



Surviving the ZTNA Journey

Bill Carico
bill@X4.com



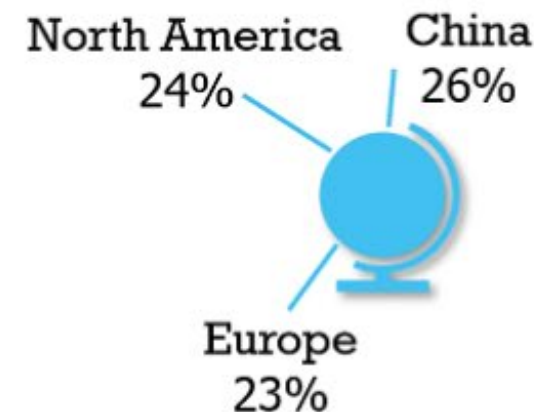
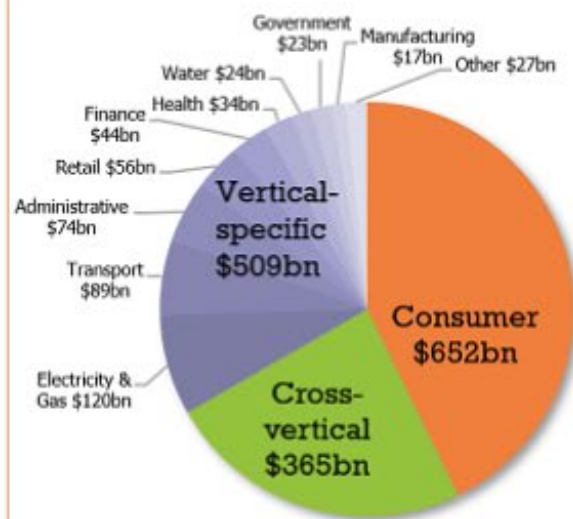
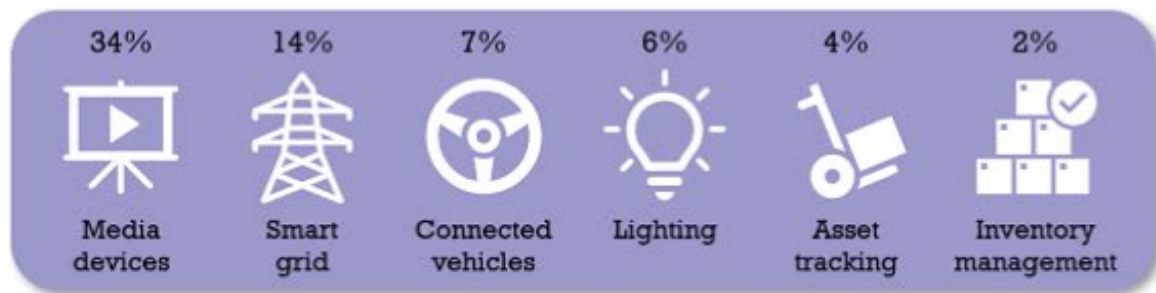
The Internet of Things (IoT) Market 2019-2030

24.1 billion

IoT connected devices in 2030 (7.6bn 2019)

\$1.5 trillion

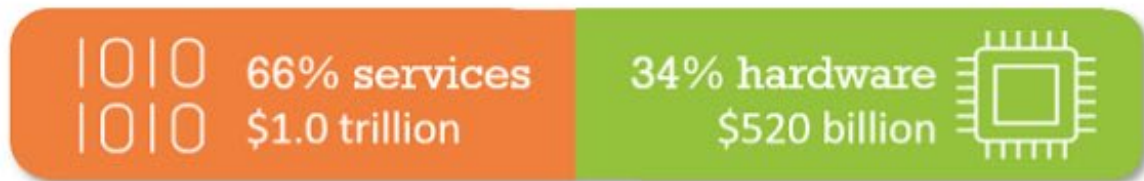
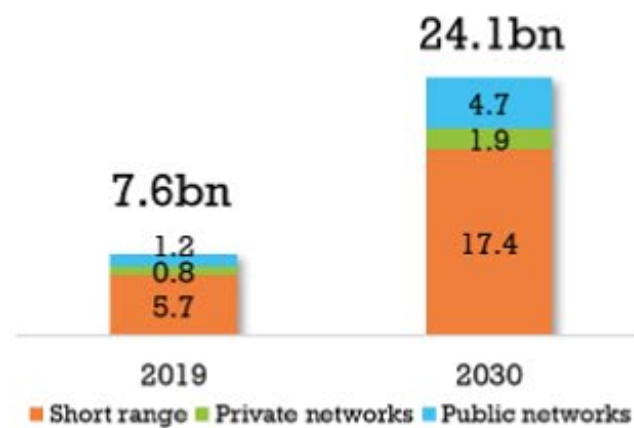
IoT revenue in 2030 (\$465bn 2019)



TRANSFORMA
INSIGHTS

transformainsights.com

@transformatweet



Survival Tips

1. Open Your Eyes...

2. Find an OS
to Trust

3.

Zero Trust has achieved
Bandwagon status.

Beware of:

- **Chaos Theory**
- **Management by Magazine**
- **The Fruit Loops Syndrome**

Open Your Eyes to the Spies

- The CIA, FBI, NHS, DNI,...
- Ch!n@, Russia, Iraq, DPRK...
- NSO Group - Pegasus
Zero Touch

Survival Tips

Find an OS to Trust:
zOS, Linux distribution,
UNIX variant, iOS,
Android,...

Open Your Eyes...

- The CIA, FBI, NHS, DNI,...

Edward Snowden's profits from memoir must go to US government, judge rules

Court says state is entitled to any profits from Permanent Record because its publication breached non-disclosure agreements



📷 'They can't (yet) ban the book, so they ban profit' ... copies of Permanent Record on sale in Berlin in September. Photograph: Jörg Carstensen/AFP/Getty Images



Bill Alderson (He/Him) • 1st

World-renowned network security trailblazer guiding enterprises to secure, r...
3w • Edited • 🔒

NSA, FBI, CIA all built lawful intercept software tools with \$B US Budgets. Then due to their poor security disciplines each of them "lost" the tools to criminals. Well documented by the press and admitted by all three agencies. Before this loss, criminals were much less capable. Criminals now equipped with \$B's in US Intel Agency Attack Tools have used them to create a B\$ ransom economy that now fully funds their development empowering their criminal economy.

The US Government due to their material gross security negligence letting criminals have lawful intercept tools largely building criminal and nation state hack attack tools should in fact pay every ransomware demand and pay for mitigation costs for every US organization and individual held hostage by their resulting incompetence and gross negligence.

