A Short Introduction to Zero Trust

John Kindervag

Chief Evangelist, Illumio

Advisor, the Cloud Security Alliance

No More Chewy Centers

September 14, 2010 | Updated: September 17, 2010

No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. This report, the first in a series, will introduce the necessity and key concepts of the Zero Trust Model.

Sec. 3. Modernizing Federal Government Cybersecurity.

(a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.


Trust is a dangerous vulnerability that is exploited by malicious actors

illumio

ZERO TRUST

A strategy designed to stop data breaches and prevent other cyber-attacks from being successful by eliminating trust from digital systems.

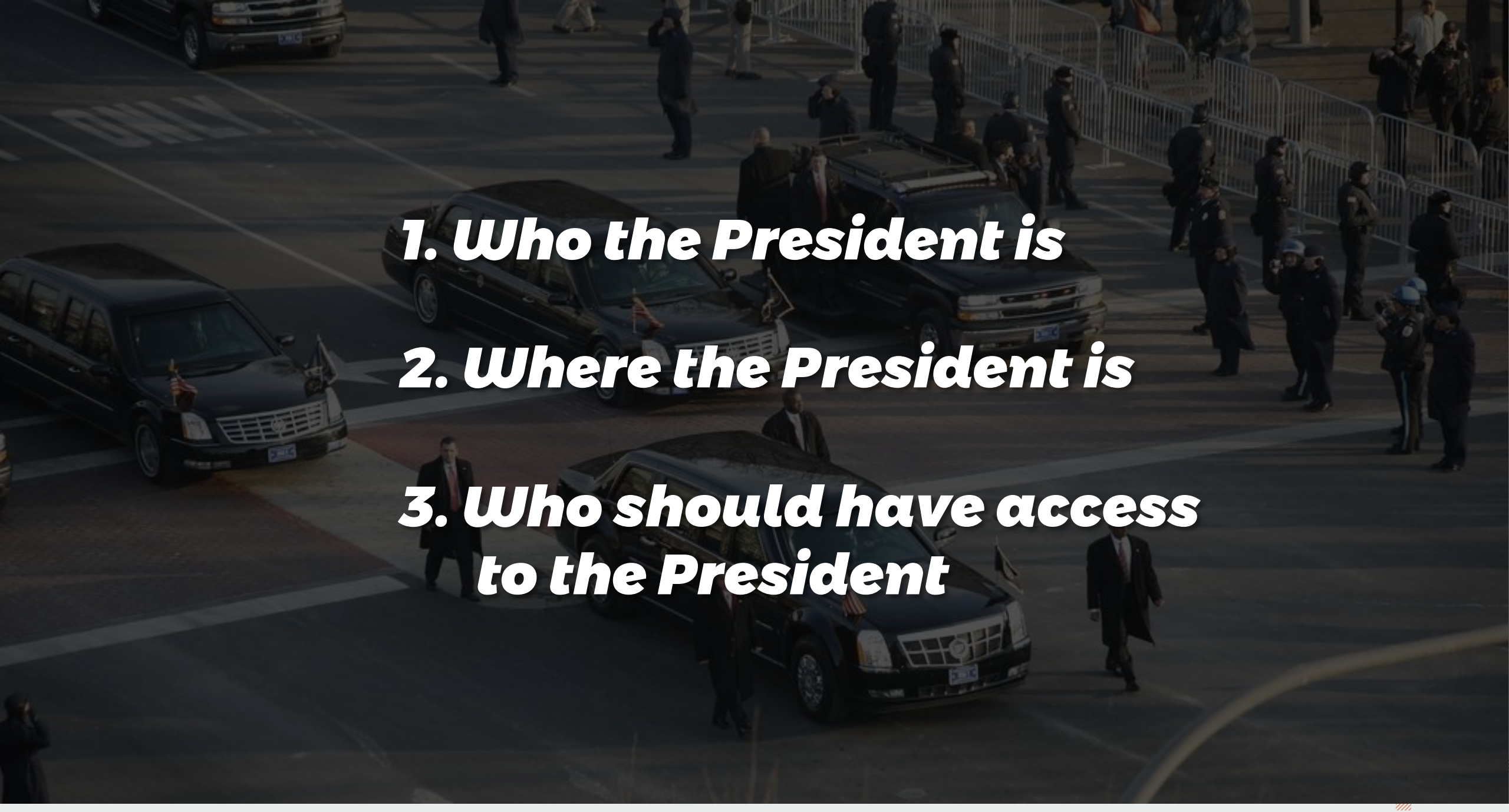
Some Zero Trust Misconceptions

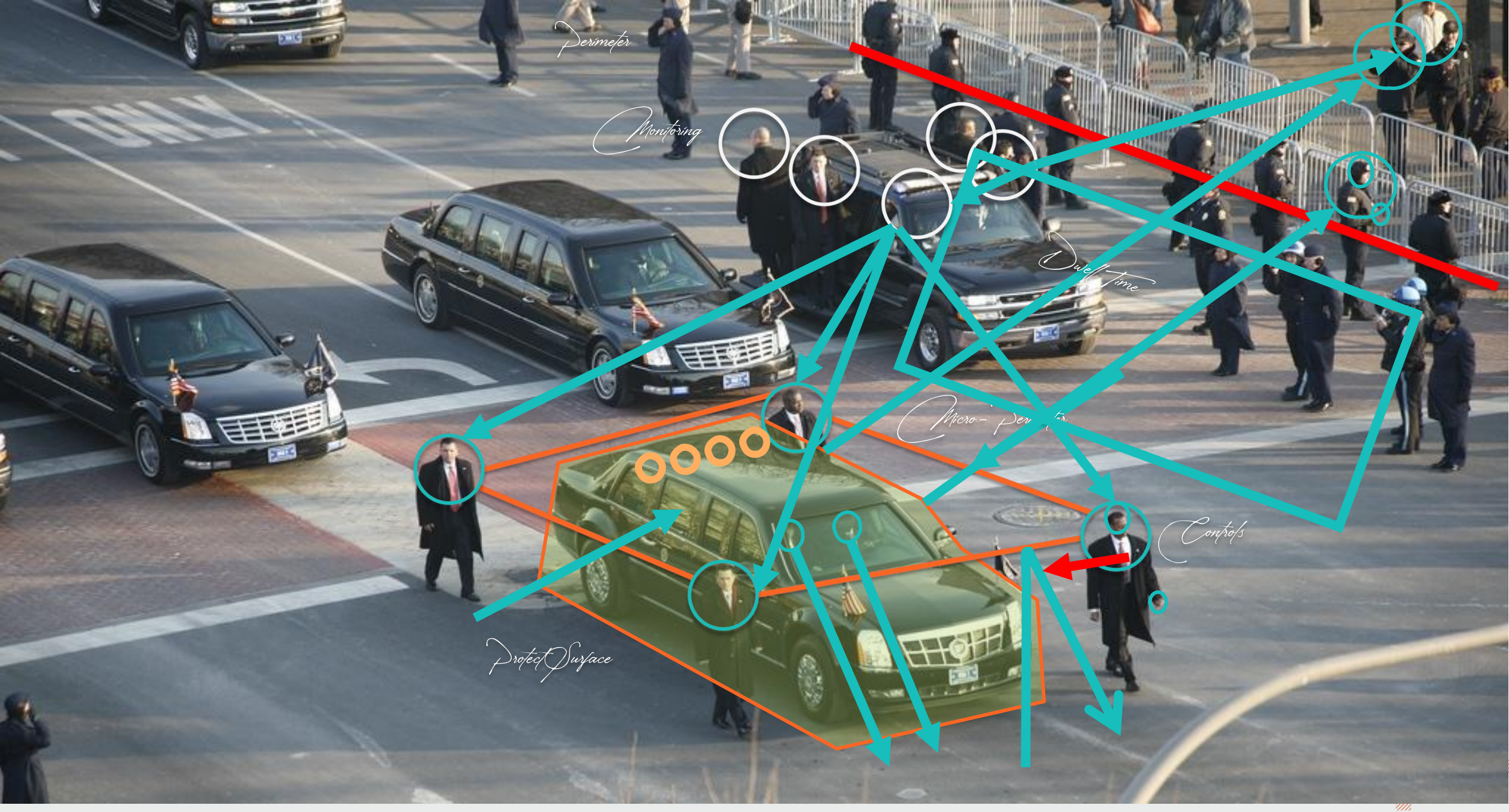
Zero Trust means making a system trusted

