Introduction

Some Key Terms
- Endpoint
- Anti-Virus (AV)
  - Malware (Mal)
  - Fingerprint
  - Hash; password/other
- Firewall
  - Traffic gateway
  - Packet inspection
- IDS/IPS - Intrusion Detection & Prevention Systems
- AI - Artificial Intelligence; BA - Behavior Analytics;
  - ML - Machine Learning; DL - Deep Learning
- MCA - Mission Critical Assets
- Threat Intelligence
- Penetration Testing - PenTest
- Active Defense
  - Active vs passive activity on your network
  - Honeypots
  - NET hardback
  - Attack Surface Baseline
- Cyber Hygiene
- Phishing
- Social Engineering
The Solutions

1. **Data/Mission Critical Assets**
   - Encryption, Access Management, Tags, DLP, Policy

2. **Application**
   - Access Management, Monitoring, Multi Factor Authentication, VMs

3. **Endpoints**
   - Local Firewall, IDS/IPS, Patch Management, ML, AI, BA, DLP, Asset Tracking, AV

4. **Network**
   - AI Suite (ML, DL, BA), IDS/IPS, Segmentation, Active Defense

5. **Perimeter**
   - AI, Firewalls, IDS/IPS, Honeypots, DLP, Tags, Basic Surface

6. **Outside Threat**

---

**What Can I Do?**

- Understand and question policies - then follow them.
- Hyper vigilant - on the home front as well.
- Educate friends, family and colleagues.
- Social media - just know.
- Over 90% of breaches come from phishing and/or social engineering.

---

**Why Should I Care?**

- Company asset protection
- National security asset protection
- National security defense
- Personal and family defense