TYTO Athene

RAVID

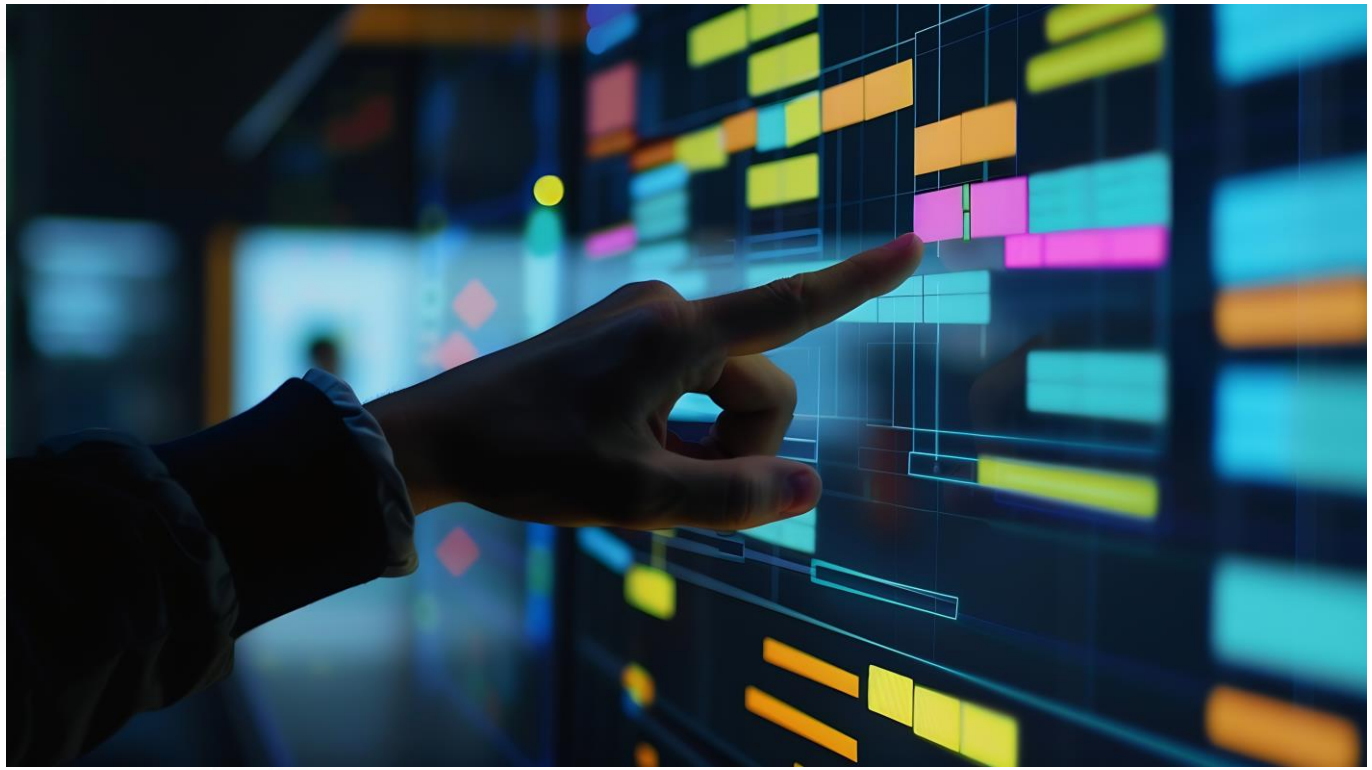
(Randomized Automated Virtual Infrastructure Defense)

AN END-TO-END AUTOMATED, STEALTH, MOVING TARGET DEFENSE ARCHITECTURE

Preparing for the future of Cyber Warfare

INNOVATION THROUGH INTEGRATION

- Everything we are describing exists now.
- We aren’t ripping and replacing, we are integrating and orchestrating virtual overlays that are commanded via APIs.
- This architecture allows for full decentralization across any cloud or on-prem instance.
- The RAVID architecture helps realize a cost savings across one, or many organizations.



