Zero Trust & Data Protection in a Borderless World

Joseph Davis
Chief Security Advisor

Microsoft
What are we trying to Achieve?

- Prevent User Impersonation (leveraged for Unauthorized Access)
- Prevent Unintended or Unauthorized access to Resources and Data and Enforce Data Confidentiality, Integrity, and Availability (CIA)
- Ensure Data Privacy as a Human Right
- If Data is misappropriated, be able to ‘LoJack®’ the Data
What are Bad Actors After?
Answer: Data

- BREACH CONFIDENTIALITY
- ALTER INTEGRITY
- EFFECT AVAILABILITY
The Traditional Enterprise Perimeter – Can you Trust it?

Encryption is the last bastion of protection.

Can you be sure a personal device accessing sensitive data is ‘secure’?

Are you providing users with a Consistent Experience?

Are you ‘assuming compromise’ of your on-premises network?

Bad actors may be Outsiders or Insiders

Can you be sure that an identity has not been compromised and is not being impersonated?

Can you limit access to data and resources both on-premises and in the Cloud?
Therefore are we having a Zero Trust conversation

**Access Control:** Keep **Assets** away from **Attackers**

1. **IT Security is Complex**
   - Many Devices, Users, & Connections

2. “**Trusted network**” security strategy
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within network

3. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed

4. **Assets increasingly leave network**
   - Bring Your Own Device, Work From Home, Mobile, and Software as a Service.

In a Zero Trust model, users and devices, both inside and outside the corporate network, are deemed untrustworthy. Access is granted based on a dynamic evaluation of the risk associated with each request.
This “Zero Trust” idea has been evolving for a while

- 2004: Jericho Forum Formally Established
- ~2004: Network Access Control (NAC) Architectures
- 2010: Forrester coins “Zero Trust” Term
- 2014: Microsoft Advocates “Assume Breach”
- 2016: Microsoft Conditional Access Released
- 2017: Zero Trust Networks

Slow mainstream adoption for both network identity models:

- Network – Expensive and challenging to implement
  Google’s BeyondCorp success is rarely replicated
- Identity – Natural resistance to big changes
  Security has a deep history/affinity with networking
Zero Trust Access Control Strategy

Never Trust. Always verify.

Signal

to make an informed decision

Device Risk
• Device Management
• Threat Detection
• and more...

User Risk
• Multi-factor Authentication
• Behavior Analytics
• and more...

Decision

based on organization’s policy

1. Apply to inbound requests
2. Re-evaluate during session

Enforcement

of policy across resources

Modern Applications
SaaS Applications
Legacy Applications
Data and Information
Zero Trust and Access to Data

- Leverage Artificial Intelligence to determine Data Classification and Context
- Classification can be used as a Signal in every transaction
- Protect Data WHEREVER it exists in a perimeter-less world
- Tag and Track Data Revoke Access (Kill Switch)
Recommended Zero Trust Priorities
Do the most important stuff first

1. **Align segmentation strategy & teams** by unifying network, identity, & app segmentation into a single strategy (as you migrate to Azure)

2. **Build identity-based perimeter** to protect modern and legacy enterprise assets

3. **Refine network perimeter** using microsegmentation (if required for residual risk)
Learning: Zero Trust is a long-term strategy

Closely related to other initiatives

- **Zero Trust Access Control**
  Establish Identity Perimeter with Conditional Access to Resources

- **Security Operations Center Modernization**
  Shift Tooling and Processes to Endpoint, Identity, and Application Layers

- **Secure Administration**
  Infrastructure/Datacenter access for admins

- **Network Transformation**
  Internet-only clients / Firewalls for Datacenters only
  Evaluate Microsegmentation

- **Resource Modernization**
  Enable ZT Access to Legacy Apps
email: josdavi@microsoft.com

LinkedIn: https://linkedin.com/in/josephdavis

Twitter: @securityjwd

Medium: https://medium.com/@securityjwd