Nathan Underwood

Christian. Husband. Father. Aspiring hacker. Martial Arts nerd. Amateur radio guy. Perpetual n00b.

Nathan's fascination with technology started as a hobby in the1980's and evolved into a career. In the years since, Nathan has served in a number of roles from helpdesk to SysAdmin to IT Directory.

Nathan co-founded Cyber Tech Café in 2002 to provide IT Support Services to the SMB market and later co-founded Piratica in 2014 to focus on IT Security.

MACTECH PRO EVENTS

Zero Trust Networking

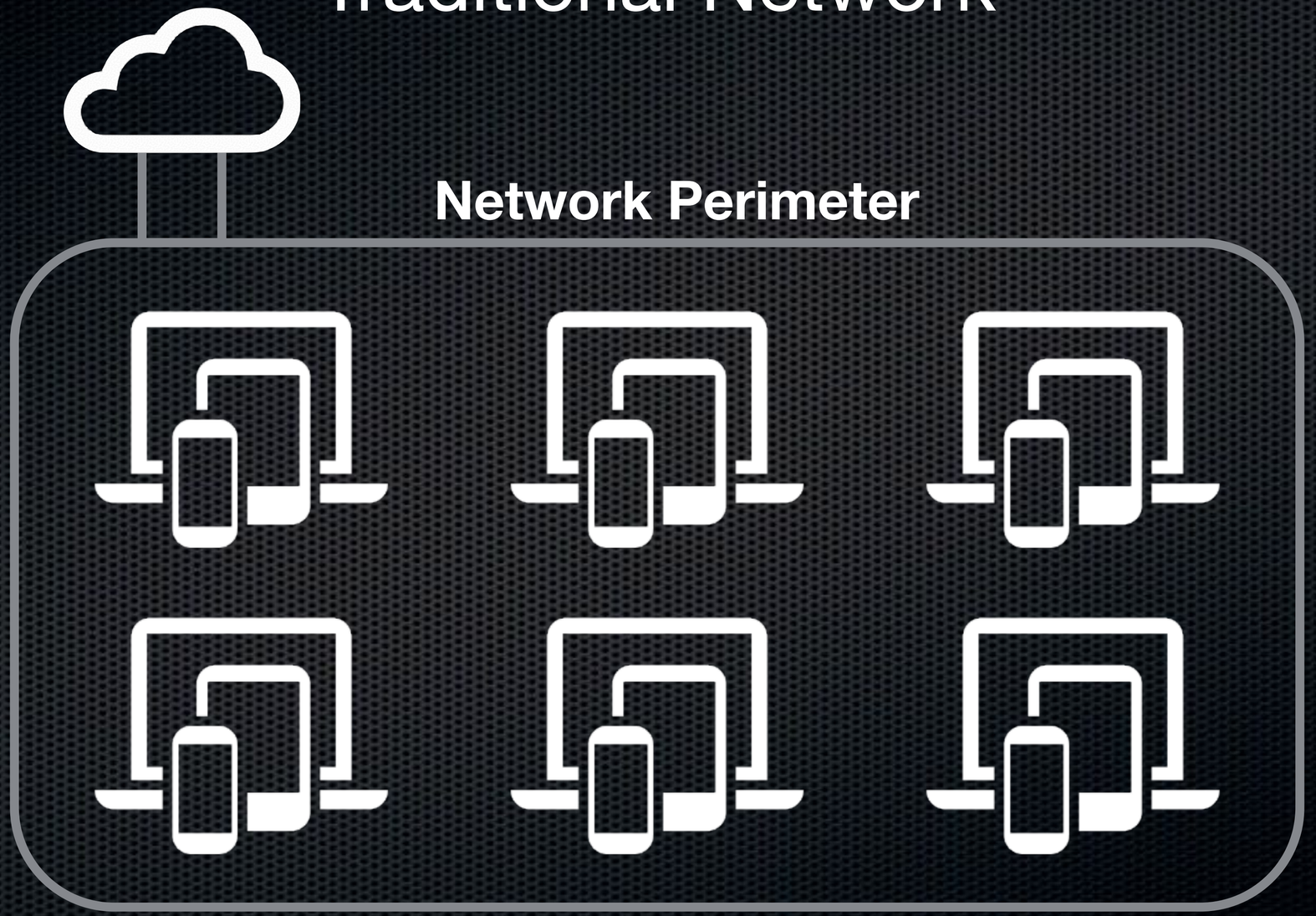
Topics

- Traditional Networks
- Zero Trust Networks
- Why should you adopt Zero Trust?
- “Thinking Different” about Networks
- Technology Behind Zero Trust
- Getting Started with Zero Trust

