Brad Chapman

Brad is a highly versatile systems engineer and Jamf Certified Expert with over 10 years experience across the entertainment industry, from small business networks to managing over 40,000 systems worldwide with a team of engineers.

Fluent in Mac, Windows, and UNIX, his strengths include infrastructure planning, troubleshooting & debugging, deployment automation, documentation & training, and enhancing the user experience with behind-the-scenes magic. He has prior experience at Apple as a Retail Specialist and as an Enterprise SE.

He is proficient in Spanish and German. His hobbies include photography, music, and repair of appliances and automobiles. He is also a member of the Los Angeles Master Chorale, a 100-voice professional ensemble that routinely performs at Walt Disney Concert Hall and the Hollywood Bowl.

Zero Trust Networking

Topics

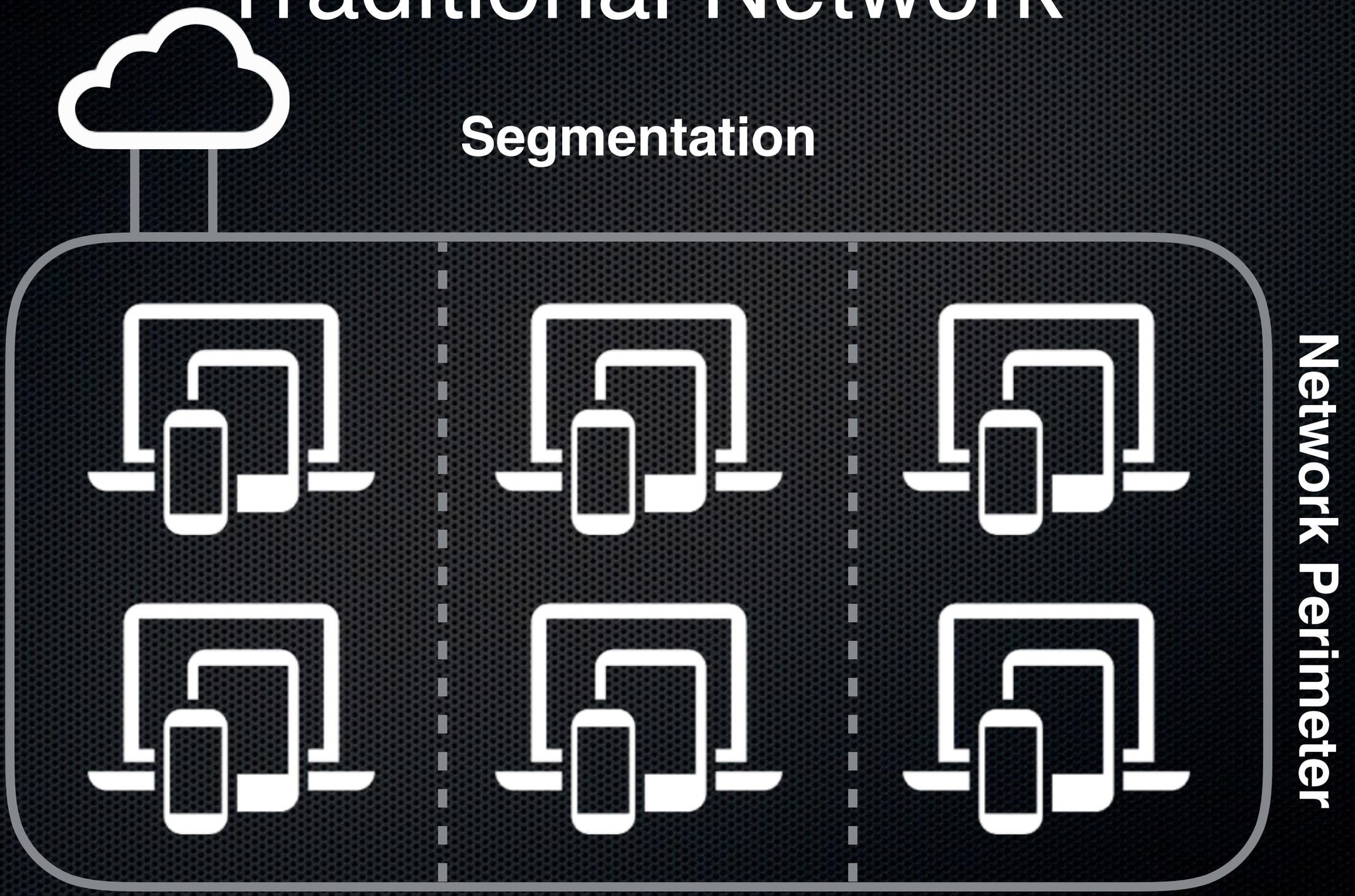
- Traditional Networks
- Zero Trust Networks
- Why should you adopt Zero Trust?
- “Thinking Different” about Networks
- Technology Behind Zero Trust
- Getting Started with Zero Trust