RAVID

AN END-TO-END AMTD APPROACH

Think of “Cyber and “Infrastructure” as the digital battlefield and apply the lessons learned

A Fully Stealth Infrastructure:

Your network and apps are fully invisible and Non-Routable from the Internet.

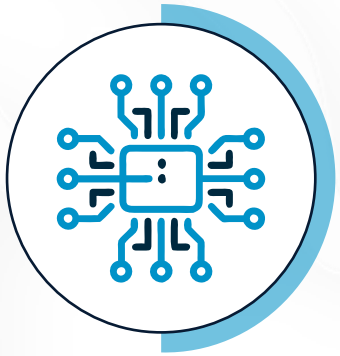
A Fully Automated Moving Target Defense:

The Network, The Applications, and The Infrastructure change to a moving target, fully orchestrated. Resilient, redundant, optimized, and secure.

TYTO Athene

RAVID

AN END-TO-END-AMTD APPROACH



Network

Infrastructure

Applications

HARVEST NOW, DECRYPT LATER

Antiquated, point-to-point networking solutions are no longer secure, or performant. VPN's or "Tunnels" can be attacked, captured, and broken at the nation state level.

HNDL attack – (Harvest Now, Decrypt Later)

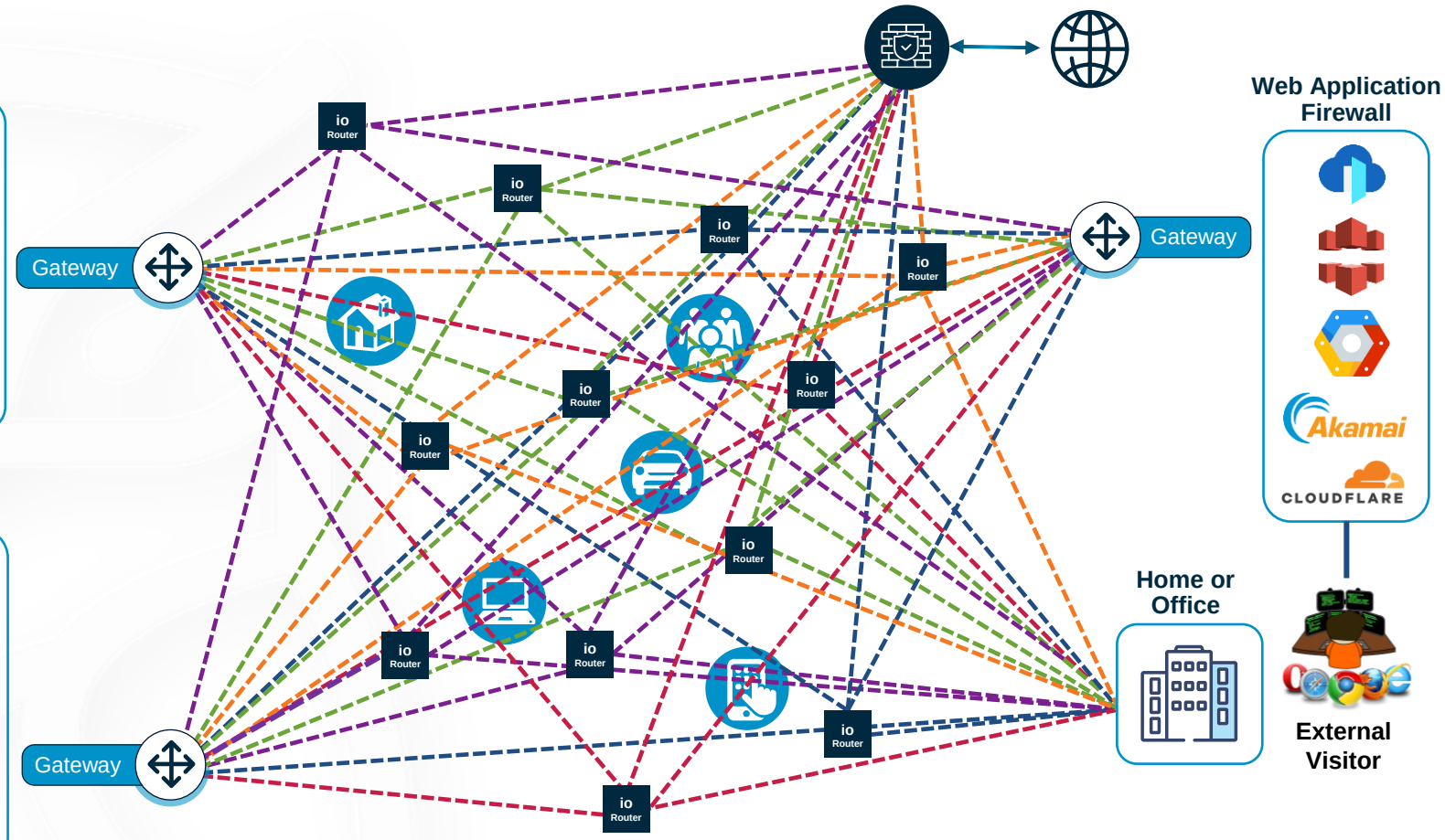
Don't treat the symptoms, treat the cause.