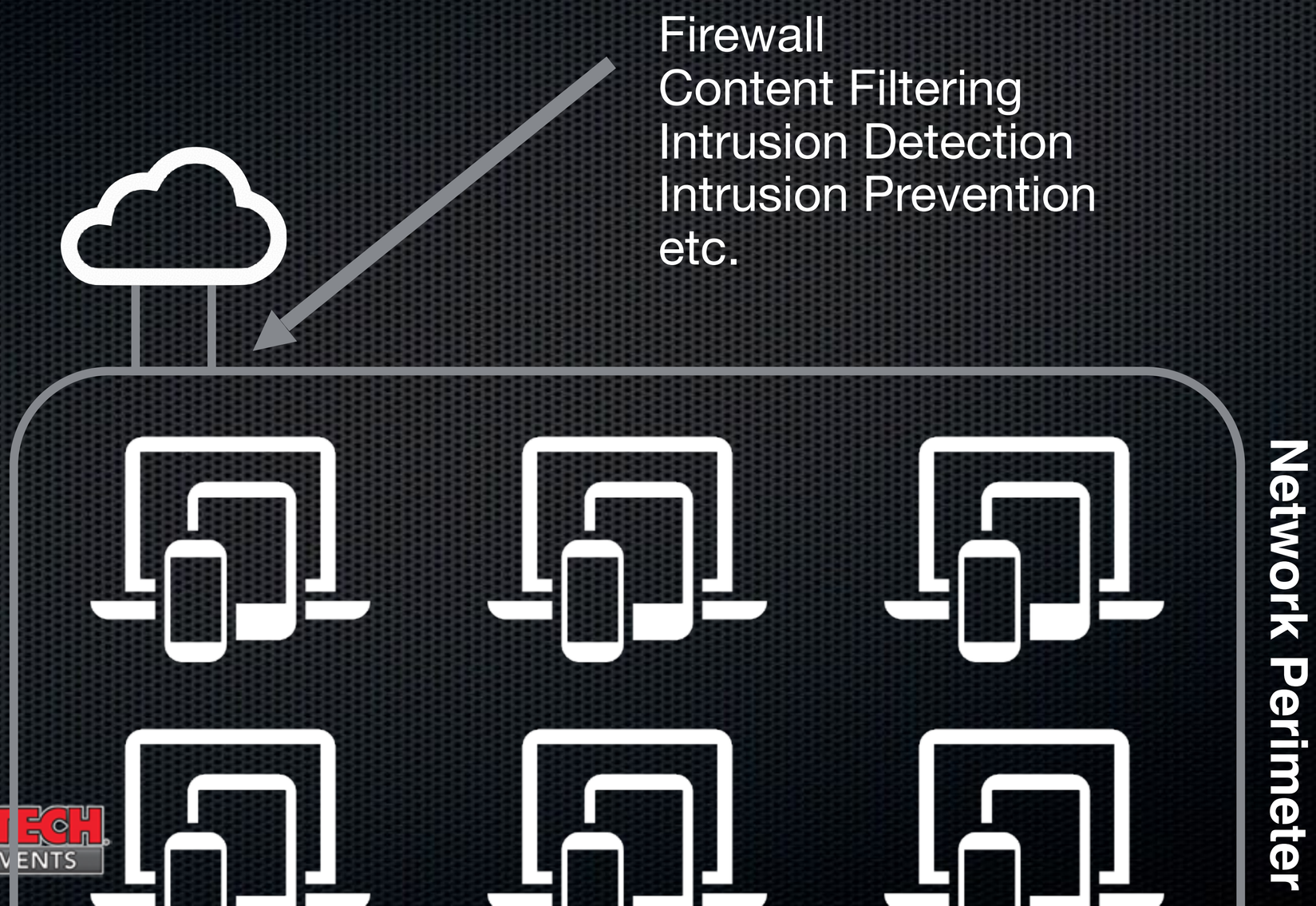
MACTECH PRO EVENTS

What is a traditional network?

