VERSATILITY

When Cyberattacks Happen at AI Speed

Closing the Cybersecurity Speed Gap

Booz Allen

Booz Allen

WHAT WE'LL COVER

BLUF

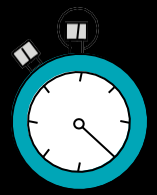
Michael Lundberg, Booz Allen Hamilton's VP of Defensive Cyber Solutions

- Today's prevailing cybersecurity narrative suggests that AI gives attackers a lasting advantage.
- In practice, the advantage accrues to whichever side can operate faster, attacker or defender.
- A prepared defense can see detection happen in seconds and containment begin while an intrusion is still unfolding.
- Organizations can take back some of the AI-speed advantage if they are willing to change how they defend.

CHALLENGE

The Cybersecurity Speed Gap

Activities that once unfolded over days now take minutes, and, in some cases, seconds.



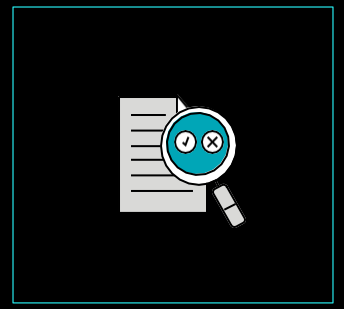
Average time from initial access to lateral movement has fallen below 30 minutes, with the fastest cases measured in seconds.

This is the cybersecurity speed gap—now the primary factor shaping security outcomes.

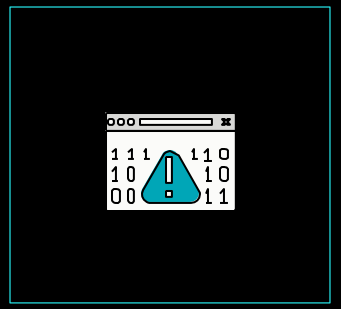
CHALLENGE

Why Traditional Defense Models Fail

Perimeter and centralized defenses are still the norm.



Logs are either dropped or not analyzed due to scale, complexity, and cost.



Identifying and patching CVEs takes weeks.

