BUILDING A ZERO TRUST ARCHITECTURE

Natalio Pincever
Sr. Director, Product Management Federal Gov

Geoffrey Carlisle
Solution Architect, Product Management Federal Gov
TRUST IS A DANGEROUS VULNERABILITY THAT IS EXPLOITED BY MALICIOUS ACTORS
Zero Trust is a security model that prevents breaches by eliminating assumed trust in the digital world and instead consistently verifies all traffic from all users, devices, and applications at all locations.
A Zero Trust Strategy Reduces Attack Opportunities

**Problem**
Broken trust model exploited by hackers

**Action**
Build a zero trust network

**Benefit**
Helps stop data breaches
1. Who the President is...
2. Where the President is...
3. Who should have access to the President...
5-Steps to Deploying Zero Trust
5 Steps to Deploying Zero Trust

1. Define your Protect Surface
   - Next-Generation Firewall
   - Cortex™ Data Lake
   - Cortex™ XDR
   - Transformation Services

2. Map the transaction flows
   - Next-Generation Firewall
   - Cortex™ Data Lake
   - Cortex™ XDR
   - Traps
   - Transformation Services

3. Build a Zero Trust architecture
   - Next-Generation Firewall
   - Cortex™ Data Lake
   - Cortex™ XDR
   - Traps
   - GlobalProtect
   - Prisma Access
   - Transformation Services

4. Create Zero Trust Policy
   - Panorama
   - WildFire
   - Threat Prevention
   - URL Filtering
   - Prisma SaaS
   - Transformation Services

5. Monitor and maintain the network
   - Cortex™ Data Lake
   - Cortex™ XDR
   - AutoFocus
   - MineMeld
   - Demisto
   - PrismaCloud
   - Transformation Services
Legacy Rules are Complex to Manage
Create a Zero Trust Policy: The Kipling Method

Zero Trust policies must address *who, what, when, where, and how?*

<table>
<thead>
<tr>
<th>Who</th>
<th>What</th>
<th>When</th>
<th>Where</th>
<th>Why</th>
<th>How</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>App ID</td>
<td>Time</td>
<td>System Object</td>
<td>Classification</td>
<td>Content ID</td>
<td></td>
</tr>
<tr>
<td>Sales</td>
<td>Salesforce</td>
<td>Working Hours</td>
<td>US</td>
<td>Toxic</td>
<td>SFDC_CID</td>
<td>Allow</td>
</tr>
<tr>
<td>Epic_Users</td>
<td>Epic</td>
<td>Any</td>
<td>Epic_Svr</td>
<td>Toxic</td>
<td>Epic_CID</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Use Cases
Zero Trust for Mobile Workers

- Extending policy to devices attempting to access the protect surface
- Preventing employees or their devices from compromise by known and unknown threats
Zero Trust in A Multi-Cloud Environment

- Protect Workloads where ever they go (across north-south, east-west traffic)
- Multi-layered segmentation reduces opportunities of attack
- Block and quickly respond to advanced threats across network, devices & clouds
Zero Trust for Enterprise with Satellite Facilities

- Policy enforcement across users and devices accessing protect surface
- Prevent threats across branch, campus, datacenter and cloud
Customer Use Case
Customer Use Case

Overview:
• Due to the sensitive nature of their work the customer decided to look into a zero trust architecture for networking.

Customer Requirements:
• Complete visibility of ALL traffic from the inside out.
• Strict policy enforcement and continuous monitoring for attacks and abuse in isolated environments.

Customer Strategy:
• Control and monitor east west traffic within the data centers and between network locations.
• Control east west traffic between workstations on the same LAN segment (micro-segmentation).

Customer Architecture:
• 140 segmentation gateways across two networks with multiple instances of Panorama and Demisto (automation platform).
• Ability to deploy automated policies at scale and speed in an automated fashion.
Thank You

paloaltonetworks.com
npincever@paloaltonetworks.com
gcarlisle@paloaltonetworks.com
Twitter: @PaloAltoNtwks