Zero Trust is about identity

There are Zero Trust products

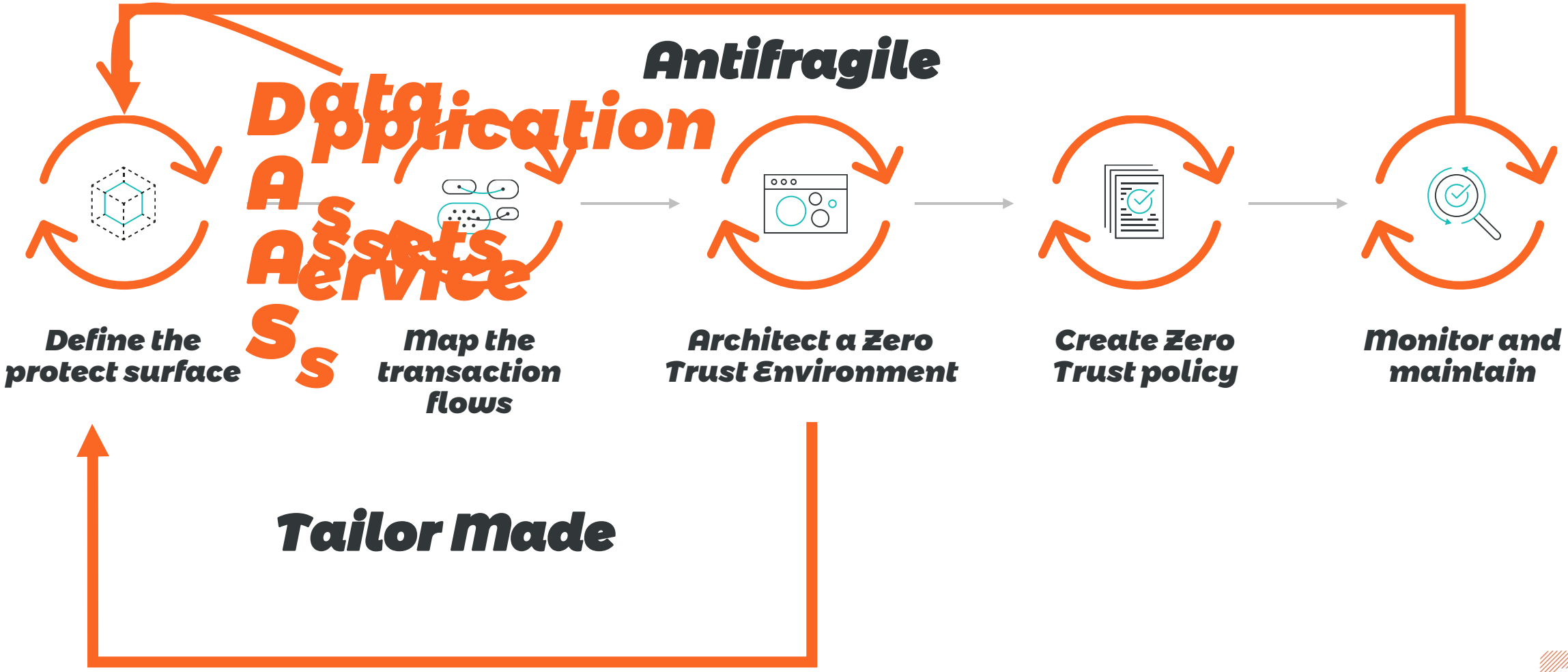
Zero Trust is complicated


1. Who the President is
2. Where the President is
3. Who should have access to the President


Perimeter
Monitoring
Dwell Time
Micro-Perimeter
Controls
Protect Surface


ZERO TRUST

The 5-Step Methodology for Deploying Zero Trust Guides Your Journey



My Mission: Change the Zero Trust Narrative

From Identity to Segmentation as the key technology focus

"all future networks need to be segmented by default"

