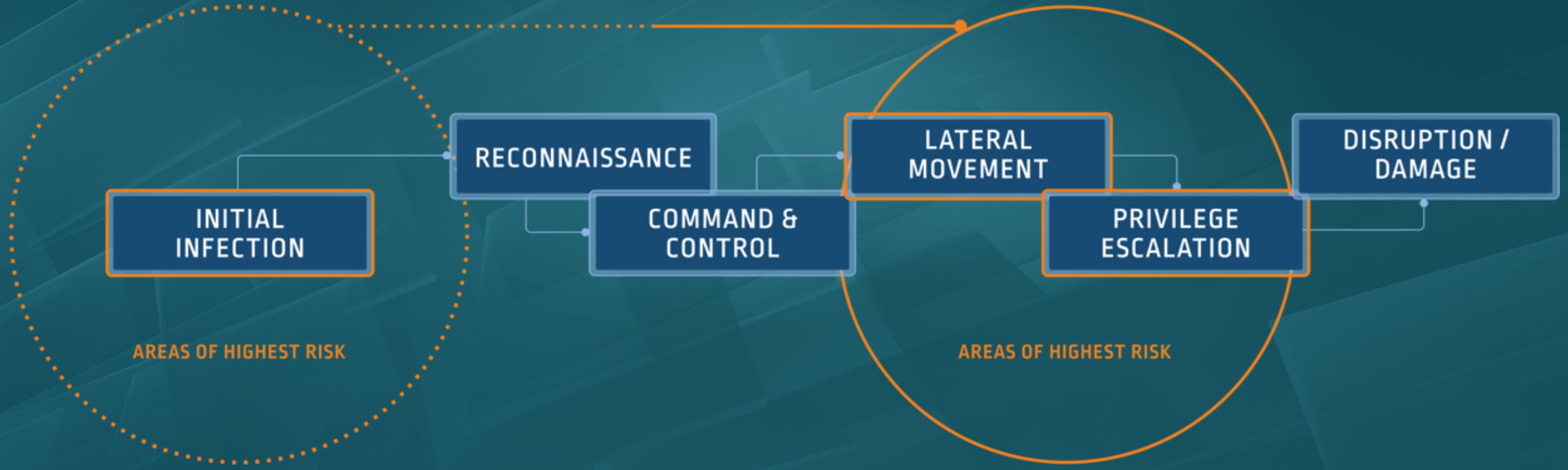
CYBERARK®

HOW TO STAY ONE STEP AHEAD IN AN ASSUME-BREACH WORLD

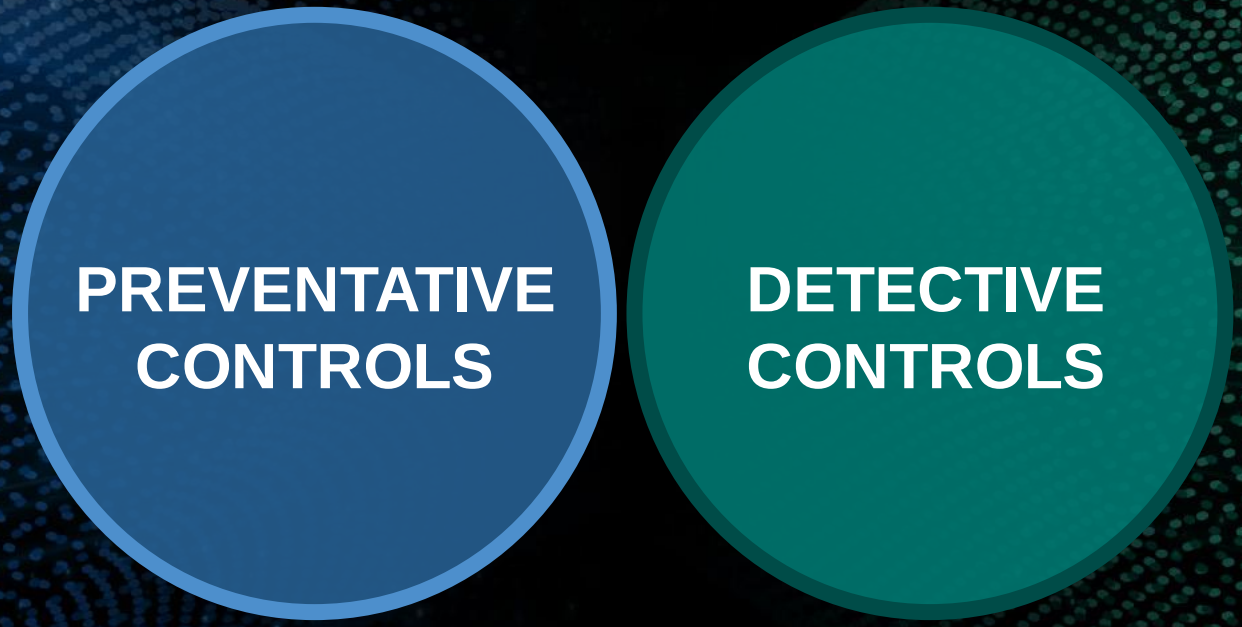
Andy Thompson, CyberArk Labs Research Evangelist

