ZERO TRUST Architecture

Developed By **Karen Y. Baez**

OBJECTIVE

The objective of this presentation is to:

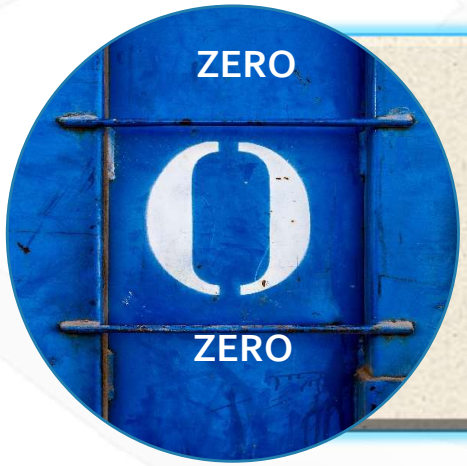
1) Understand the term known as ZERO Trust.
2) Understand how it applies to the Enterprise Architecture Strategy.
3) Understand the process required to determine the best approach to execute the process.

SCOPE

The scope of this presentation applies to, but is not limited to, the following:

1) Personnel Responsible for developing the organizations Enterprise Level Architecture.
2) Personnel Responsible for implementing Security Engineering Principles.
3) Personnel Responsible for managing the organization PERIMETER level systems.

WHAT IS ZERO TRUST



Zero Trust is a framework that can be leverage to optimize the security architectures and technologies for future flexibility

It enforces security engineering principles from an Enterprise Architecture perspective by emphasizing the importance of segmentation, packet filtering, access control, audit and monitoring and central management of systems within the organization's perimeter.

NOTE: The description of ZERO Trust has been slightly modified to incorporate our perspective of what the framework should factor in outside of PERIMETER level securtiy.

HOW LONG HAS THE CONCEPT OF ZERO TRUST BEING AROUND

16 YEARS

John Kindervag

The Defense Information Systems Agency (DISA) and the Department of Defense published their work on a more secure enterprise strategy dubbed "black core" [BCORE]. Black core involved moving from a perimeter-based security model to one that focused on the security of individual transactions. The work of the Jericho Forum in **2004** publicized the idea of de-perimeterization—limiting implicit trust based on network location and the limitations of relying on single, static defenses over a large network segment [JERICHO].

The concepts of de-perimeterization evolved and improved into the larger concept of zero trust, which was later coined by *John Kindervag* while at Forrester.

Zero trust then became the term used to describe various cybersecurity solutions that moved security away from implied trust based on network location and instead focused on evaluating trust on a per-transaction basis.

WHAT AREAS ARE IMPACTED BY ZERO TRUST

- Network Architecture
- Network Infrastructure
- Systems Security Engineering

NETWORK PERIMETER COMPONENTS

- Switches
- Firewalls
- Routers
- Wireless Gateways
- Virtual Private Network (VPN) Gateway
- Intrusion Detection Systems (IDS)
- Intrusion Prevention System (IPS)
- Web Application Firewall (WAF)
- Network Access Control (NAC)

WHAT IS ZERO TRUST MAIN FOCUS

The main focus is…

- Switches and Firewalls
- Packet Filtering And Distribution
- Perimeter Management

WHAT IS THE ULTIMATE GOAL

The ultimate GOAL is to enforce a SEGMENTED NETWORK Architecture.

Adopting a Zero Trust architecture provides business resonance, defines the business use of segmentation, and provides a methodology for building a segmented network.

Enforcement takes place within the following Open Systems Interconnection (OSI) Layers:

Layer 7 Application	Supports Communication of applications within networks through Application Layer Management, Application Services and Processes, HTTP(S), POP_3, FTP, DNS
Layer 2 Data Link	Assigns the appropriate address to the data packets. Physical Addressing (MAC & LLC), Packet Transmission, Switches, WAP, Ethernet Communication

