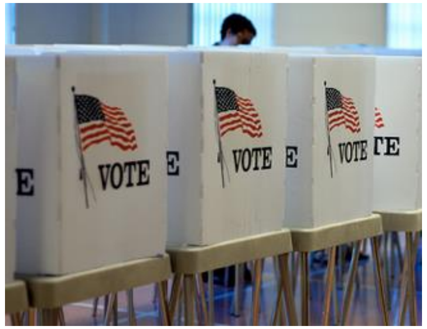
Virsec

Securing Defense & Critical Infrastructure Control Systems Applications

Ray DeMeo

Protecting Applications is Imperative

Applications control Critical Infrastructure



In most cyber attacks, whether it began through the application or not, an application vulnerability was eventually exploited

Virsec

Information Technology is rapidly merging with Operational Technology

- **Benefit:** Data can be remotely monitored, aggregated and analyzed at higher levels – Gives more automation & efficiency

- **Risk:** Increases the vulnerability of the individual systems
  …& also the entire network

“Air gapping” is no longer a feasible solution for security

- As more ICS and Defense Systems devices use network connectivity
- Threats are increasingly able to jump the gap

Some Examples

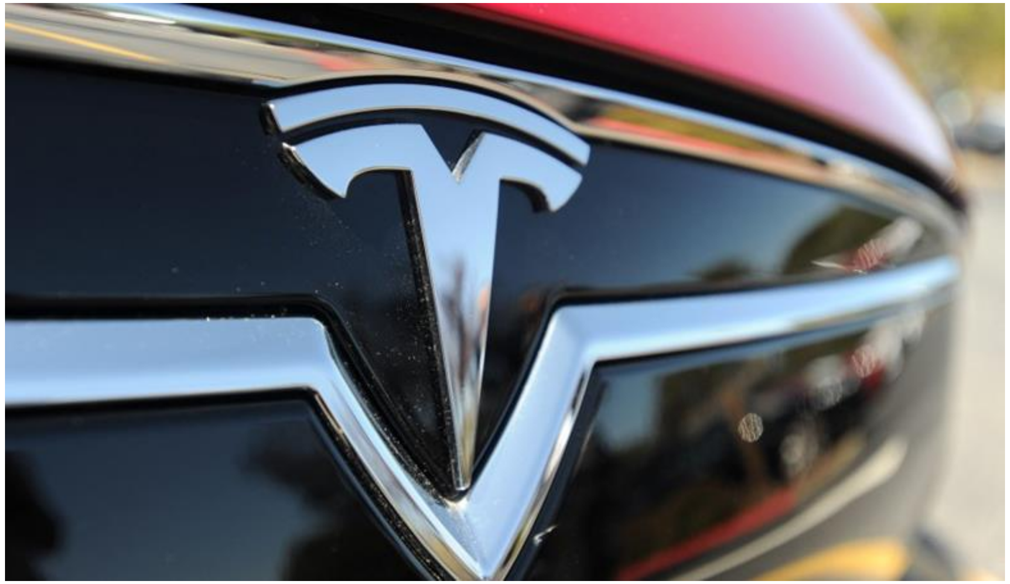
Everything is attached to an IP network

- OPM
- Yahoo 500M emails
- Tesla – remotely applied the brakes
- Ukraine grid hack

Or is close to one

- Aircraft & Ship maintenance systems (concern that malware will jump, and then go undetected)
- Certain air-gapped targets hit, but attack started through web-connected systems
- EW approaches to injecting malware

