Beyond the Buzzwords: The Core Principles of a Zero Trust Model

Aaron Moss
aaron.moss@secureideas.com

Aaron Moss

Senior Security Consultant Secure Ideas, LLC

- Based in Tulsa, OK
- Professional Hacker
- Security Consulting since 2017

Jack of All Trades Master of Maybe A Couple

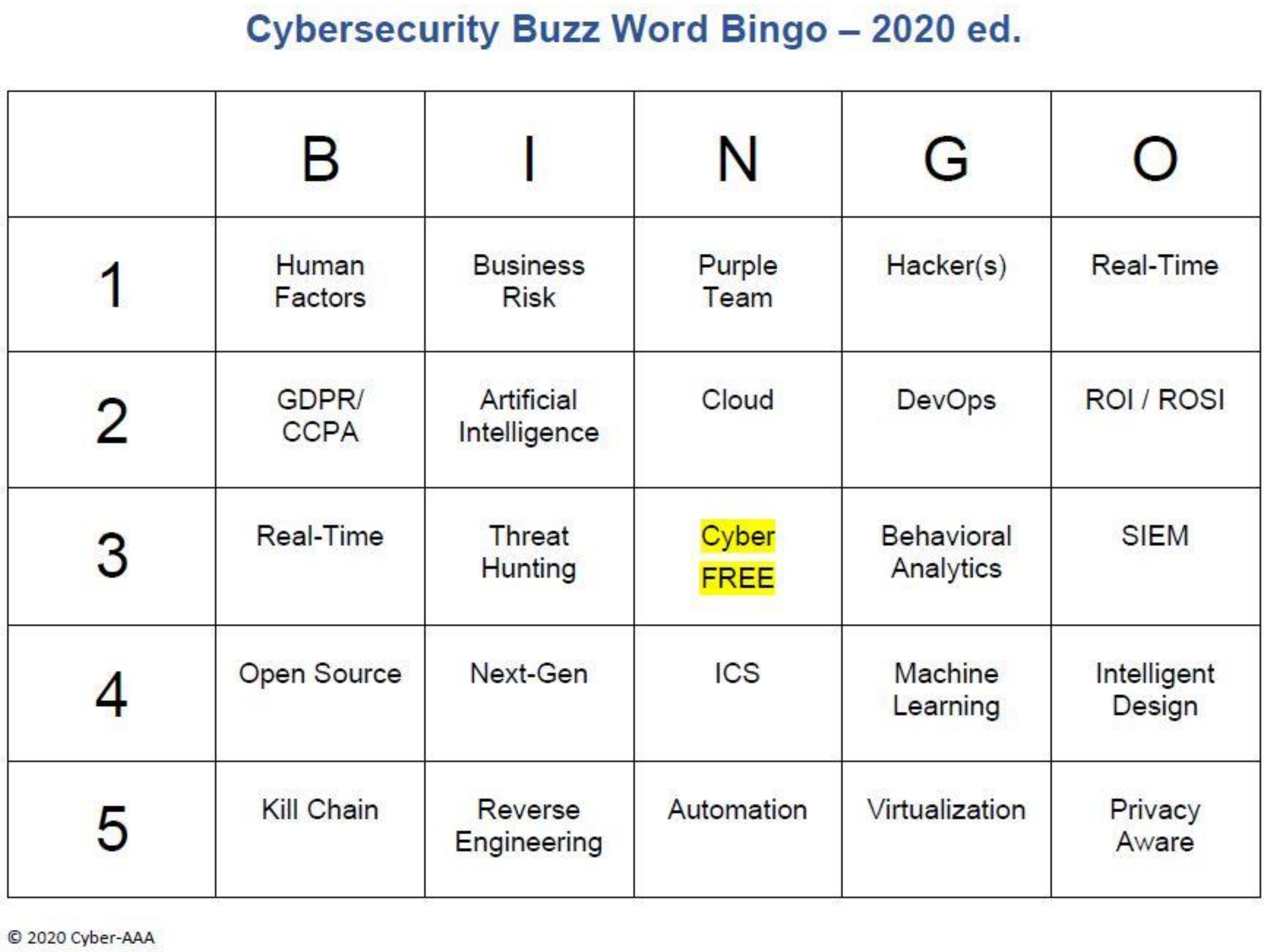
- Helpdesk
- IT Director
- Consulting

Contact

- aaron.moss@secureideas.com
- @hotdogggitty

Secure Ideas professionally evil®

Let’s Dive In



Cybersecurity Buzz Word Bingo – 2020 ed.

