LeastTrust IT

# Cybersecurity: AI readiness

Maturing from perimeter defense to data-centric security

# Evolving Cyber Strategy

1990s

## Antivirus

“Passwords”

2000s

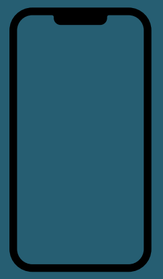
## Network Security

“Defend the Perimeter”

2010s

## Zero Trust

“Identity is the New Perimeter”



2020s

## Data Reference

“All data is non-relational”

# Perimeter Defense Basics (Past)

- Traditional "Castle and Moat" approach
- Focused on defending the perimeter
- Firewalls as primary defense
- Clear network boundaries

Why It's No Longer Enough:

- Cloud services
- Remote work
- Distributed systems
- **Treats all data the same inside the walls**

# Identity-Centric Security (Present)

Zero Trust Architecture

- "Never trust, always verify"
- Identity as the new perimeter
- Continuous verification

Key Components:

- Multi-factor authentication
- Least privilege access
- Microsegmentation
- Identity verification at every step
- **Data is governed by access (file, folder, or SQL field)**

# Data Centric (Future)

- Data as the Control Point
- Context, Classification and Governance
- Sensitive, Proprietary, Privacy, Public
- Data lineage tracking and logging

Focus Areas:

- Data discovery & Tagging
- Continuous Context & Classification
- 1-2 years out : AI Driven rule creation & alerting
- **Data is governed by context (unstructured search and inference)**

# Future Cybersecurity: Data tagging and context drives access

How prepared are you for this shift?

## AI accelerates data search, inference, and utilization

In the past, unstructured data would be very difficult to find (“security by obsecurity”) - AI skips the data structuring necessity

## How can we fuel AI yet assure optimal contextual access?

Classify and tag all data with essential tags including:
Privacy (easy), Sensitive (medium), Proprietary (difficult)

Privacy (Social Security 000-00-0000 - Regex)
Sensitive (CUI,  manual procedures)
Proprietary (Trade Secrets, abritrary tags)
Public - all other data

# Inference cannot be underestimated

S.E.C. Mosiac Theory: Data classified as non material, non public can infer material, non public information.

# Step 1

Dont retire historical defenses. They are considered necessary cyber hygeine and will continue to deter attacks and data leaks. They also provide telemetry and logging that complements and enriches data tracking (access logs, EDR and network data)

- Specific governance that will become more critical
    - Access tracking
    - Usage monitoring
    - Retention policies
    - Audit trails

# Step 2

Set a goal to classify as much data as economically viable. Start with regex based privacy data, then move to sensitive and proprietary

1. Saas can automate privacy data tagging: *Microsoft Purview, Varonis, Netrix, Cavelo*
2. Non-repetitive patterns or sensitive data like CUI or Intellectual property require human tagging, policies and procedures to classisfy watermark and secure.

Secure your valuable information

# Step 2 Cont.

Develop and educate corporate culture that recognizes and self classifies data. Test, measure, audit, iterate for improvement over time.

Carrots and sticks to drive intended behavior

# Step 3

Eventually manual tagging logs can be utilized for supervised learning and model training that will offload and assist the task. Context, edits, and tracking history are a valuable dataset to machine learning

## **Key TakeAways & Tasks**:

Granular data tagging, context, and classification are necessary to effectively govern in the AI age.

- Start regex automated classification with Saas
- Initiate procedures, policies, and incentives for manual classifications
- Mandate corporate training for current and onboarding employees.
- Measure, audit, and track classifications progress
- Initiate supervised machine learning for tagging