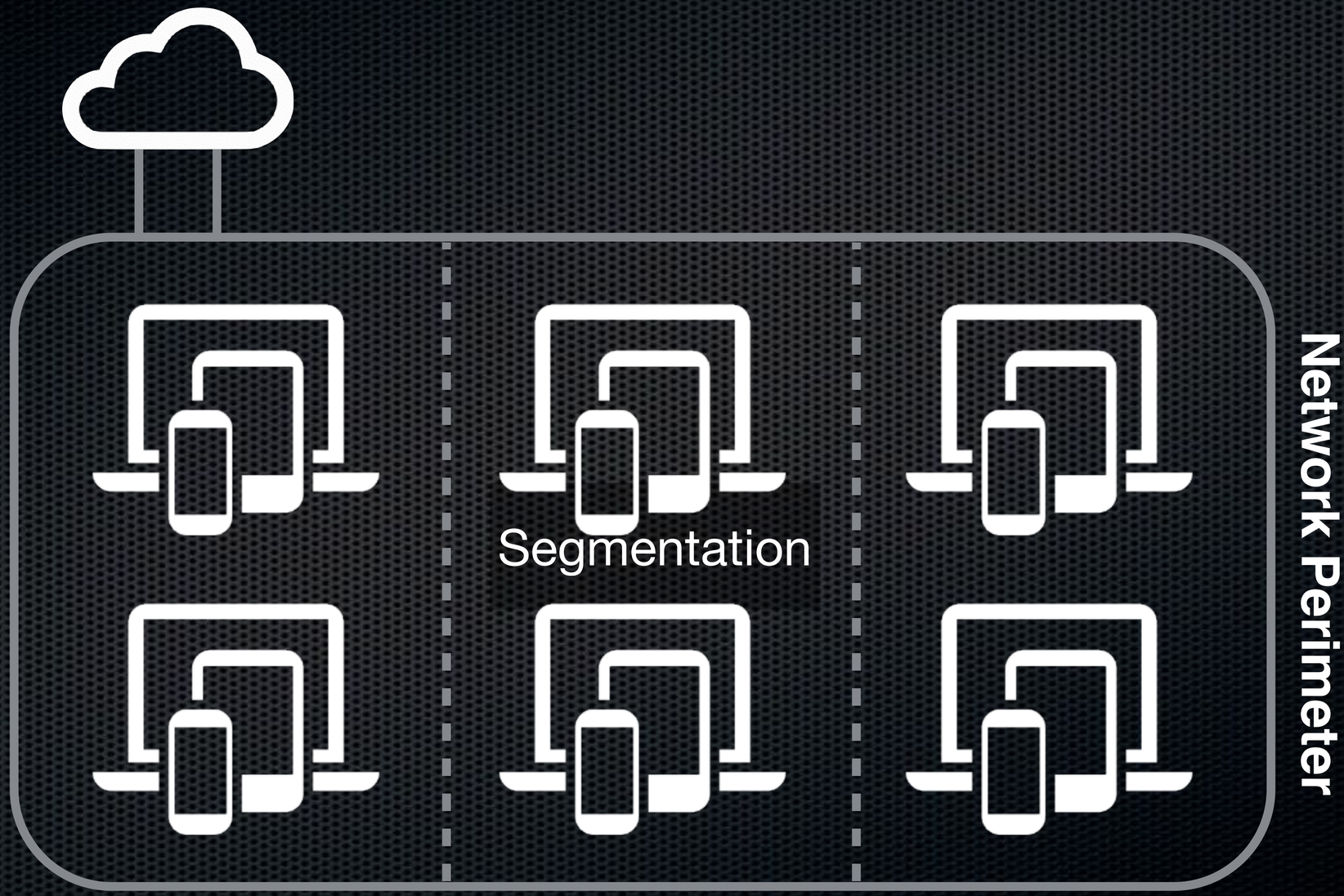
Traditional Network



Traditional Network



Traditional Network



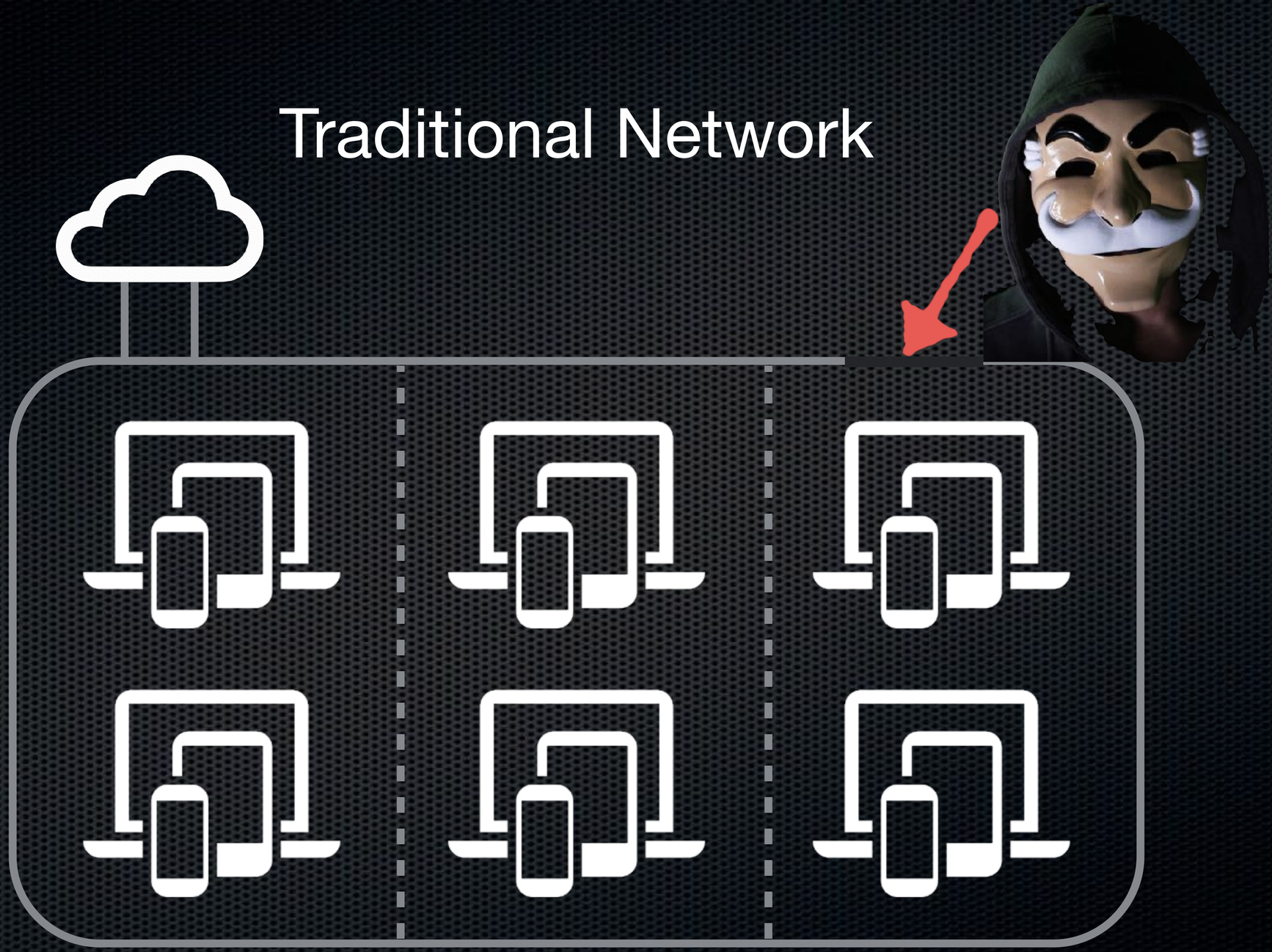
MACTECH PRO EVENTS

Traditional Network

Segmentation

- Splitting network into sub-networks
- Restricting Communication between Subnets
- VLANs, Firewalls, DMZs

