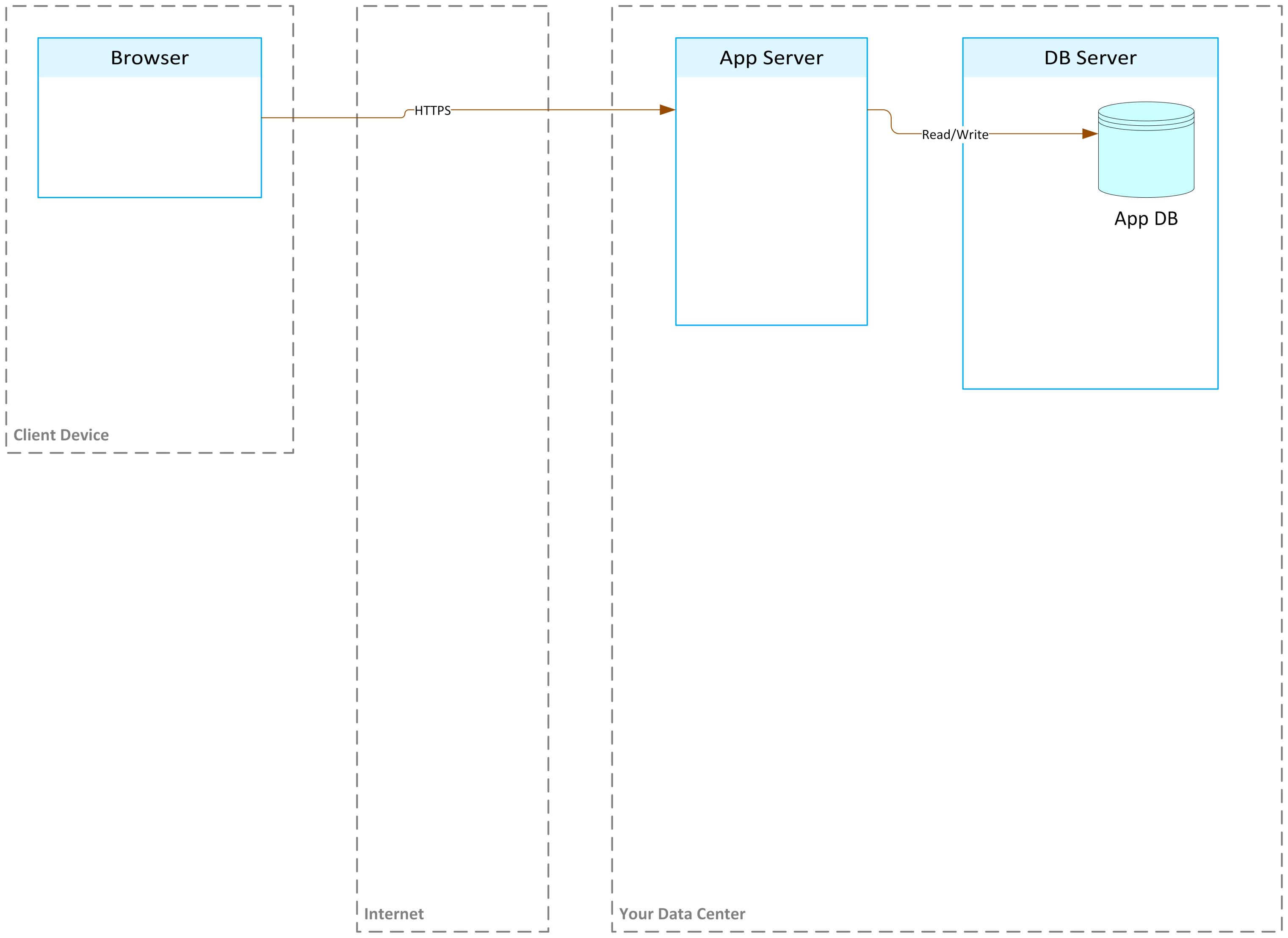
How Does This Addition Change Our Thinking?