Tesla Hack, Sept 2016



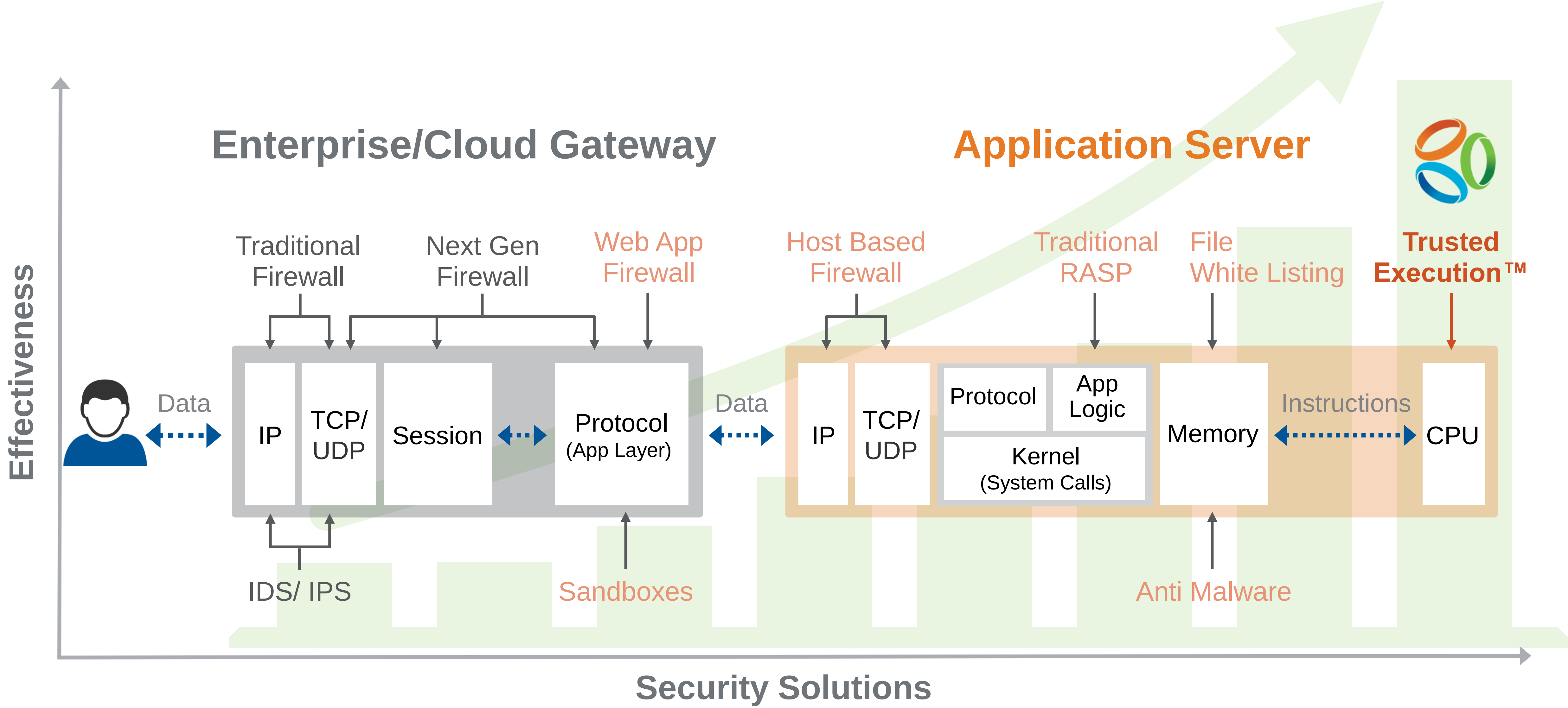
Researchers gained remote control of a Tesla vehicle by hacking into onboard Controller Area Network (CAN) bus.

- Dug up a vulnerability in the Tesla S' web browser
- Injected malware via browser when vehicle was close enough to a malicious WiFi hot spot to connect
- Used another vulnerability in the Tesla's Linux OS to gain full privileges on the car's head unit, the computer in its dashboard
- Then simply overwrote the gateway's firmware with their own to connect to the CAN bus
- Remotely activated the moving vehicle's brakes

Converged, or not, there is commonality among advanced cyber threats in 3 ways:

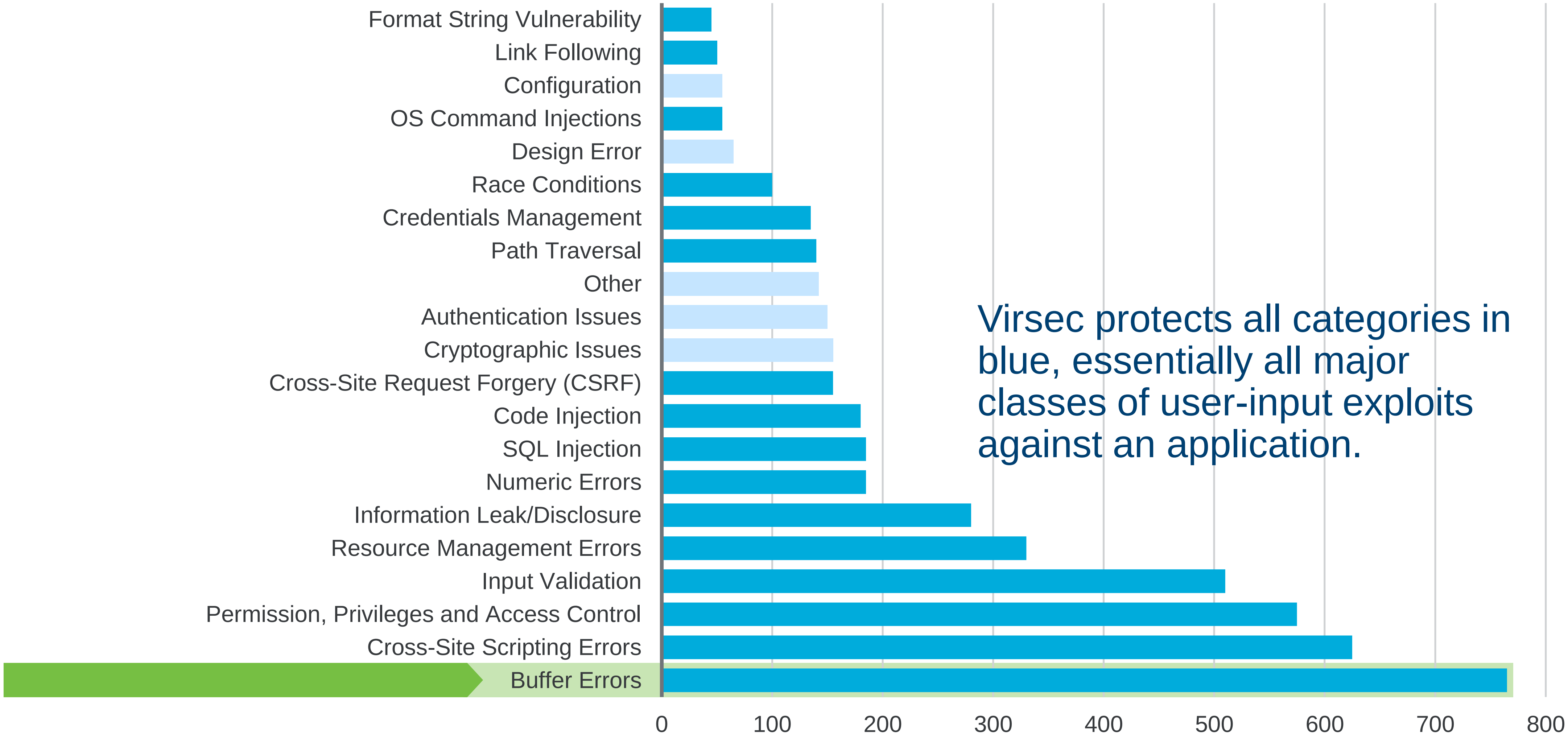
- Applications are the most frequent point of entry
- Apps are almost always the means of malicious control
- Processor memory is the ultimate goal of an advanced hacker