What is a Zero Trust Network?

Traditional Network

Traditional Network

Traditional Network



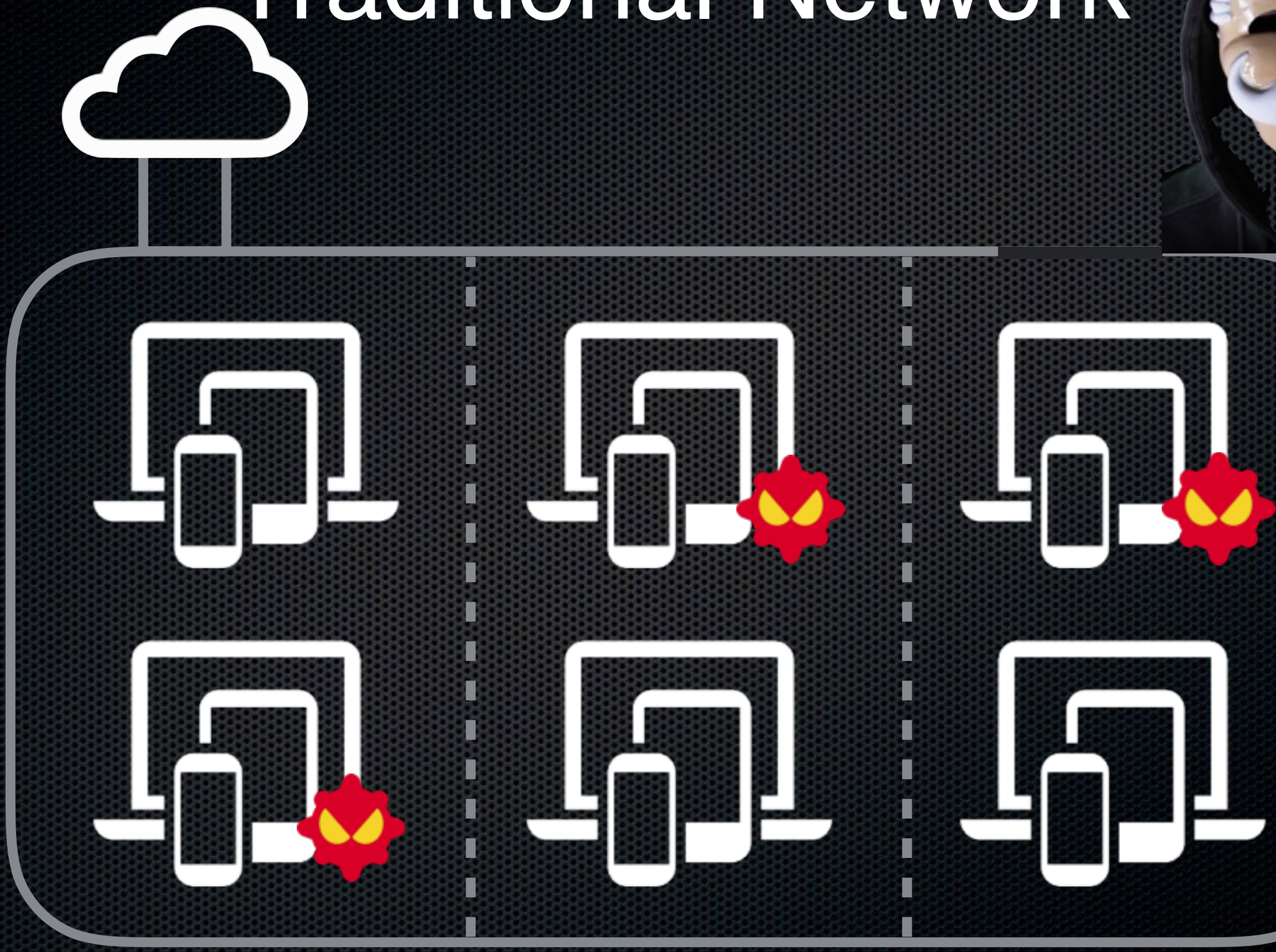
Traditional Network

Segmentation

