OUR HEALTH

CCSQ WORLD USABILITY DAY

Zero Trust: 101

Karlene Stecchi, EVP

Tantus Technologies, Inc.

NOVEMBER 8, 2022

Human-Centered Design Center of Excellence

Agenda

- The Security Landscape Today
- The Deceptively Easy Question
- Access Today and Access Under Zero Trust
- Is Zero Trust a Technology?
- Why is Everyone Talking About Zero Trust Now?
- Does My Organization Have to Address Zero Trust?
- Challenges to Implementing Zero Trust
- Where Do We Start?
- Industry Models
- Key Sources

What's the Security Landscape Today?

Impact of security breaches is growing.

Ransomware attacks are on the rise.

Passwords, passwords, passwords.

People are working from everywhere.

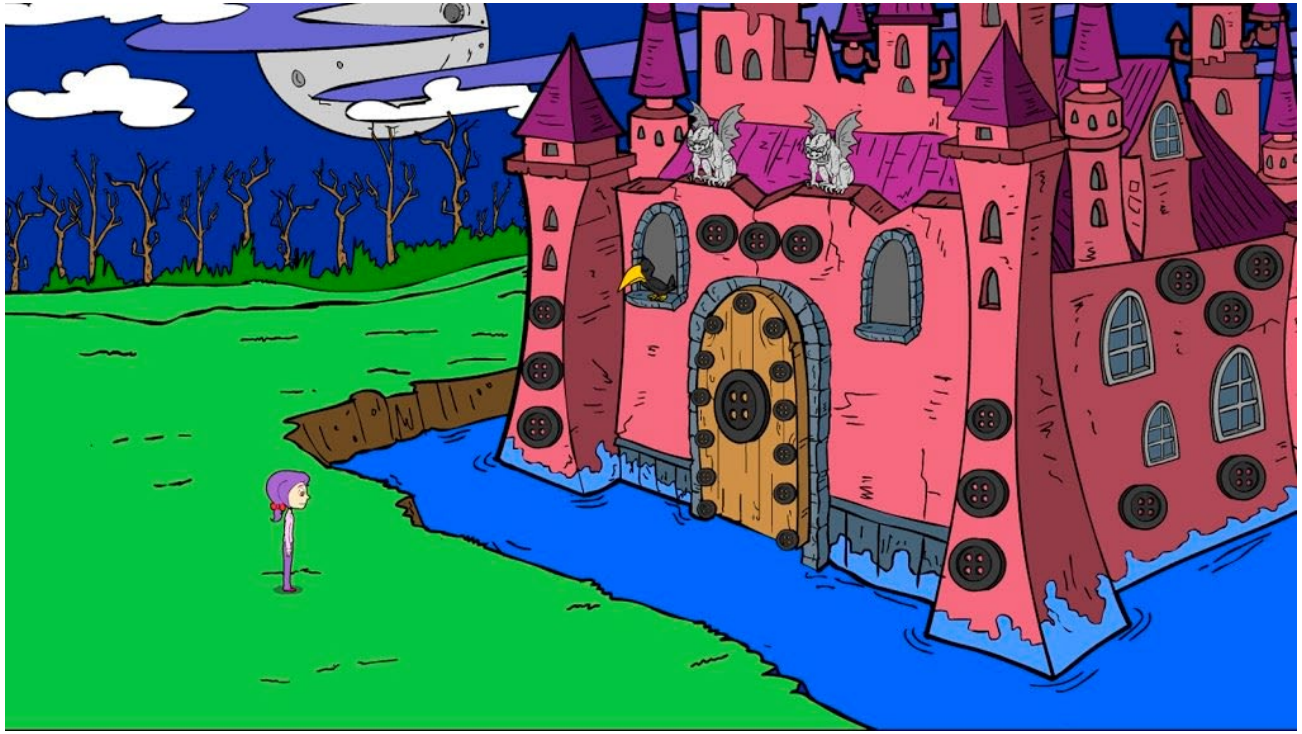
Increased reliance on devices connected to the network.

Zero Trust: A Deceptively Simple Question

Should this user on this device under this context be allowed to access this resource?

How Do We Control Access Today?