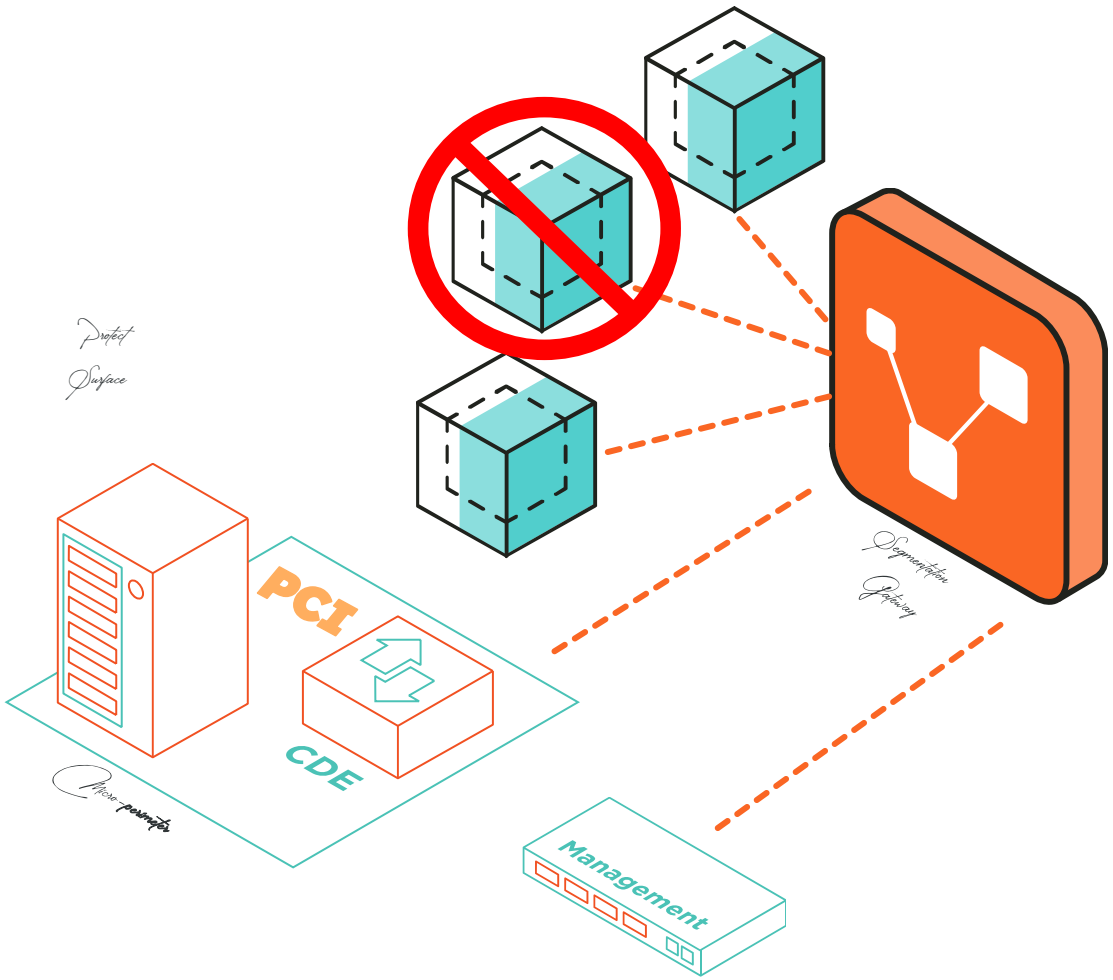
Zero Trust Network Architecture Characteristics: Segmented, Parallelized, And Centralized

The Zero Trust Model of information security can embolden network designers to do unique and powerful things. It will engender infrastructure and security professionals to build security into networks by default. Current designs merely overlay existing networks with more and more controls