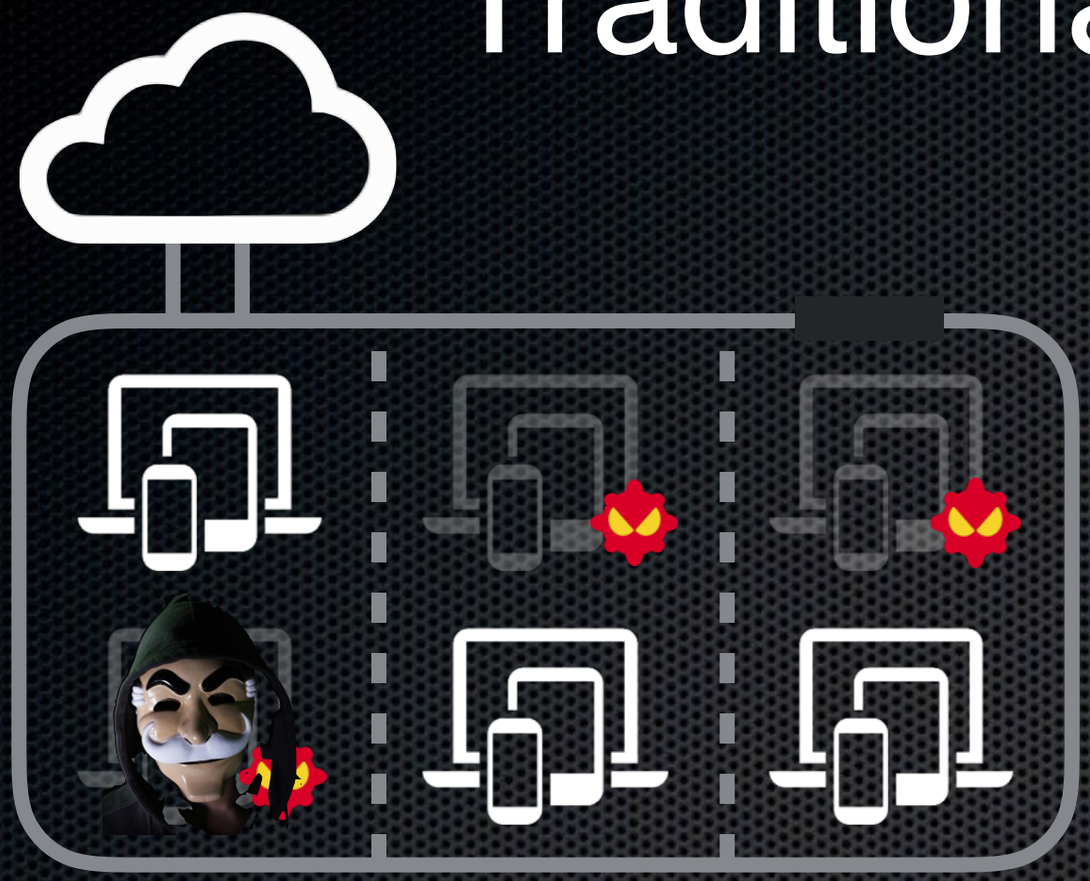
- Splitting network into sub-networks
- Restricting Communication between Subnets
- VLANs, Firewalls, DMZs
- Like a sledgehammer to a nail