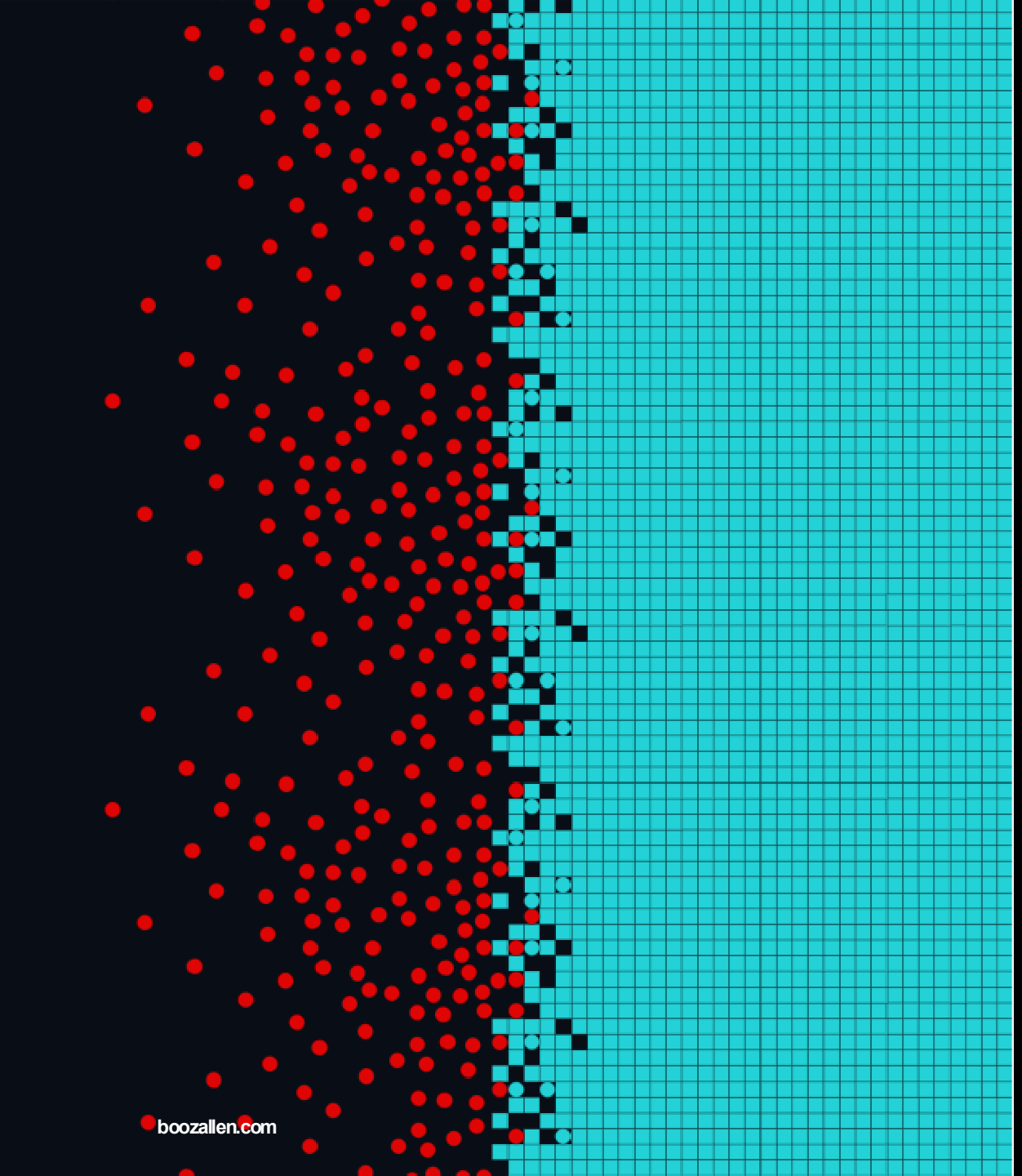
SOLUTION

Strategy Overview: Three Shifts to Operate at AI Speed

Attack to Defend

AI-Enabled Cyber Operations

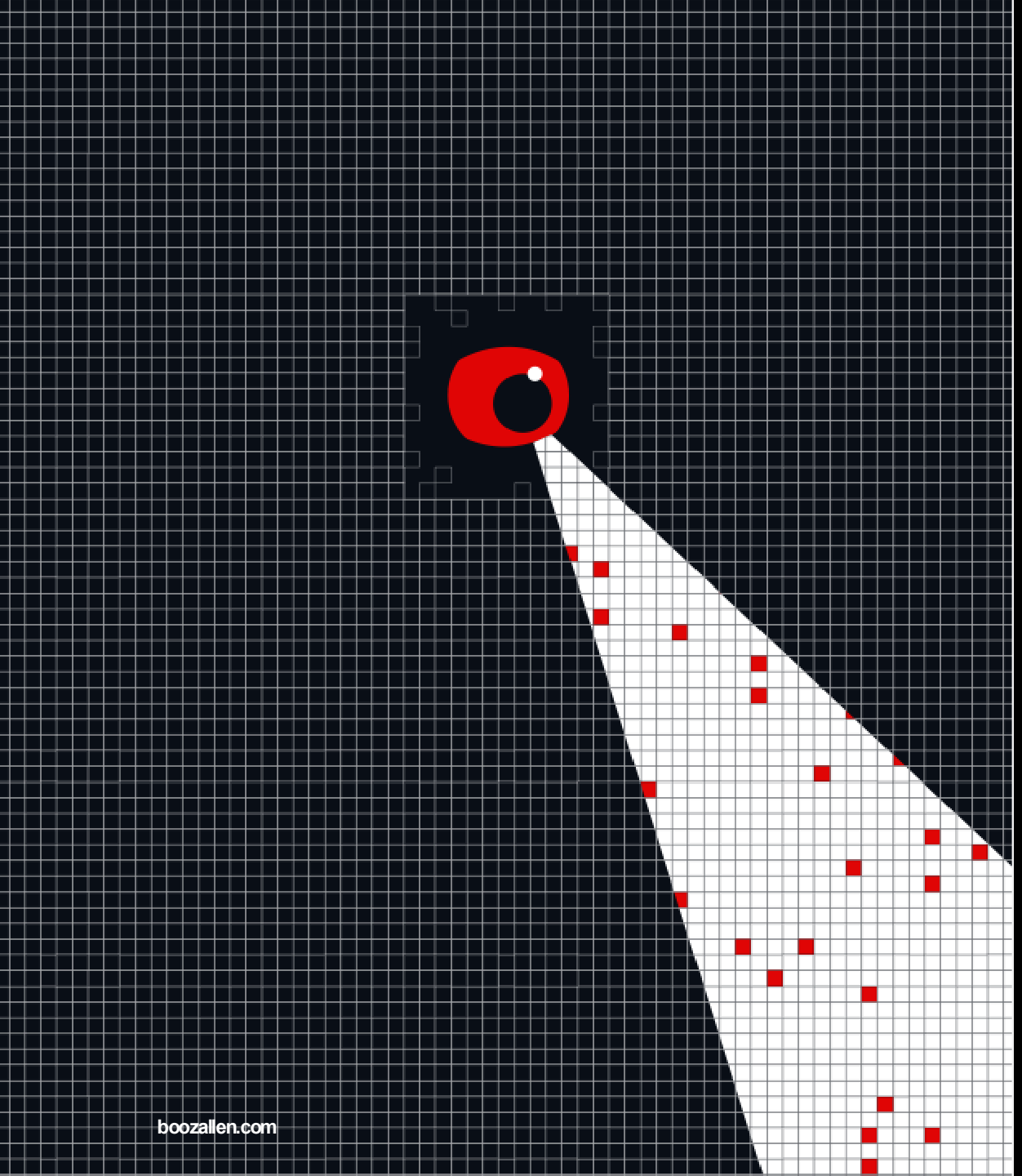
Advanced Zero Trust Architecture



CLOSING THE SPEED GAP

Strategy 1: Attack to Defend

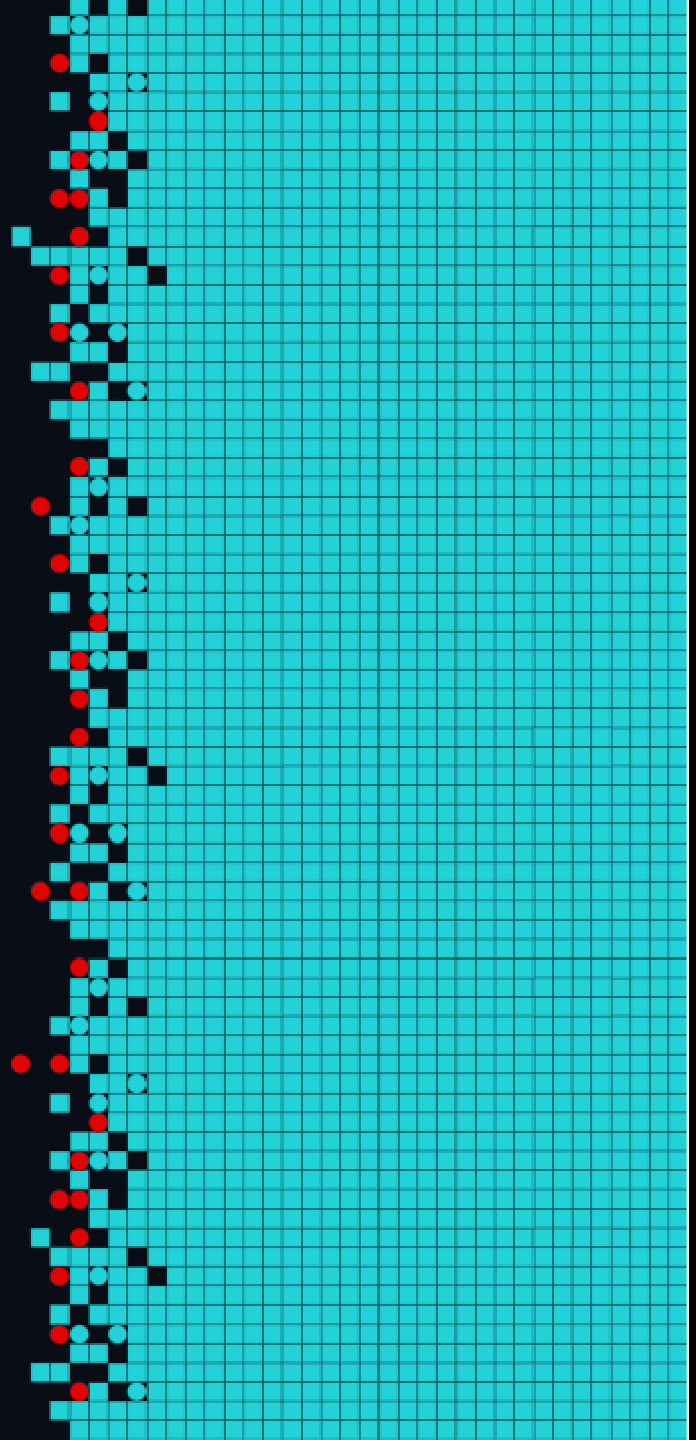
- Shift from reactive patching to continuous, AI-driven discovery of vulnerabilities.
- Use AI-driven techniques to continuously test internally and externally to identify weaknesses before attackers can.
- Dynamically develop detections tailored to a given environment (Vellox Ranger), reducing overhead and noise for analysts and automation.