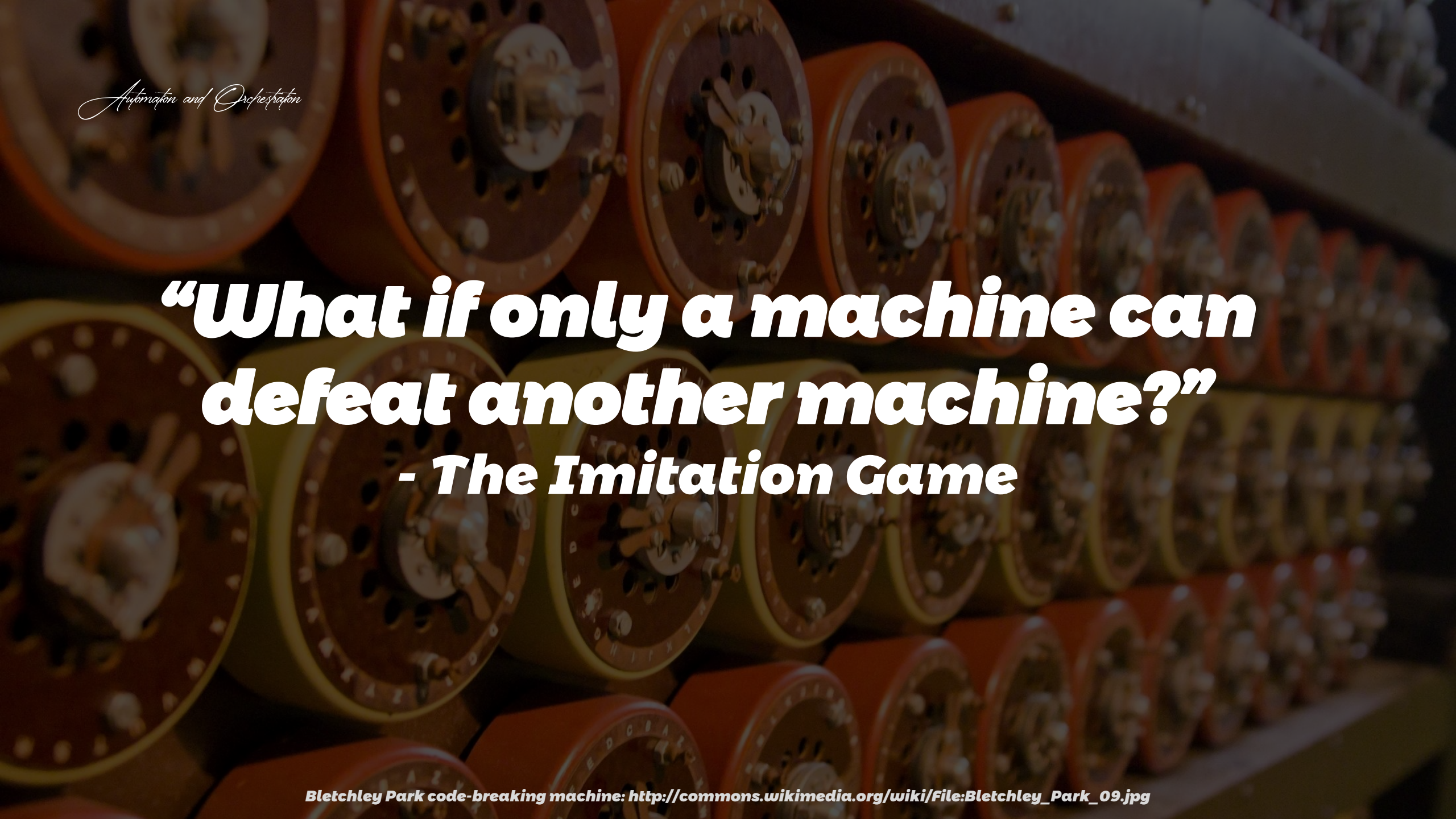
Some networkers advocate the use of virtual LANs (VLANs) for segmentation purposes, but they are highly insecure. Think of VLANs as the yellow line on the road. Traffic is not supposed to cross that yellow line, but there's nothing preventing a vehicle from doing so. In the same way, VLANs define a network traffic isolation policy, but they aren't technologically capable of preventing a malicious actor from moving between VLANs and gaining access to privileged information.[2] Therefore, new ways of segmenting networks must be created because all future networks need to be segmented by default.

to cross that yellow line, but there's nothing preventing a vehicle from doing so. In the same way, VLANs define a network traffic isolation policy, but they aren't technologically capable of preventing a malicious actor from moving between VLANs and gaining access to privileged information.[2] Therefore, new ways of segmenting networks must be created because all future networks need to be segmented by default.