April 18, 2022 Axios

Report: NSO Group's spyware is everywhere



Photo by JACK GUEZ / AFP

Open Your Eyes

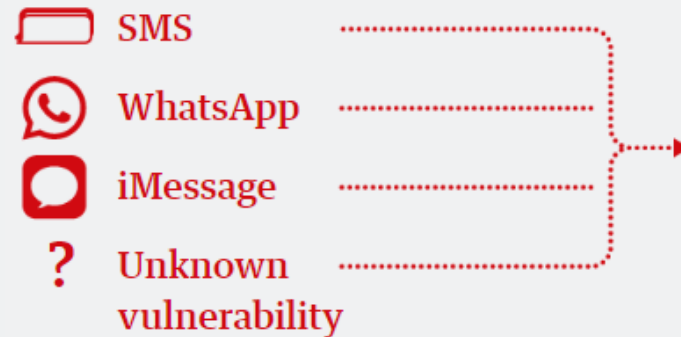
- NSO Group Pegasus (Zero Touch spyware)

In an exchange of [public letters](#) in 2019, [NSO Group] told Amnesty International and other activists that they would do “whatever is necessary” to ensure NSO’s weapons-grade software would only be used to fight crime and terrorism. But the claim, it now appears, was hollow.

How Pegasus infiltrates a phone and what it can do

Attack vectors

Pegasus can be installed on a phone through vulnerabilities in common apps, or by tricking a target into clicking a malicious link



Capabilities

Once installed, Pegasus can theoretically harvest any data from the device and transmit it back to the attacker



Guardian graphic

Challenge Everything

Don't trust vendors and consultants...

- To be truthful about scalability limits
- That more features are better
- To configure with logical defaults



- Ask their references for references
- Perform load testing
- Beware of the Elephant in the room!
*i.e. Research Solar Winds breach
and Microsoft's Midori project*


Beware of Experts and Wayward Billionaires

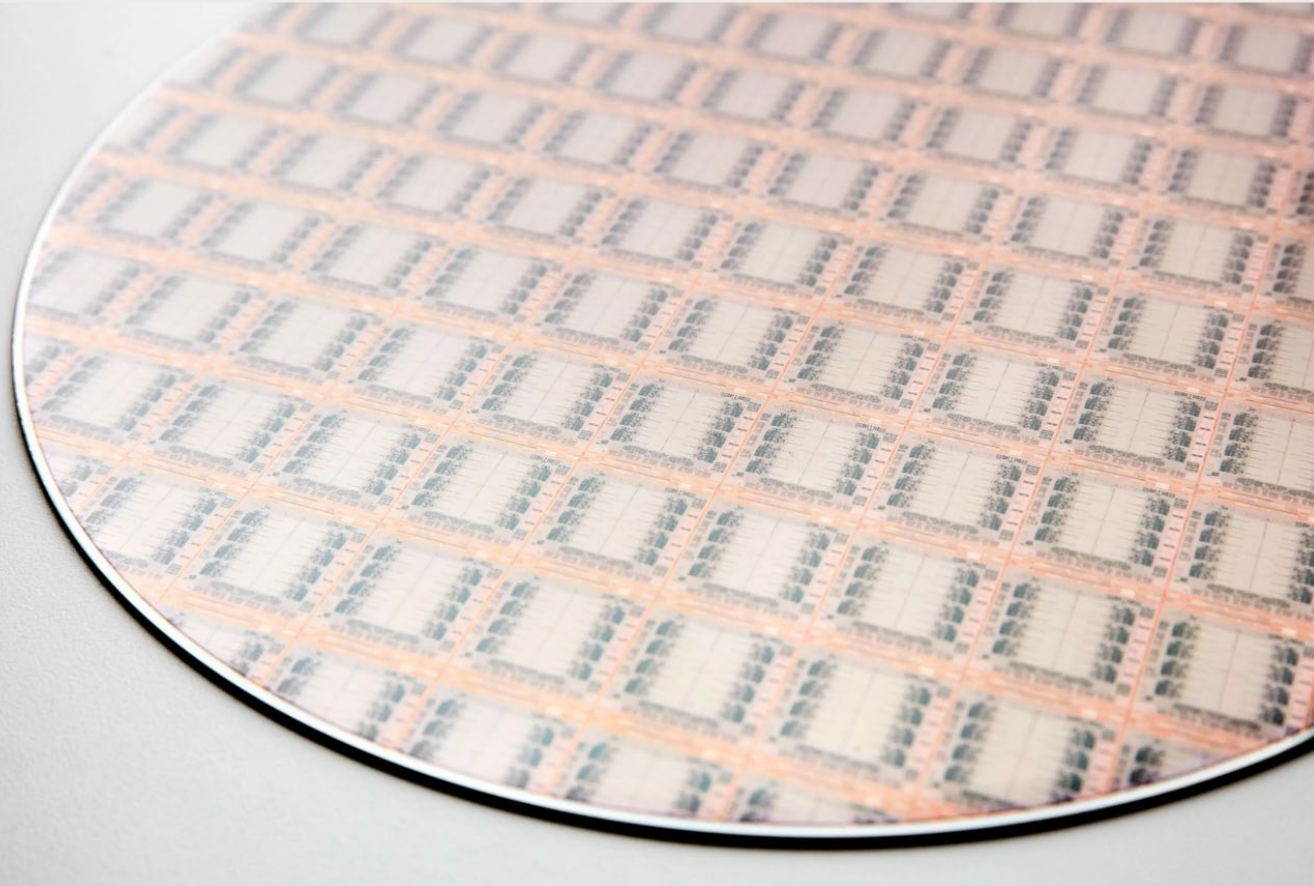
"What seems to be the perfect business plan or the latest technology today may soon be as out of date as the 8-track tape player, the vacuum-tube television, or the mainframe computer."

Bill Gates, The Road Ahead 1995-96

27 years later, the mainframe is still the backbone of the world economy, with large banks routinely handling 25,000 financial transactions per second.

IBM's New Telum Chip Reboots the Mainframe › Big Blue's z16 computer—and the cache-savvy design at its core—gives new relevance to the platform

BY DEXTER JOHNSON | 29 APR 2022 | 4 MIN READ | 



IBM's Telum processor, shown here in its wafer state, contains **eight (8) cores** clocked at over **5 gigahertz**. And crucially, each core has its own **32-megabyte level 2 cache**. Delivering on the promise of this innovation—at a system-wide scale—was one of the key challenges for IBM's new z16 mainframe.