	B	I	N	G	O
1	Human Factors	Business Risk	Purple Team	Hacker(s)	Real-Time
2	GDPR/ CCPA	Artificial Intelligence	Cloud	DevOps	ROI / ROSI
3	Real-Time	Threat Hunting	Cyber FREE	Behavioral Analytics	SIEM
4	Open Source	Next-Gen	ICS	Machine Learning	Intelligent Design
5	Kill Chain	Reverse Engineering	Automation	Virtualization	Privacy Aware

© 2020 Cyber-AAA

plain adjective

[plein]

easy to perceive or understand; clear.

"the advantages were plain to see"

synonyms: obvious, clear, crystal clear, as clear as crystal, evident,

pursuant to
substantive
circumvent
remuneratio
Nomenclature
remittance
promulgate
Incentivise
accentuate
Gobbledyg
malfeasance
errone
fiduc
here
mitigatin
disb
xpunge
Verbo
const
Antec
tipula
asce
reda
cogni
omicile
vernacu
ameliorate
eously
notwithstan
Juxtaposition
Non Sequitur

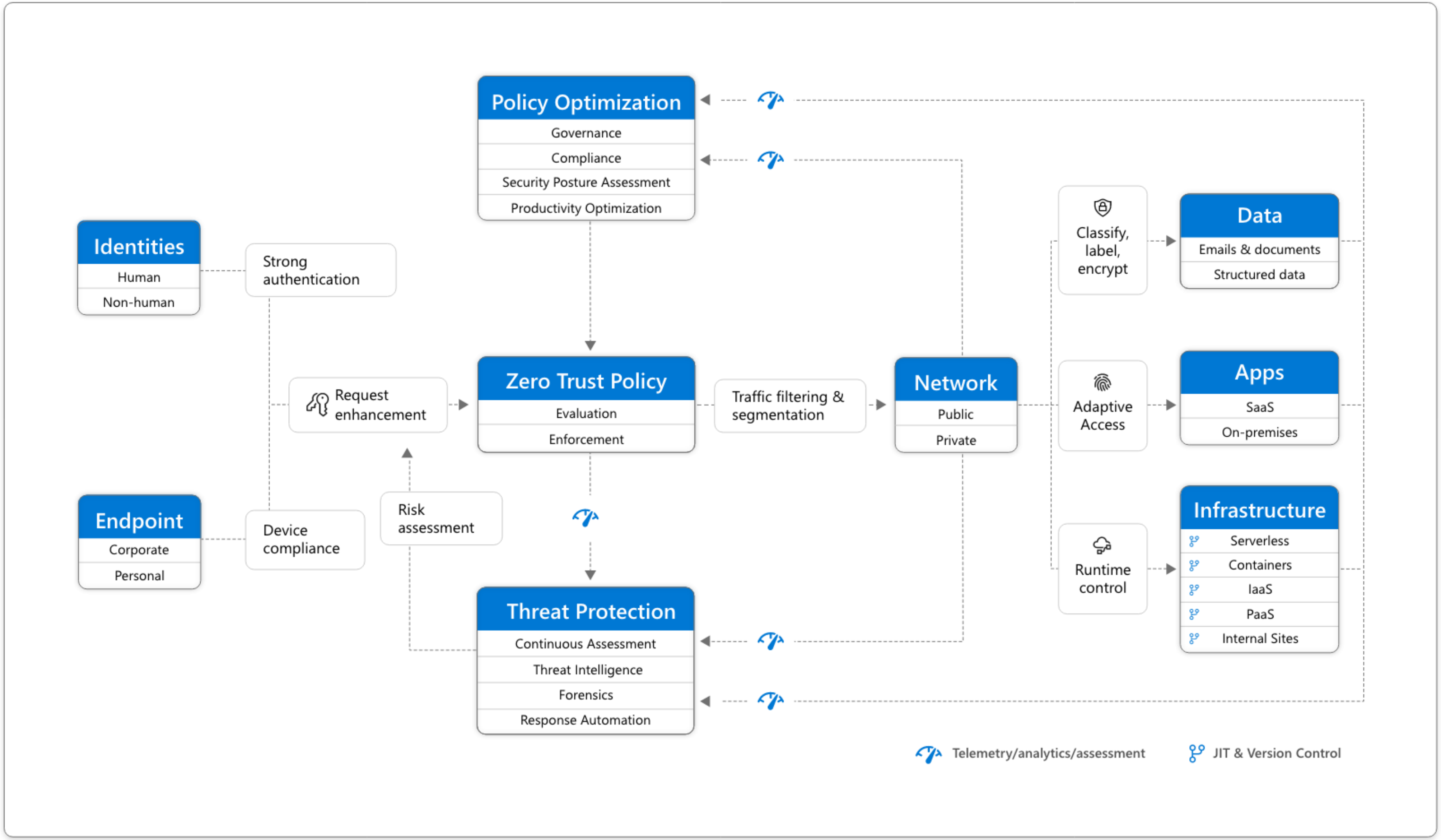
What is Zero Trust?