Traditional Network

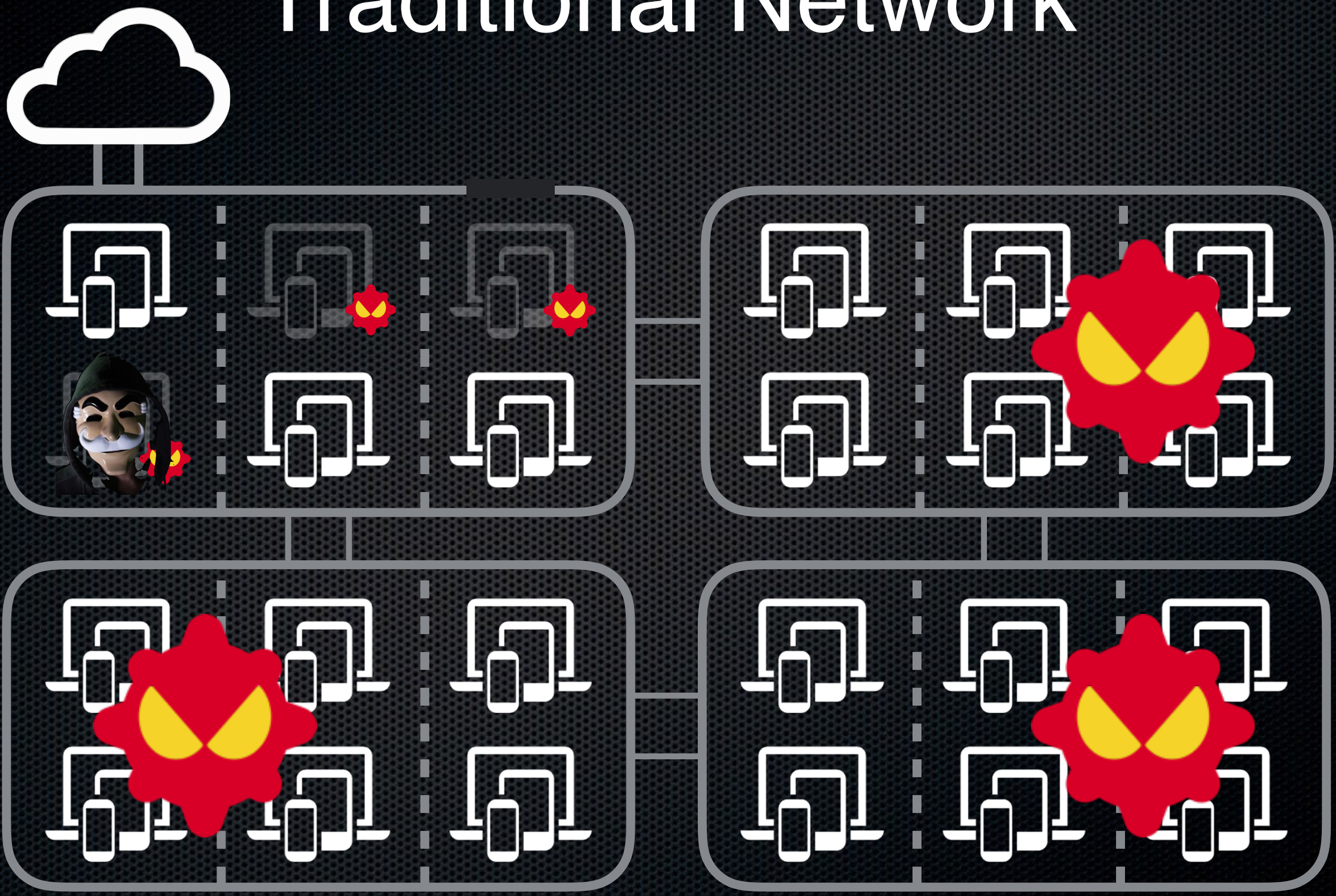
Traditional Network



Traditional Network



Traditional Network



Cost of Cybercrime

$3 Trillion

2015

Cost of Cybercrime

$6 Trillion

2021

Cost of Cybercrime

$6,000,000,000,000

2021

Cost of Cybercrime

High Profile Breaches

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

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

…so what do you do?