SOURCE: IBM



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



654 KNOWN EXPLOITED VULNERABILITIES IN 2021

[Known Exploited Vulnerabilities Catalog](#) | [CISA](#)

654 Unique Vulnerabilities by Vendor for 2021

Microsoft	185
Cisco	59
Adobe	38
Apple	28
Google	27
Apache	21
Oracle	20
VMware	14
Citrix	8
Mozilla	7
SAP	6
IBM	5
Accellion	4
Linux	4

Types of Exploits out of 654 Total

- ✓ remote code execution - 232
- ✓ privilege escalation - 106
- ✓ use-after-free - 55
- ✓ command injection - 47
- ✓ memory corruption – 41
- ✓ bypassing... - 37 (...authentication - 28, ...a security feature - 9, ...authorization - 3)
- ✓ buffer overflow – 34
- ✓ attackers execute arbitrary code - 33
- ✓ Java – 24
- ✓ Microsoft Internet Explorer – 24
- ✓ Google Chrome - 22
- ✓ crafted HTML - 16
- ✓ Microsoft Exchange Server - 14
- ✓ improper access control - 9
- ✓ improper authorization - 4
- ✓ encryption related - 4
- ✓ root access - 4 (Android 3, Linux 1)

SHIELDS  UP

Colonial Pipeline ransomware attack linked to Microsoft Exchange vulnerabilities [Updated]

A new day, a new Microsoft Exchange situation.

ROBERT CARNEVALE 12/18/2021



Source: Windows Central

Keep in Touch

Sign up now to get the latest news, deals & more from Windows Central!

Your Email Address

I would like to receive news and offers from other Future brands.

Yes No

I would like to receive mail from Future partners.

Yes No

SIGN ME UP

No spam, we promise. You can unsubscribe at any time and we'll never share your details without your permission.

Microsoft Exchange linked to the root of the cyberattack

Investopedia
Updated Nov 11, 2020

The 10 Most Expensive
Cyberattacks of All Time

#1 MyDoom (MS Windows)

Estimated cost: \$38 billion
Year initiated: 2004

SECURITYWEEK

April 29, 2021

BadAlloc: Microsoft Flags Major Security Holes in OT, IoT Devices

Security researchers at Microsoft are raising the alarm for multiple gaping security holes in a wide range of enterprise internet-connected devices, warning that the high-risk bugs expose businesses to remote code execution attacks.

c|net

March 5, 2021 2:21 p.m. PT

Microsoft Exchange attackers strike more than 30,000 US organizations

A vulnerability Microsoft has already fixed in an urgent security update this week is wreaking havoc on businesses, and has caught the attention of the White House.

Redmond

02/04/2000

Microsoft Warns of New NT 4.0 Security Breach

Windows NT 4.0 Workstation, Server, Enterprise Edition, and Terminal Server Edition are all affected by the vulnerability.

THE BALTIMORE SUN

AUGUST 30, 2002

Microsoft says its systems since '96 have security flaw

EDMOND, Wash. - Microsoft Corp. said yesterday that all versions of its Windows operating system released since 1996 have a security flaw that may bar users from encrypting e-mail and using some Web sites.

ZDNet

August 22, 2001 - 00:00 GMT (7:00 PDT)

Having already done \$2 billion in damage, the final cost of the Code Red worm could eventually top Love Bug's \$8.7 billion price tag.

WIRED

SECURITY 01.14.2020 05:38 PM

Windows 10 Has a Security Flaw So Severe the NSA Disclosed It

In a shift toward transparency, the National Security Agency announced a bug that could have left over 900 million PCs vulnerable to attack.

PC

August 28, 2020

Windows Computers Were Targets of 83% of All Malware Attacks in Q1 2020

AV Test shows that Windows computers are the most vulnerable to malware attacks and are targeted more than any other operating system.

c|net

April 14, 2021 7:34 a.m. PT

FBI operation removes backdoors from hacked Exchange servers in the US

The Justice Department on Tuesday revealed that the FBI undertook a court-approved operation to remove "malicious web shells" from compromised Microsoft Exchange email servers in the US. The web shells are snippets of code that act as backdoors and could have allowed continued unauthorized access to emails and US networks, said the DOJ.

c|net

Jan. 2, 2002 4:43 p.m. PT

Expert says Windows has a security breach

A security expert says he has found a weakness in Windows that allow a hacker to subvert the operating system.

ZDNet

November 26, 2003 - 00:06 GMT (06:06 PST)

Microsoft investigates Exchange security hole

Microsoft says its Exchange server software appears to contain a serious flaw that could allow hackers to access users' accounts.

NETWORKComputing

FEBRUARY 14, 2004

Windows Source Code Security Breach Troubles Experts

The Redmond, Wash.-based company confirmed the unauthorized release late Thursday, marking yet another security blow to Microsoft in a week that saw worm attacks and major vulnerabilities in Windows revealed.

For the last 20+ years...

SECURITYWEEK

May 08, 2017

Google Researchers Find "Worst" Windows RCE Flaw

Google Project Zero researchers Tavis Ormandy and Natalie Silvanovich claim to have found a critical vulnerability in Windows. The details of the flaw will likely be disclosed in 90 days from now even if a patch is not available.

The New York Times

MAY 1, 2014 6:08 PM

Attackers Use Microsoft Security Hole Against Energy, Defense, Finance Targets

SAN FRANCISCO - By the time Microsoft warned customers of a nasty security hole in its web browser Saturday, a sophisticated group of attackers were already using the vulnerability against defense and energy companies, according to FireEye, the security company.

SOFTPEDIA NEWS

Apr 15, 2015 09:17 GMT

Microsoft Finally Takes Down Pirated Windows 2000 Source Code After 11 Years

Microsoft has finally managed to take the pirated Windows 2000 and Windows NT 4.0 source code offline, no less than 11 years after it first got leaked to the web.

Where are you going?

- Zero trust (ZT) – evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. (*source: NIST*)
- The **cyber attack surface** has expanded due to the shift to working remotely, dependency on multiple clouds and services, the explosive growth of IoT devices, stolen cyberdefense software, and massive vulnerabilities from iOS and Android.
- Zero Trust is not a single product, solution, or tool, it's a model or framework for improving cybersecurity by combining principles, policies, products, and practices to provide tighter and more extensive end-to-end access controls and visibility into network activity.