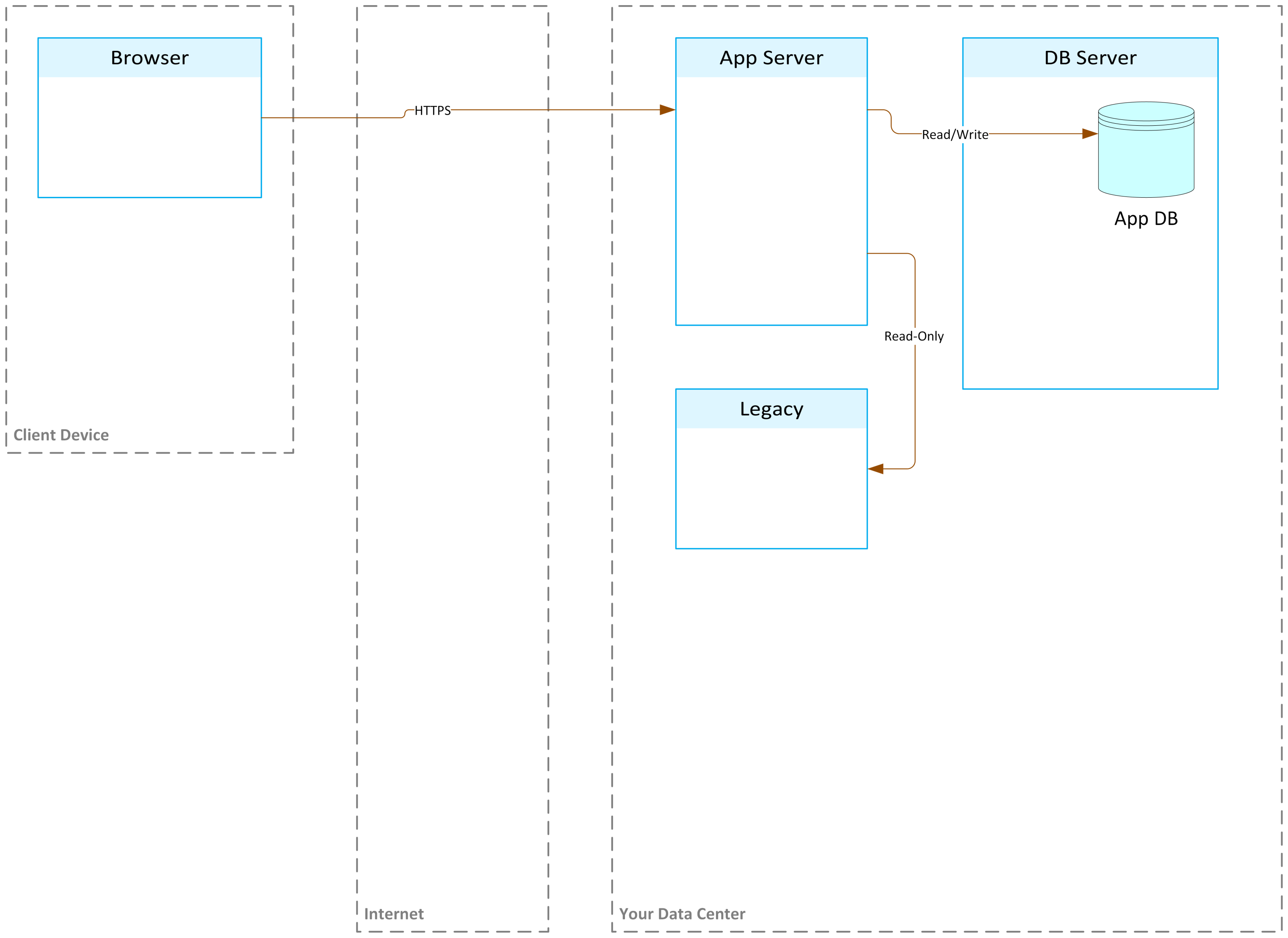
How Does This Addition Change Our Thinking?