Traditional Network

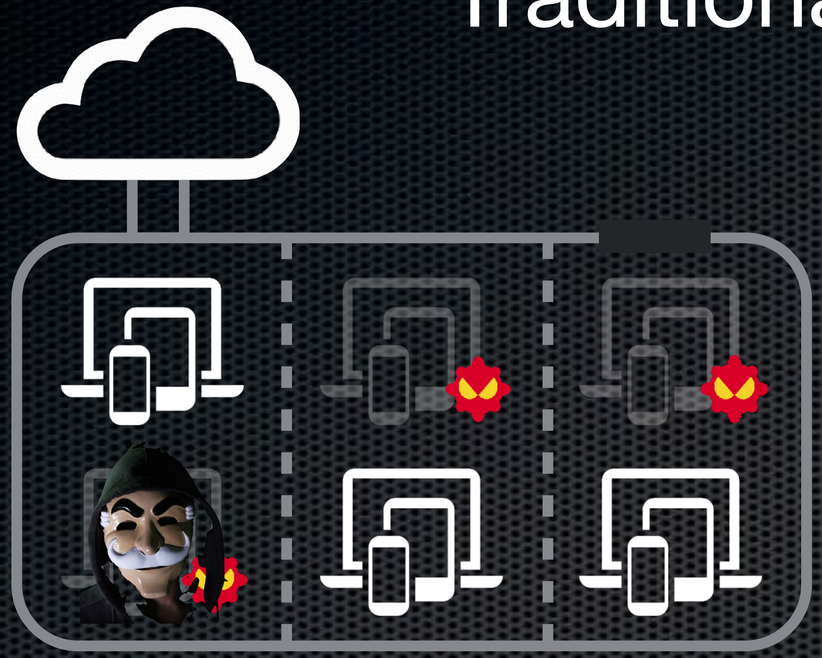


MACTECH PRO EVENTS

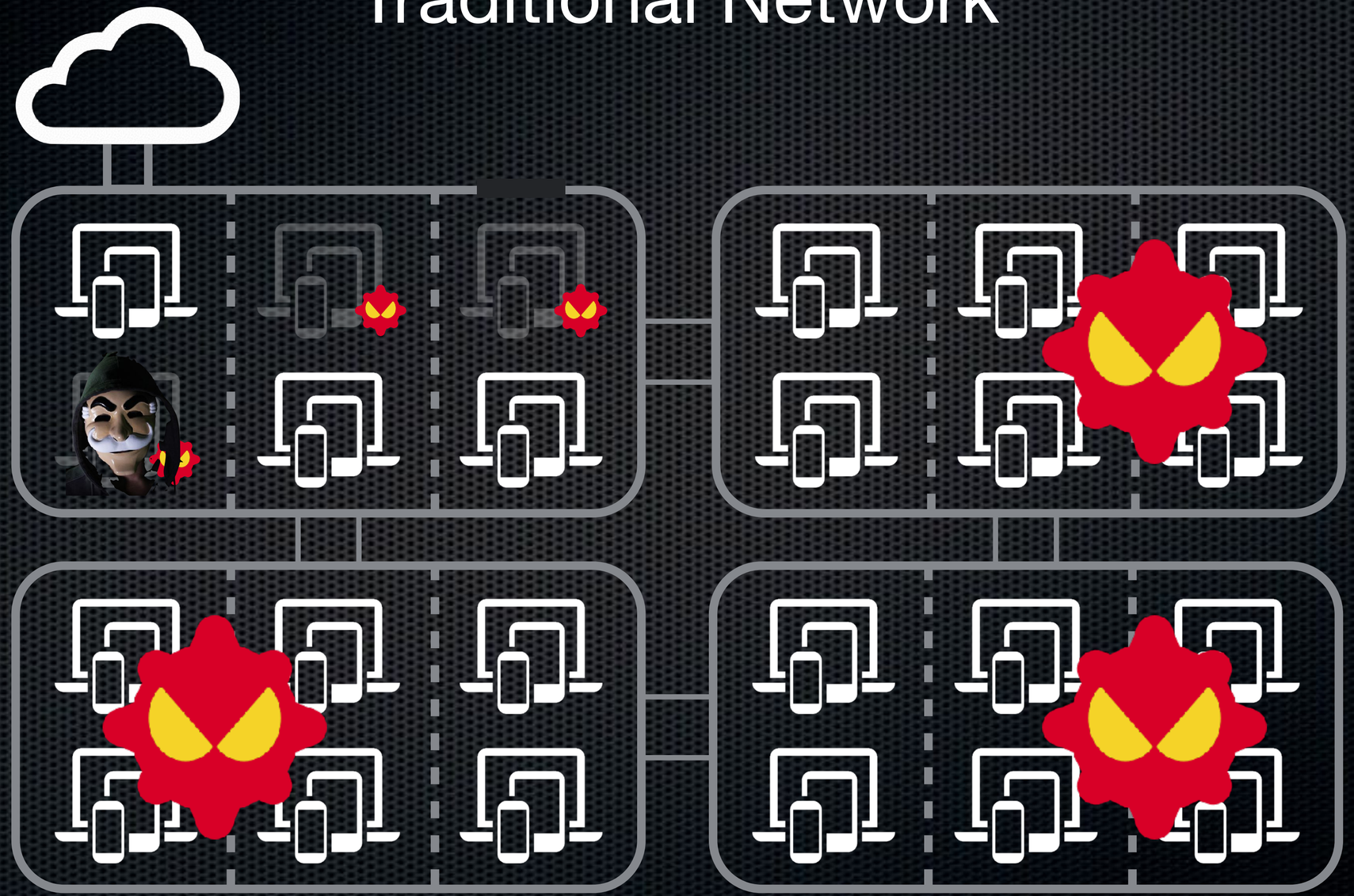
Traditional Network

MACTECH PRO EVENTS

Traditional Network



Traditional Network



MACTECH PRO EVENTS

Cost of Cybercrime

$3 Trillion

in 2015

MACTECH PRO EVENTS

Cost of Cybercrime

$6 Trillion

in 2021

MACTECH PRO EVENTS

Cost of Cybercrime

$6,000,000,000,000

in 2021

MACTECH PRO EVENTS

Cost of Cybercrime

High Profile Breaches

- Stuxnet Worm
- Target Retail
- Sony Pictures
- …many others…

MACTECH PRO EVENTS

Traditional Network: Weaknesses

- Multiple points of entry
- Firewall Rules become unmanageable
- Cloud Services are more nuanced
- Insider threat is a major omission
- All-or-nothing security model

Mitigation Strategy?

Head in the Sand

Obscure Reality

Point Fingers

Evade Ownership

Excerpt from "The X-Files S01E24 "The Erlenmeyer Flask" ©1993 Fox

MACTECH PRO EVENTS

Trust, but Verify

доверяй, но проверяй

Trust, but Verify

“the old adage is in need of an update.”

John Kerry, Former Secretary of State

MACTECH PRO EVENTS

Verify and Verify

Trust no one

Untrusted

Untrusted

What is Zero Trust, and why should I care?