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER CSRC

PUBLICATIONS

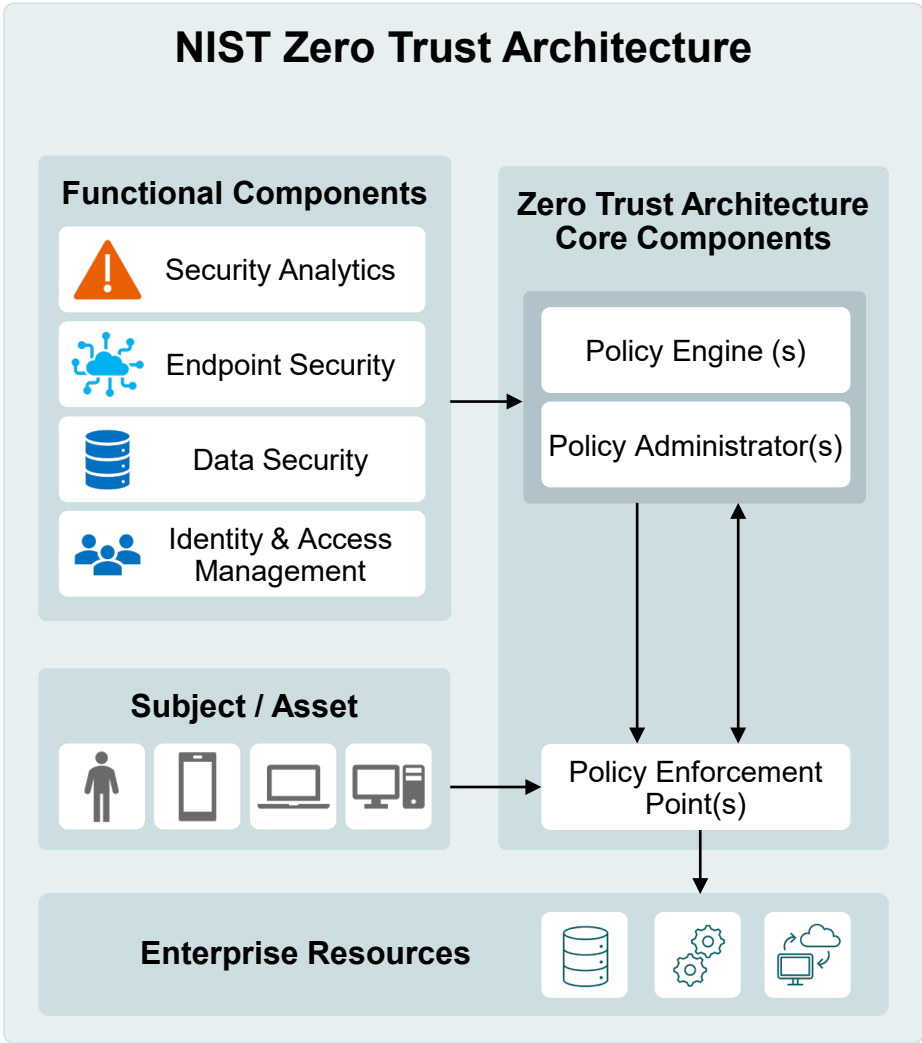
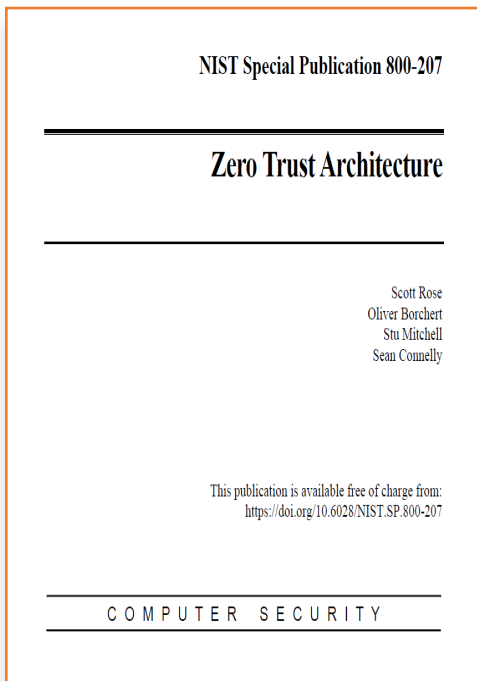
SP 800-207