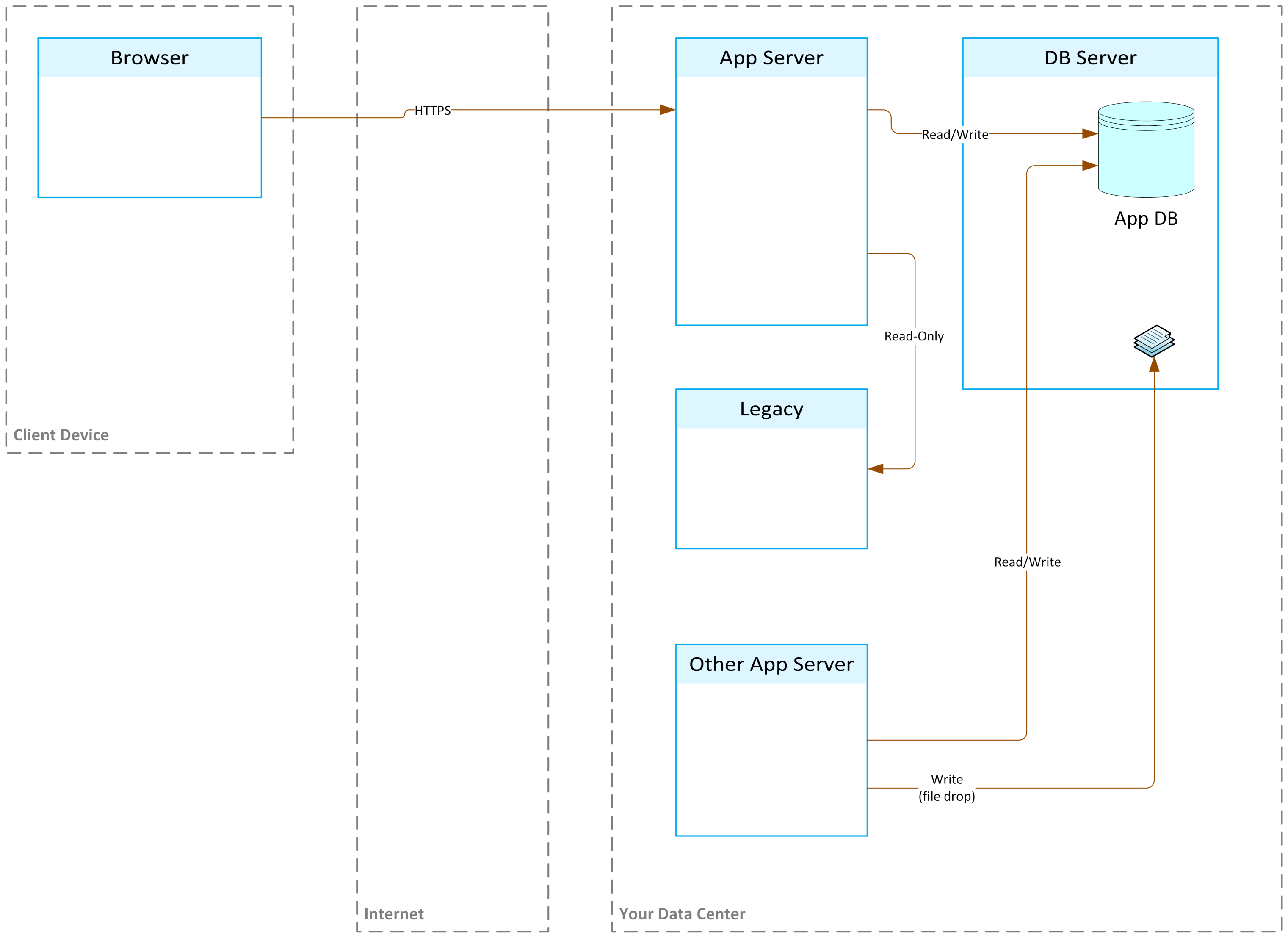
Any Concerns?



How Does This Addition Change Our Thinking?