THE ATTACK PATHWAY



THERE'S NO SILVER BULLET

DEFENSE IN-DEPTH



SOLARWINDS BREACH: ZEROING IN

"We believe for any solution to be effective; prescriptions must apply a **"zero trust" presumption**, **access provided on a least privileged basis**…"

SolarWinds CEO Sudhakar Ramakrishna

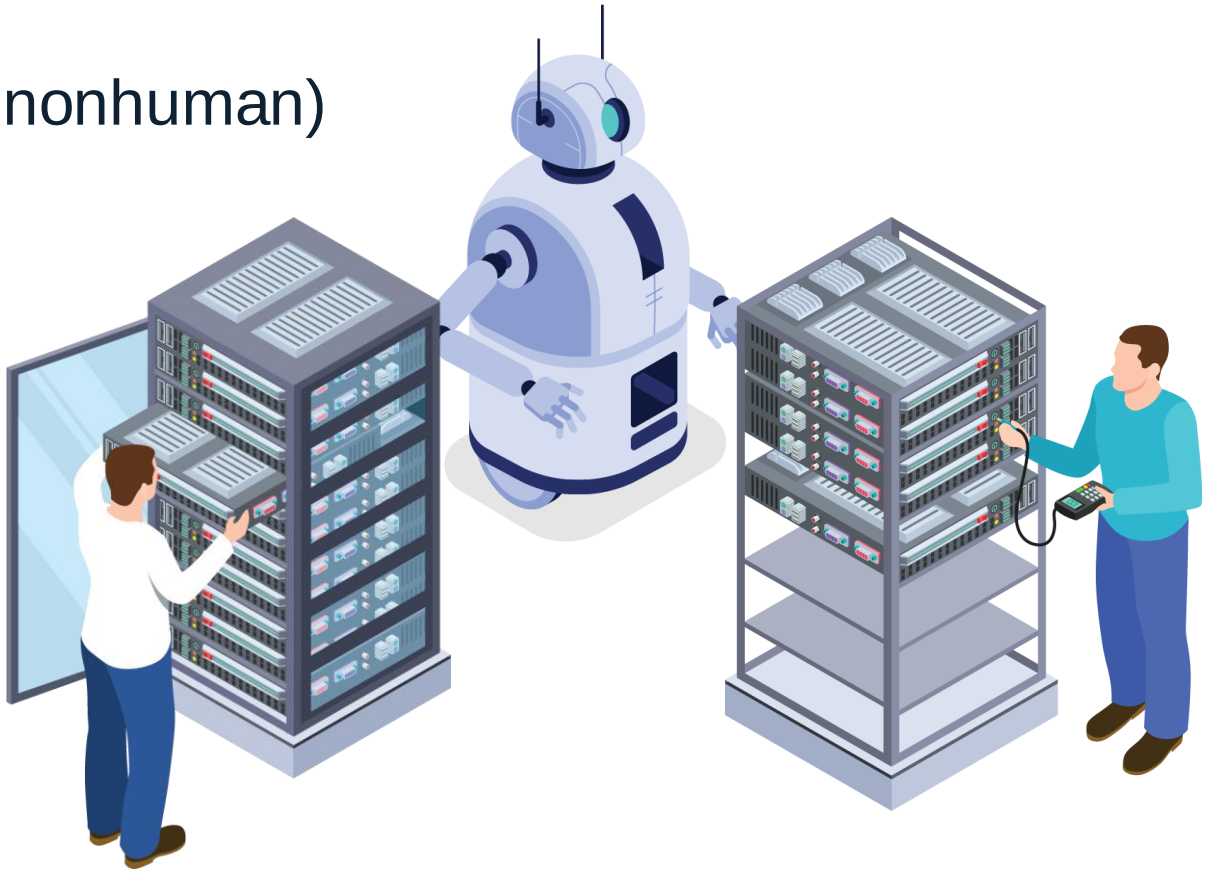
U.S. Senate Testimony – February 23, 2021