Virsec Trusted Execution vs Other Approaches



Coverage of US CERT NVD Category Vulnerabilities

Source: National Vulnerability Database

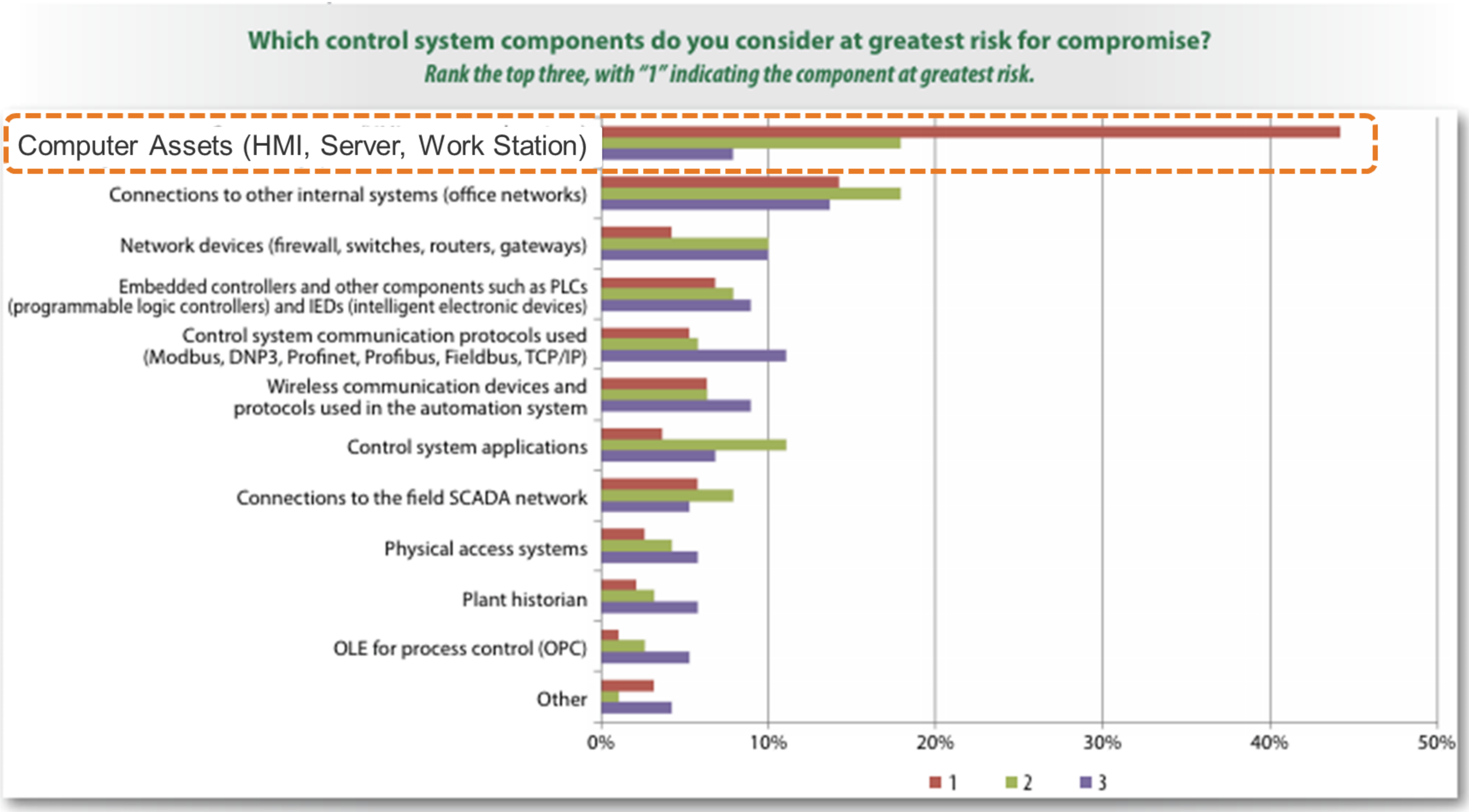


Virsec protects all categories in blue, essentially all major classes of user-input exploits against an application.

SANS Institute survey on ICS security

- Identified ICS software applications (like HMI, application servers, engineering workstations) at greatest risk for compromise
- Vendors of ICS applications are rapidly adopting Secure Software Development (Secure SDLC) processes to address these concerns
- Unfortunately….
  - Pre-secure SDLC legacy systems are very widespread
  - Secure SDLC does not protect against indefensible and previously difficult to detect cyber-attacks, the type being developed by nation state actors and used to compromise Critical Infrastructure
  - Due to the way software executes, there is nothing that a software provider can do in their code to defend against this sort of attack