MACTECH PRO EVENTS

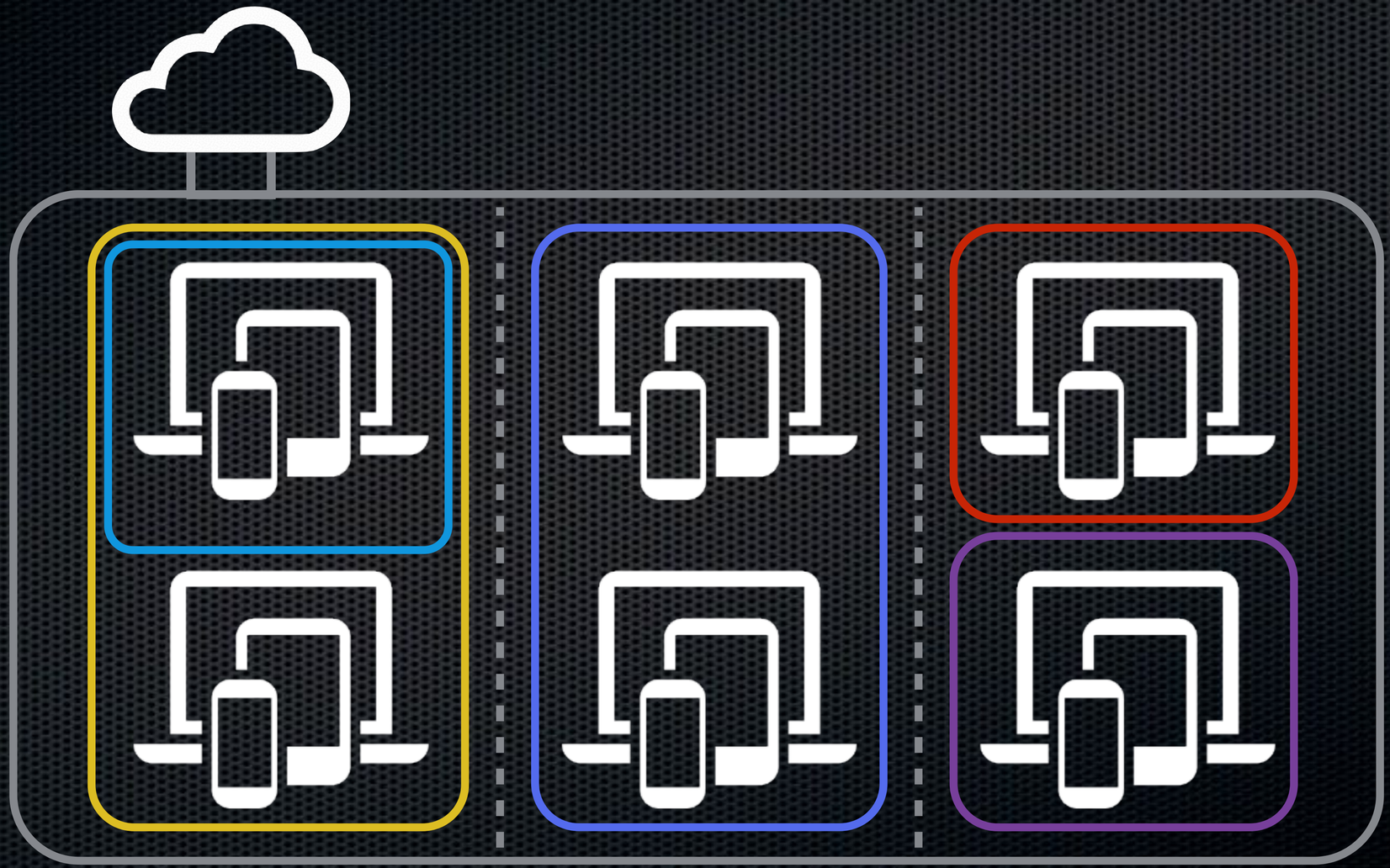
“Thinking Different” about Networks

MACTECH PRO EVENTS

Zero Trust is not a product.

It’s a philosophy.

Why Zero Trust?



MACTECH PRO EVENTS

Why Zero Trust?

Why Zero Trust?

- Works on untrusted physical networks
- Identity-based access management (IAM)
- App identity profiles on next-gen firewalls
- Certificate based authentication
- Robust and auditable access controls
- All network traffic logged and inspected

Data Access

- Security based on user and location
- Identify and map traffic / data flow
- Know the users and their apps

Access Control

- Adopt a “Least-Privileged” strategy
- Grant on a “Need to Know” basis
- Data classification

Always Verify

- Log all Traffic
- Inspect All Traffic

Authentication Methods

- Certificates
- Two-Factor (2FA)
- Multi-Factor (MFA)

MACTECH PRO EVENTS