A security mindset focused on treating every endpoint & service as untrusted by default.

Any Questions?

Thanks for coming!

High Level Diagram



Goals of Zero Trust

Improve security

- Faster Detection & Response
- More Granular Authorization
- Stop Lateral Movement

Lower costs

- Less Infrastructure
- Lower User Support

Enable remote workforce

- Even more important in a pandemic

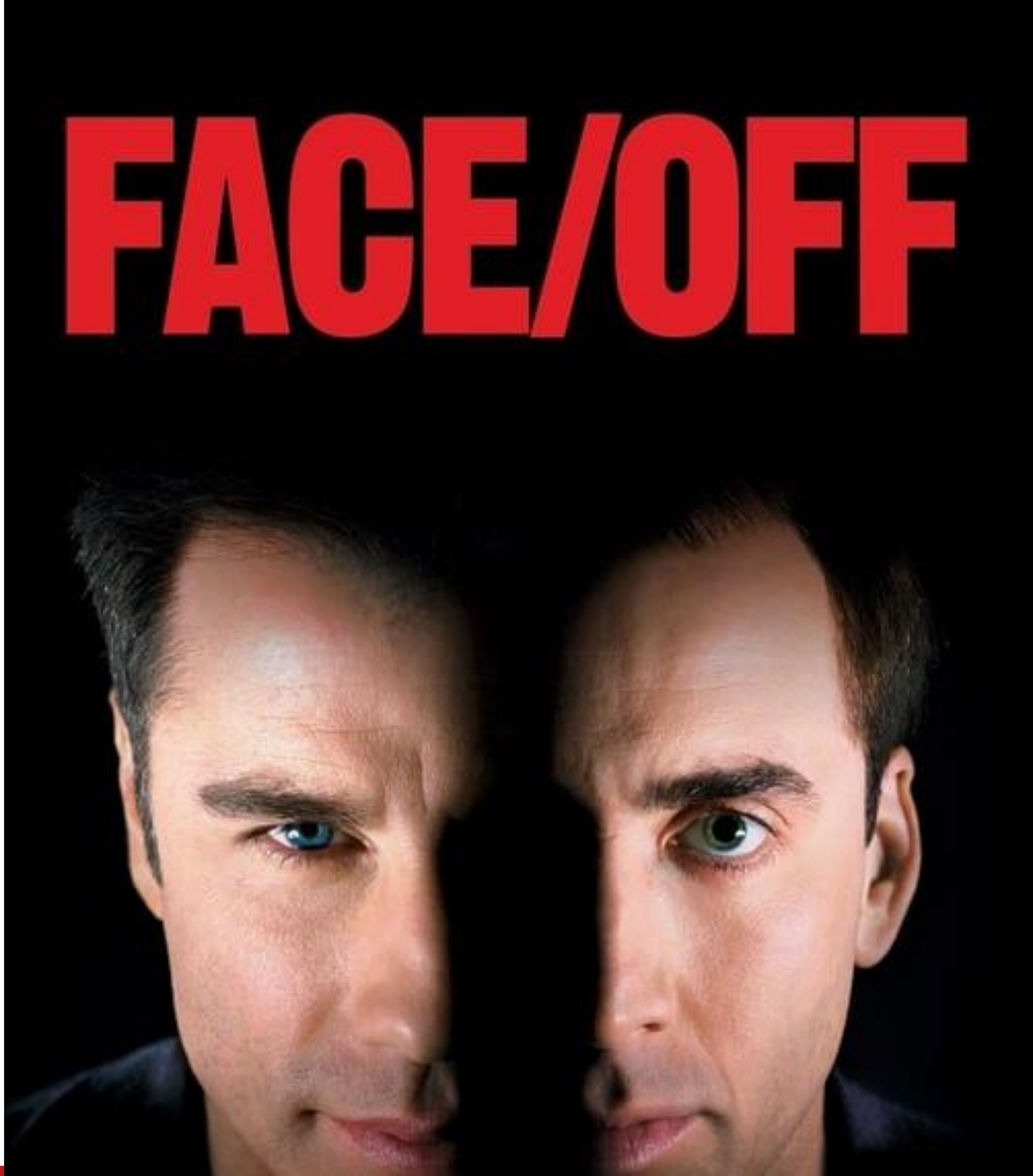
Support BYOD

- Let people use the device they prefer

Reduce central points of failure.