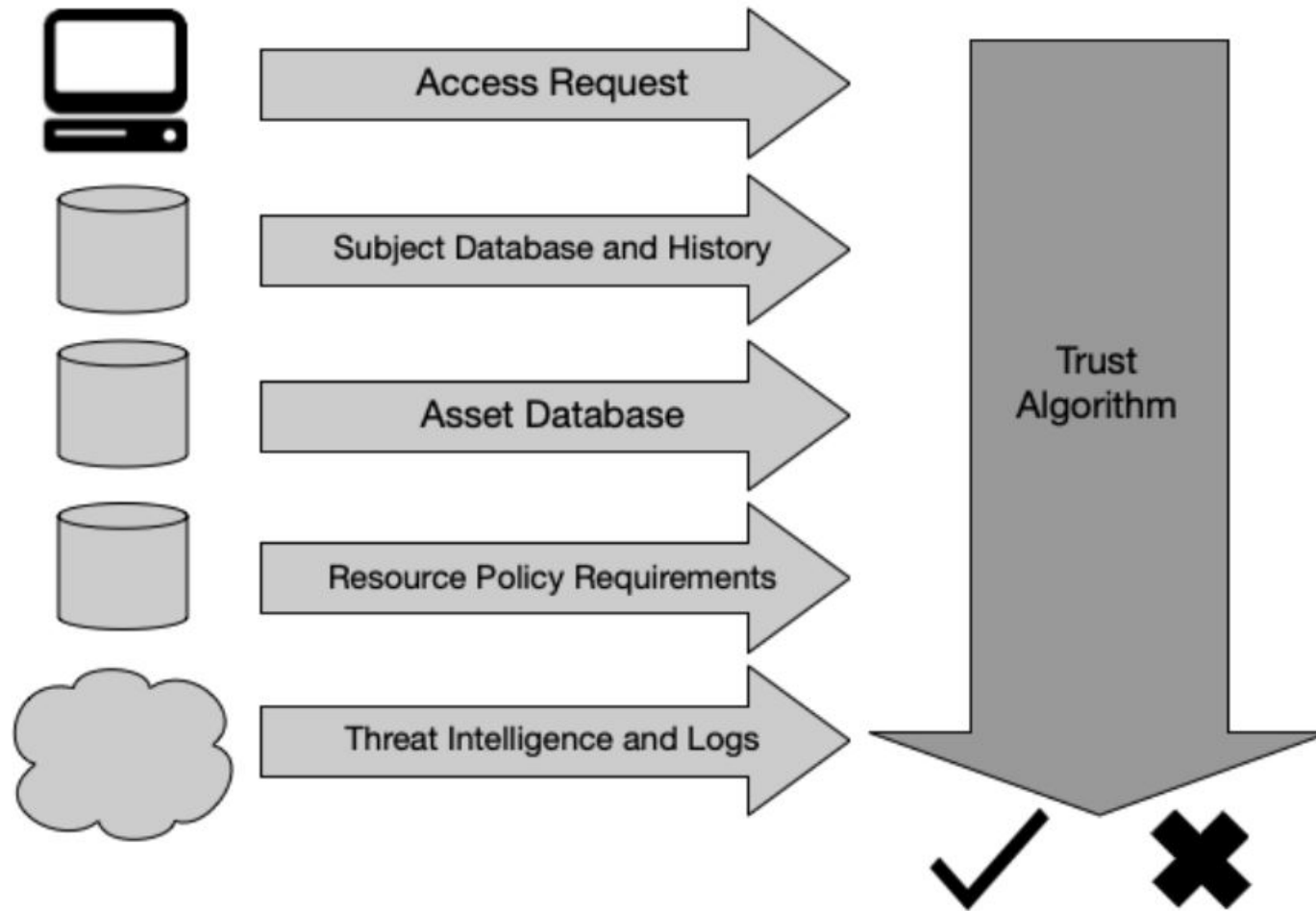
Zero Trust Architecture



Date Published: August 2020

Planning Note (12/11/2020):

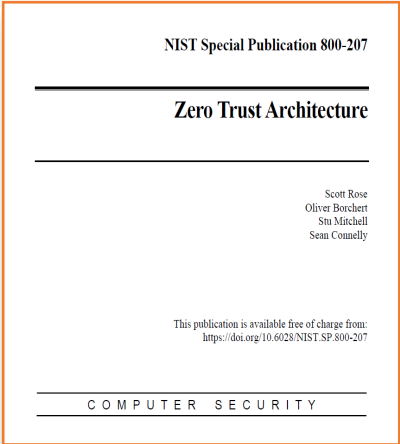
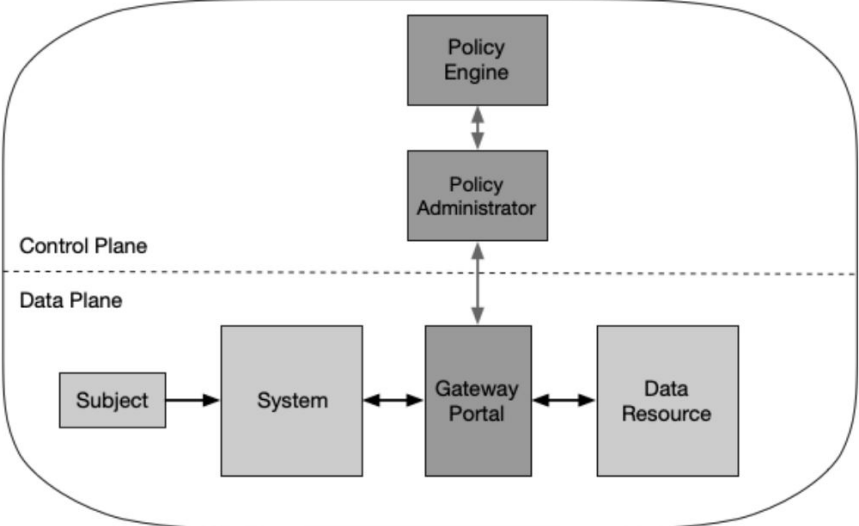




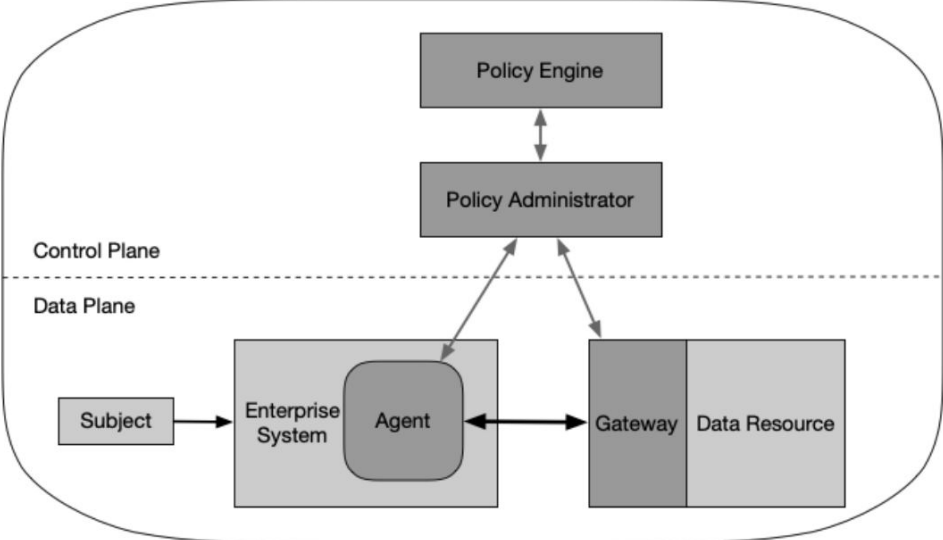
Trust Algorithm Input

- Zero Trust allows access control to be managed for each user, device, application, and service.
- Each entity has its own secure perimeter. No more vulnerabilities from the old mindset of implicitly trusting something already on the network. To ensure security, every user, device or system must be verified at each network access point.
- Once operational you must continuously remain vigilant monitoring for suspicious activity. Enforce access authentication for anything and everyone, and log and monitor all network activity.

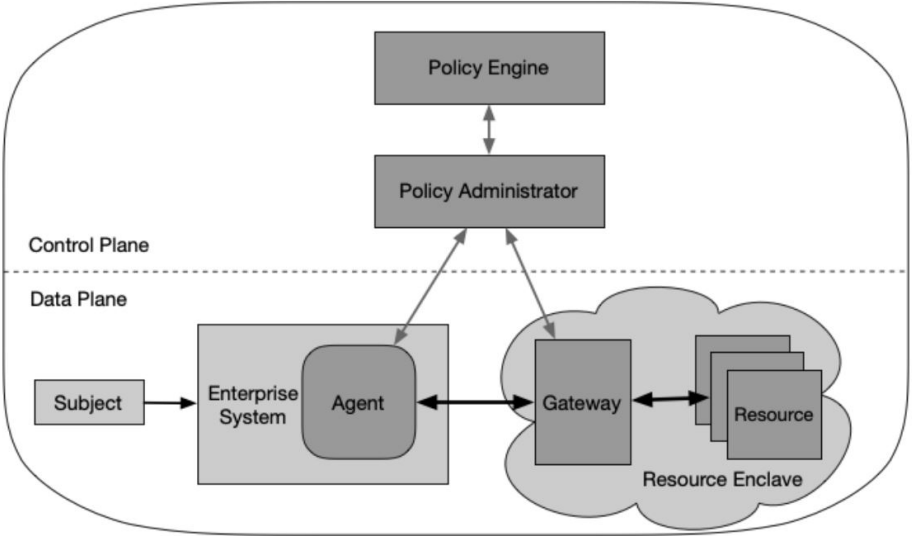
Resource Portal Model



Device-Agent Gateway Model



Gateway Enclave Model



Consistent Network and Security Policy

User/Device Identity

Context

SASE Cloud Infrastructure

WAN Edge Services

- SD-WAN
- WAN Optimization
- Quality of Service
- Routing
- SaaS Acceleration
- Content Delivery/ Caching
- etc.