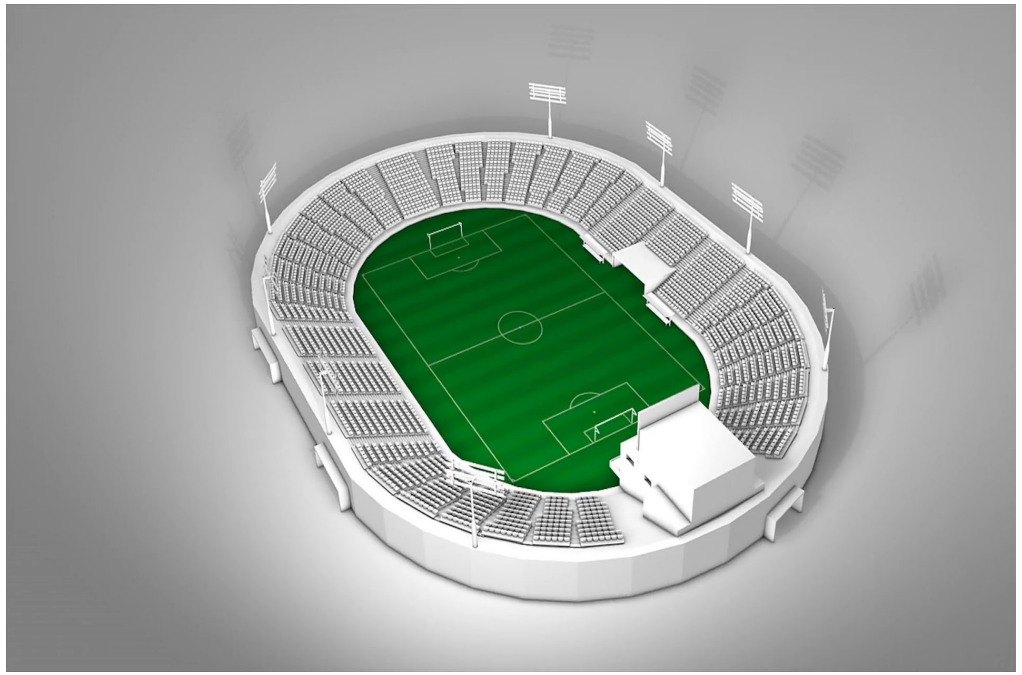
- Perimeter Style Security, or “Castle and Moat.”
- Once the user is in, they’re trusted to act and access only those areas intended to access.
- Increased threats/threat sources, more reliance on applications/cloud – we need to better address vulnerabilities.



How Does Zero Trust Treat Access Differently?

- Centered on the belief that organizations should not automatically trust anything inside or outside the perimeters:
  - The organization must verify anything and everything trying to connect to its systems before granting access.
  - Zero implicit trust, or zero inherited trust.
  - ***Appropriate amount of access at the appropriate time***.

Zero Trust approaches it more like a stadium…



Is Zero Trust a Technology?

- Think of Zero Trust as an approach, not a single solution, and it definitely isn't one size fits all:
  - Matures over time.
  - Involves many parts of the organization.

- Core Zero Trust question: Should this user on this device under this context be allowed to access this resource?
  - Policy – Who has access and when?
  - Technology – How do we verify identity?
  - Architecture – How do we use tools to keep bad actors out? How to we integrate tools?
  - Culture/Training – How do we promote better security behaviors?

Why Is Everyone Talking About Zero Trust Now?

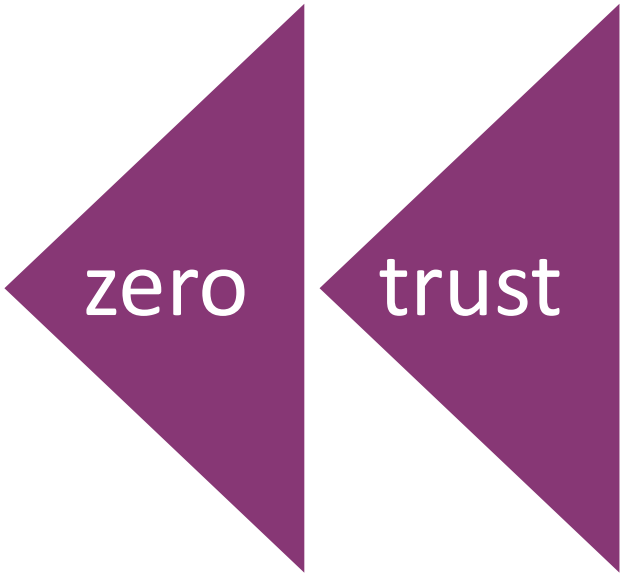
- Concept has been around since 2010.
- Increased ransomware and consumers demanding protection of their data.
- Executive Order 14028.
- M-22-09.

Should My Organization Address Zero Trust?

- Threat Cases:
  - Ransomware.
  - Supply chain attacks.
  - Insider threats.
- Organizational Considerations:
  - User experience impact considerations.
  - Industry compliance requirements (financial sector, U.S. Government Zero Trust Mandate).
  - Retaining cyber insurance or certain types of business insurance.
- Health Care and Health Organizations:
  - Huge range of assets, users, and access needs.
  - Stakes are high – medical records, Personally Identifiable Information, access issues have serious consequences.

