Digital Transformation is to Business what Zero Trust is to a Security!
Agenda

- What it IS and What is NOT?
- Past & Present
- Value, Benefits and Pillars of Zero Trust
- Where to start?
Charlie CISO

We've implemented zero trust.

I don't believe you.

Exactly.
Definition

"Forrester Research defines the Zero Trust Model as "a conceptual and architectural model for how security teams should redesign networks into secure micro perimeters, strengthen data security using obfuscation techniques, limit the risks associated with excessive user privileges and access, and dramatically improve security detection and response with analytics and automation."

Zero Trust’s main purpose is **Removal of Implicit Trust**

Zero Trust focuses on **DATA** centric and **RISK** based **ACCESS** approach
Zero Trust is **NOT**

- a quick win
- an “Off-the-shelf” product
- a one-off or IT only project
- a play for only identity or network vendors
- an idea where trust is removed completely

Zero Trust is

- requiring a programmatic approach
- a combination of process & technology
- helping with reduction of complexity
- application, identity and data focused
- contextual and dynamic in nature
Zero trust started out as a networking concept with a specific perimeter in mind.
Controlled Access Design (Everything back hauled)
Direct to Internet
Mobilization of the Workforce

User, Group, OU

Pat From Accounting

On Any Device
- On Her Cell Phone
- On Her Tablet
- On Her Laptop
(Managed or Unmanaged)

From Any Location
- At the Office
- At Home
- At the Cafe

To Any Application

Share Any Information
- Financials
- Ideas
- Pictures

Content / Classification
• Connectivity is ubiquitous

• Exponential growth of Cloud and Mobility

• Users demand instant access to applications and data
Disruption
New strategies and thinking

Growth
Transformation fuels growth

Consumerization
The workplace is no longer where people work.
Digital Business Opportunities

Digital Business Strategy

Digital Business Optimization
- Sell More
- Reduce Costs
- Digitalize Workforce
- Optimize Client Experience
- Improve Efficiency
- New Digital Services, Products
- Autonomous Buying and Selling
- Seamless Partner Network Integration
- Create an Ecosystem

Digital Business Transformation

Existing Business Model

New Business Model(s)

New Privacy and Security Model(s)
Zero Trust is a profound cultural transformation that impacts all business and organizational activities.

Digital Transformation is to business what Zero Trust is to a Security!
Value, Benefits & Pillars
Building a Security program based on Zero Trust will drastically decrease an organization’s risk exposure.
Benefits

<table>
<thead>
<tr>
<th>Prevention of lateral movement</th>
<th>Predefined application/resource access governance</th>
<th>Provides strong authentication, conditional/least privileged access</th>
<th>Gain full visibility and control within your ecosystem (On-premises and Cloud)</th>
<th>Enables the ability for risk-based access decisions at scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protects your customer’s data</td>
<td>Minimizes loss of organizations intellectual property</td>
<td>Helps compliance audit initiatives</td>
<td>Supports the transition to the cloud</td>
<td>Aids in Security program transformation</td>
</tr>
</tbody>
</table>
Pillars

- Identity Attestation
- Endpoint Interrogation
- Application Verification
- Data Access Validation
- Contextual Access Policy
- Monitoring

- Directory structure
- Federation
- MFA & PAM
- State of an endpoint
- Criteria satisfaction
- User to endpoint mapping
- Standard or NOT
- Application mapping
- Role assignment
- Classification
- Inspection & data flow
- Access relationship & patterns
- Risk score
- Adaptive enforcement
- Session isolation
- Detection
- Prevention
- Reporting
<table>
<thead>
<tr>
<th>Trust</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Activity</td>
<td>Non-Sensitive Data (Read Only)</td>
<td>Non-Sensitive Data (Read &amp; Write)</td>
<td>Limited Sensitive Data (Read)</td>
<td>Sensitive Data (Read &amp; Write)</td>
<td>Sensitive Data (Read &amp; Write &amp; Store on Device)</td>
</tr>
<tr>
<td>Identity</td>
<td>Limited Access Validation</td>
<td>Multifactor Authentication</td>
<td>Multifactor Authentication</td>
<td>Multifactor Authentication</td>
<td>Multifactor Authentication</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Unmanaged Device</td>
<td>Unmanaged Device</td>
<td>Unmanaged Device</td>
<td>Unmanaged Device</td>
<td>Managed Device</td>
</tr>
<tr>
<td>Application</td>
<td>Unsanctioned App</td>
<td>Unsanctioned App</td>
<td>Sanctioned App</td>
<td>Sanctioned App</td>
<td>Sanctioned App</td>
</tr>
</tbody>
</table>

| Example         | Social Media                        | Google Drive, Box, Office365         | Confidential Reports                | Email                               | HR Data, Board Materials, Large Database |

Trust is a Continuum
Where to Start with Zero Trust
<table>
<thead>
<tr>
<th>What to Consider Before Implementing Zero Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must architect with your business in mind first (business outcome)</td>
</tr>
<tr>
<td>Understand your current process and deficiencies</td>
</tr>
<tr>
<td>Understand your threats and risk</td>
</tr>
<tr>
<td>Understand your technology stack</td>
</tr>
<tr>
<td>Map required capabilities, data and transaction flows</td>
</tr>
<tr>
<td>Understand your end user requirements (transparency, easy of use, availability)</td>
</tr>
</tbody>
</table>
Implementing Zero Trust

- Document your model, architectural principles, patterns, and standards (Holistic Modular Architecture)
- Start with idea of equalizing internet and intranet
- Simplify your operating environment (remove redundancy)
- Design, build, test, deploy rather than deploy and hope you got it right and integration exists

Think BIG and Start Small
Re-Architect & Simplify

Focus is on minimizing damage

Focus is on minimizing vulnerability and potential for harm

Control Approaches

Shift Down and Left

Source: Managing Risk and Information Security 2nd edition Malcolm Harkins
Security stack pillars

IDENTITY

Authentication & SSO

Identity

Web
SaaS
IaaS/PaaS
DC & Private Access

Secure Access

Response Actions

User & Entity Data

Threat Intel Exchange

ENDPOINT

Response Actions

UEBA & SOAR

AppSec
Secure Access
Identity
Endpoint
Questions
EVOLUTION OF INFORMATION SECURITY TECHNOLOGY

- **High**
  - **Data** (increasing)
  - **Host** (decreasing)
  - **Network** (increasing)

- **Medium**
  - **Data** (decreasing)
  - **Host** (increasing)
  - **Network** (decreasing)

- **Low**
  - **Data** (low)
  - **Host** (low)
  - **Network** (low)

**Time Frames**
- **Historical**
- **Near-term**
- **Mid-term**
- **Long-term**