TYTO Athene

CYBER BATTLEFIELD

THE NETWORK

- The Network is no-longer an attack vector, but instead the first line of defense, providing a CLOAKING effect to the infrastructure.



THE CYBER BATTLEFIELD

ACTIVE FAILOVER: SPINNING RECOURSES UP AND DOWN AT RANDOM

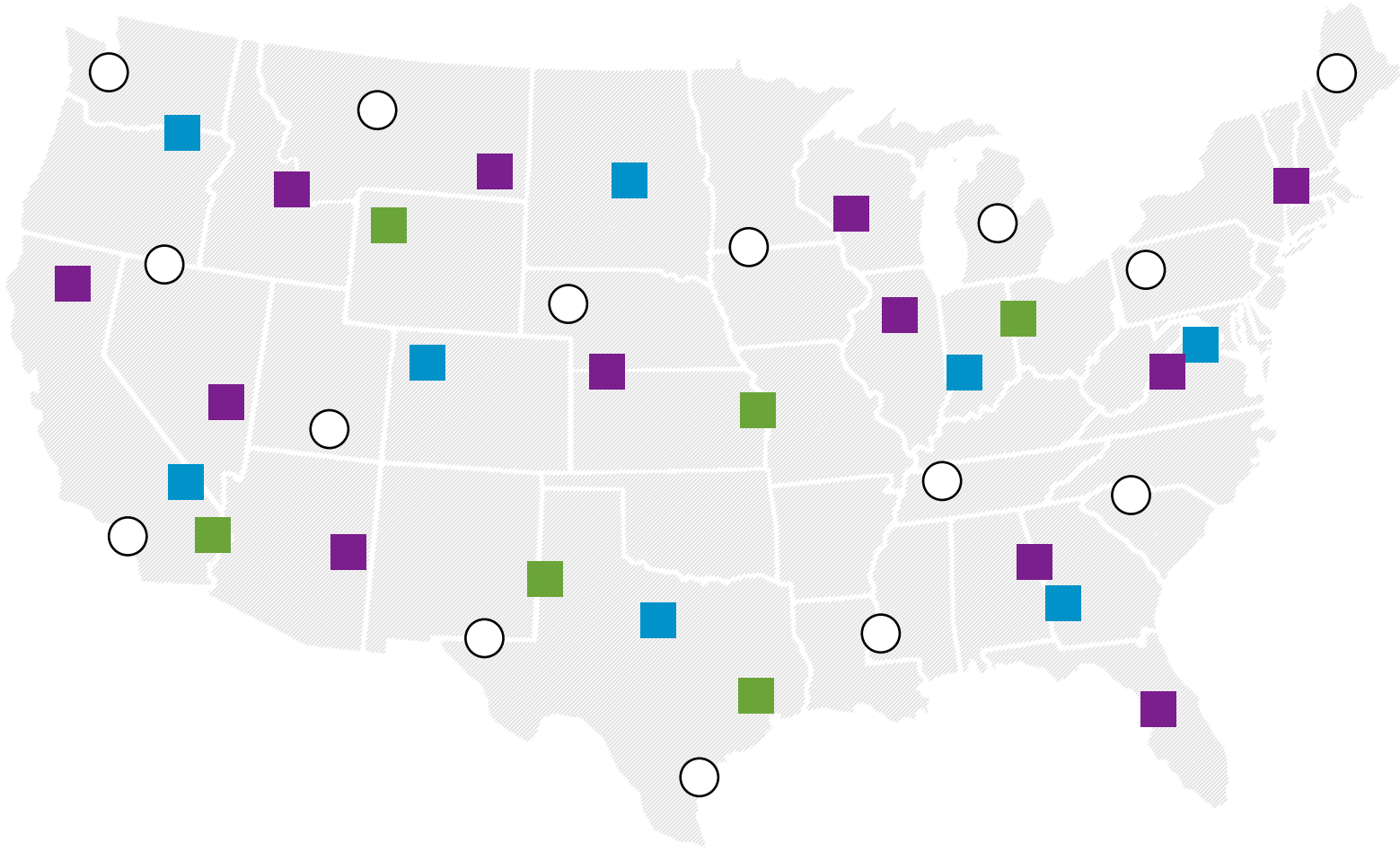
- Virtual resources only exist for a limited amount of time, before “failing over” to a new location within cyberspace.

