Justin Esgar

Justin Esgar is a returning speaker to MacTech, having presented in Los Angeles, New York and DC over the last few years. Justin is dedicated to helping others make their businesses great. Whether through technology via his Apple Consulting agency, Virtua Computers, his conference for the business side of IT Consulting, ACEs Conference, or through his own IT business consulting firm, Virtua Consulting, Justin has made it his goal to help as many businesses grow as possible. Justin loves to hear stories. So make sure you tell him yours!

MACTECH PRO EVENTS

Zero Trust Networking

Thanks!

Quick shout out to Brad Chapman in Los Angeles for all the work he did on the content of this presentation.

MACTECH PRO EVENTS

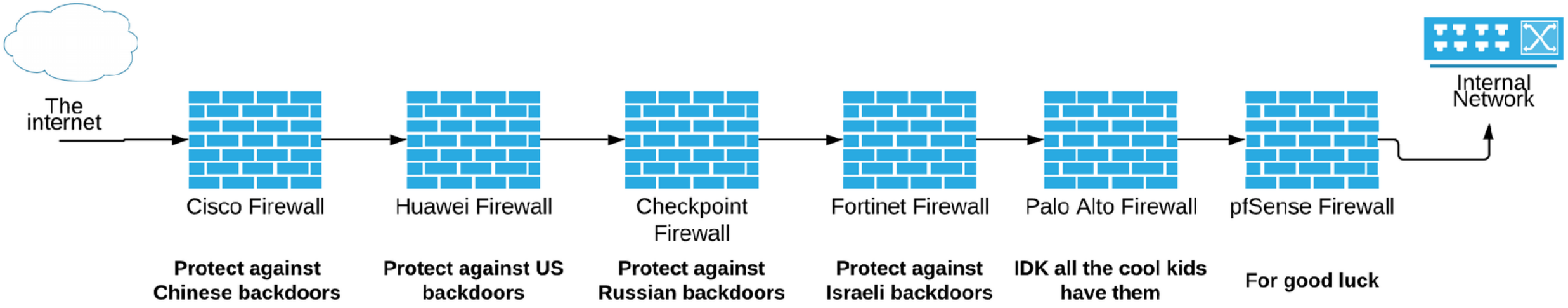
Topics

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

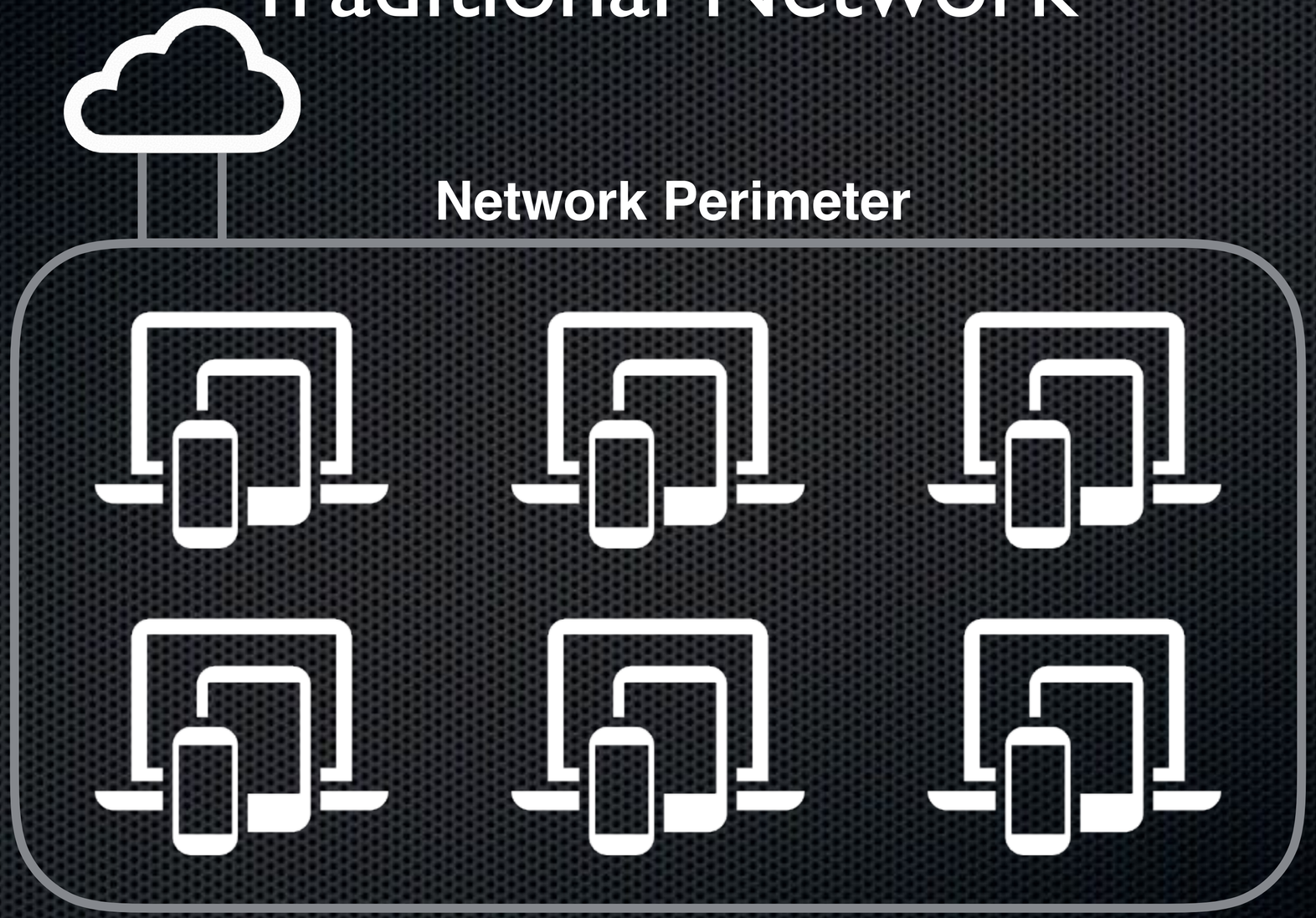
MACTECH PRO EVENTS

What is a Zero Trust Network?

