

Zero Trust or Bust

Thomas Rivera, CISSP, CIPP/US, CDPSE

Cybersecurity & Privacy Professional

VMware Carbon Black

Co-chair, SNIA – Data Protection & Privacy Committee (DPPC)

Chair, IEEE – Zero Trust Security Working Group

Secretary, INCITS Technical Committee Cybersecurity & Privacy (CS1)

Secretary, IEEE Cybersecurity & Privacy Standards Committee (CPSC)



SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
 - Any slide or slides used must be reproduced in their entirety without modification
 - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Zero Trust: Defined

- Zero Trust is:
 - A collection of security methodologies that work together to enforce access
 - With the view that your network has already been compromised
 - Using contextual information from:
 - Identity
 - Security
 - IT Infrastructure
 - Risk and Analytics tools
 - Enabling dynamic/continuous/granular enforcement of security policies

Zero Trust: History



Jericho Forum - "Outside is the new inside"

Forrester - Zero Trust Research by Jon Kindervag

The Forrester Wave™: Zero Trust eXtended (ZTX)

Google's BeyondCorp

Gartner's 2017 CARTA framework

Jericho Forum™


Conclusion

De-perimeterization has happened, is happening, and is inevitable; central protection is decreasing in effectiveness:

- It will happen in your corporate lifetime.
- Therefore, you need to plan for it and should have a roadmap of how to get there.
- The Jericho Forum has a generic roadmap to assist in the planning.

Copyright © 2007, Jericho Forum. All rights reserved. Jericho Forum™ is a trademark of the Jericho Forum.

BeyondCorp



More images

BeyondCorp

BeyondCorp is an implementation, by Google, of zero-trust computer security concepts creating a zero trust network. It was created in 2009 in response to an APT attack. An open source implementation inspired by Google's research paper on an access proxy is known as "transcend". [Wikipedia](#)

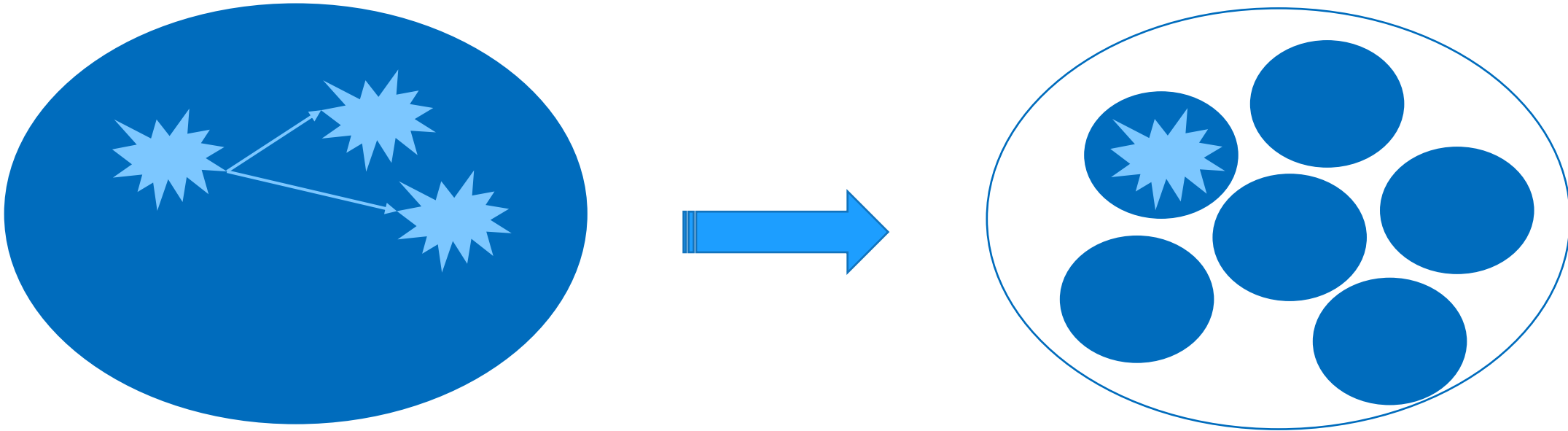
Zero Trust: Characteristics

- Zero Trust includes the following characteristics:
 - Consistent security strategy of users accessing data that resides in any form – from anywhere
 - Assumes a “never trust and always verify” stance for data access and/or services
 - Continuous authorization regardless of the originating request location
 - Increased visibility and analytics across the entire network

Zero Trust: Assertions

- Zero Trust includes the following assertions:
 - The network is always assumed to be hostile
 - External & internal threats exist in the environment at all times
 - Network locality is not sufficient for deciding trust
 - Every device, user, and network flow is authenticated and authorized
 - Policies must be dynamic & calculated from as many data sources as possible

Zero Trust Assumes compromise



- So, compartmentalization is necessary

Complete Compartmentalization is not very Useful...

- So, Zero Trust applies compartment-specific policies, continuously

Least Privilege + Requires knowing all “subjects”

Least Functionality + Requires knowing all “objects”

Least Accessibility (crypt) + Requires knowing access needs

Least Exposure (posture) + Requires assessing device/service/platform integrity

Coherence (peer, temporal) Requires knowing intended, expected and observed behavior, at that specific time

...