Identity Management

- Identify and Add Context
- Keep Roles Up-to-Date

Technology & Processes of Zero Trust Networking

MACTECH PRO EVENTS

Technology & Processes

Zero Trust Combines:

- Existing Technologies
- Governance

MACTECH PRO EVENTS

Technology & Processes

Micro-segmentation of networks

Granular Perimeter Enforcement

- User
- Location
- Device / Computer
- Application

MACTECH PRO EVENTS

Technology & Processes

- Multi-Factor Authentication
  - 2FA
  - TOTP
- Identity & Access Management (IAM)
- IAM can be combined with MFA
  - Examples: Apple ID, O365 + Ping/Duo

Technology & Processes

- Policy orchestration
- Network traffic analytics
- Baseline encryption
- Scoring based on analytics

MACTECH PRO EVENTS

Technology & Processes

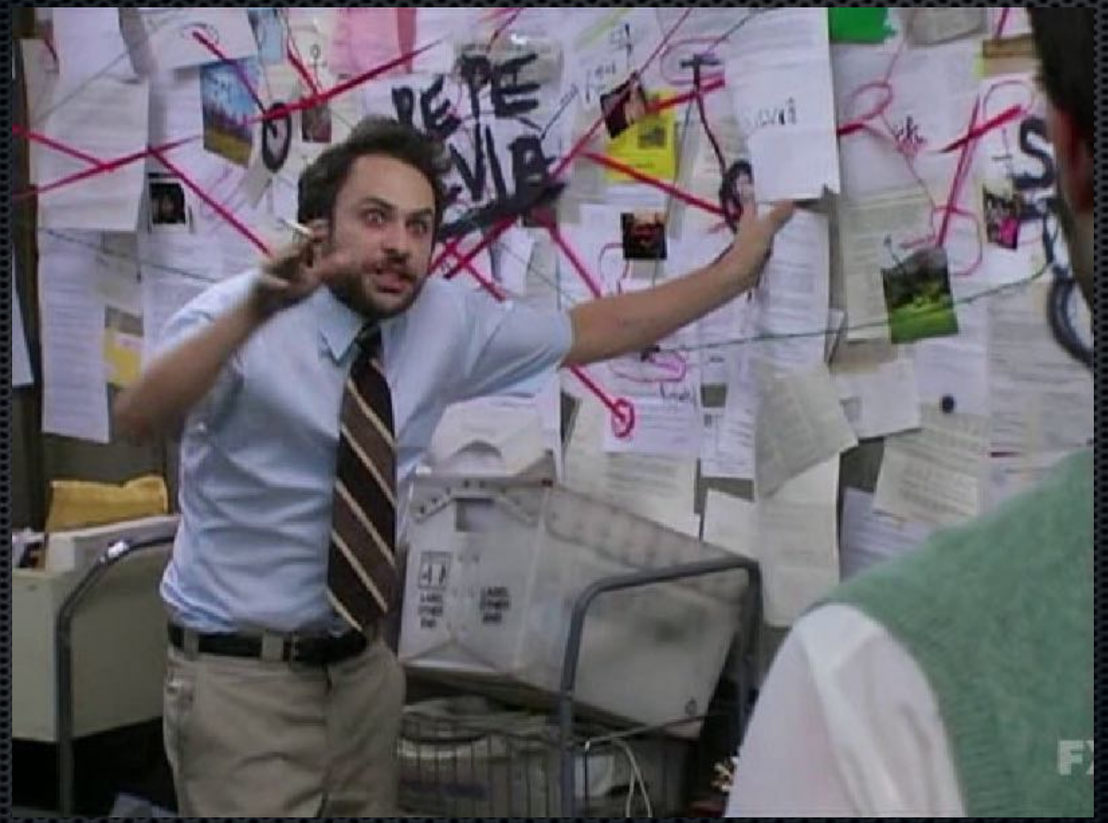
- File system permissions
- Databases
- Does this user need access to *all* of this?