Zero Trust Defines Network Segmentation



1. **Why are you segmenting?**
2. **How are you enforcing Segmentation?**

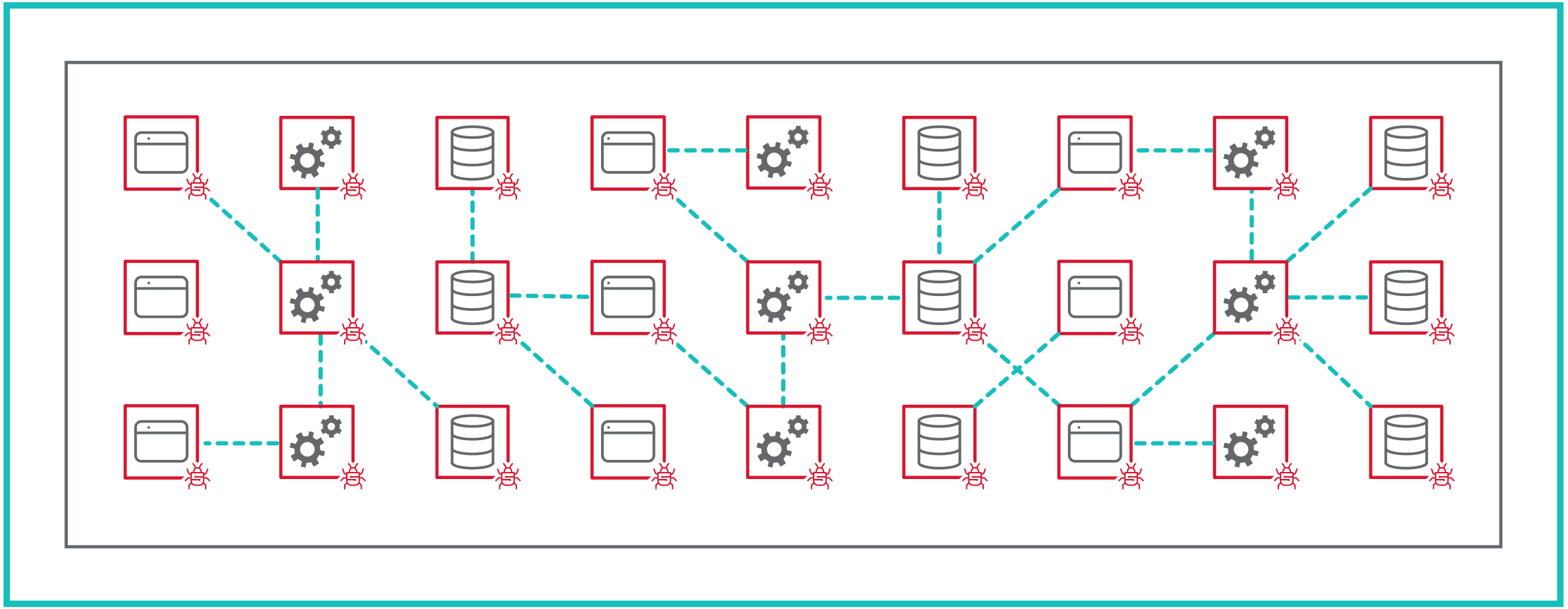


“What if only a machine can defeat another machine?”