ZERO TRUST Architecture

Overview of key items

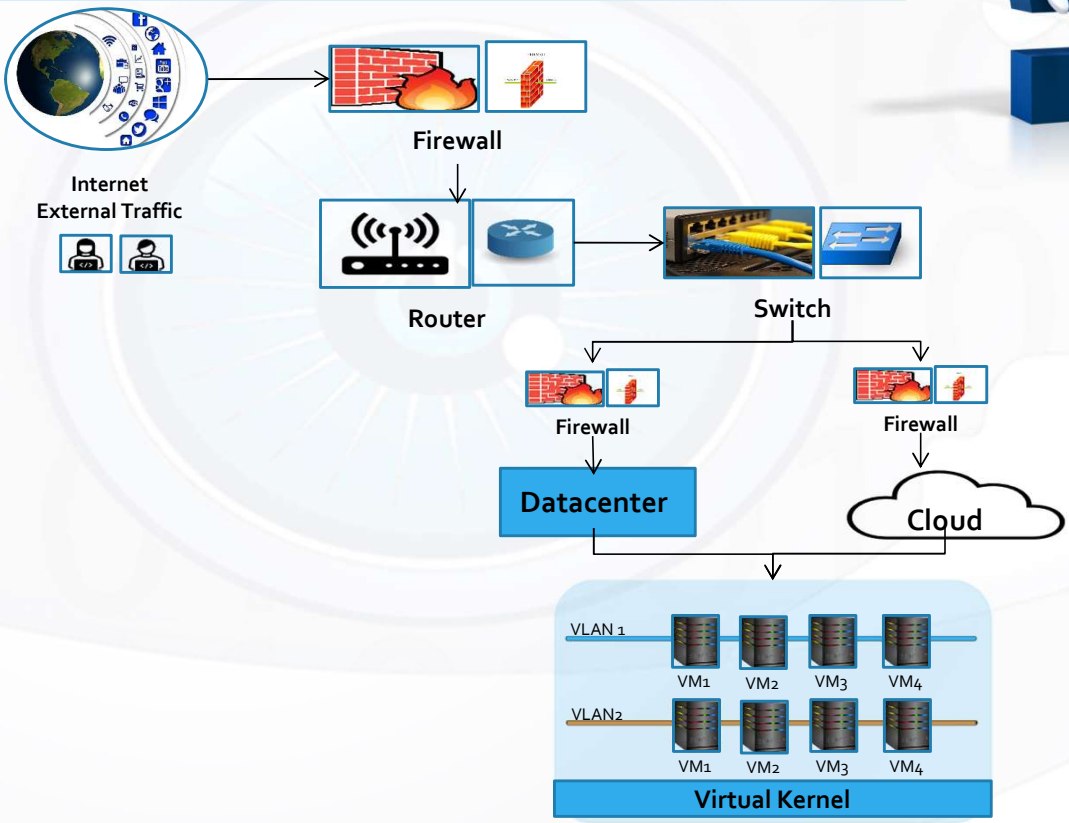
WHAT ARE THE KEY ARCHITECTURE AREAS IMPACTED

Network Segmentation	Physical Level Segmentation of Environments to reinforce logical segmentation strategies.
Data Parallelization	Limiting packets being process by Switches per CORE by leveraging re-distribution techniques to other systems for processing, such as the workstations OS.
Centralized Management	The organization leverages central management tools for network devices .

WHAT IS NETWORK SEGMENTATION

Network segmentation is the process of dividing a network into smaller sections. These sections are created by placing barriers between parts of the system that don't need to interact.

Once you segment a network, every subnet functions as an independent system with unique access and security controls. Such network design allows you to control the flow of data traffic between sections. You can stop all traffic in one segment from reaching another.



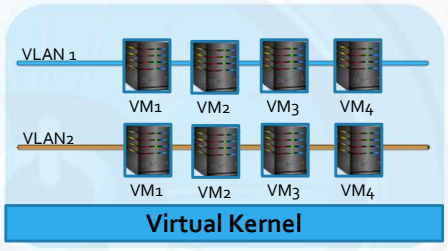
TYPES OF SEGMENTATION

A Network can be segmented in two ways…

Firewall

Router

Switch



	1 > PHYSICAL	2 > VIRTUAL LAN
PROS	• Each subnet requires a physical switch, physical wiring, and its own firewall. • It provides maximum security between environments.	• Each environment is separated by a VLAN and each VLAN has a firewall. • Affordable and easier to implement.
CONS	• Can be complex to implement. • More expensive to implement and maintain.	• VLAN Hopping Risk • Less secured than physical segmentation.