Reference Node

Compute

IO Storage

Virtual Network Packet Router



AMTD
DYNAMIC VIRTUAL INFRASTRUCTURE (DVI)

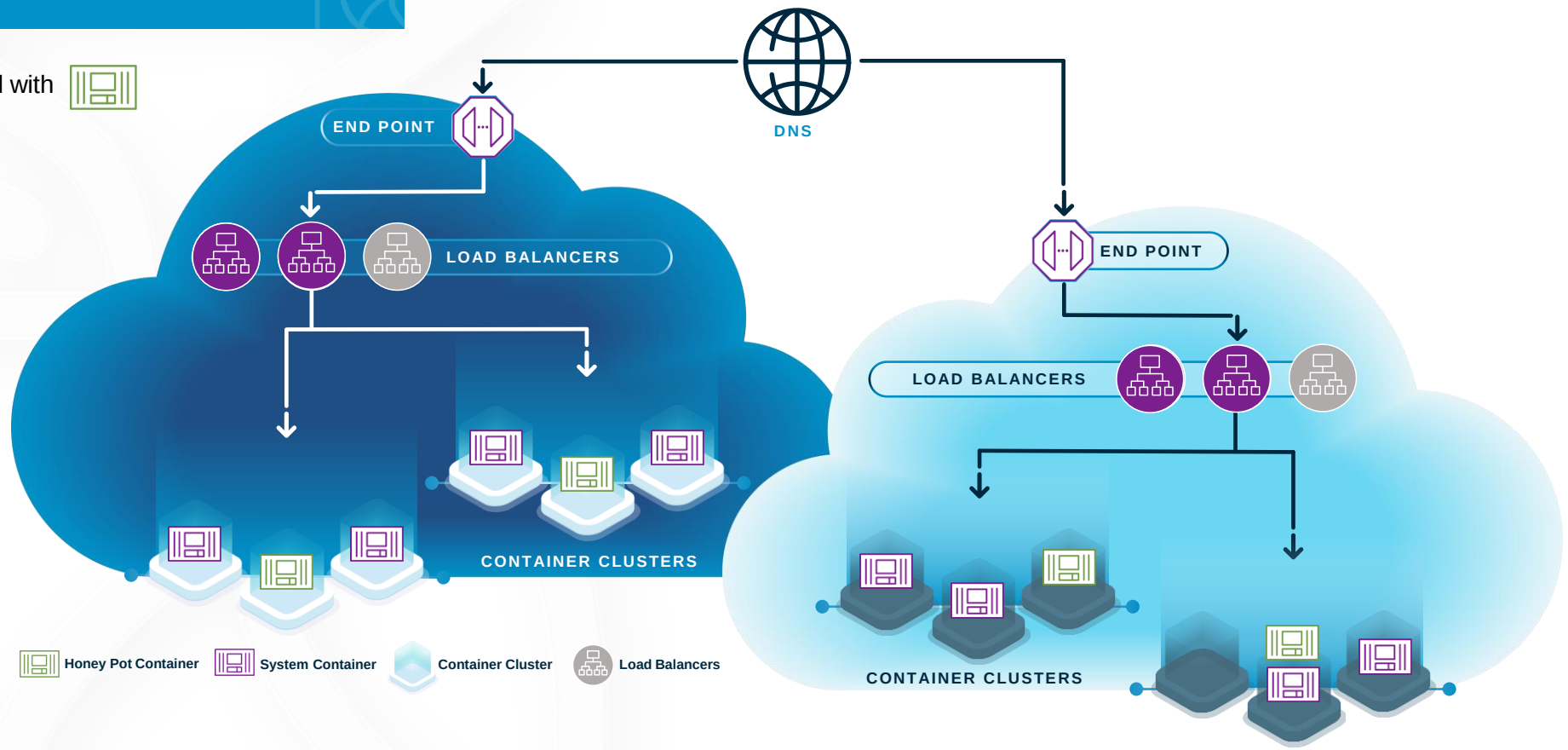
In this example scenario depiction, an application is deployed in a Kubernetes cluster ready for traffic.

Fix Honeypot Containers: intermingled with the rest as a fixed target.

Deployed and does not change, until next deployment is released (could be days or weeks).

DVI starts to move these containers around automatically, keeping DNS and load balancing up to date as it moves.

Load Balancers can also be moved, automatically, and seamlessly associating children and directing traffic.

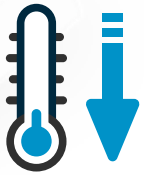


AMTD-DVI

HOW DO WE DO IT?

- Use Deployment and Teardown Automation to initiate move process (features available today in many platforms: k8s, AWS, Azure, Pivotal, etc).
- Using a timing-based rolling deployment to hydrate / dehydrate and confuse adversaries.

- Always use the latest image to assure any unexpected changes do not last.



- An actual DevSecOps pipeline event (real change), will automatically trigger a DVI automation pause, and allow for a specified cool down after the pipeline has successfully completed before restarting.

