BankDirector

Breakout 1: Demystifying Zero Trust Security

#BDAudit23

Omar Refaqat
Crowe LLP

Crowe

Zero Trust Security

A Primer for Bank Directors

June 2023

What does Zero Trust Security mean?

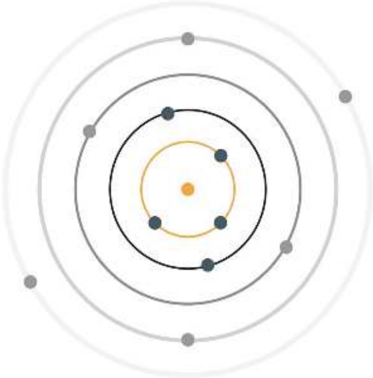
As one industry CISO puts it:

“ It means whatever the person on the other side of the table is trying to sell me. “

Let's Start with what Zero Trust is not ….

It’s **not a single Product** or a **Solution** or a **Service**

It’s **not a short-term project** that that can be quickly implemented



It’s **not a small change** in how an IT organization operates

.

It is **not a Magic Bullet!**

.

A Thought Experiment

You are the security leader of an organization, and you get a call from a reputable security researcher:

"We have found evidence that your network has been infiltrated and an attacker has established a foothold in your network….

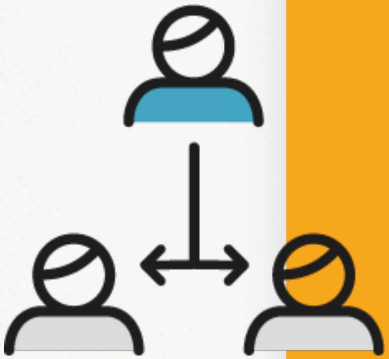
We don't know how it happened, which or how many systems, accounts, devices or users have been compromised…."

How would you react?

You would want to ensure that:

- Anyone accessing a resource are who they claim to be
- Users have access to only what they need and nothing more
- All critical information is encrypted, and keys are closely guarded
- Continuous monitoring for any unusual activity
- You are not dependent on perimeter security controls

Trust No One!



What is Zero-Trust?

It is a design philosophy

It is a security mindset

It is a technology plan

It is a journey

It is an architecture (ZTA)

What is Zero-Trust?

National Institute of Standards and Technology U.S. Department of Commerce

In August of 2020, The National Institute of Standards and Technology (NIST) published its guidelines on "Zero Trust Architecture" in Special Publication 800-207.

> " Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. "

Recent momentum...

Cybersecurity and Infrastructure Security Agency (CISA) developed a Zero Trust Maturity Model in April 2021 to assist agencies as they implement zero trust architectures

Zero Trust Architecture was introduced as a federal government requirement by May 2021 Executive Order 14028 *Improving the Nation's Cybersecurity* as necessary means *to* bolster national cybersecurity.

> "(b) Within 60 days of the date of this order, the head of each agency shall:
> (ii) develop a plan to implement Zero Trust Architecture,…"

In November 2022, the Department of Defense (DoD) Releases Zero Trust Strategy and Roadmap calling for implementation by FY27

The FFIEC has identified Zero-Trust as a key emerging technology in Architecture, Infrastructure, and Operations (AIO) booklet, which is part of the FFIEC Information Technology Examination Handbook.

Key Enabling Technologies

User & Entity Behavior Analytics (UEBA)

Solutions collect logs and alerts from all connected data sources, analyze them and build baseline behavioral profiles of organization’s entities (such as users, hosts, IP addresses, and applications) .

Using a variety of techniques UEBA solutions can then identify anomalous activity and help determine if an asset has been compromised

Advanced SIEM

Advanced monitoring to facilitate automated behavior-based decision making.

Monitoring of the entire technology footprint, and analytics that drive continuous improvement.

Encryption & PKI

Encryption of all sensitive data at rest and in transit, inside and outside the network.

A robust Public-Key Infrastructure (or an alternative) to authenticate and maintain integrity of all communications

Dynamic Access Controls

Access technologies that can dynamically determine authorization and authentication based on behavior modeling, trust profiles, anomaly diagnosis and threat modeling.

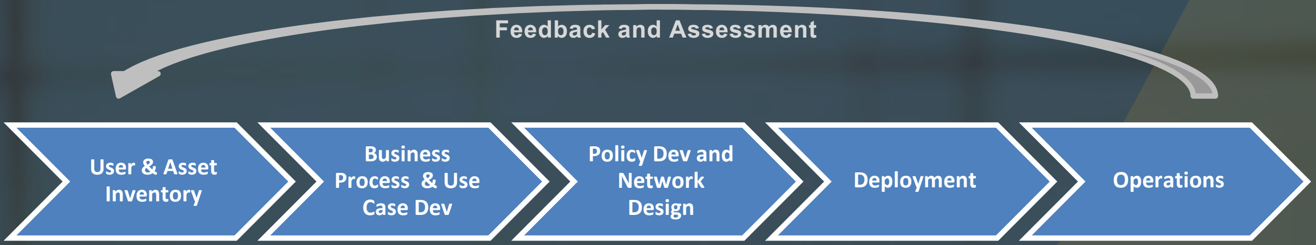
Micro-segmentation

Placing individual or groups of resources on a unique network segment protected by a gateway security device such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices.

The gateway security devices can react and reconfigure as needed to respond to threats or changes in the workflow

Adopting ZTA…

Migrating to ZTA requires an organization to have detailed knowledge of its assets (physical and virtual), subjects (including user privileges), and business processes.



Define the area to protect based on data, applications, assets and services.

Essential to have clear view of users, assets, data flows and workflows

Identify and map the business processes, data flows, and their relation in the missions of the org.

Start with a low-risk business process for the first transition to ZTA

Build policies for the network and identity access based on ZT principles.

Design a ZTA around the network area or systems to protect.

Identify solutions suitable to implement the tenets of ZT

Deploy Access management solutions following least privilege principles.

Deploy micro-segmentation technologies.

Establish public key and encryption infrastructure

Start operations in report-only mode to ensure effectiveness and minimize business disruptions.

1

1

Use this data to build behavior baselines and trust profiles.

Use SIM data for continuous monitoring and improvement

Takeaways

- Recognize that Zero Trust is not a single solution or technology.
- Understand where your organization is in their journey towards ZTA.
- Challenge management to provide a roadmap that is logical, realistic and well-planned.
- Recognize the foundational technologies that make up ZTA.
- Recognize that most organizations will not be able to roll out zero-trust at once across their entire technology estate.

As Directors we should acknowledge and encourage progress even if it is fragmented, iterative and occurring in segments

Thank you!

Crowe

Omar Refaqat, CISSP
Managing Director
omar.refaqat@crowe.com
+1 (312) 632-6951