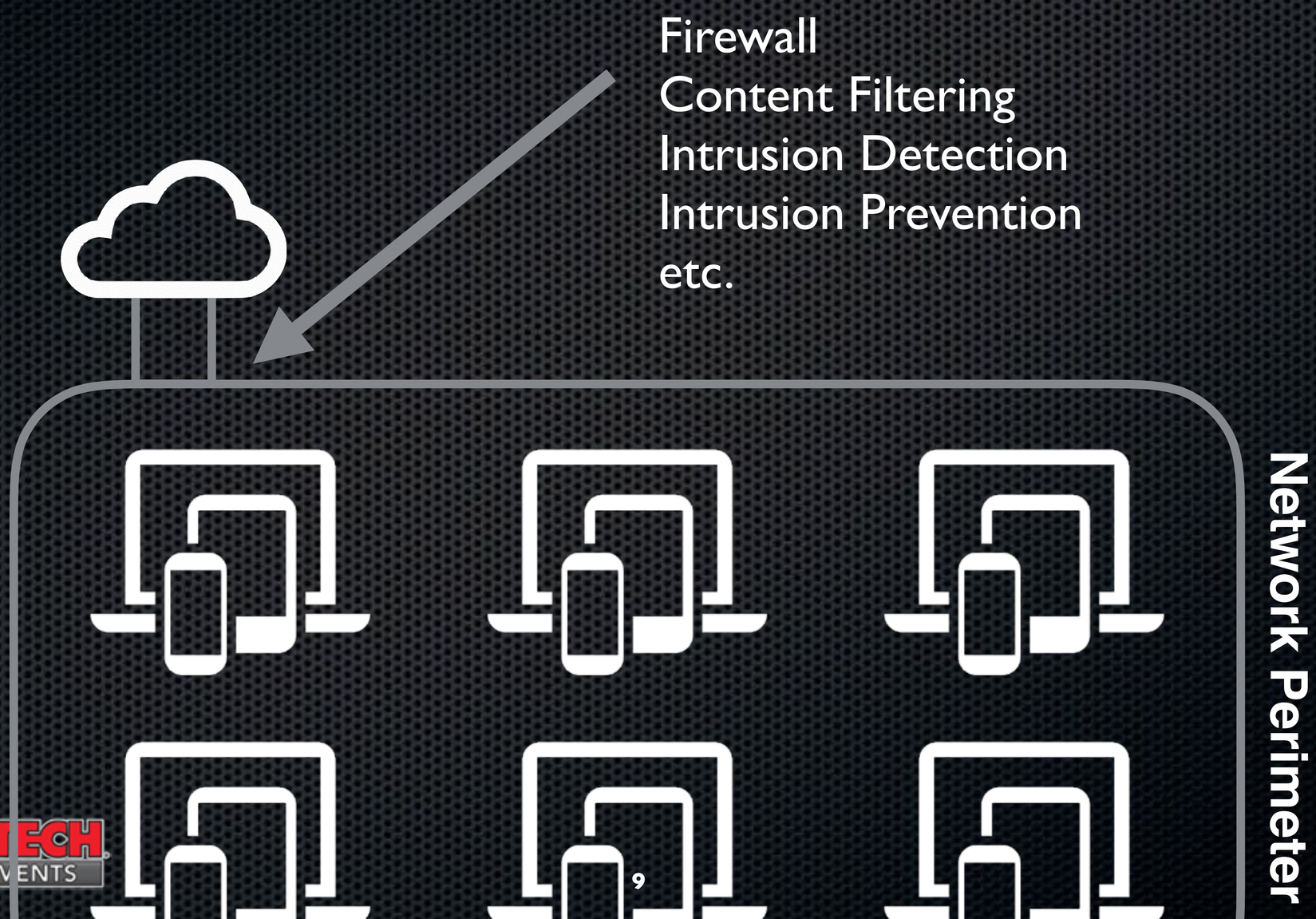
Traditional Network



Traditional Network



Traditional Network



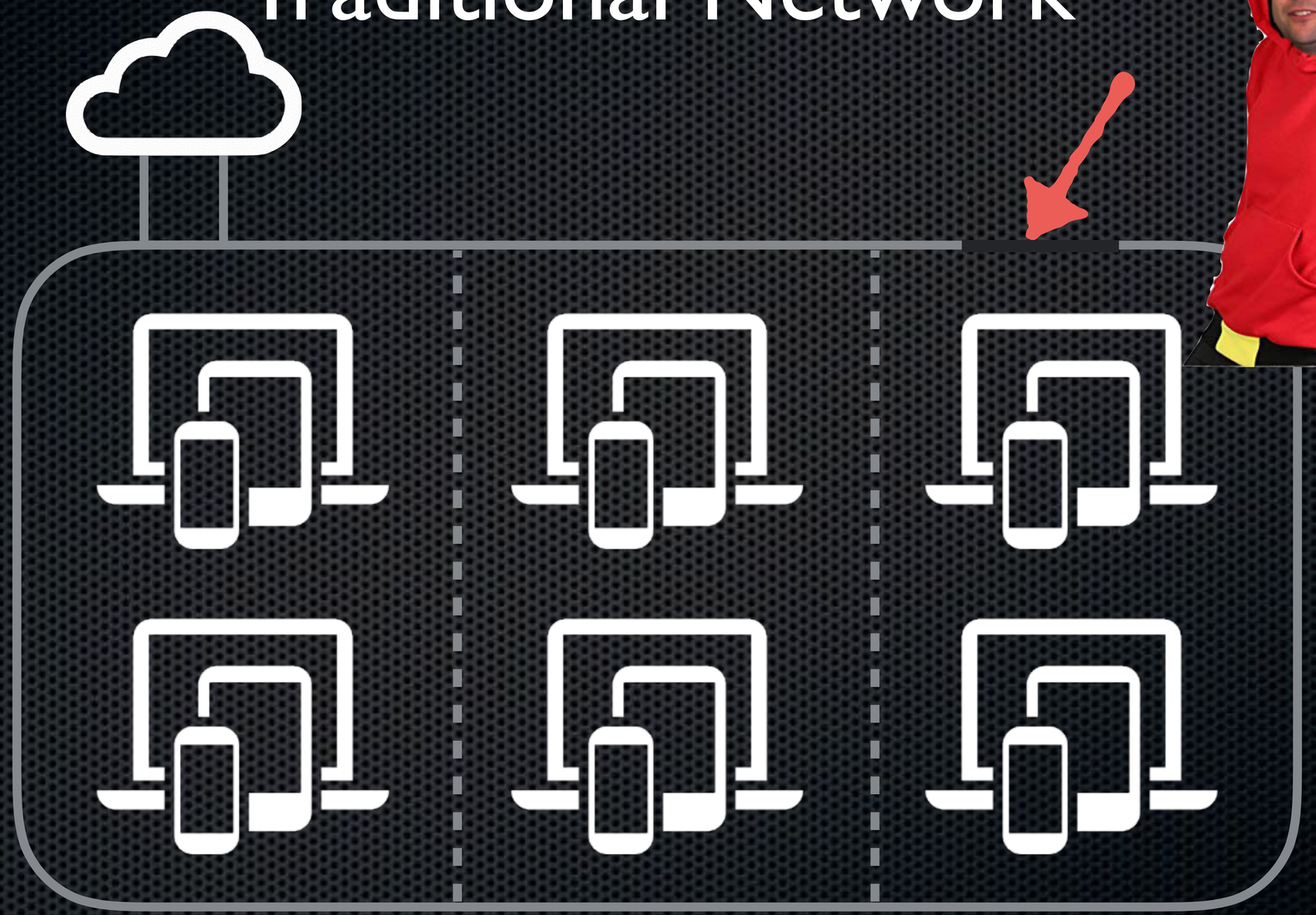
Traditional Network

Traditional Network