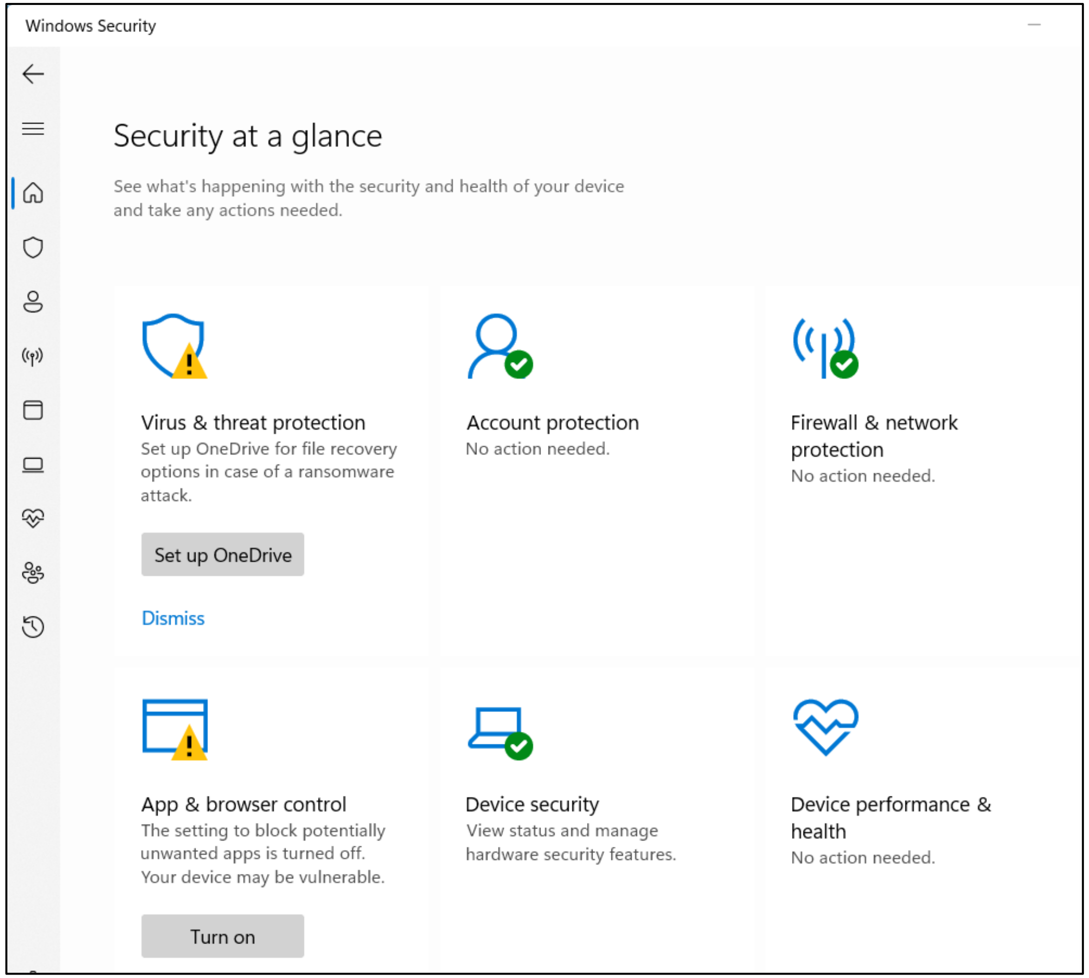
Key Principles of Zero Trust

- Assume Everything is Hostile
  - No More Internal/External
- Default Deny
- Focus on Data/Functionality Access
- Least Privilege
- Cloud Everything
  - Not just “Someone else’s computer.”
- Automation
  - Security Automation, Orchestration, and Response (SOAR)
- Analytics
  - Advanced SIEM
  - Security Metrics



Key Components: Tighter Endpoint Control

- Full Disk Encryption
- Anti-malware
- Application Whitelisting