Technology & Processes

- Certificates
- 802.1x Networking

MACTECH PRO EVENTS

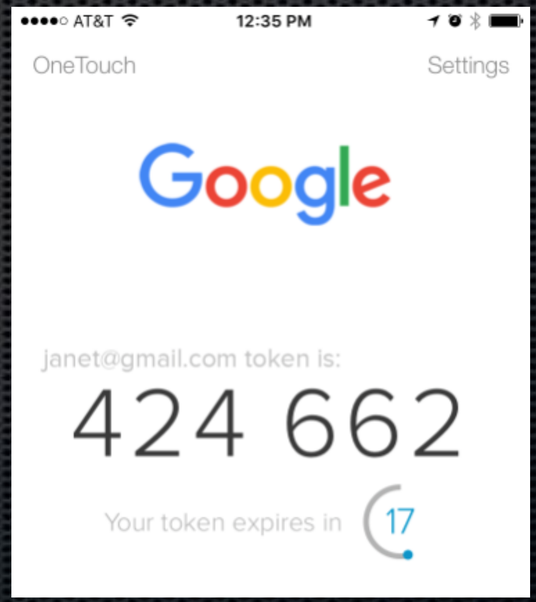
Getting Started with Zero Trust



MACTECH PRO EVENTS

Getting Started with Zero Trust

- M cation



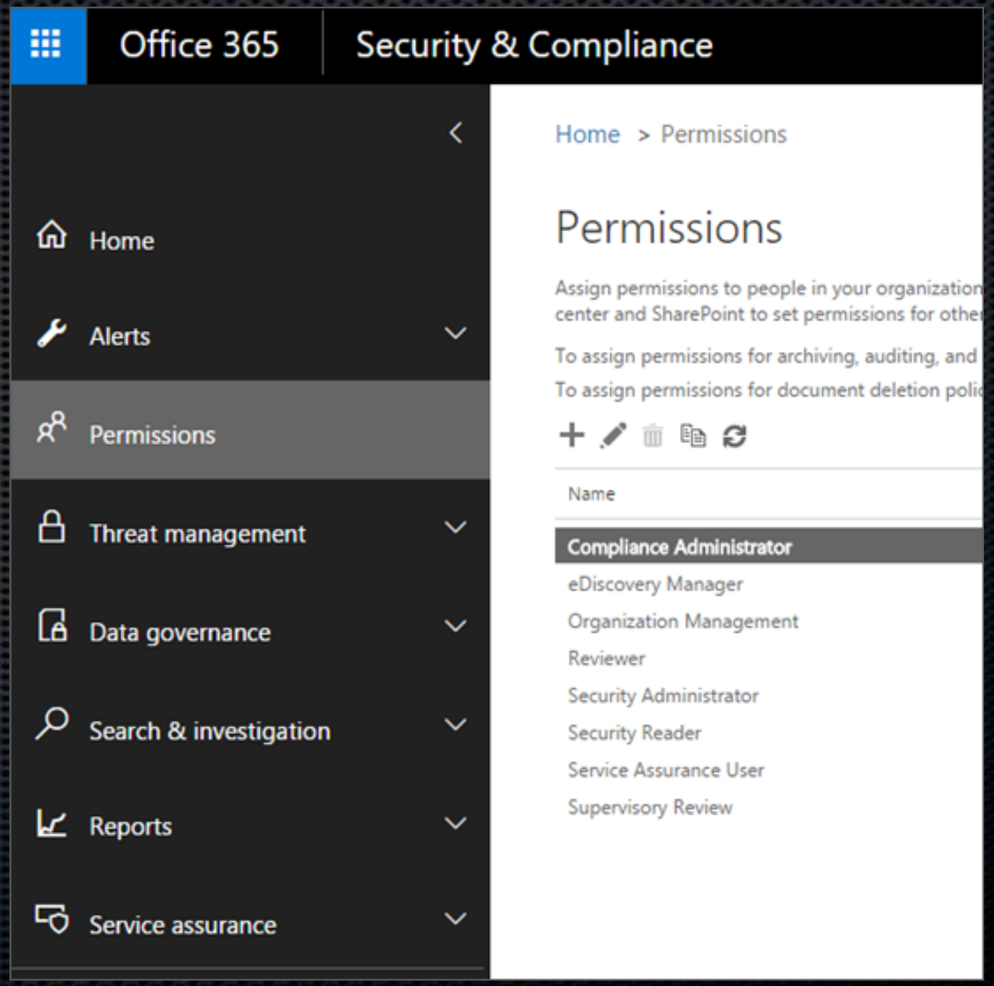
MACTECH PRO EVENTS

Getting Started with Zero Trust

- Identity & Access Management (IAM)
- Single Sign-on (SSO)

Getting Started with Zero Trust

- Permissions



MACTECH PRO EVENTS

Getting Started with Zero Trust

- Multi-Factor Authentication (MFA)
- Identity & Access Management (IAM)
- Single Sign-on (SSO)
- Appropriate permissions
- Thorough process audit