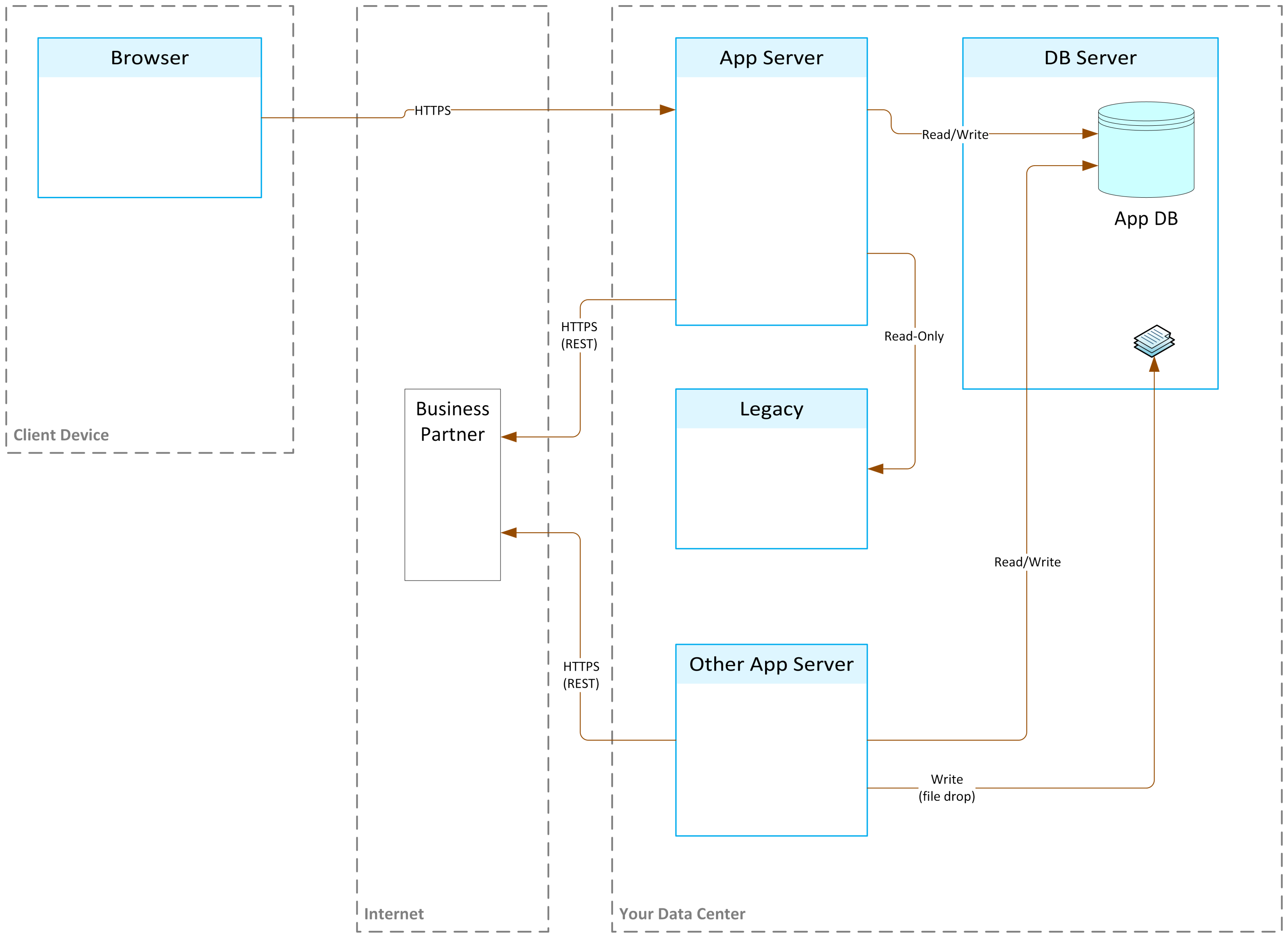


How Does This Addition Change Our Thinking?