ICS: Greatest Risk at Supervisory and Web Tier Apps



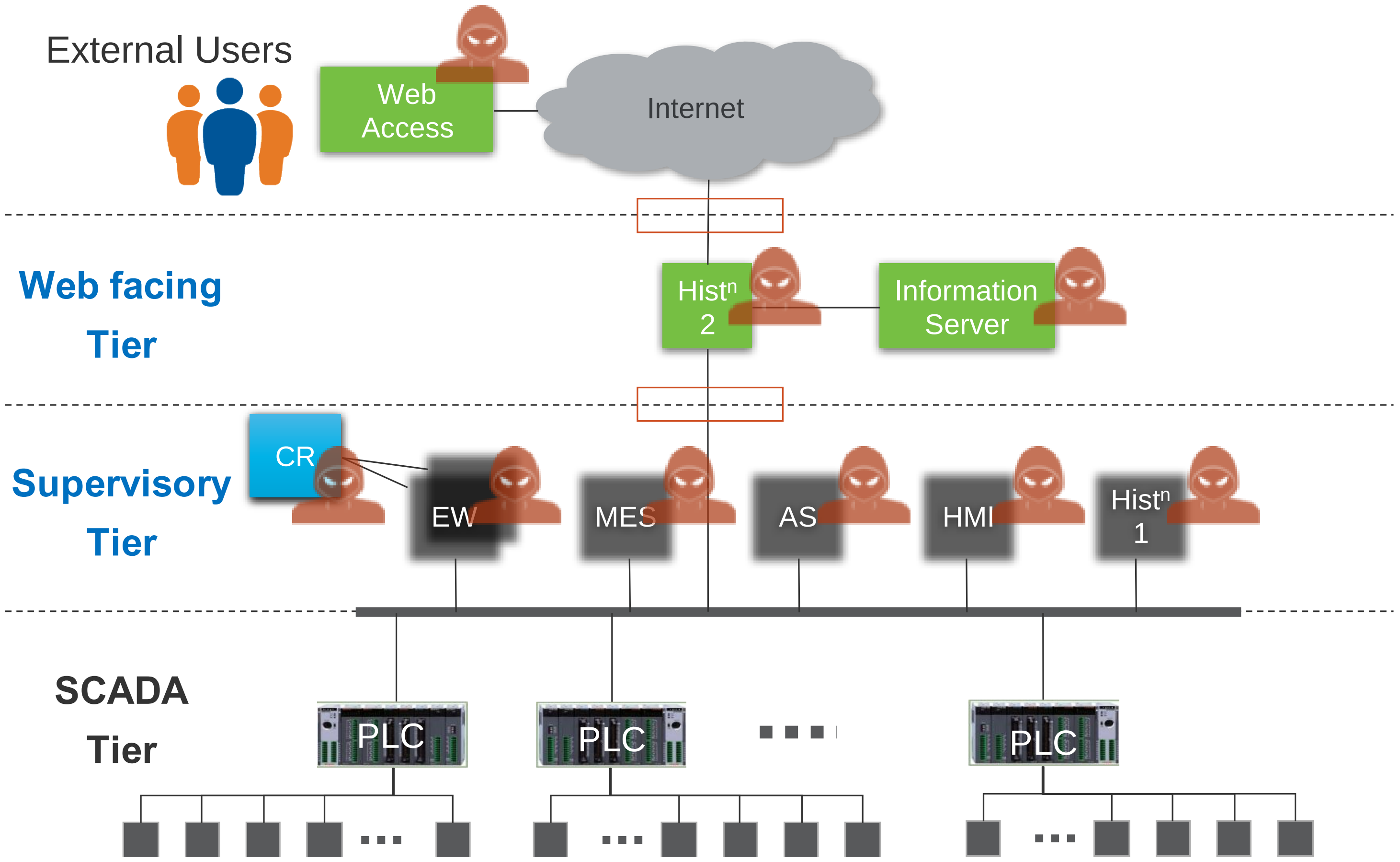
Source: SANS Institute - The State of Security in Control Systems Today, June 2015

How to address

- A holistic solution to protect against such previously indefensible cyber attacks.
- Protects all applications - against attacks via memory
  - binary apps
  - web apps
  - app infrastructure
- File system and malformed input data
  - Protects in-house developed, 3rd party or open source components, without touching the source code, all in run-time
  - ARMAS makes it impossible for sophisticated hackers, including nation-state actors, to compromise applications and helps the security team detect and respond instantaneously
  - Consistent benchmark results show no false positives (100% accurate) given its non-signature based Trusted Execution™ technology.

ICS: Exposure at Supervisory and Web-facing Tiers

- Multiple attack surfaces
- Impacts Uptime, Defense Readiness, Safety, Compliance, Penalties
- Secure SDLC alone is inadequate
- Lots of legacy - pre-secure SDLC
- Rise of sophisticated memory attacks - considered “**indefensible**”



Virsec ARMAS

Protects **ICS Supervisory and Web-facing Tiers** against ALL Core Threat Vectors

BINARY *AND* INTERPRETED CODE PROTECTION IN ONE PLATFORM

Threat: Memory Attacks

Malicious Code Injection into Application Memory (e.g. DLL Injection, ROP, Buffer Errors)