Zero Trust Rewind – What is Zero Trust?

- It's a framework/strategy for preventing unauthorized access to data and services, coupled with access control enforcement – it isn't just a tool or a technology.
- Shift security from "castle/moat" or implicit trust to "stadium style" that only gives the **appropriate amount of access at the appropriate time**.
- Executive Order 14028 and M-22-09 define milestones for zero trust implementation in the federal space.



Challenges to Implementing Zero Trust

- Legacy systems and networks rely on “implicit trust” and modernization requires significant investment.
- No consensus on a formal adoption model, some of the adoption models available focus only on the network layer.
- Adoption requires engagement and cooperation from senior leadership, IT staff, users, etc.

Challenges to Implementing Zero Trust: The Usability Problem

- The tools and practices used to enforce the model create friction and frustration for users:
  - Clunky VPNs slow down traffic.
  - Frequent password resets drive users crazy.
  - Device management is too invasive for personal devices.

USERS ACTIVELY CIRCUMVENT SECURITY MEASURES, RESULTING IN BEHAVIORS THAT LEAVE ORGANIZATIONS UNPROTECTED.

We have to incorporate usability testing and users in Zero Trust solution design.

Where Do We Start?

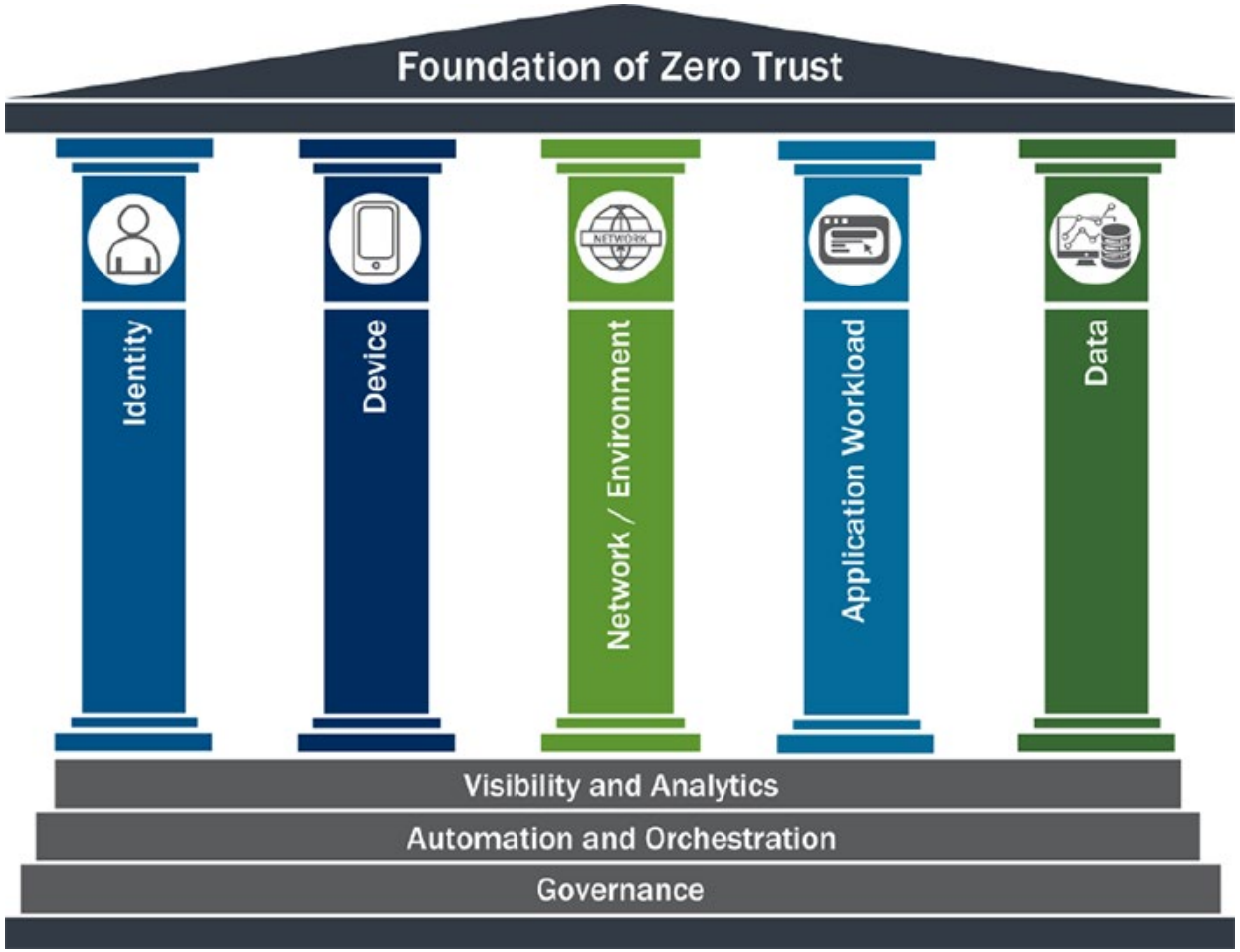
- Most organizations already have some elements of zero trust in place.
- Leverage an Agile approach, that matures over time, focusing on:
  - Discover.
  - Observe.
  - Respond.
  - Protect.
- Find an experienced partner: strategy, security, change management.
- There are models and frameworks available.