ENDPOINT DEFENSE

- Least privilege and application control
- Complement to AV/XDR
- Deception technology

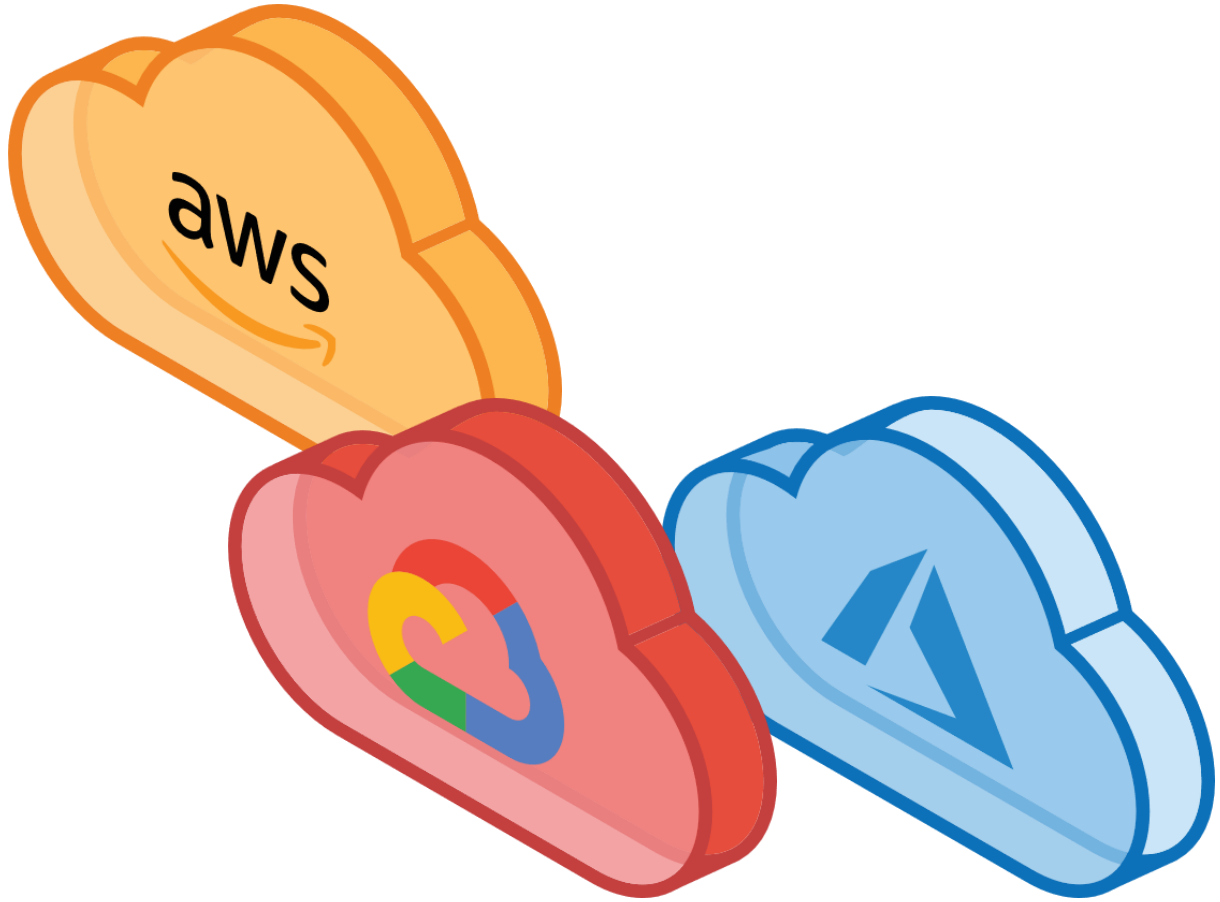
ON-PREM DEFENSE

- Credential management and key rotation
- Session isolation
- Service Account Management (RPA and nonhuman)