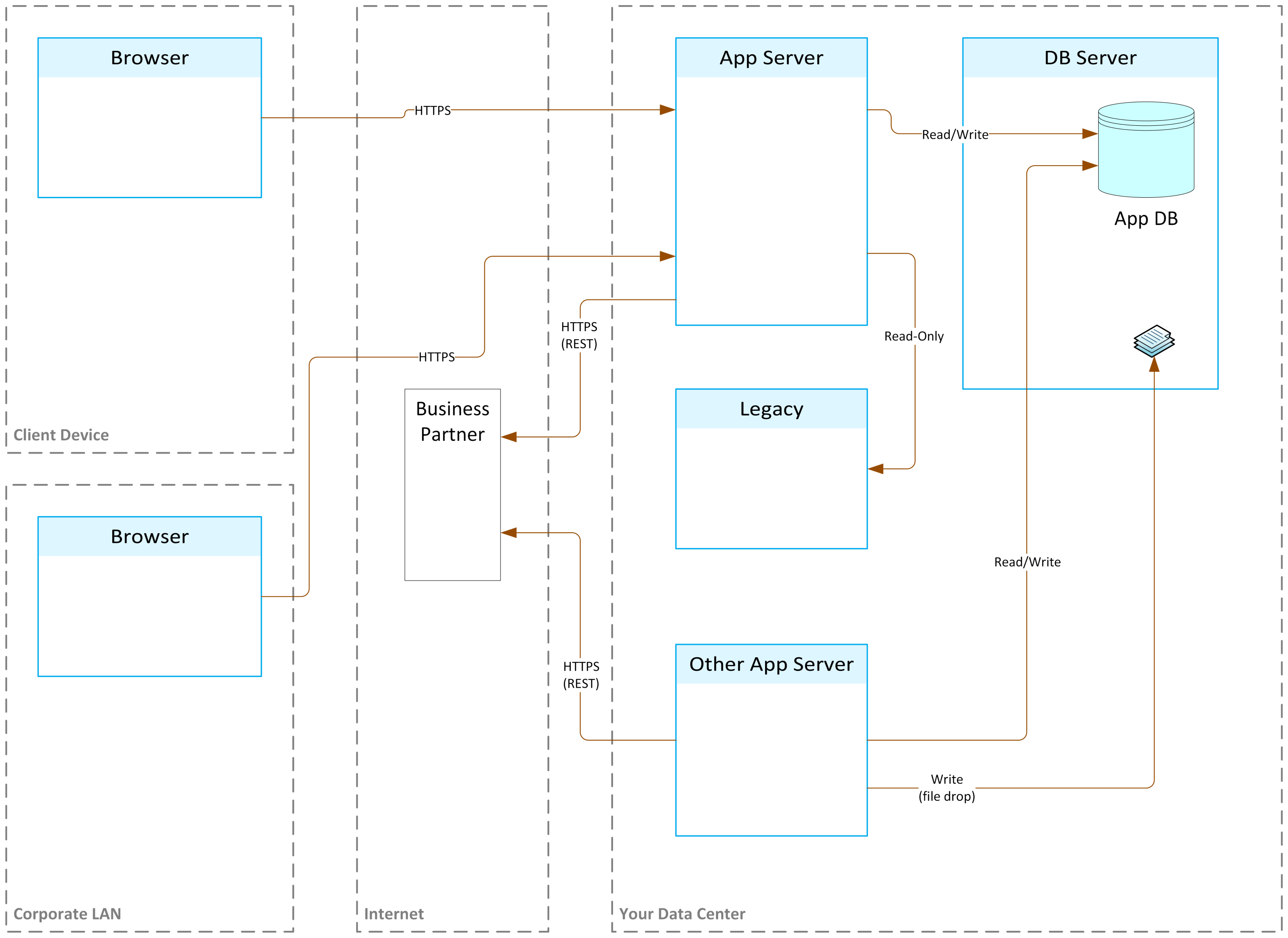


Cigital

How Does This Addition Change Our Thinking?