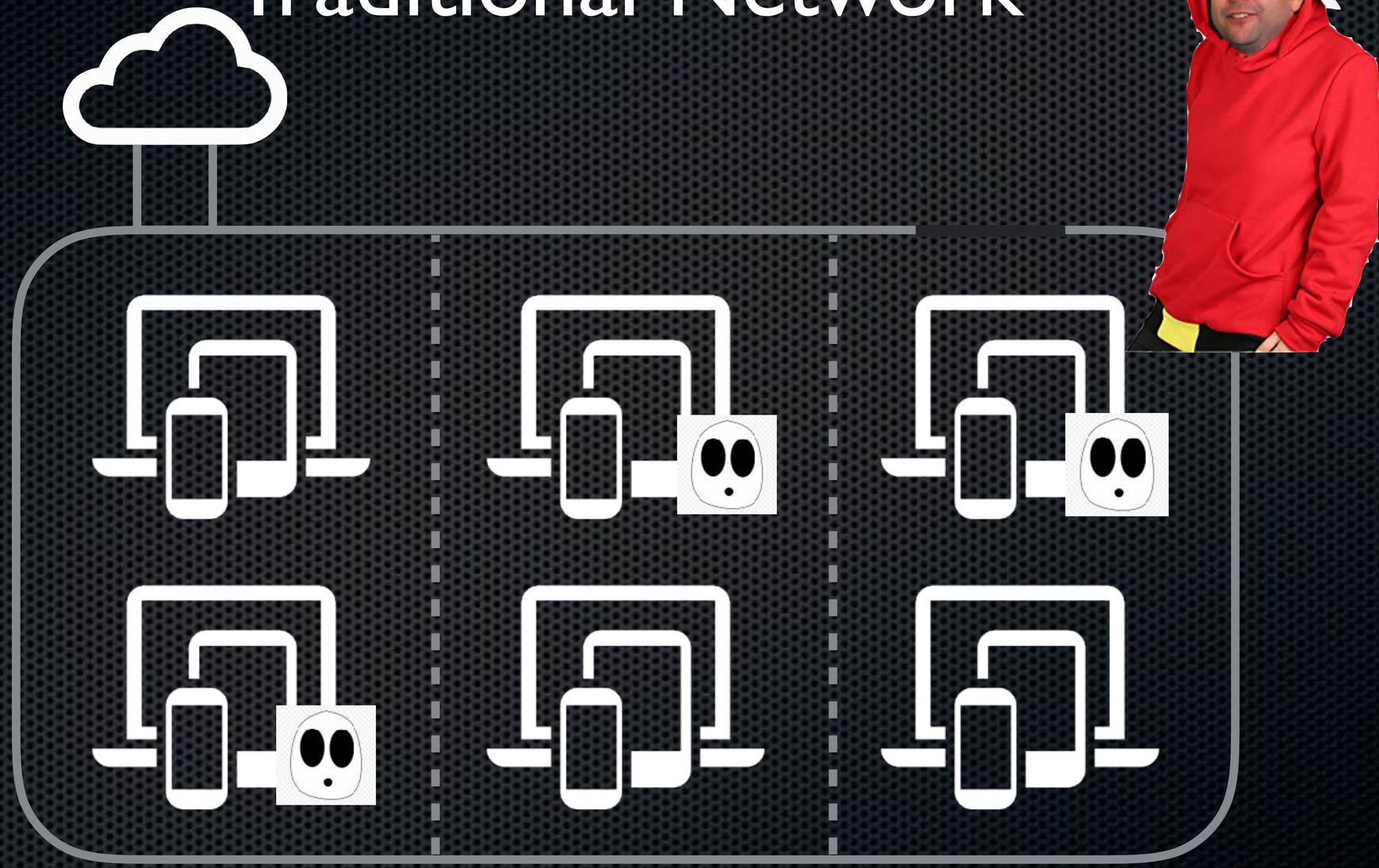
Segmentation

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

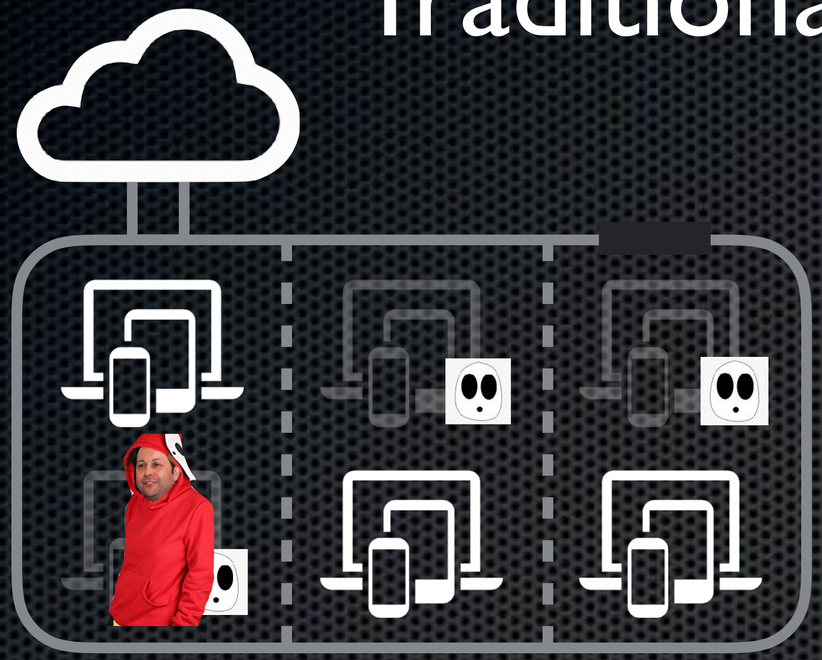
Traditional Network



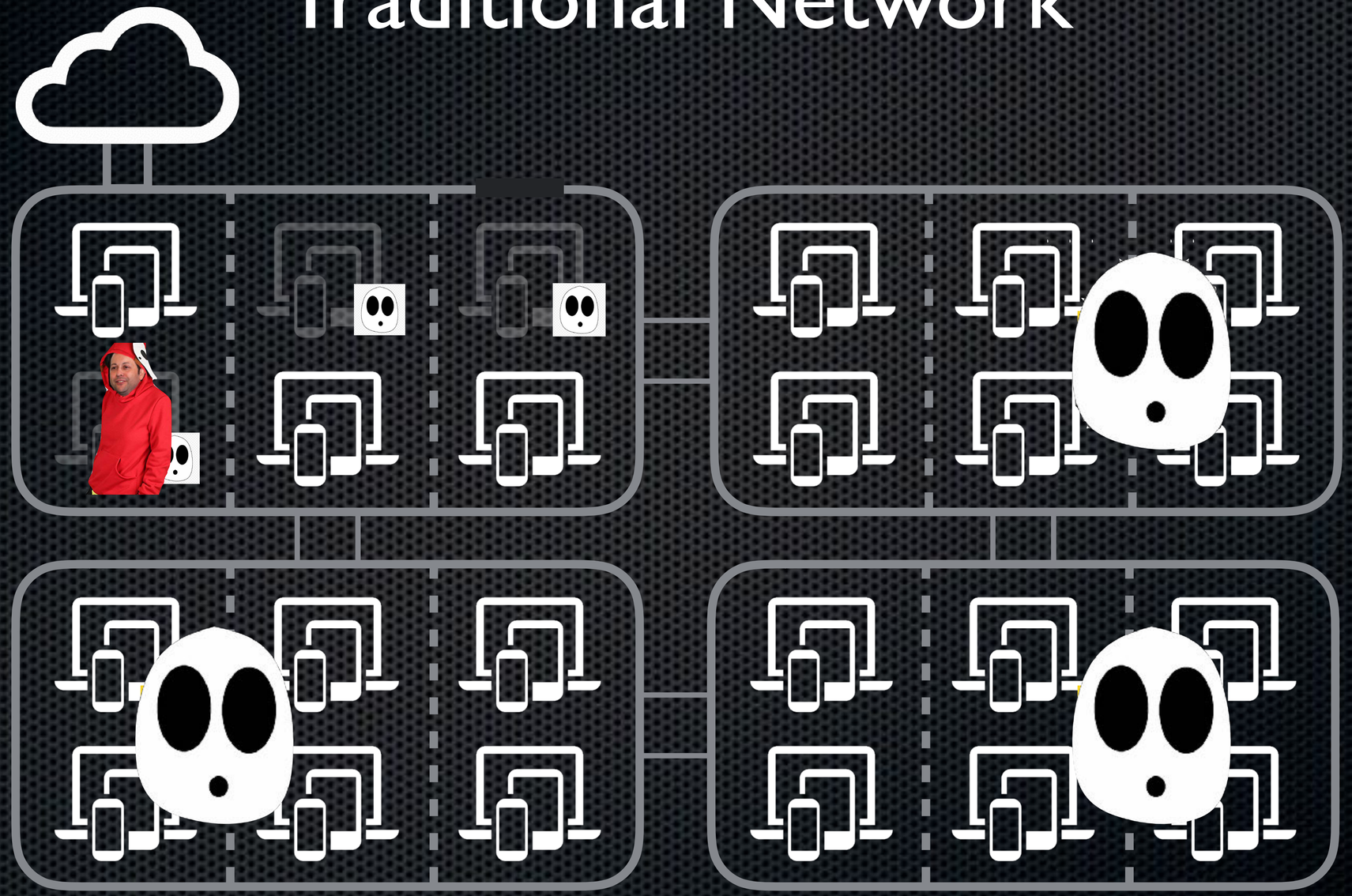
Traditional Network