Threat: File-based Attacks

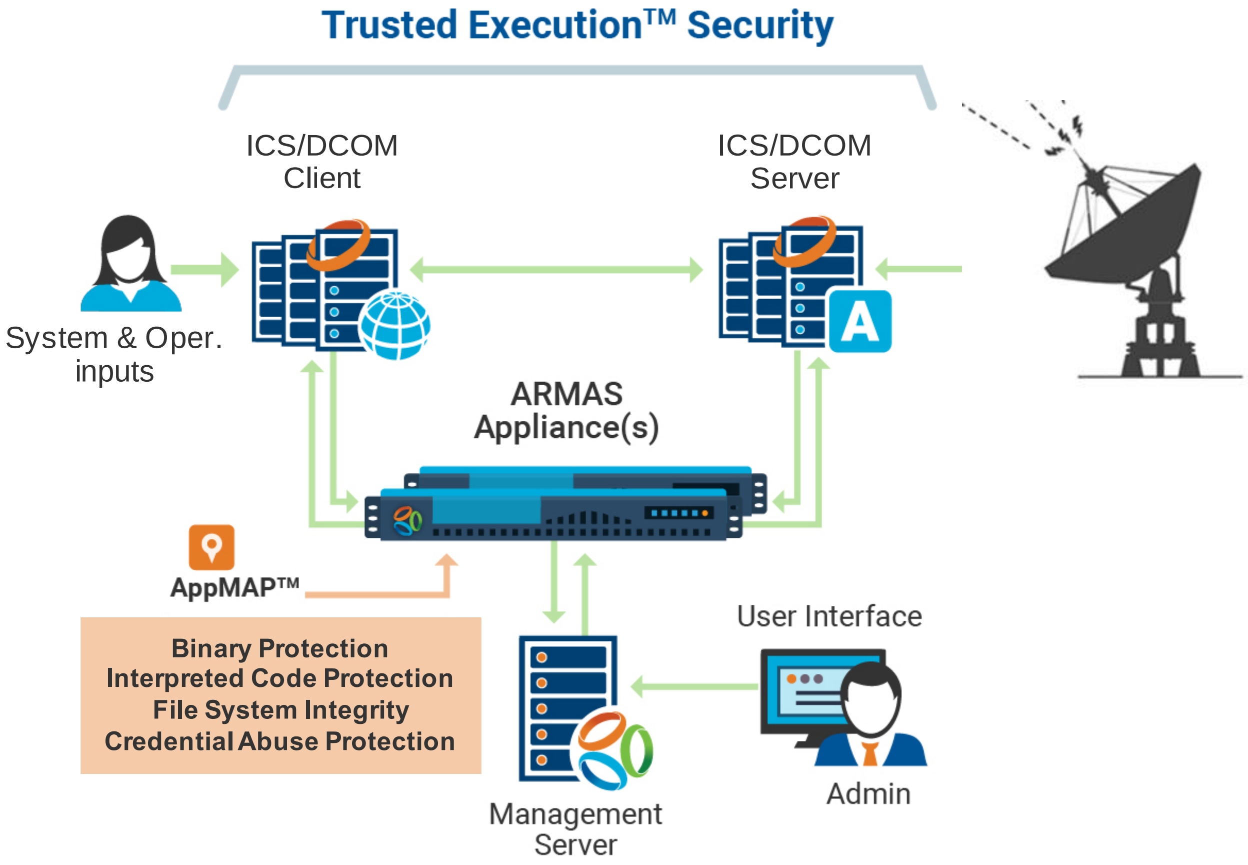
Exploits using files (e.g. DLL hijack) or illegal file system modifications (e.g. file permissions, ownerships, etc)

Threat: Data-borne Attacks

Malicious Data Injection to compromise Interpreted Applications (e.g. WIS, Ent. Apps)

Threat: Credential Abuse

Control User Access to Critical Assets via Apps for External User and Insider protection