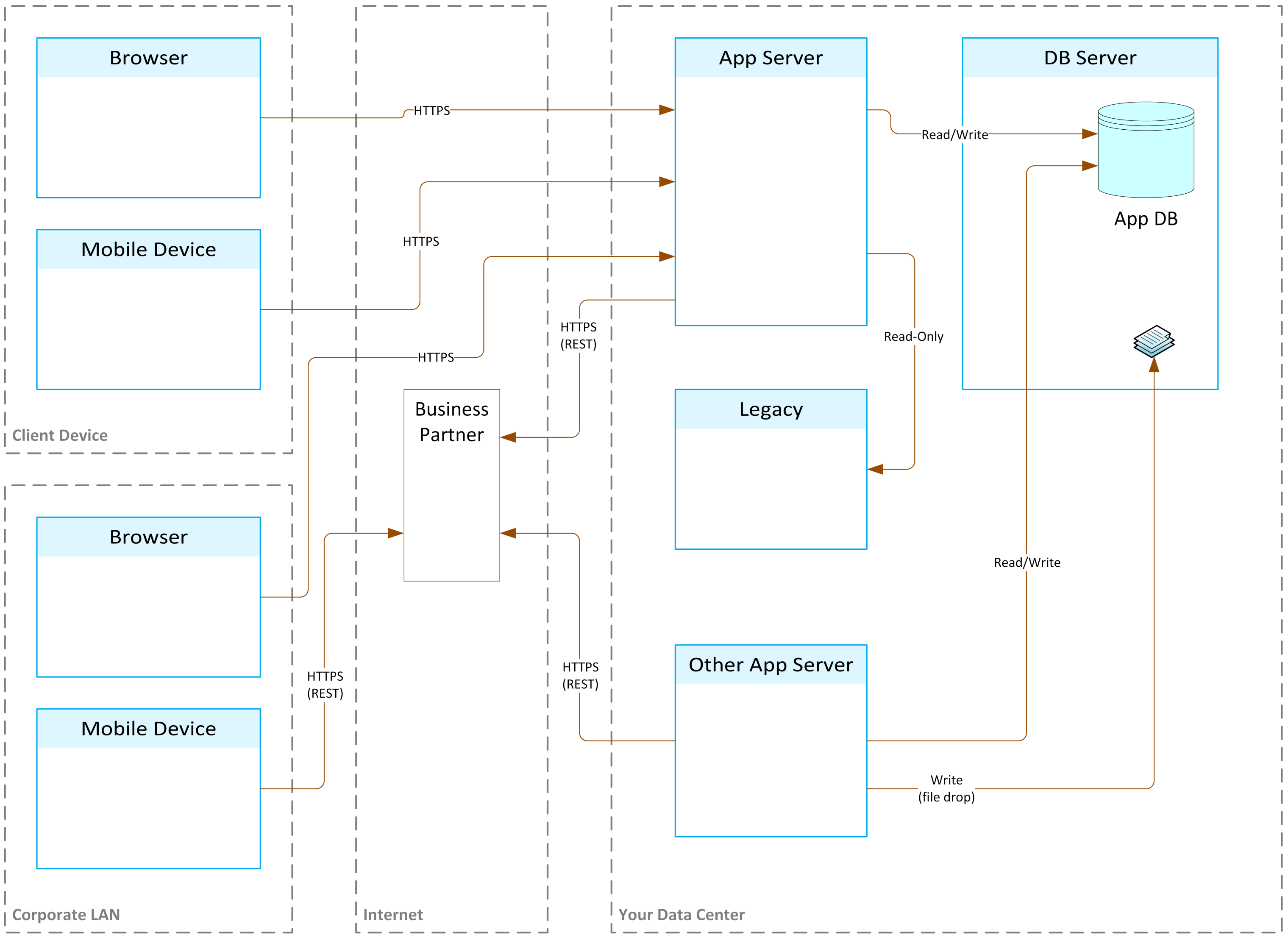


How Does This Addition Change Our Thinking?



Cigital

How Does This Addition Change Our Thinking?



Cigital

FINDING FLAWS

How Will You Find Flaws?