Security Services Edge

- Secure Web Gateway
- CASB
- ZTNA/VPN
- FWaaS
- Remote Browser Isolation
- Encryption/ Decryption
- etc.

Threat Awareness

Sensitive Data Awareness

- Employees
- Contractors
- Partners
- Devices
- Distributed Applications
- Remote
- Mobile
- Offices
- Edge

- Applications
- APIs
- Data
- Devices
- SaaS
- IaaS
- Data Center
- Branch
- Edge


Entities Anywhere

Zero Trust Access

Resources Everywhere

Consistent User Experience

Source: Gartner
741491_C



Advantages of ZTNA over VPN

“Trust nothing, verify everything”

Device Health

Works Anywhere

More Transparent

Better Visibility

Easier Administration



Buyers
Guide:
*What to look
for in a ZTNA
solution*

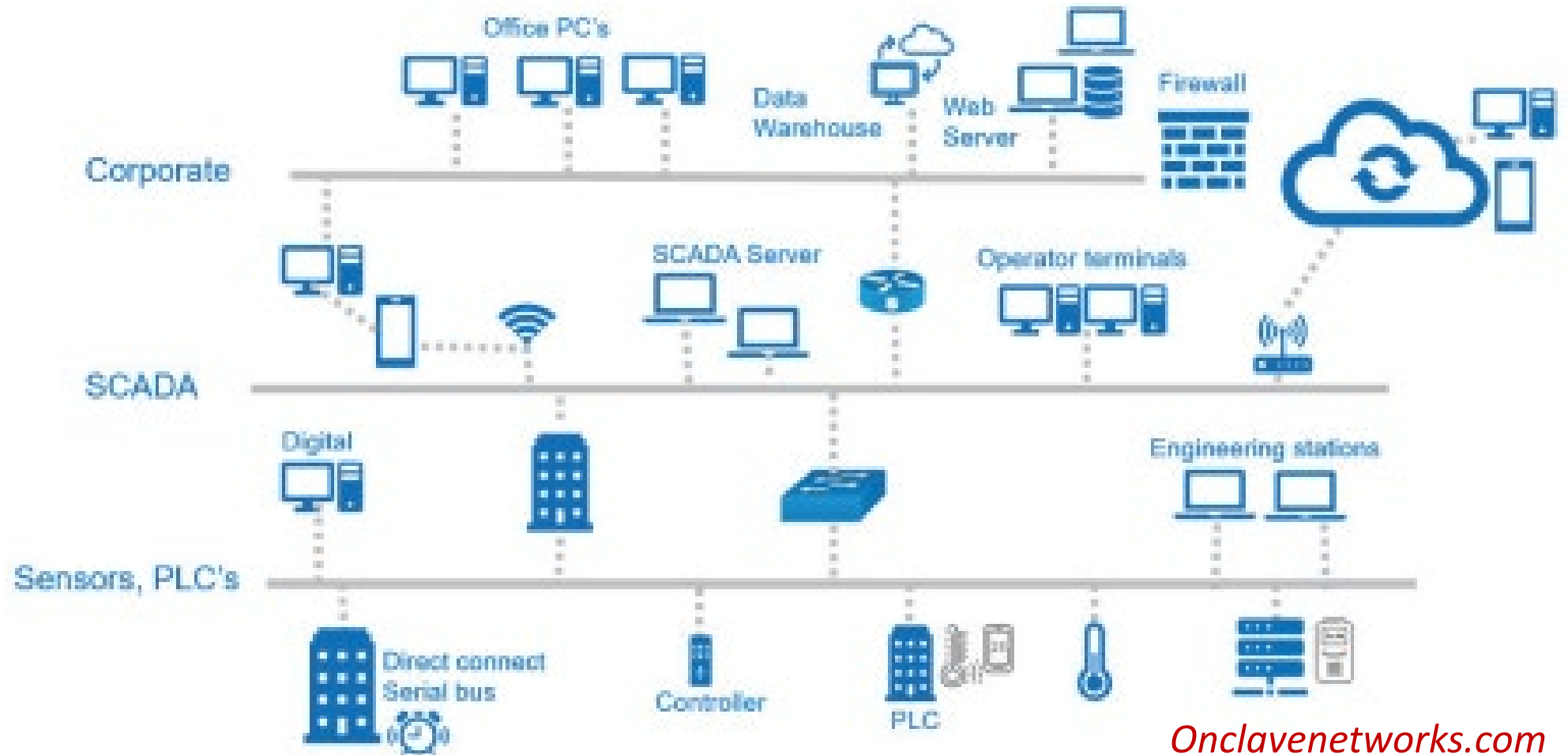
Cloud-delivered,
cloud-managed

Integration with your other
cybersecurity solutions

Excellent user and
management experience

How to Gain an Edge

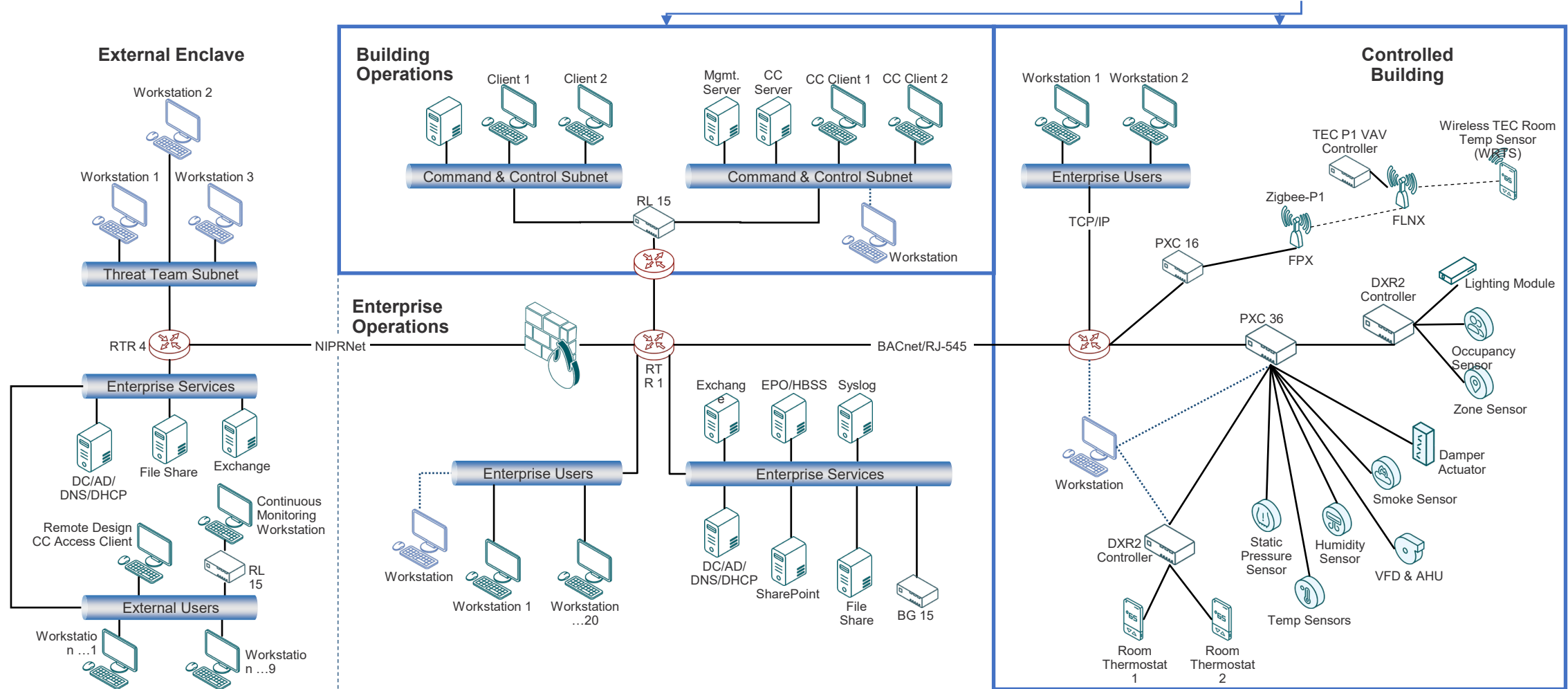
Eliminate your operational technology (OT) and IoT attack surface!



SuccessfulTest @ DoD's National Cyber Range (NCR)

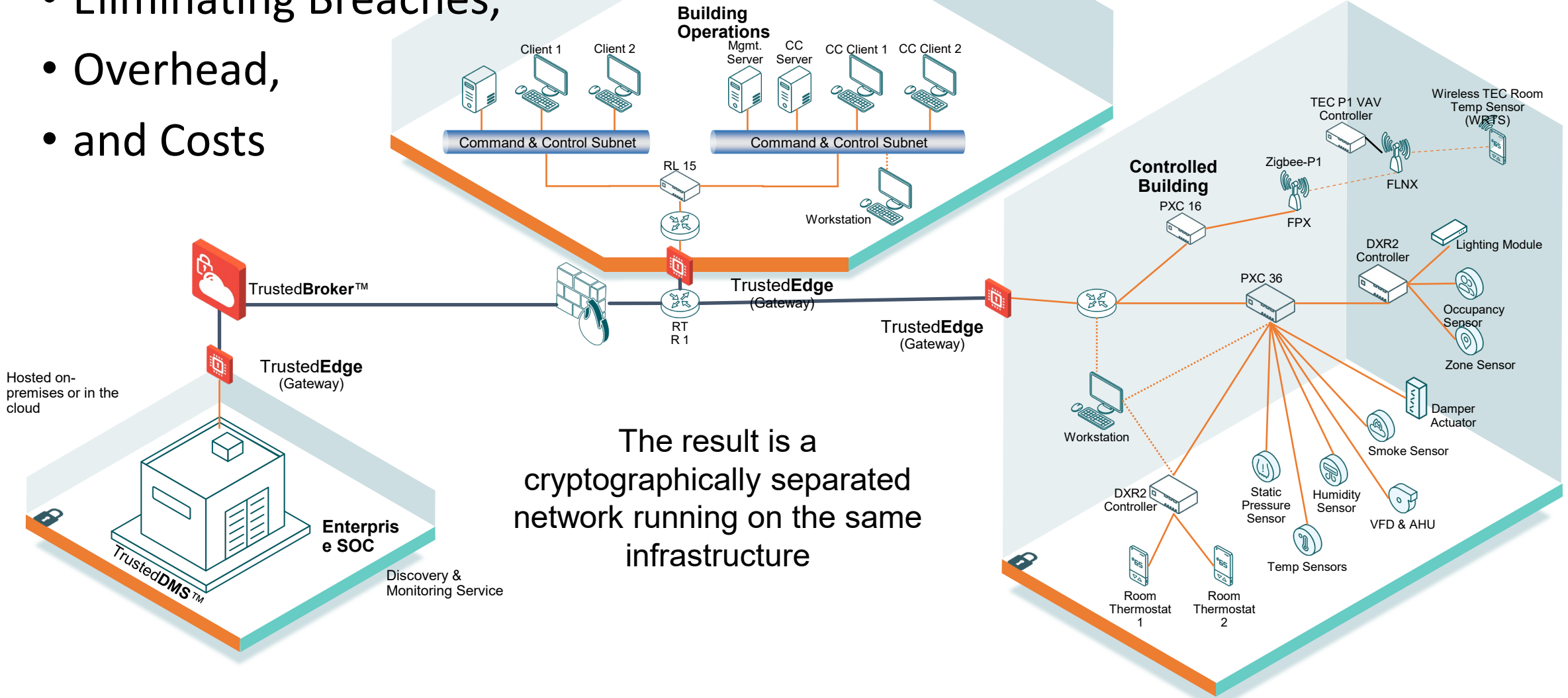
- Took a Typical, Vulnerable, Co-mingled Network Environment, from this...

(OT/ICS Segments)



NCR Architecture Transformed in Hours...