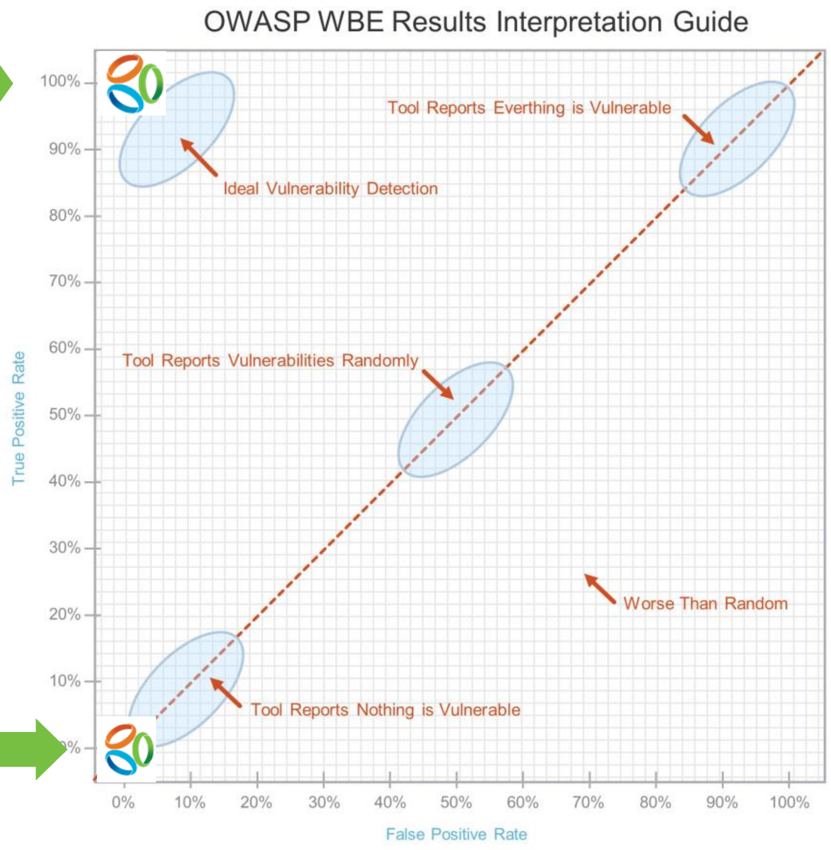


No False Positive Application Security on the Interpreted (Visible) Code – OWASP Benchmark Project

- ARMAS detected all 272 pages of true positives in the app
- Avoided 232 pages of false positive pages in the app
- fs-RASP was 100% accurate on SQLi
- Compared to a 2.5 year old RASP product which found 178 (65%) pages
- Leading DAST found 89 (31%) pages to be vulnerable

ARMAS^{TM}
True Positive: 100%

ARMAS^{TM}
False Positive: 0%



Other Advanced Memory Exploits caught by ARMAS

Also dll injection

- **Buffer overflows**
  - e.g. exploits targeting the recent glibC vulnerability

> **Extremely severe bug leaves dizzying number of software and devices vulnerable**
>
> **Since 2008**, vulnerability has left apps and hardware open to **remote hijacking**
>
> *Ars Technica, Feb 16, 2016*

- **Return-Oriented Programming**

> **Increasing prevalence of DEP, ASLR has forced attackers to find new techniques**
>
> Almost **all exploits** discovered in the last two years have used **return-oriented programming**
>
> *Microsoft, RSA 2015*

- More exploit vectors: **DLL Hijacking, Path Traversal, …**

ARMAS for ICS, Defense Applications

PROTECTS	WHERE
Grandfathered legacy applications	No developers exist
Custom apps developed in-house	Time and money prohibit waiting until all issues have been remediated
“Too Big To Fail” applications	The consequences of a breach are too high (existential threats)
OS and 3rd party binaries	No source code and keeping patches up-to-date not an option
Apps with highly sensitive or data protected by regulations	Even additional insider auditing and access controls are necessary

ARMAS Testimonials

A New Level of Accuracy and Completeness in Application Protection

“Virsec’s solution, ARMAS, provides an advanced detection mechanism against certain **indefensible and previously difficult to detect cyber-attacks**, the type that are being developed by nation state actors and may be used to compromise the critical infrastructure. Due to the way software works and executes, there was nothing that a software provider could do in their code to defend against this sort of attack.”

- ***Chief Security Architect, Product Security Organization, Global leader in ICS Systems***

Virsec

A Powerful New Way Forward

Efficacy

- Stops zero-day attacks
- OWASP benchmark with no false positives

Immediate Prevention

- Microsecond detection and blocking

Unprecedented Visibility

- Ability to report on data touched and seen by specific users
- New levels of user-data compliance reporting

TCO Cost Effectiveness

- More efficient use of analysts
- No need to touch source code
- Deployment automation integration

Virsec

Thank You!

Virsec