Excerpt from “Tinker, Tailor, Soldier, Spy” ©2011 Focus Features

доверяй, но проверяй

“the old adage, ‘Trust, but Verify’ is out the door. Verify, Verify, Verify update.”

John Kerry, Former Secretary of State

Verify and Verify

Trust no one

Untrusted

Untrusted

Why should you adopt the “Zero Trust” model?

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

Why Zero Trust?

“Thinking Different” about Networks

Zero Trust is not a product.

It’s a philosophy.

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

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

Identity Management

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

Technology & Processes of Zero Trust Networking

Technology & Processes

- Existing Technologies
- Governance Processes

Technology & Processes

Micro-segmentation of networks

Granular Perimeter Enforcement

- User
- Location
- Device / Computer
- Application

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

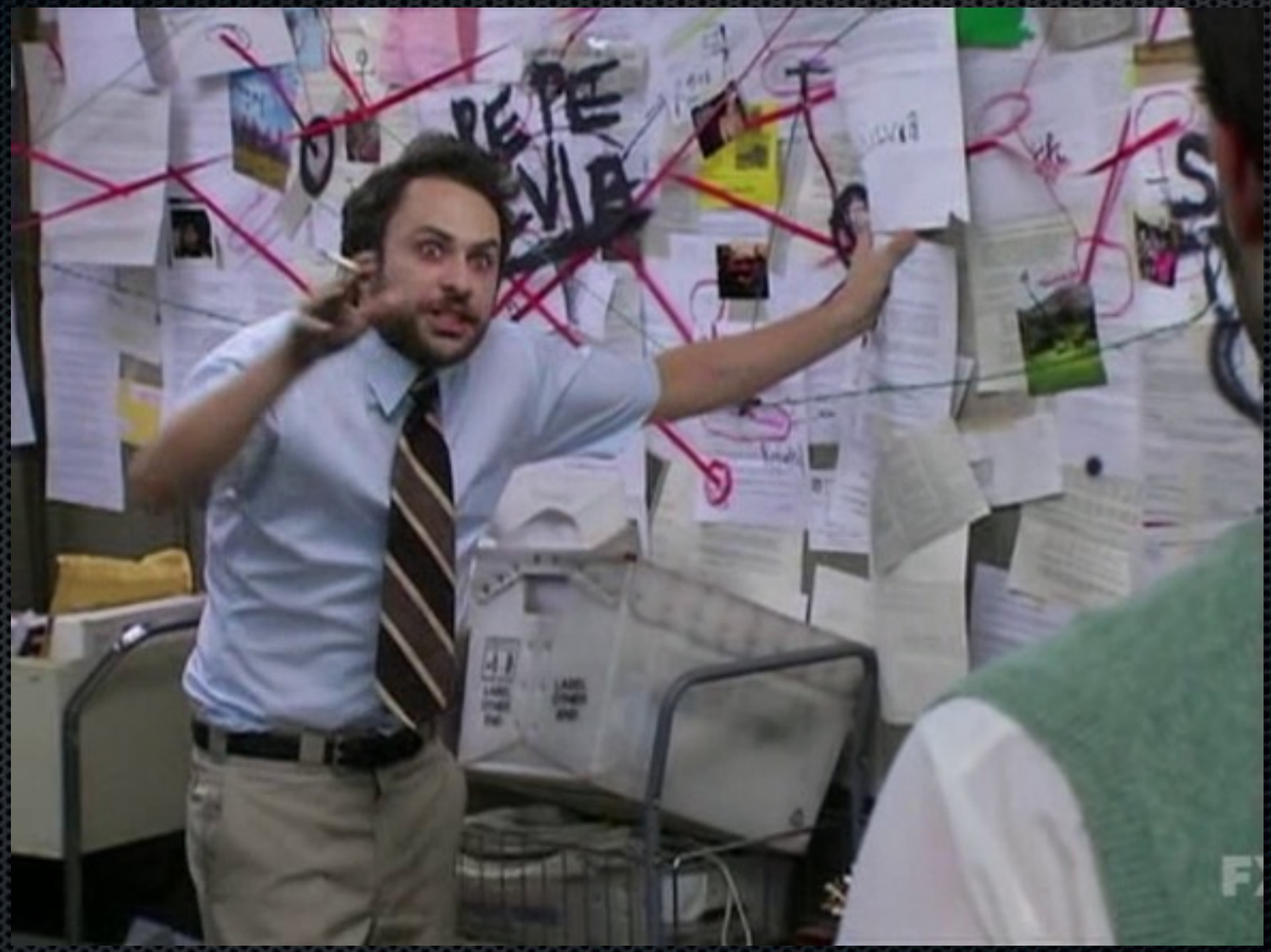
Technology & Processes

- File system permissions

Tech Behind Zero Trust

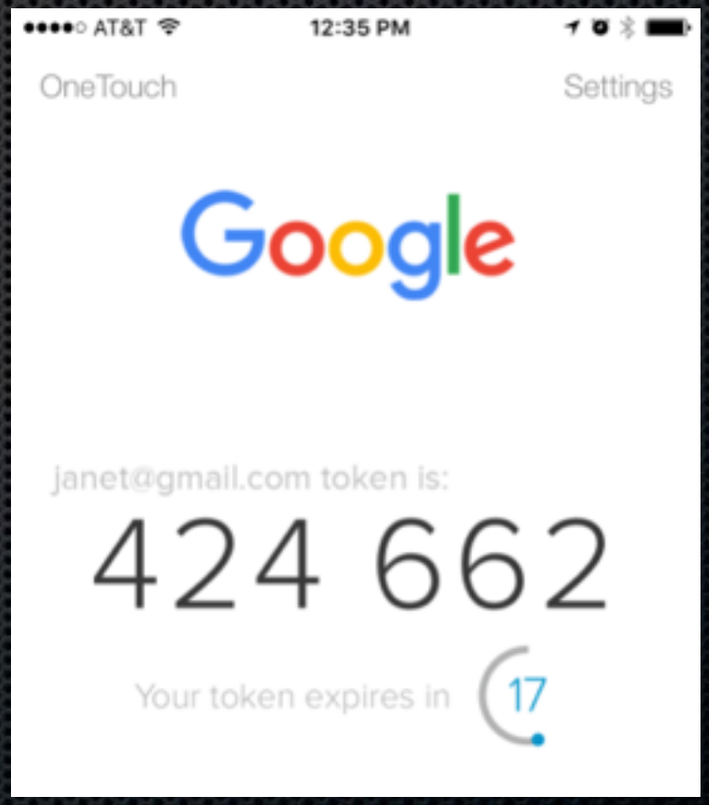
- 802.1x

Getting Started with Zero Trust



Getting Started with Zero Trust

- Multi-Factor Authentication (MFA)