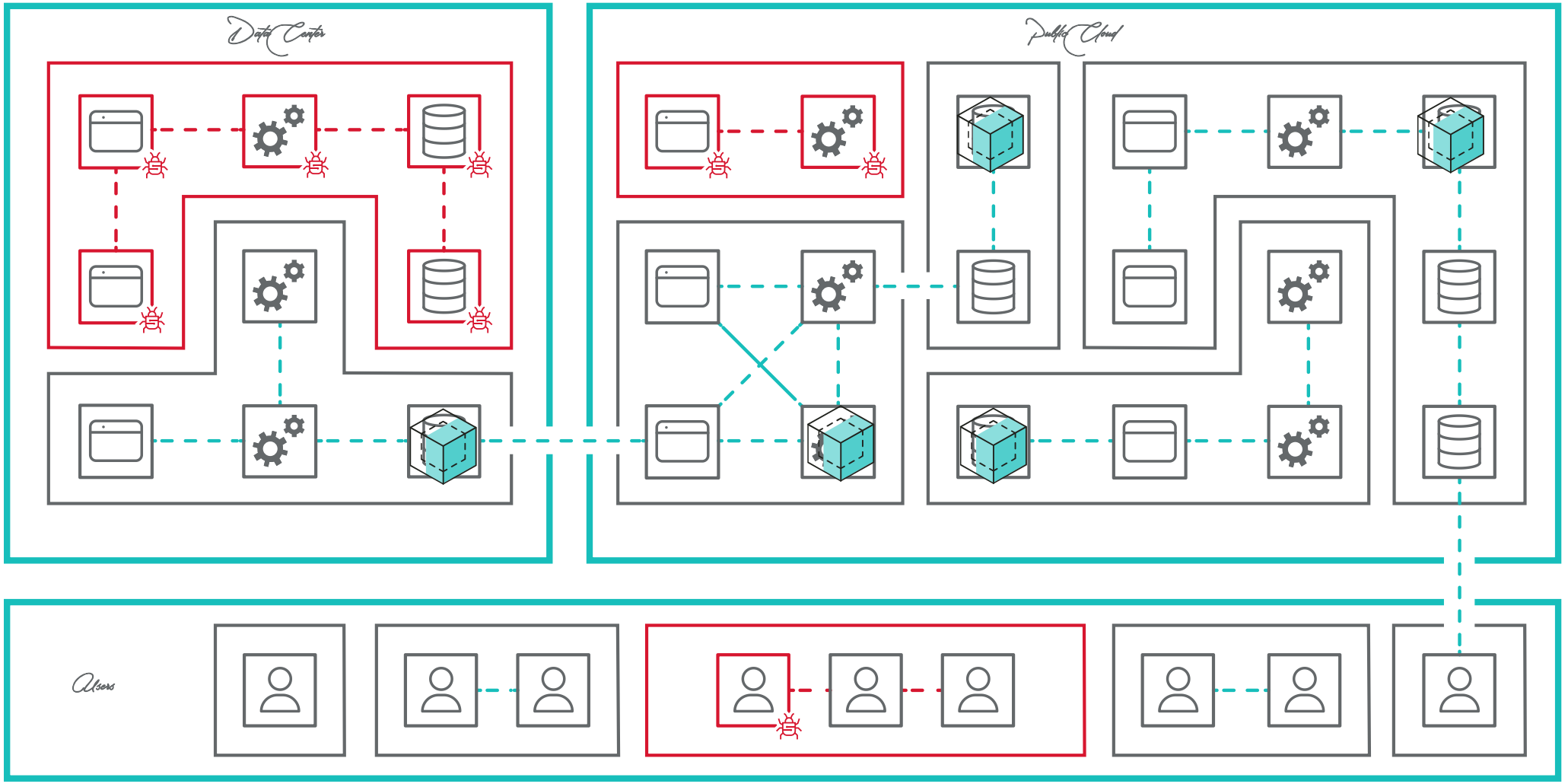
- The Imitation Game

Bletchley Park code-breaking machine: http://commons.wikimedia.org/wiki/File:Bletchley_Park_09.jpg