Traditional Network



Traditional Network



Cost of Cybercrime

$3 Trillion

in 2015

Cost of Cybercrime

$6 Trillion

in 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

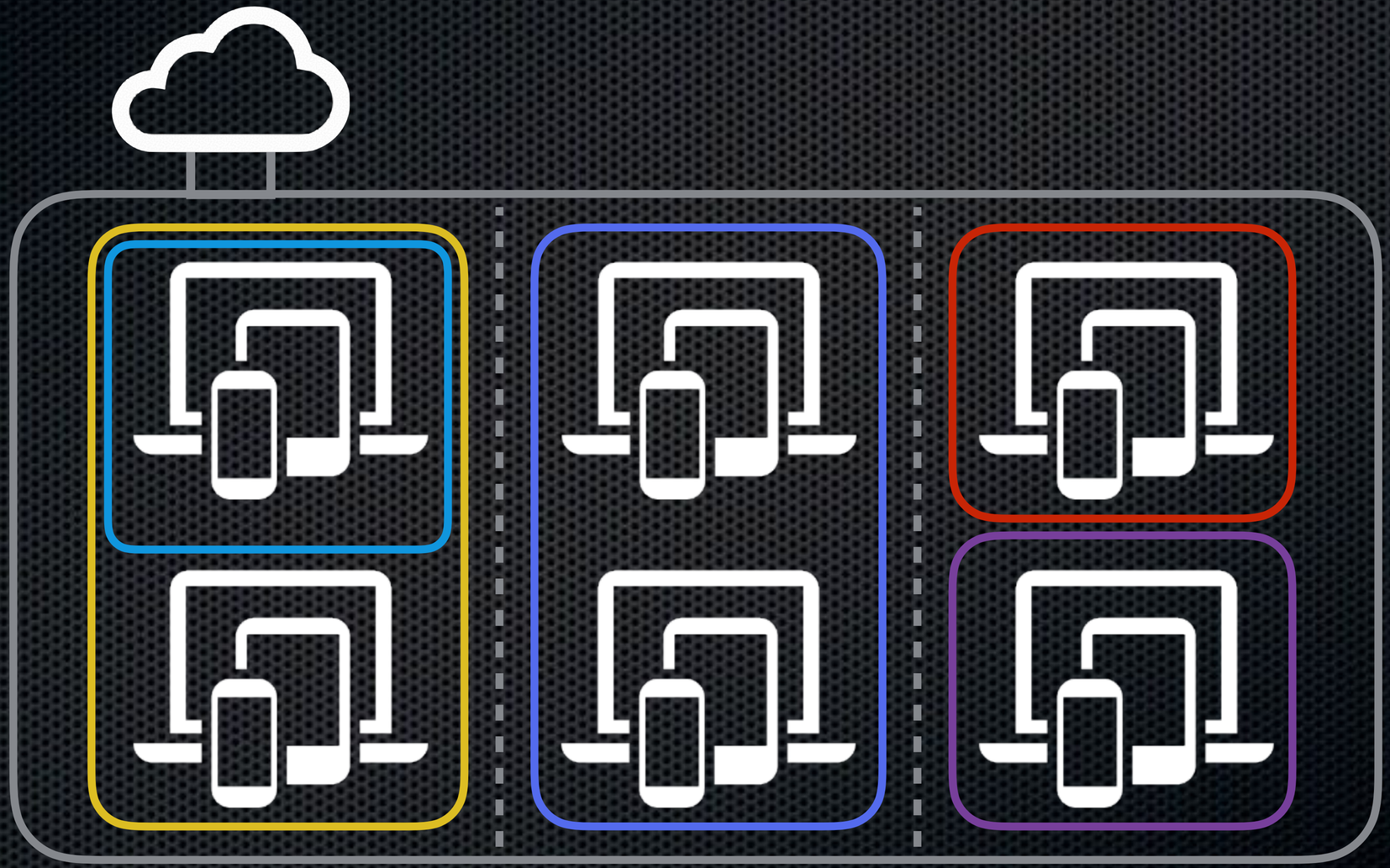