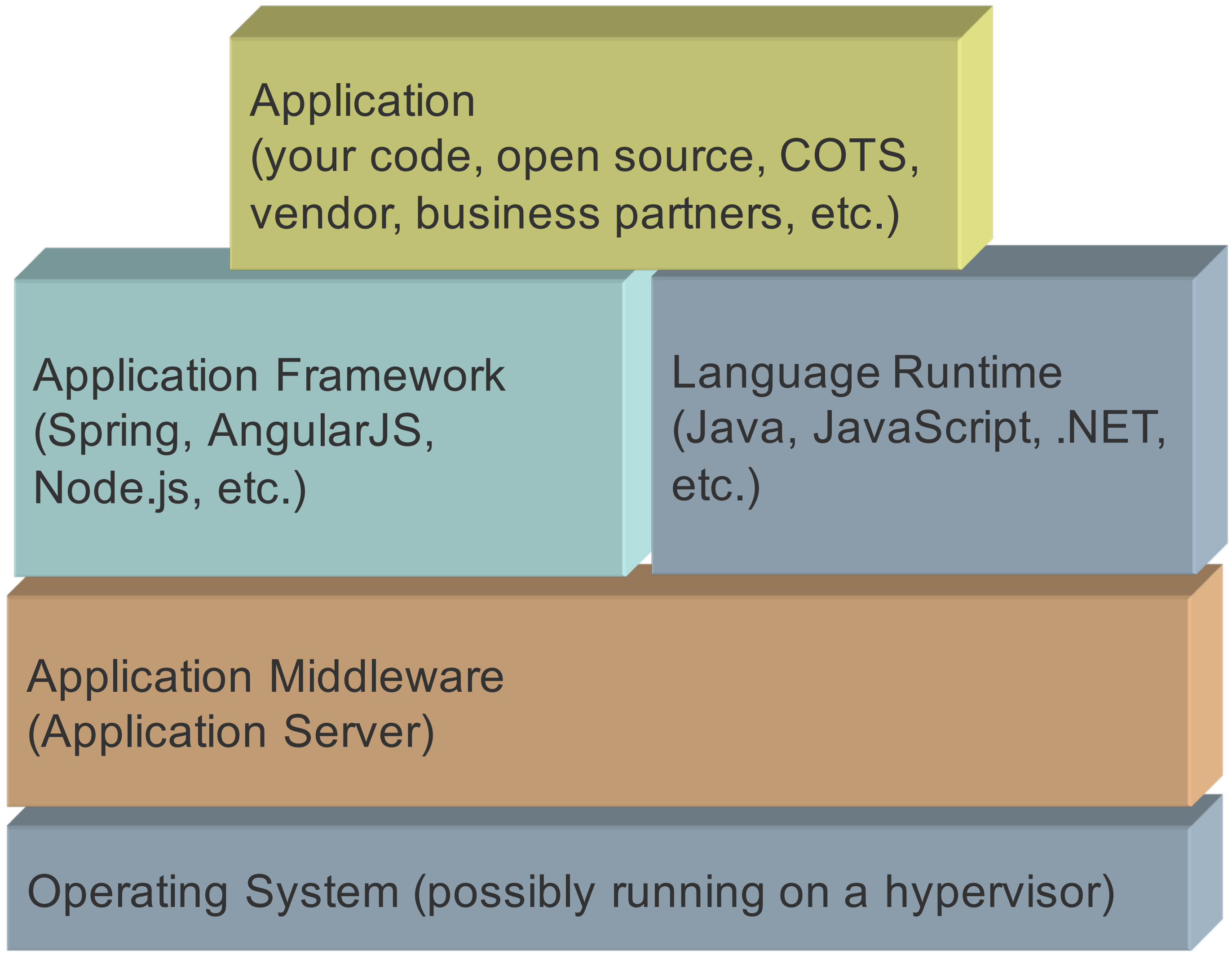
- Penetration Tests?
  - May stumble across some – but generally takes a lot of time and knowledge of the system (white-box / gray-box testing)
- Code Review?
  - Unlikely if done with a tool; maybe if reviewed by a person
- Install appliance on network?
  - No
- Write a Splunk rule; write an SIEM rule?
  - Not likely

- Need analysis to focus on the design

Finding Flaws

- Dependency Analysis
- Known Attack Analysis
- System Specific Analysis

Dependency Analysis


Application
(your code, open source, COTS, vendor, business partners, etc.)
Application Framework
(Spring, AngularJS, Node.js, etc.)
Language Runtime
(Java, JavaScript, .NET, etc.)
Application Middleware
(Application Server)
Operating System (possibly running on a hypervisor)

Dependency Analysis

That software you include provides features you use, but…

- Can you disable features you do not intend to use?
- Is it configured to be secure by default or do you have to do that
- The software has its own vulnerabilities and weaknesses
- Security controls provided may be weak, or weaker than you might otherwise accept

Cigital

Known Attack Analysis

- We know about a large number of defects
- They are well documented, and well understood
- There are tools that can find certain instances of these defects
- There are tools to launch attacks using these defects

CWE Common Weakness Enumeration
A Community-Developed Dictionary of Software Weakness Types

OWASP
The Open Web Application Security Project

OWASP Top 10 - 2013
The Ten Most Critical Web Application Security Risks

PORTSWIGGER
WEB SECURITY

Cigital

Known Attack Analysis

Common flaws from public sources

- Client-side trust issues
- Authentication or Authorization bypass
- Incorrect use of Crypto
- Poor session management

- What is <u>your</u> most common bug?
- What is <u>your</u> most common flaw?
- You need to be able to answer BOTH of these questions

Known Attack Analysis

Design elements historically vulnerable to attack:

- Components talking over a network
- Code to execute is only known at runtime
- Stateless communication
- Client code and data

Cigital

System Specific Analysis

Finds defects unlikely to be found by other techniques

- Weakness in a custom protocol
- Reusing authentication credentials for different risk-rated actions
- Not following good software security design principles

Cigital

System Specific Analysis

- Part of this analysis can be done with Threat Modeling
- Business logic defects
- Custom protocol / sequence defects
- Flaws related to interactions with business partners
- Defects unique to YOUR system