Getting Started with Zero Trust

jamf | CONNECT

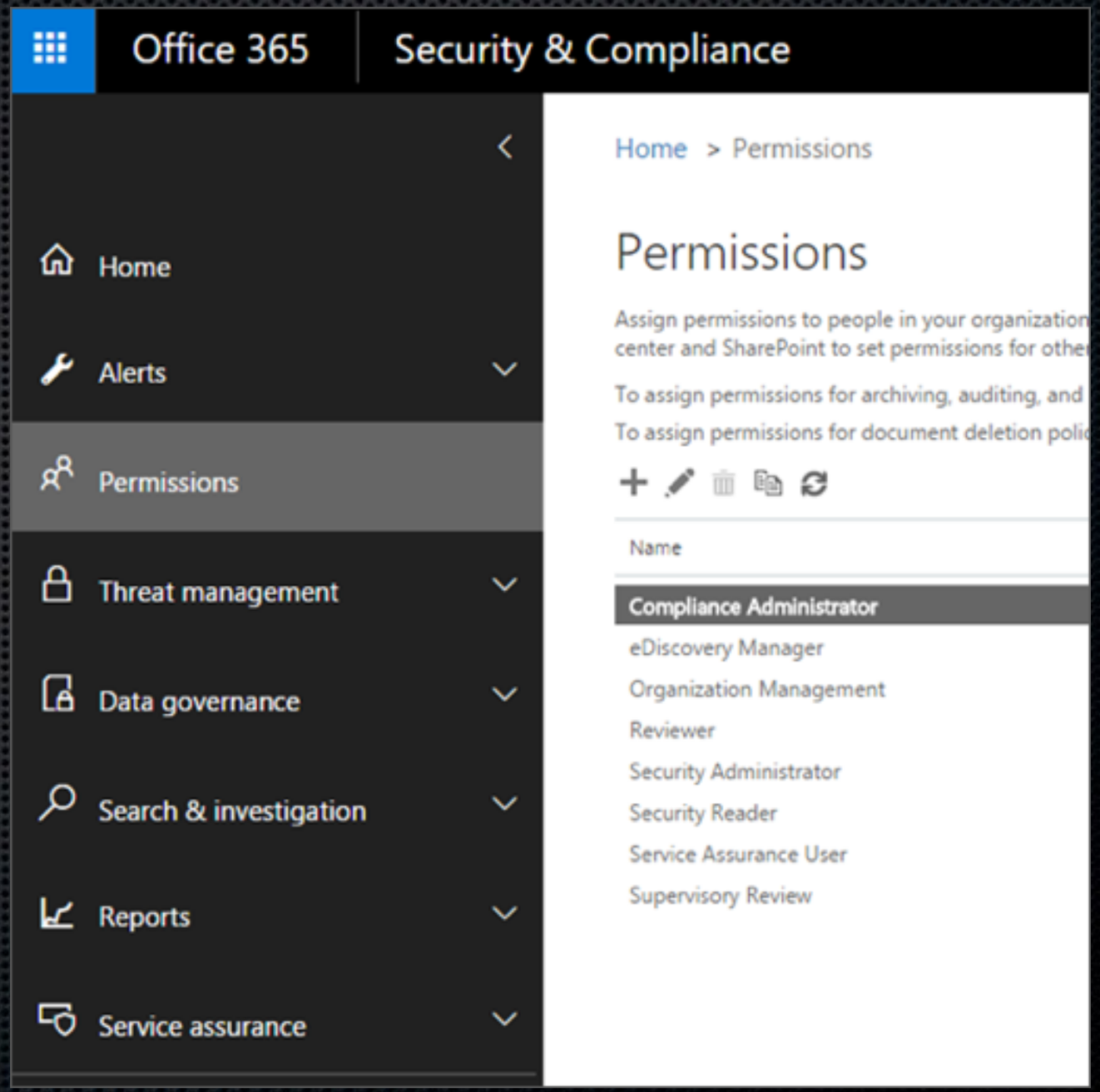
- Identity & Access Management (IAM)
- Single Sign-on (SSO)