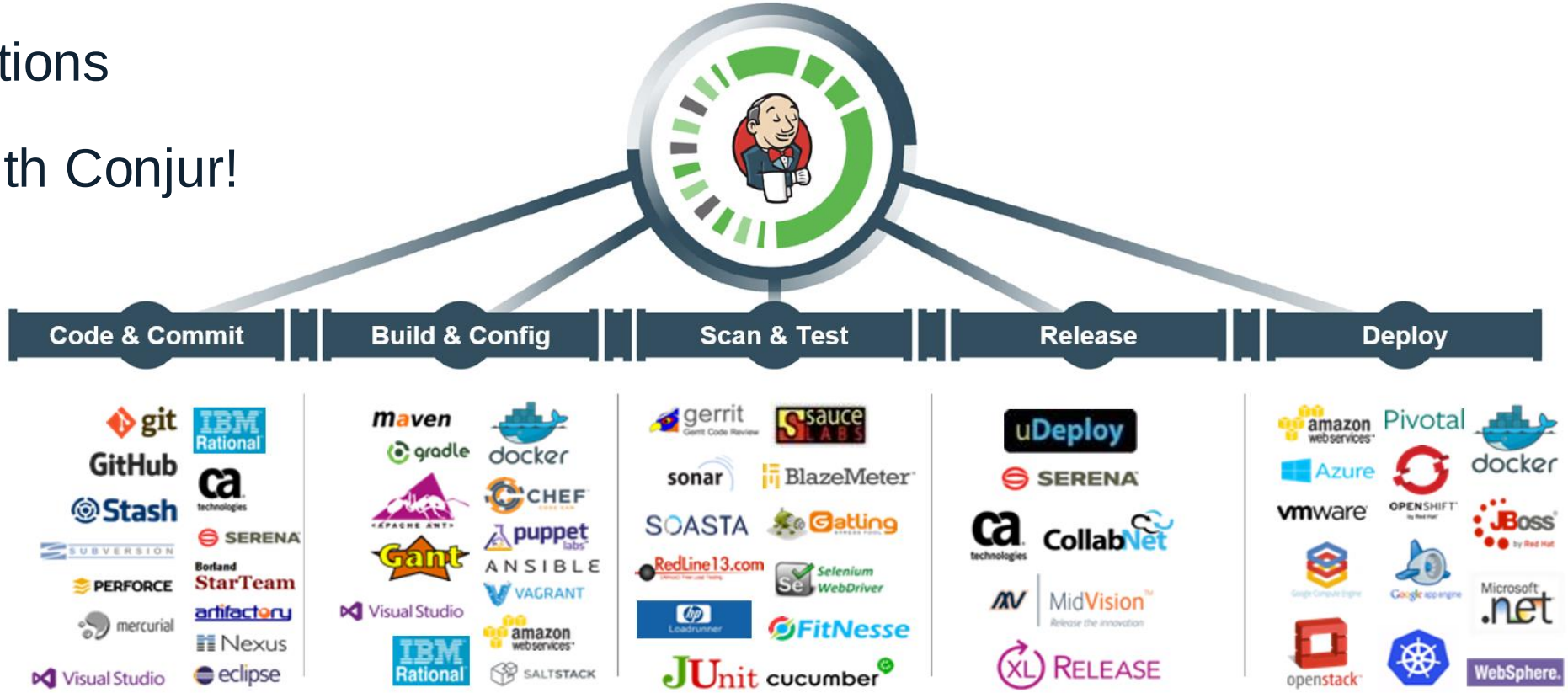
CLOUD DEFENSE

- Console management (PSM)
- Least privilege (CEM)
- Container security (k8 <3)