MACTECH PRO EVENTS

Getting Started with Zero Trust

- Multi-Factor Authentication (MFA)
- Identity & Access Management (IAM)
- Single Sign-on (SSO)
- Appropriate permissions
- Thorough process audit
- Next-Gen Access (NGA)

MACTECH PRO EVENTS

Zero Trust

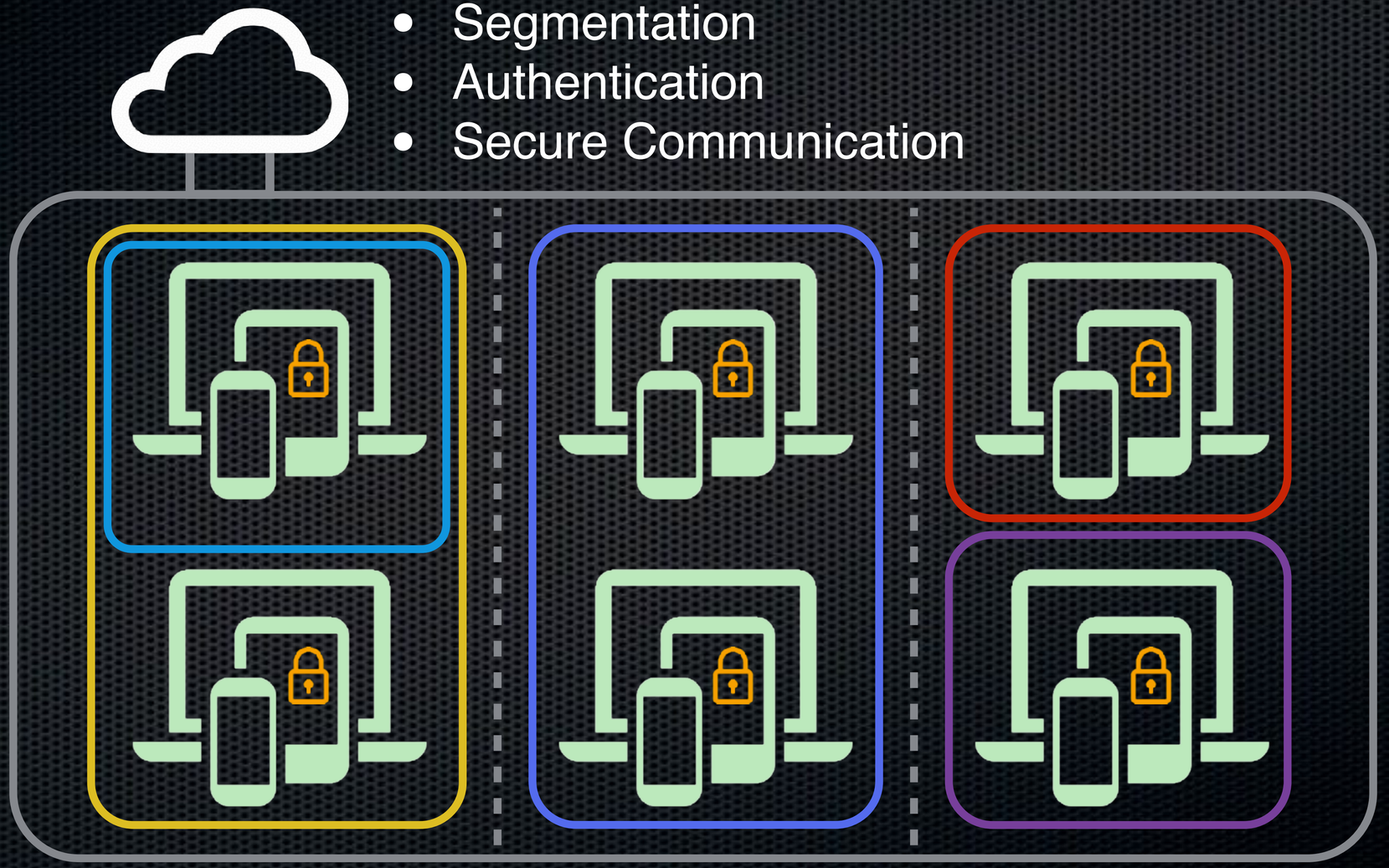
Untrusted

Untrusted

MACTECH PRO EVENTS

Zero Trust

- Segmentation
- Authentication
- Secure Communication



MACTECH PRO EVENTS

Why Zero Trust?

Resources

- The Zero Trust Network Architecture by John Kindervag
  (google… DNA zero trust network forrester filetype:pdf)
- Integrate Jamf Pro with Intune for compliance
- Integrating with Microsoft Intune to Enforce Compliance on Mac Computers Managed by Jamf Pro
- Centrify: What is Zero Trust Privilege?
- O'Reilly: Zero Trust Networks
  book by Evan Gilman, Doug Barth

MACTECH PRO EVENTS

Resources

- haveibeenpwned.com
- NIST SP 800-63B
- https://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/
- SANS Institute Case Study: Target Breach
- Endpoint protection:
  - intego.com / flextivity.com
  - github.com/google/santa
  - objective-see.com

MACTECH PRO EVENTS

Questions?

Nathan Underwood
nathan@piratica.us

MACTECH PRO EVENTS