okta

Centrify®

Getting Started with Zero Trust

- Permissions



Getting Started with Zero Trust

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

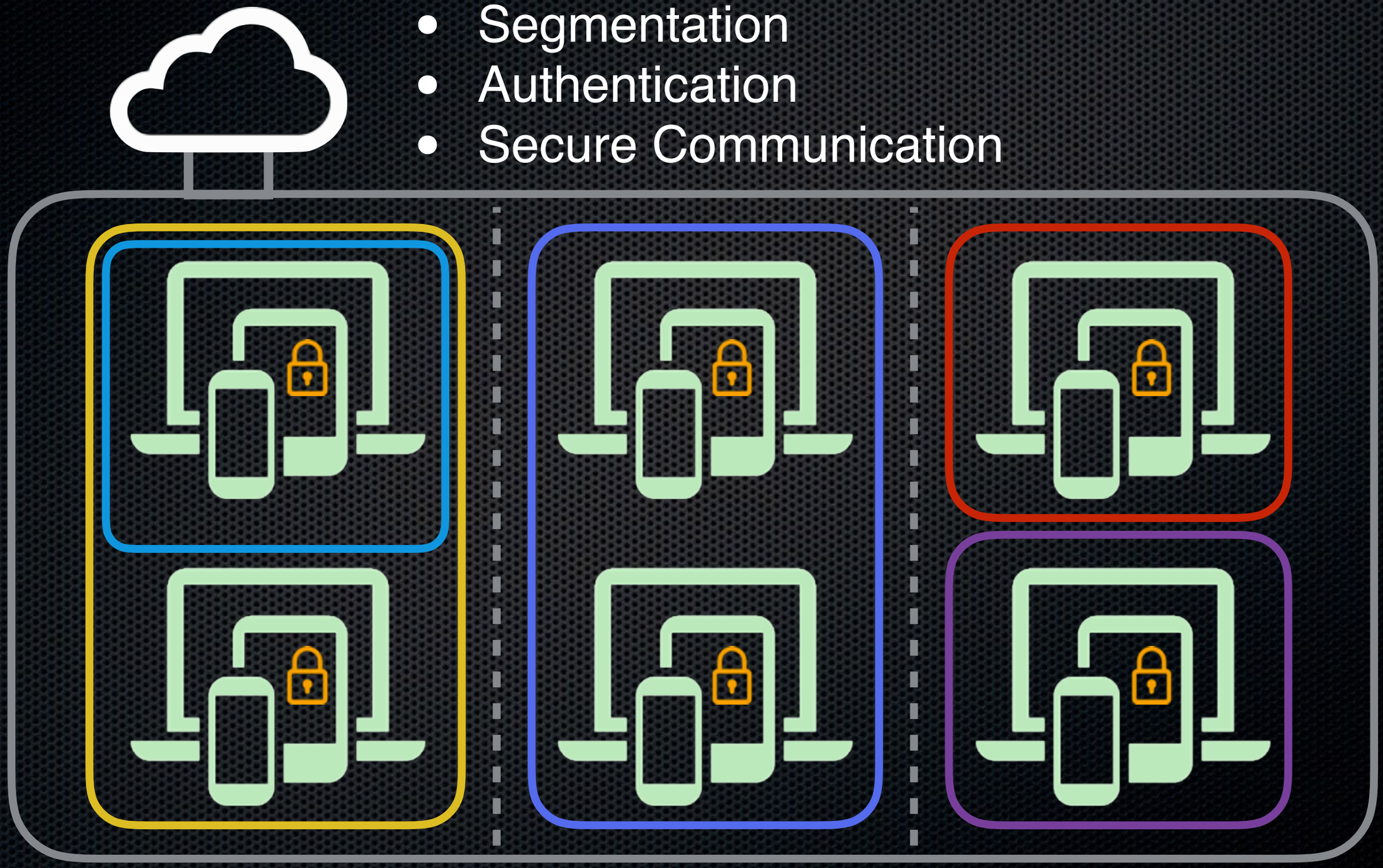
Zero Trust

Untrusted

Untrusted

Zero Trust

- Segmentation
- Authentication
- Secure Communication



Recap

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

Resources

- The Zero Trust Network Architecture by John Kindervag
  (google dork: 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 Zero Trust Privilege
- O'Reilly Zero Trust Networks
  By Evan Gilman, Doug Barth

Resources

- haveibeenpwned.com
- NIST SP 800-63B
- Google Santa Project
- SANS Institute Case Study: Target Breach

Questions?

Brad Chapman
bradtchapman@gmail.com

MACTECH PRO EVENTS

MACTECH®

PRO EVENTS