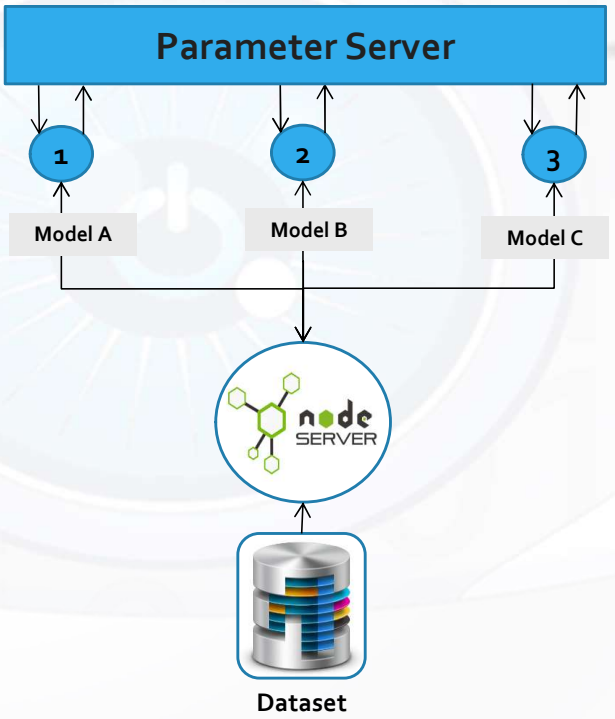
NOTE: A mix of both strategies is highly recommended.

WHAT IS DATA PARALLELIZATION

Data Parallelization focuses on the flow and the structure of the information transmitted or process by a system. The key for data parallelization involves partitioning data equally among several processing nodes.

A node is a self-contained computer comprised of compute cores, primary memory, and secondary storage. The nodes communicate and coordinate their actions to achieve a common goal through mechanisms such as *shared memory* and *message passing*.

A processing node then processes each individual data type independently in parallel. This approach is suitable when processing large levels of data.



WHAT IS CENTRALIZED MANAGEMENT

When it comes to Centralized Management, ZERO Trust focuses in two key areas:

- Perimeter Components
- Application Nodes/Firewall

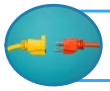
When this areas are centrally managed, the organization can…

- Manage Incoming / Outgoing Traffic
- Validate End-Users Accessing the LAN
- Enforce Data Protection
- Granular/Consistent Technical Policies
- Manage Real-time Monitoring
- Enforce Access Controls

This puzzle piece is essential when we enter ***Tier 2: Business Processes*** which focuses on the Enterprise Level Architecture.

WHAT ARE THE KEY COMPONENTS OF ZERO TRUST

"microcore and perimeter" (MCAP)



Microcores

Tools that support "Network Segmentation Gateways" and are abled to handle high-speed, support multiple 10 Gig interfaces, and can provide Quality of Service (QoS) or packet shaping to maintain performance.

Perimeters

Understanding the environments and/or data that must be protected by Limiting packets process by Switches per CORE by leveraging re-distribution techniques to other systems for processing, such as the workstations OS.

MICROCORE AND PERIMETER (MCAP) OVERVIEW

- Each of the switching zones attached to an interface is called a "microcore and perimeter" (MCAP).
- Each segmented zone is its own microcore switch, and you can consider each zone as a micro-perimeter because all the resources within a specific microcore share similar functionality and global policy attributes.
- All MCAPs can be centrally manage by aggregating all the switches within all the MCAPs into a unified switching fabric.
- All traffic to and from each MCAP must be inspected and logged.