- Reduced Attack Surface, Segmented with Secure Remote Access –
- Eliminating Breaches,
- Overhead,
- and Costs



The result is a cryptographically separated network running on the same infrastructure



Release

IMMEDIATE RELEASE

DoD Announces Release of JADC2 Implementation Plan

MARCH 17, 2022

Deputy Secretary of Defense (DSD) Dr. Kathleen Hicks signed the Department of Defense Joint All-Domain Command and Control (JADC2) Implementation Plan on March 15, 2022.

DEPARTMENT OF DEFENSE

March 2022



SUMMARY OF THE JOINT ALL-DOMAIN COMMAND & CONTROL (JADC2) STRATEGY

JADC2

The warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed of relevance.

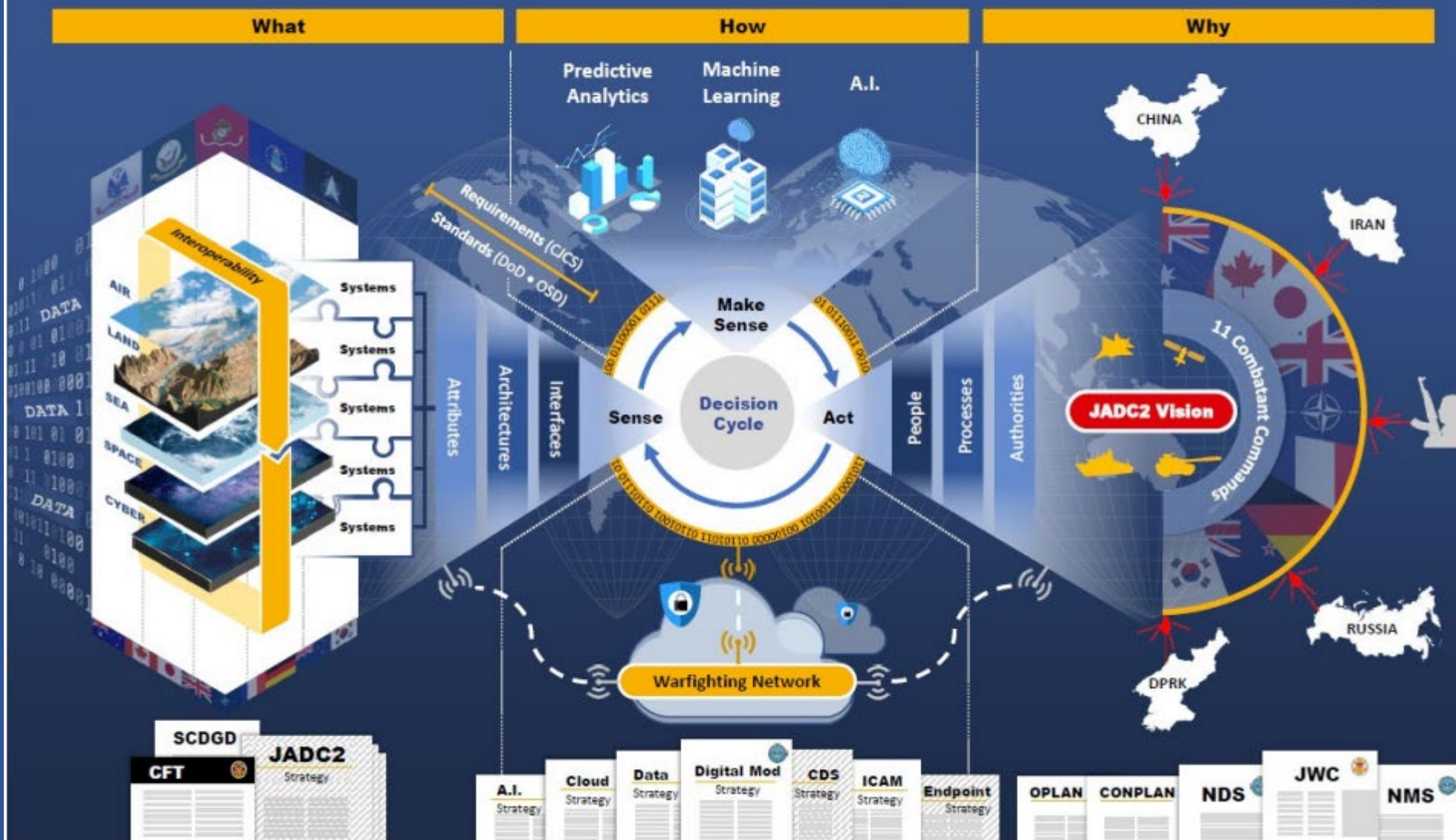


Figure 1 JADC2 Placemat

...the speed of relevance..

Survival Tips

Zero Trust has achieved
Bandwagon status.

Beware of:

- **The Chaos Theory Trap**
 - Predicting Complexity
 - Don't Assume shared definitions
- **Management by Magazine**
 - Project Launch Publicity
 - Surveys
- **The Fruit Loops Syndrome**

Appendix: Acronyms

- API - Application Programming Interface
- BYOD - Bring Your Own Device
- CDM - Continuous Diagnostics and Mitigation
- DHS - Department of Homeland Security
- DNI - Department of National Intelligence
- DoS - Denial of Service
- NGFW - Next Generation Firewall
- G2B - Government to Business (private industry)
- G2G - Government to Government
- NIST - National Institute of Standards & Technology
- NPE - Non-Person Entity
- OT – Operational Technology
- PA - Policy Administrator
- PDP - Policy Decision Point
- PE - Policy Engine
- PLC- Programmable Logic Controller
- PEP - Policy Enforcement Point
- PKI - Public Key Infrastructure
- RMF - NIST Risk Management Framework
- SASE – Secure Access Service Edge
- SCADA – Supervisory Control and Data Acquisition
- SDN - Software Defined Network
- SDWAN - Software Defined Wide Area Network
- SDP - Software Defined Perimeter
- SIEM - Security Information and Event Monitoring
- TIC - Trusted Internet Connections
- TLA – Three Letter Acronym
- VPN - Virtual Private Network
- ZT - Zero Trust or Zero Touch
- ZTA - Zero Trust Architecture
- ZTNA - Zero Trust Network Access

Presenter - Bill Carico

Founder ACTScorp.com

(1981 – Present)

- over 1800 clients
- **X4 Internet**
- **X4 Coalition**
- **X4edu.com** (*Mastering IT series*)
- **Injusticeproject.org**

email: bill@x4.com



Special thanks to Bill Alderson and his wife Kim for their friendship, their service to our nation, and their dedication to strengthening our cyber defenses.

Legal Notice: Names of companies and products used herein are trademarks or registered trademarks of their respective holder.

Copyrighted © 2022, ACTS Corporation, all rights reserved.