- Managed & Monitored (EDR/MDR/XDR)
- Behavioral/Heuristic detection
- Content Filtering
- Data Loss Prevention



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
Set up OneDrive for file recovery options in case of a ransomware attack.

Account protection
No action needed.

Firewall & network protection
No action needed.

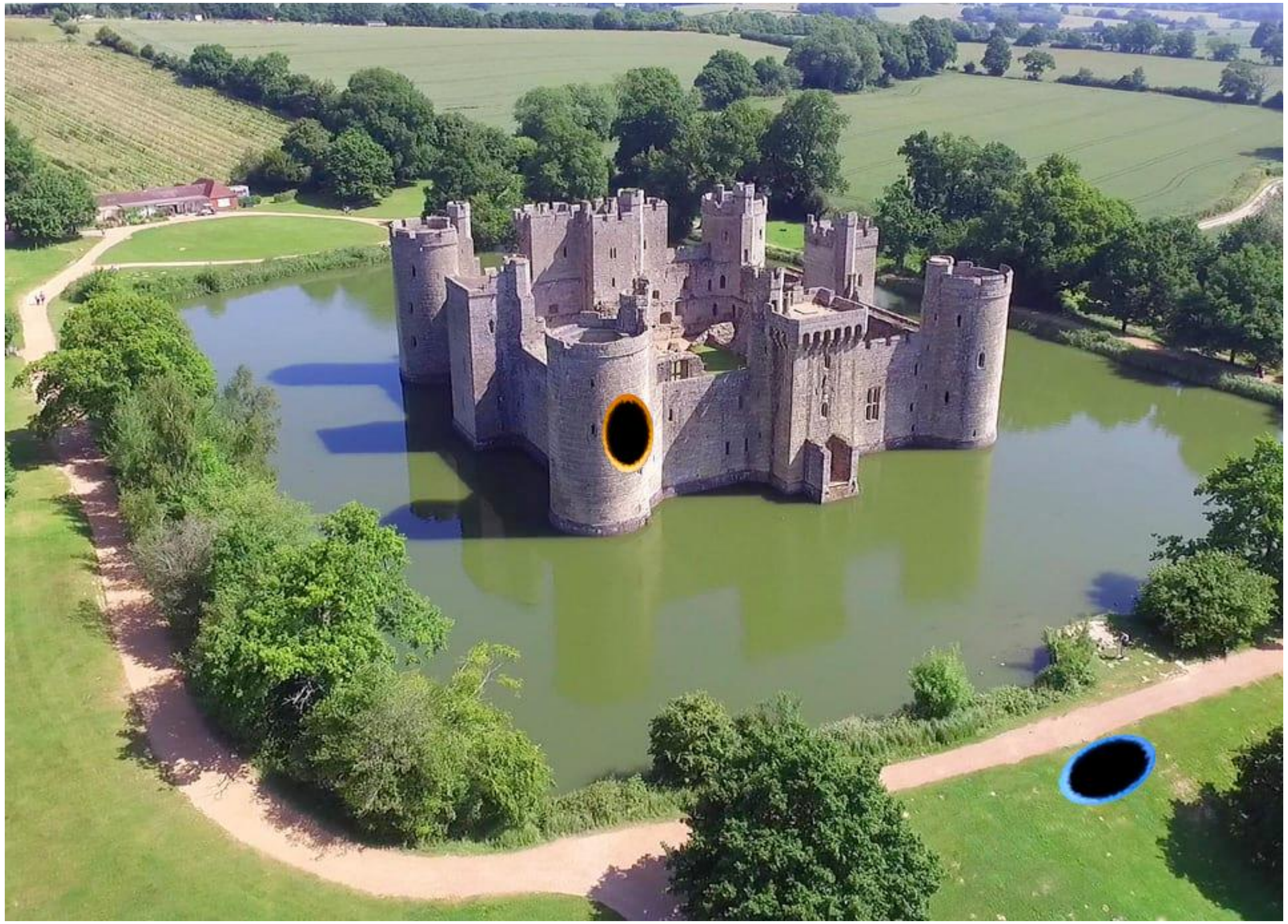
App & browser control
The setting to block potentially unwanted apps is turned off. Your device may be vulnerable.