Evade Ownership

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

MACTECH PRO EVENTS

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

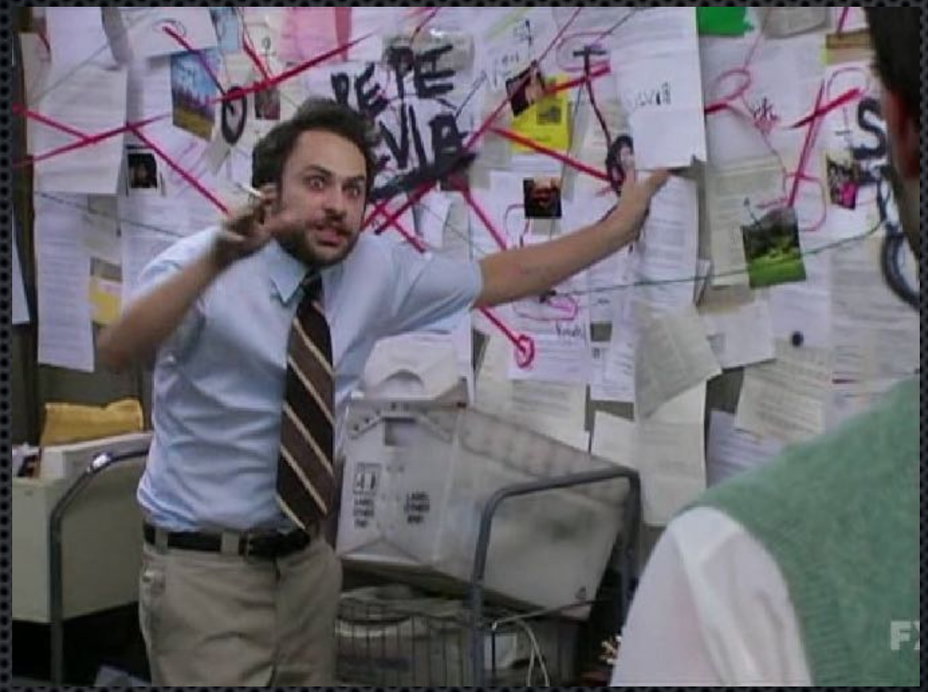