Cigital

THINGS TO CONSIDER OR CHALLENGES YOU MAY FACE

Cigital

Assuming You’re Doing Enough

Assuming You're Doing Enough – An Example

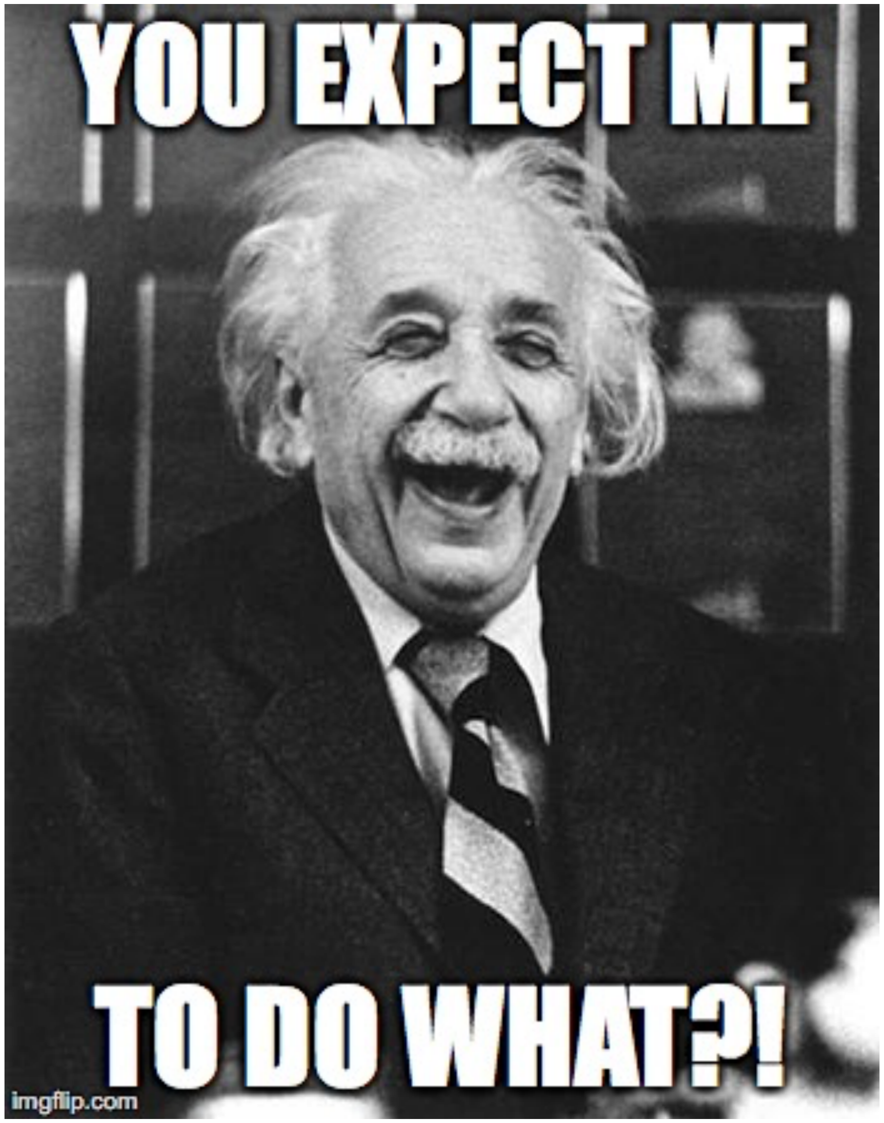
SSI Capabilities

- Secure SDLC with Gates
- Satellite
- Metrics
- Portfolio Management
- Policy and Standards
- Vendor Management
- Defect Discovery – Design
- Defect Discovery – Fuzzing
- Defect Discovery – Penetration Testing
- Defect Discovery – Quality Assurance
- Defect Discovery – Code Review
- Defect Discovery – Research
- Defect Management
- Attack Intelligence
- Open Source Management
- Risk & Compliance
- Secure by Design
- SSG Outreach
- Competency Management
- IT Operations

Cigital

Application Is Already Deployed

This Is Too Hard



Cigital

This Is Easy– I’m Going To Do This Everywhere

WRAP-UP

Cigital

Summary

- You CAN do this
  - Start small
  - Set reasonable expectations
  - Find your top few flaws – you may be surprised with what you find

- You HAVE to do this
  - Seriously, you have to do this
- It finds defects that can not be found using other techniques

Cigital

THANK YOU