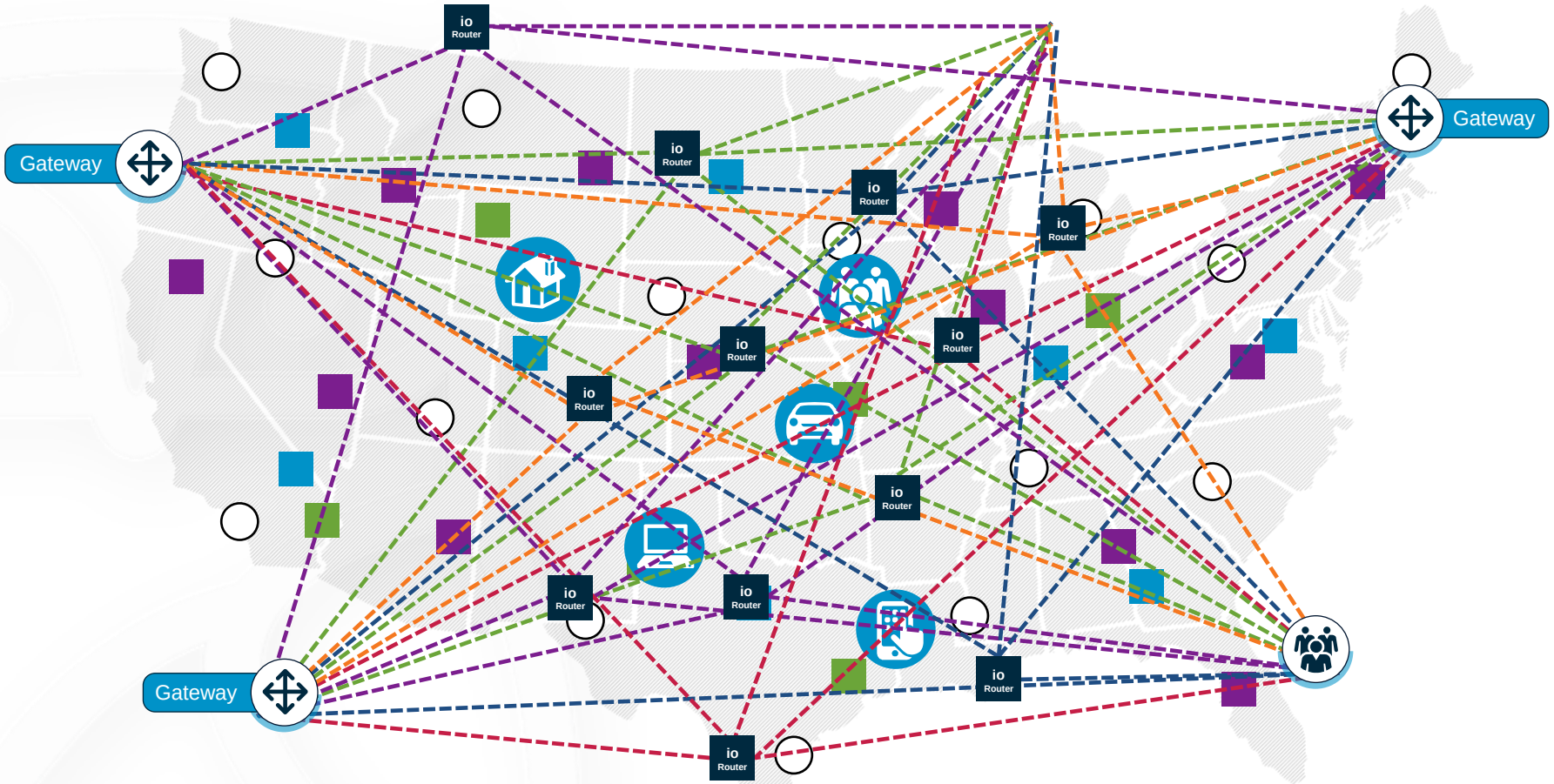
- Prior to dehydration or teardown, assess workload for deviation, quarantine as needed for analysis.

- Maintain fixed honeypot to serve as easier targets that collect attack vectors to improve Intrusion Prevention signatures.