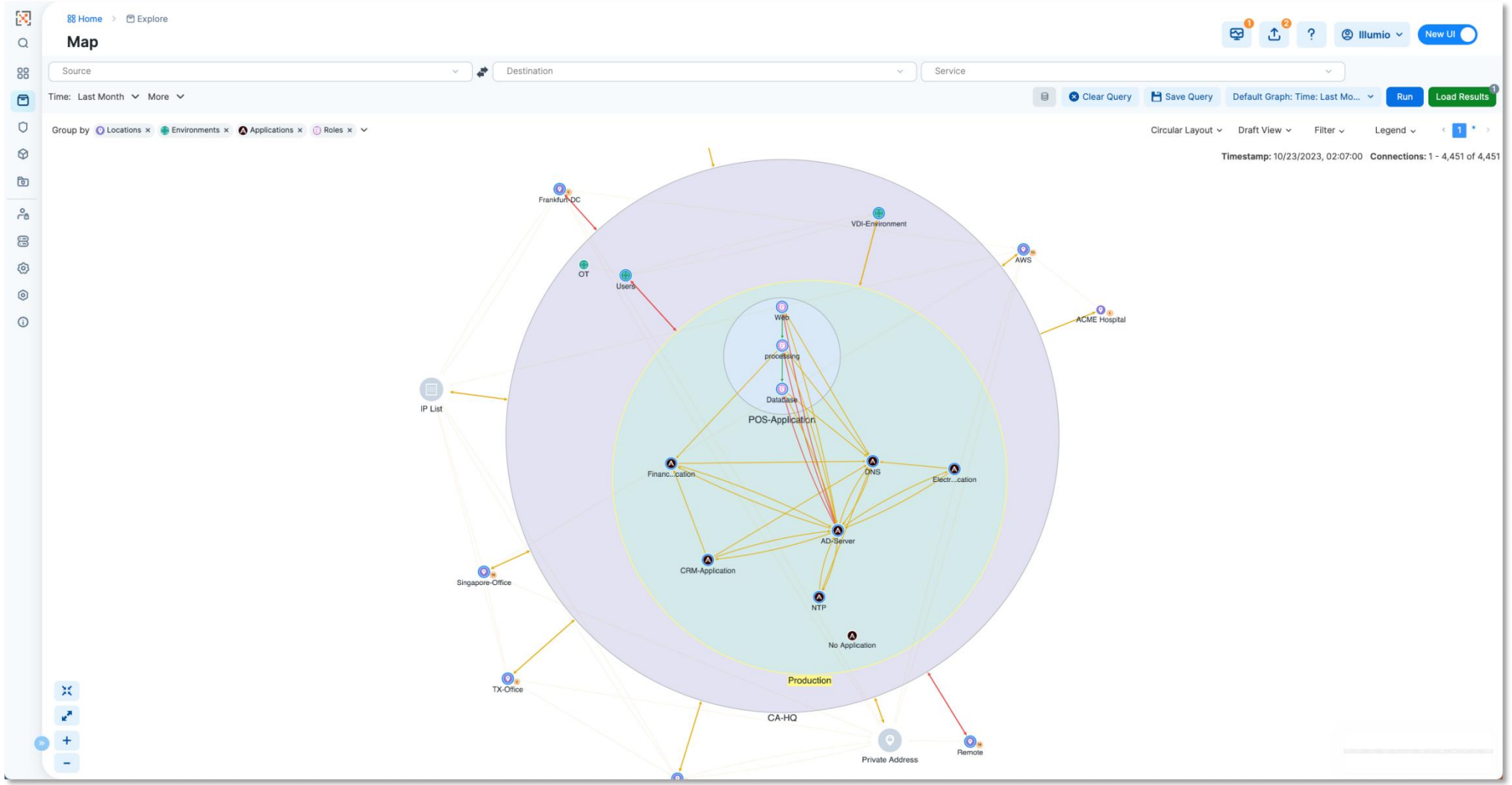
Flat Networks Are Dangerous



Zero Trust Segmentation Creates Protect Surfaces



ZTS Makes Zero Trust Easy to Consume



KEEP IN TOUCH

John

Kindervag

john.kindervag@illumio.com

twitter.com/kindervag

illumio

Thank you