Key Security Controls from NIST SP 800-53

Overview of key items

WHAT CONTROL FAMILIES ARE ADDRESSED BY ZERO TRUST

System and Services Acquisition (SA)

Planning (PL)

Access Control (AC)

Identification and Authentication (IA)

System and Communications Protection (SC)

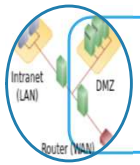
Audit and Accountability (AU)

Configuration Management (CM)

System and Information Integrity (SI)

WHAT MUST THE ORGANIZATION HAVE IN PLACE

For a successful security assessment to take place, the organization must have the following in place:



Network Diagram(s)

List of Perimeter Security Tools

Mission Critical Systems

Data Flow Diagram

Network Architecture Plan

Engineering Principles

Complete Asset Inventory

Existing Audit Results

Policies and Procedures

WHAT SHOULD THE ORGANIZATION KNOW AHEAD OF TIME

There's two key questions that the organization MUST be abled to answer, and they are:

1. **WHY and HOW are you segmenting the network?**
2. **WHAT type of DATA and Assets are you trying to protect?**

Understanding the answers to the two key questions above will help us determine how to best help you achieve ZERO Trust methodologies. In addition, the organization must have a clear understanding of…

- **The Network(s) current state.**
- **List of Tools currently in place and the capabilities offered by each.**
- **Requirements needed to achieve the desired Network state, as it pertains to monitoring and managing the network traffic and flow.**

DOES ZERO TRUST IMPLEMENTATION REQUIRE EXPENSIVE TOOLS

ZERO Trust isn't about buying a shiny tool that claims to secure your network; however, if the organization doesn't have key perimeter tools in place, it might. In fact, 90% of the time, companies already have the necessary technology in place to enforce Zero Trust methodologies.

The key is to understand the structure of the organization and the capabilities of the tools already in place. Certainly, some tools may be required; however, the focus isn't on buying new tools, but rather determining what's already in place and how such can be re-engineered to apply the ZERO Trust framework.

CAN ZERO TRUST ADDRESS OTHER AREAS OUTSIDE THE PERIMETER

ZERO Trust methodologies can be expanded into other areas outside of the perimeter and can incorporate different data parallelization mechanisms outside of those noted in this presentation.

However, for the purpose of this presentation, we only address those areas tied to the original ideology.

CAN ZERO TRUST IMPLEMENTATION FUNCTION ALONE

ZERO Trust is simply another piece of the puzzle and it requires other pieces to properly protect the organization assets. Organizations who are serious about securing their environment must understand that multiple frameworks are necessary. This frameworks include, but are not limited to:

1- Risk Management Framework (ideally NIST)
2- Cybersecurity Framework (NIST)

And any other framework impacting the organization based on the sectors targeted.

HOW CAN CYBERADEPTNESS HELP

CyberAdeptness incorporates a review of ZERO Trust methodologies as part of its Enterprise Level Security Assessment addressing NIST Risk Management Framework Tier 2 - which specifically addresses the organizations Network Architecture.

As part of the assessment, we review perimeter level components to determine if the organization enforces any of the methodologies noted within the ZERO Trust framework and provide recommendations as deemed necessary on how to improve existing settings and/or incorporate changes to enforce ZERO Trust.

However, we do not get involved in the deployment methodology process. We leave that to the organization and its internal resources to address.

IS ZERO TRUST SUFFICIENT TO PREVENT CYBER ATTACKS

Perimeter Security has been around for decades and while it can help limit cyber attacks- is not enough, but it is a good starting point. For an organization to truly secure the environment, they need to address all other areas within the various Open Systems Interconnection (OSI) Layers and that can only happen when Security Engineering Principles are applied across the network and within each individual OSI layer.

Send them to
info@cyberadeptness.com

Need Help?

We have over 20+ years of combined experience in the field and a unique process to streamline the requirements.

Contact us today to schedule a meeting and determine how we may be of help to your organization. Our processes are flexible to accommodate compliance needs, regardless of sector (i.e., Healthcare, Finance, Law, Education, etc.).

References

- **Parallel Computing >** https://www.sciencedirect.com/topics/computer-science/parallelization
- **Build Security Into Your Network's DNA: The Zero Trust Network Architecture >** http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf
- **You Want Network Segmentation, But You Need Zero Trust >** https://www.paloaltonetworks.com/blog/2019/01/you-want-network-segmentation-but-you-need-zero-trust/
- **Network Segmentation: Concepts and Practices >** https://insights.sei.cmu.edu/blog/network-segmentation-concepts-and-practices/
- **High-Performance Business Intelligence >** https://www.sciencedirect.com/topics/computer-science/model-parallelism