Device security
View status and manage hardware security features.

Device performance & health
No action needed.

Key Components: Zero Trust Network Access (ZTNA)

- Not your grandma’s VPN
- Adaptive access
- Dynamic permissions (Micro Segmentation)
- Device management (MDM)



Key Components: Real-time Monitoring & Alerting

Key Components: Identity & Access Management (IAM)

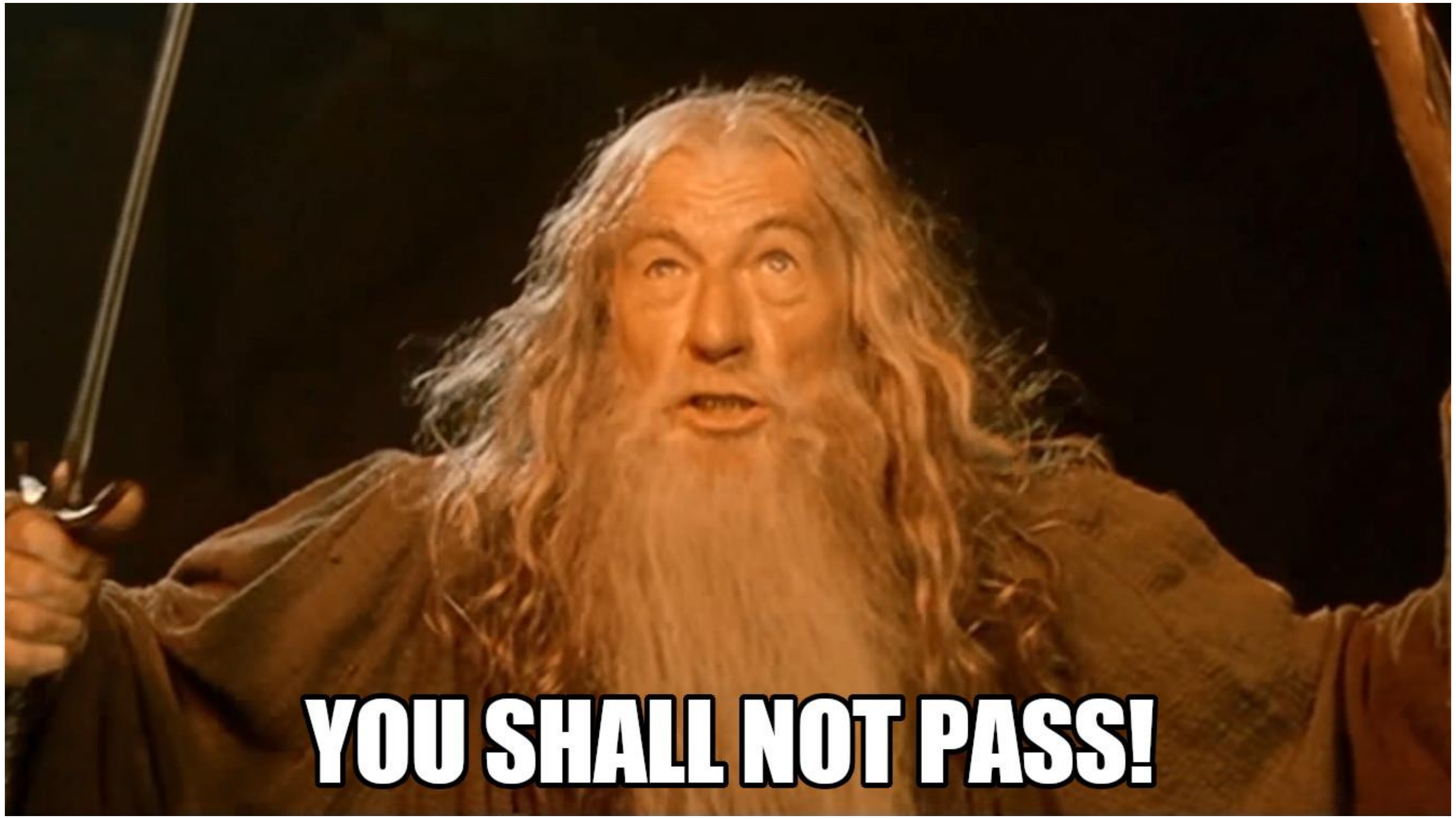
- Authentication AND Authorization
- As critical as machine identification
- Federated Authentication
  - Standardized Systems of Record
  - Fewer Passwords
- MFA (not just two-step auth)
- Correlated Authorization
  - As many data points as possible
  - Location
  - Patch Levels
  - Configuration Compliance
  - Unusual Activity
  - Threat Intelligence Feeds

Key Components: Policy Engine and Enforcement

- Policies
  - Defining what is or isn't allowed

- Realtime Enforcement
  - Automated responses
  - Dynamic, adaptive access

- Dependent on all other datapoints
  - Log data
  - Threat intelligence
  - Behavioral standards
  - The more, the better



Implementing Zero Trust

Requirements

- Plan, Plan, Plan
- Be Realistic
- Detailed, Documented Access Requirements
  - Requires Data Classification
- Plan for Legacy Systems
- LOTS of testing of various components
  - Commoditization will happen eventually

Getting Started: One Approach

1. Focus on monitoring/detection first
   - Distributed systems with no visibility is very bad.

2. Tighten endpoint security
   - Move traditional tools towards host-based solutions rather than perimeter-based.

3. Continue migrating to distributed, cloud-based systems.

4. Document required access & restrict privileges

5. Enforce adaptive access/micro-segmentation
   - Zero Trust Network Access (ZTNA)

Auditing Considerations of ZT Environments

- Are policies well designed and effective?
  - Are there defined goals for each? Do they accomplish the goals?
  - Are there missing policies that should be enforced?

- Are the necessary data points reaching the policy engine?
  - What happens if logs stop arriving?
  - False Negatives are worse than False Positives.

- Are the appropriate tools in place and working together properly?
  - Security tools may not integrate as well as the salesman promised.

- As an environment shifts towards Zero Trust, are the new controls sufficient to relax more traditional security controls?
  - Understand the roadmap & what each control is intended to do.
  - Requires careful coordination with IT.

Any Questions?

(For real this time)

Aaron Moss
aaron.moss@secureideas.com