THE FUTURE

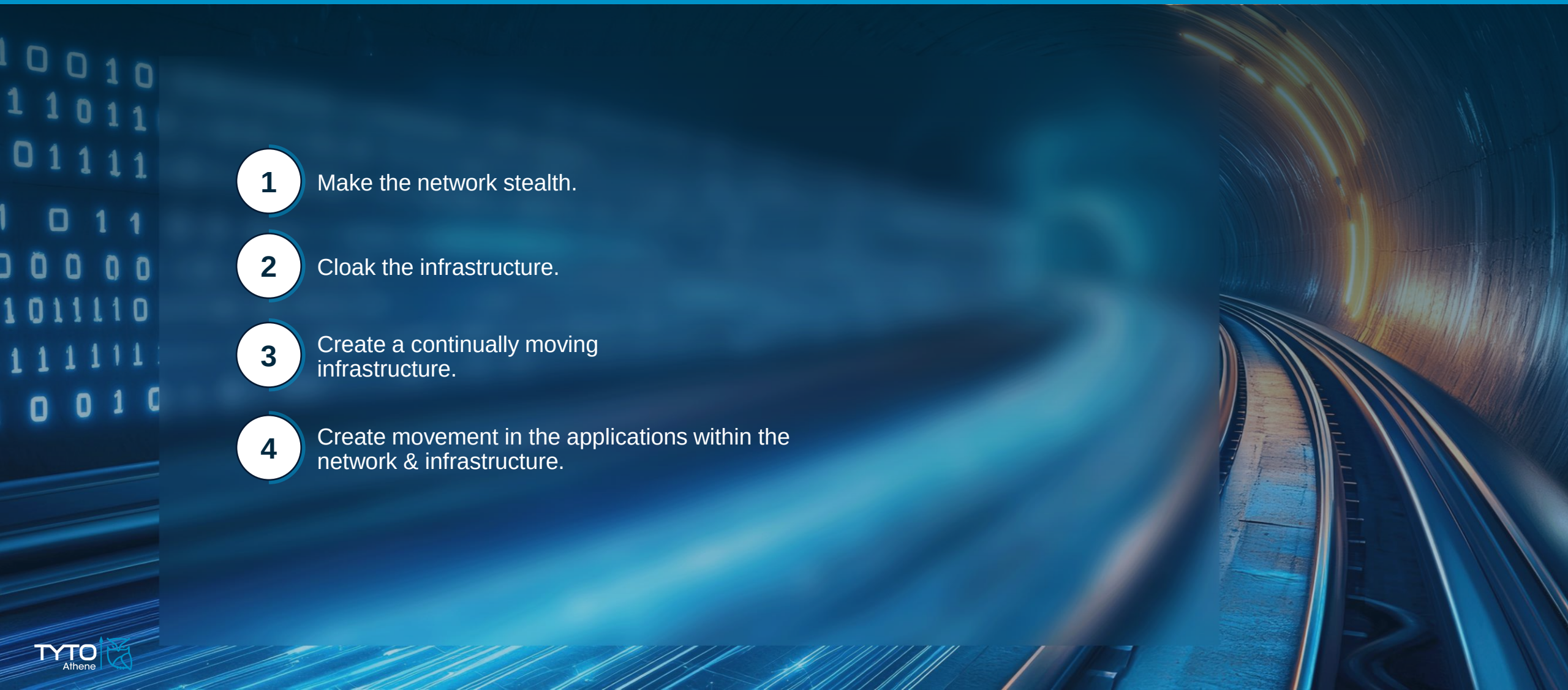
THEY CAN'T ATTACK WHAT THEY CAN'T FIND

- API Endpoints are no longer stationary objects waiting to be attacked or authorized.
- They must now be summoned to a specific place and time within the allowed physical infrastructure and will only exist for the duration of the session, then they will vanish.



INVISIBILITY & MOVEMENT

SECURITY & PERFORMANCE



1. Make the network stealth.
2. Cloak the infrastructure.
3. Create a continually moving infrastructure.
4. Create movement in the applications within the network & infrastructure.

TYTO Athene

THANK YOU

Presented By

Harris Nussbaum

Subject Matter Expert III, Architecture & Engineering

MindPoint Group - A Tyto Athene Company

harrisn@mindpointgroup.com

843.813.2619

Tyto Athene
11950 Democracy Drive
Suite 650
Reston, VA 20190
info@gotyto.com

https://goTyto.com