Industry Models

- Forrester
  - Originally released in 2010.
  - Re-released as Zero Trust eXtended (ZTX).
  - Data at the center of the model and includes data classification and protection as core requirements for Zero Trust.
- Gartner
  - Continuous Adaptive Risk and Trust Assessment (CARTA).
  - Puts continuous risk assessment at the center of the model as it pertains to users, devices, applications, data, workloads, etc.
- DHS Cyber and Infrastructure Security Agency (CISA)
  - Represents implementation across five distinct pillars – including Identity, Device, Network, Application Workload, and Data.

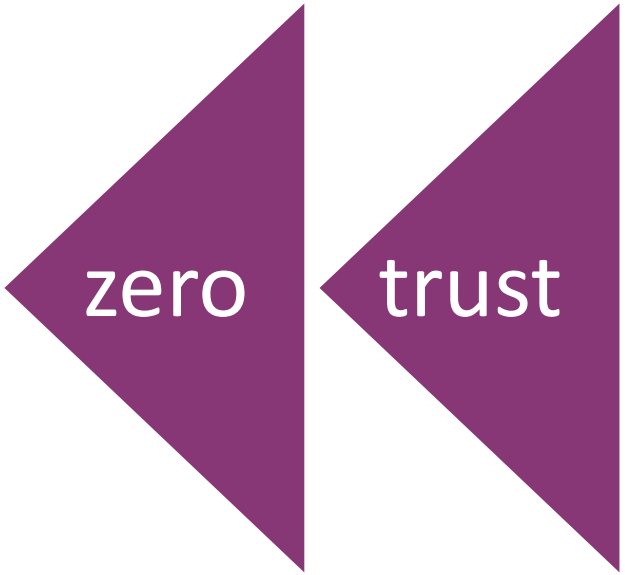
DHS CISA Zero Trust Maturity Model

- Gradient implementation across 5 pillars:
  - Minor advancements can be made over time.
  - Maturity – Traditional, Advanced, and Optimal.



Zero Trust Rewind – Implementation

- Start with where you are and what you know.
- Plan immediate changes and long-term changes that coordinate with larger IT modernization strategy.
- Take an Agile approach to maturing over time.
- Look to industry best practices and models.
- Address usability.



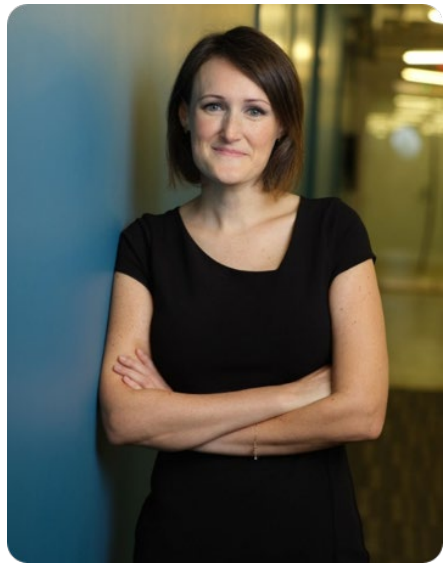
Sources

- NIST Special Publication 800-27 on Zero Trust is available at:

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- American Council for Technology and Industry Advisory Council (2019) Zero Trust Cybersecurity Current Trends. Available at: https://www.actiac.org/zero-trust-cybersecurity-current-trends
- CISA Zero Trust Maturity Model can be found at: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Need More Information?

- Tantus has supported agencies through their journey to Zero Trust, ranging from:
  - Centers for Medicare and Medicaid Services (CMS) Financial. Management Systems Group (FMSG).
  - Department of the Treasury Alcohol and Tobacco Tax and Trade Bureau (TTB).



Karlene Stecchi, EVP
Tantus Technologies
kstecchi@tantustech.com

OUR HEALTH

CCSQ WORLD USABILITY DAY

thank you!