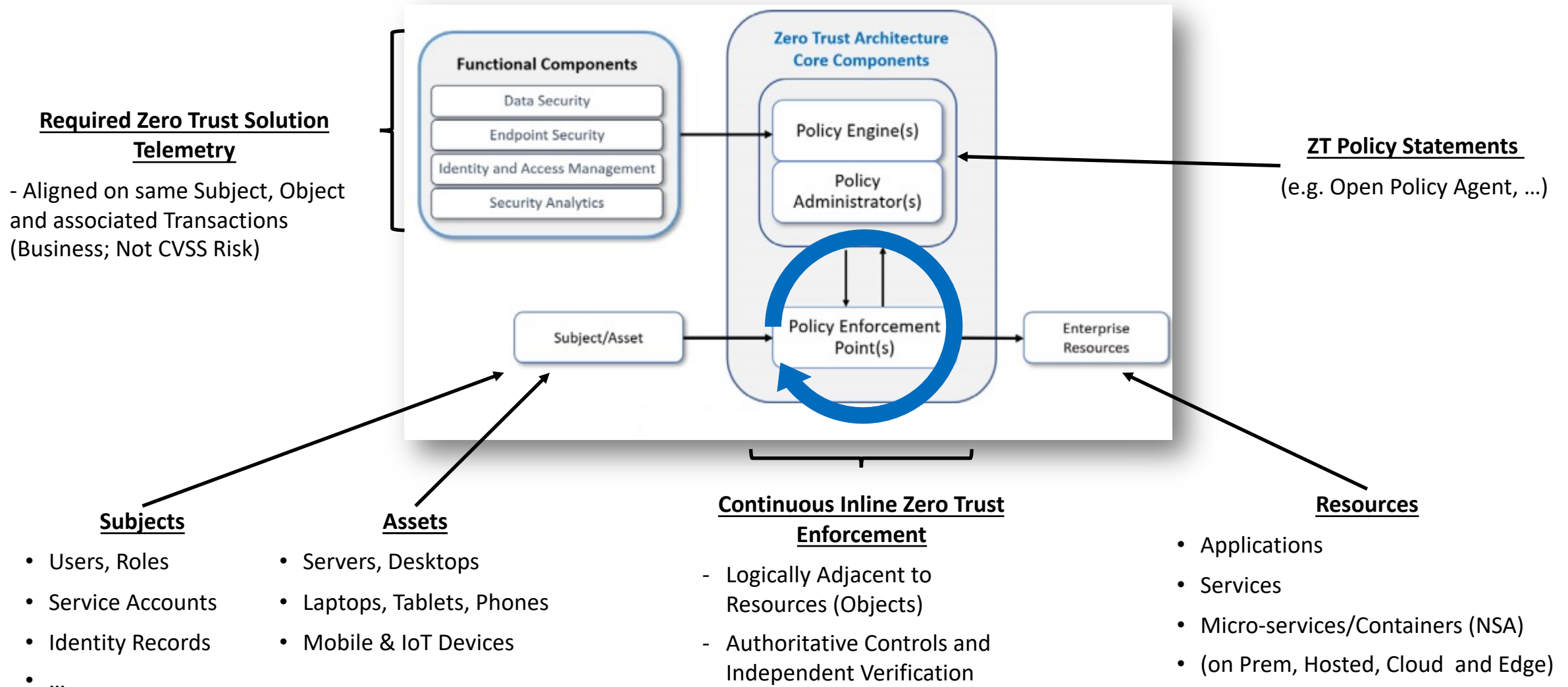
What Zero Trust Means Now

Achieving Zero Trust means:


Device Trust
Network Trust
Workload Trust
User\Identity Trust
Data Trust

- Not every product is designed to work together

High-Level ZT Implementation Architecture



Zero Trust – Why it Matters (Presidential Executive Order)



26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—
The President

Executive Order 14028 of May 12, 2021
Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

In Section 10, *Definitions*:

(k) the term “Zero Trust Architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.

Zero Trust Reference Architectures (Examples)

- NIST SP 800-207 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- DOD Zero Trust Reference Architecture
[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v1.1\(U\)_Mar21.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf)
- CISA Zero Trust Maturity Model <https://www.cisa.gov/publication/zero-trust-maturity-model>
- NSA Embracing a Zero Trust Security Model https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
- UK NCSC Zero Trust Architecture <https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles>
- EU NIS2 Zero Trust (ENISA) [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI\(2021\)689333_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
- White House (US) Executive Order 14028: “Improving the Nation’s Cybersecurity”
<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

Zero Trust: Summary

- Zero Trust is a journey – not a destination
- There are multiple Zero Trust Architectures, Frameworks and guidance documents to help guide in the planning and implementation
- Security vendor interoperability will be one of the keys to implementation success
- Phased approach is usually best when planning implementation



Join us for the Zero Trust Birds of a Feather (BOF) Session



Please take a moment to rate this session.

Your feedback is important to us.



Thank you for your Time!