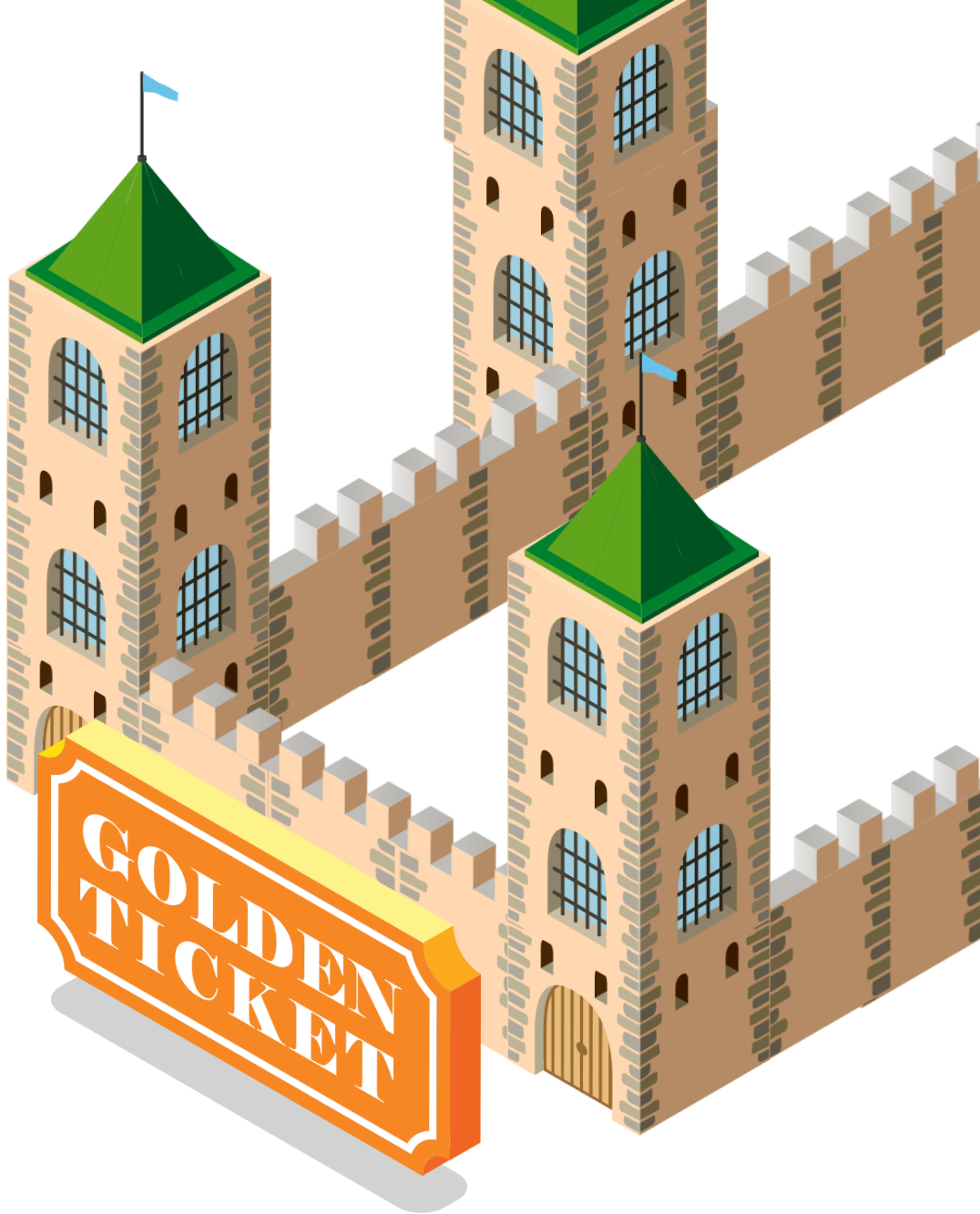
CI/CD DEFENSE

- Prioritize orchestrators
- Isolate high privileged sessions
- Developer workstations
- Manage secrets with Conjur!



FORTRESSING TIER 0

- Domain controllers
- ADFS/SAML federation (Golden SAML)
- Tier0 business continuity



HOW WILL YOU RESPOND TO A *PRIVILEGED* BREACH?

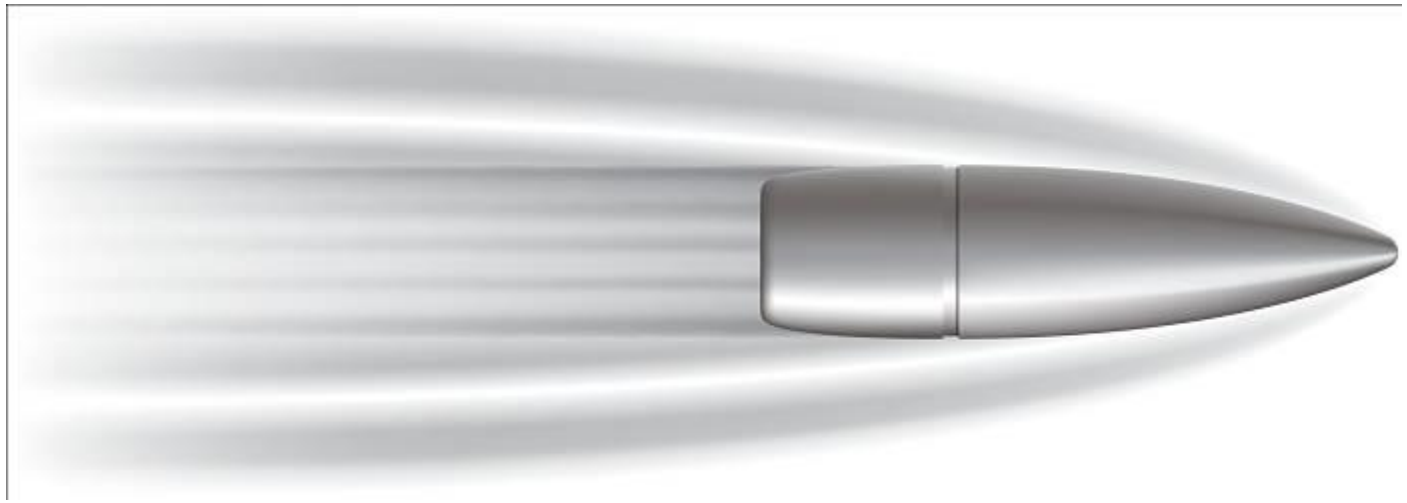
CYBERARK

THANK YOU


CYBERARK
BACKUPS

The Silver Bullet

- There is **no** silver bullet.
- CYBR will buy invaluable time.
- Detecting attacks earlier.
- Preventing attackers from theft or disruption.



AB –definition

Mentality that should be adopted by all security practitioners from c down based on enforcing LP which is instrumental to App trust.

First present attack pathway

What is the assumed breach AB mentality?