CLOSING THE SPEED GAP

Strategy 2: AI-Enabled Cyber Ops

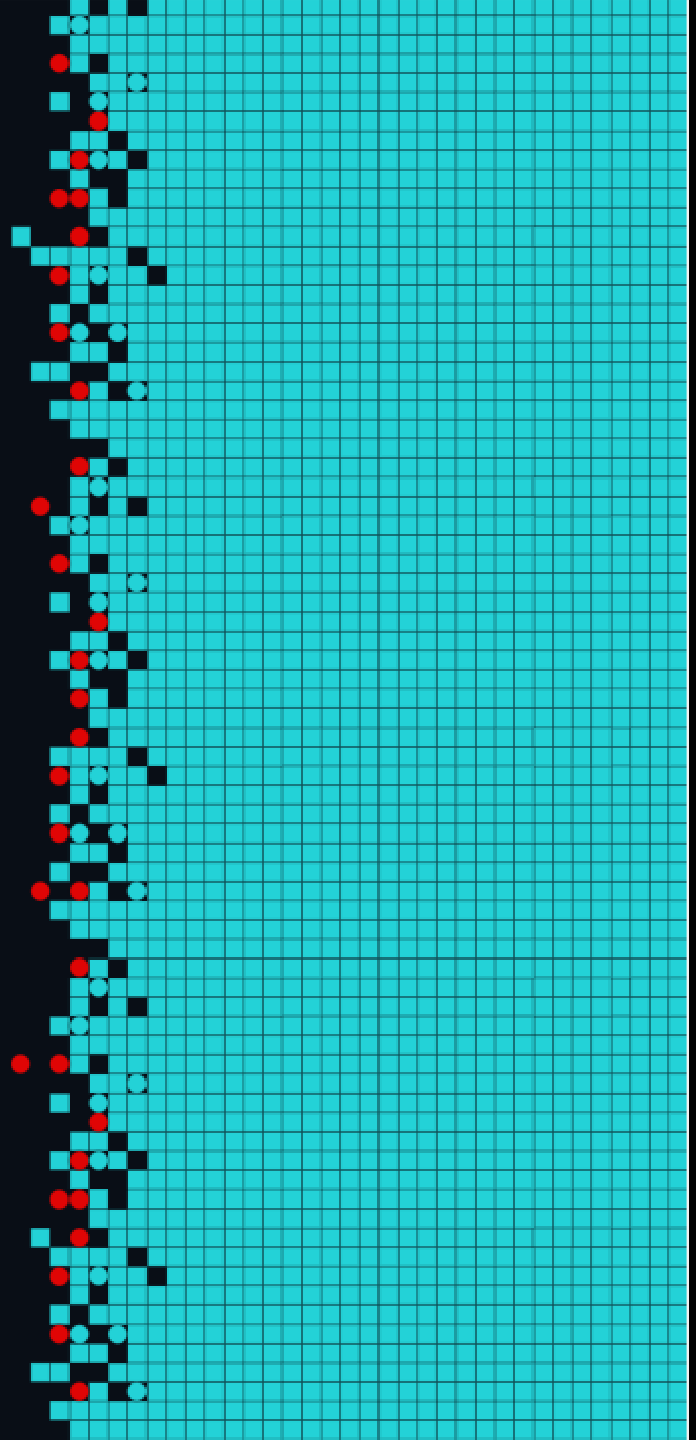
- Develop a solid foundational data pipeline and distributed analytic fabric.
- Define in advance which containment measures can be executed automatically and under what conditions.
- Shift from manual response to automated, detection, and containment.
- Orchestrate cyber operations via AI.



CLOSING THE SPEED GAP

Strategy 3: Advanced ZTA

- Machine identities now outnumber human users by as much as 80 to 1…Without strict controls, they create new pathways for attackers.
- API- and AI-security are essential for protecting against shadow IT and legitimate interactions.
- Advanced micro-segmentation limits the blast radius of an attack by restricting how far an attacker can move and what they can access.
- Shift from implicit trust to continuous verification and least privilege access.



CLOSING THE SPEED GAP

Vision Forward & Call to Action

- The gap is no longer defined by capability. It is defined by execution.
- Organizations must decide in advance how quickly they are willing to act… and how much disruption they are prepared to accept to reduce exposure.
- Cybersecurity is now defined by time. Attackers already operate at AI speed. Defenders need to meet them there.

VERSATILITY

Q&A

VERSATILITY

Thank you