Technology & Processes

- File system permissions

Tech Behind Zero Trust

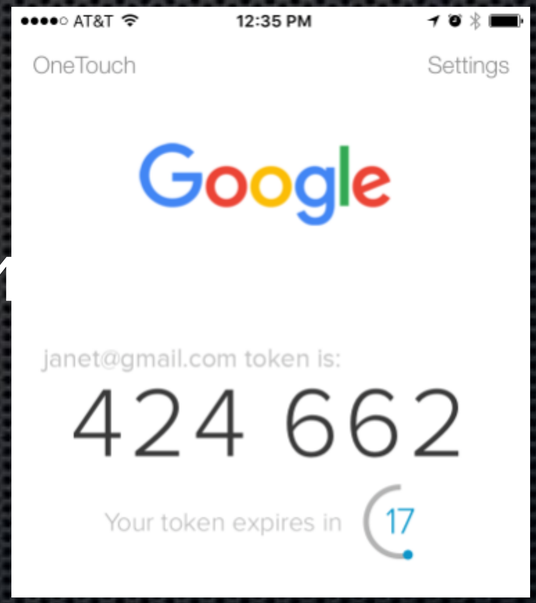
- 802.1x

Getting Started with Zero Trust



Getting Started with Zero Trust

- M tion (M

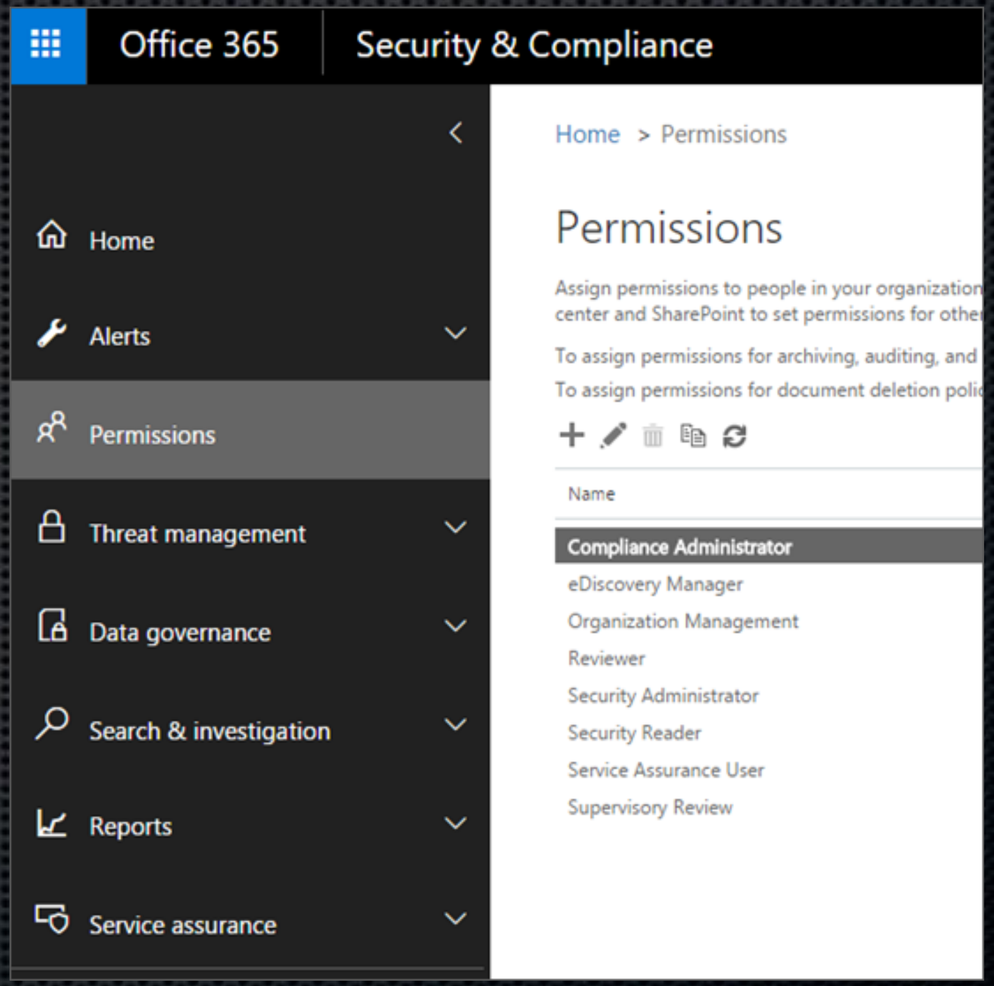


Getting Started with Zero Trust

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

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

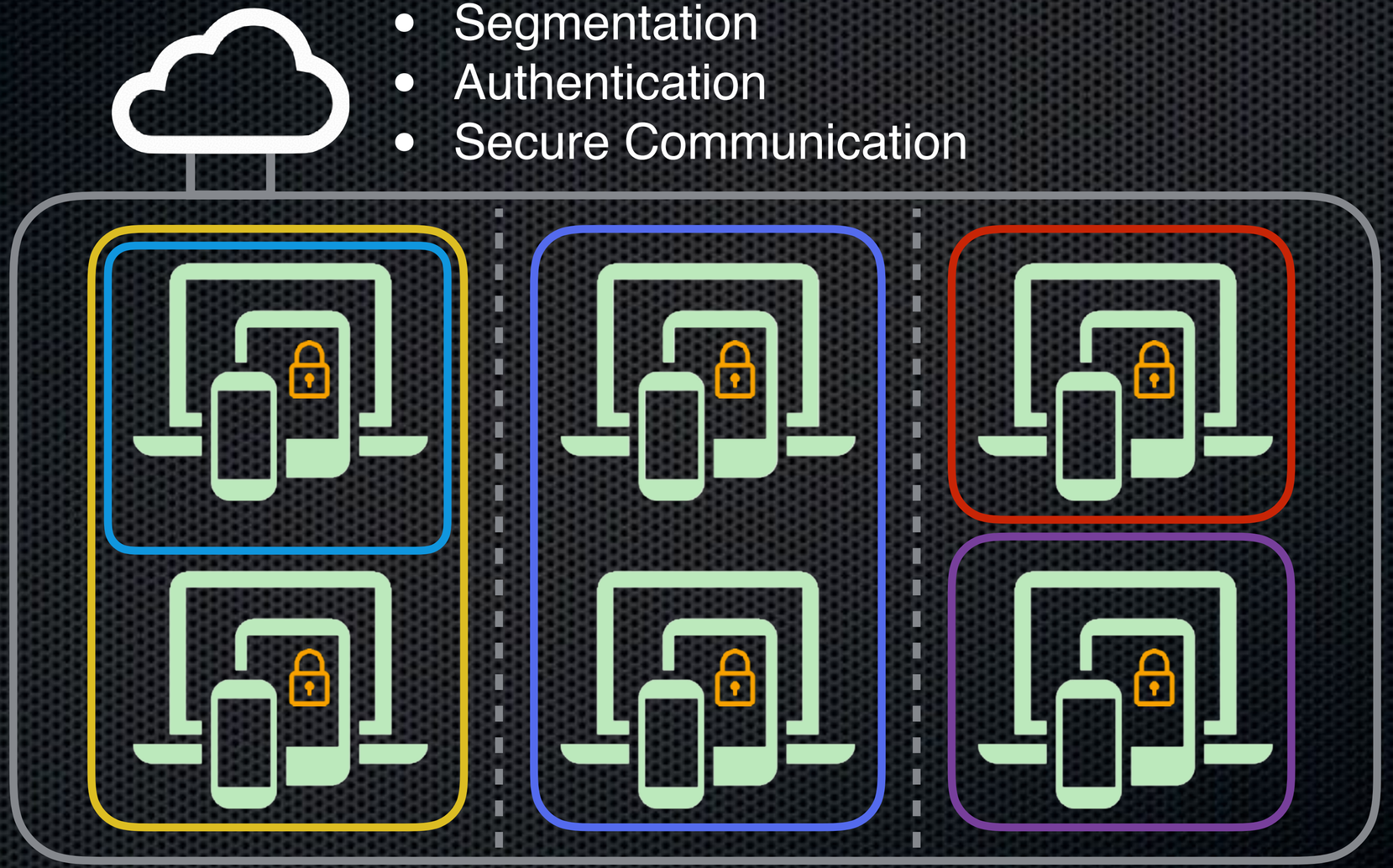
Zero Trust

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

MACTECH PRO EVENTS

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

Questions?

Justin Esgar
justin@virtuacomputers.com

MACTECH PRO EVENTS