

# Win the CyberWar with Zero Trust

# No More Chewy Centers

For Security & Risk Professionals



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.

<https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf>



## BRIEFING ROOM

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.



Tr

THE PRESIDENT'S NATIONAL SECURITY  
TELECOMMUNICATIONS ADVISORY COMMITTEE



---

## NSTAC REPORT TO THE PRESIDENT

Zero Trust and Trusted Identity Management

February 23, 2022

# ZERO TRUST

EXFILL

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

**FALSE**

Zero Trust means making a system trusted

**FALSE**

Zero Trust is about identity

**FALSE**

There are Zero Trust products

**FALSE**

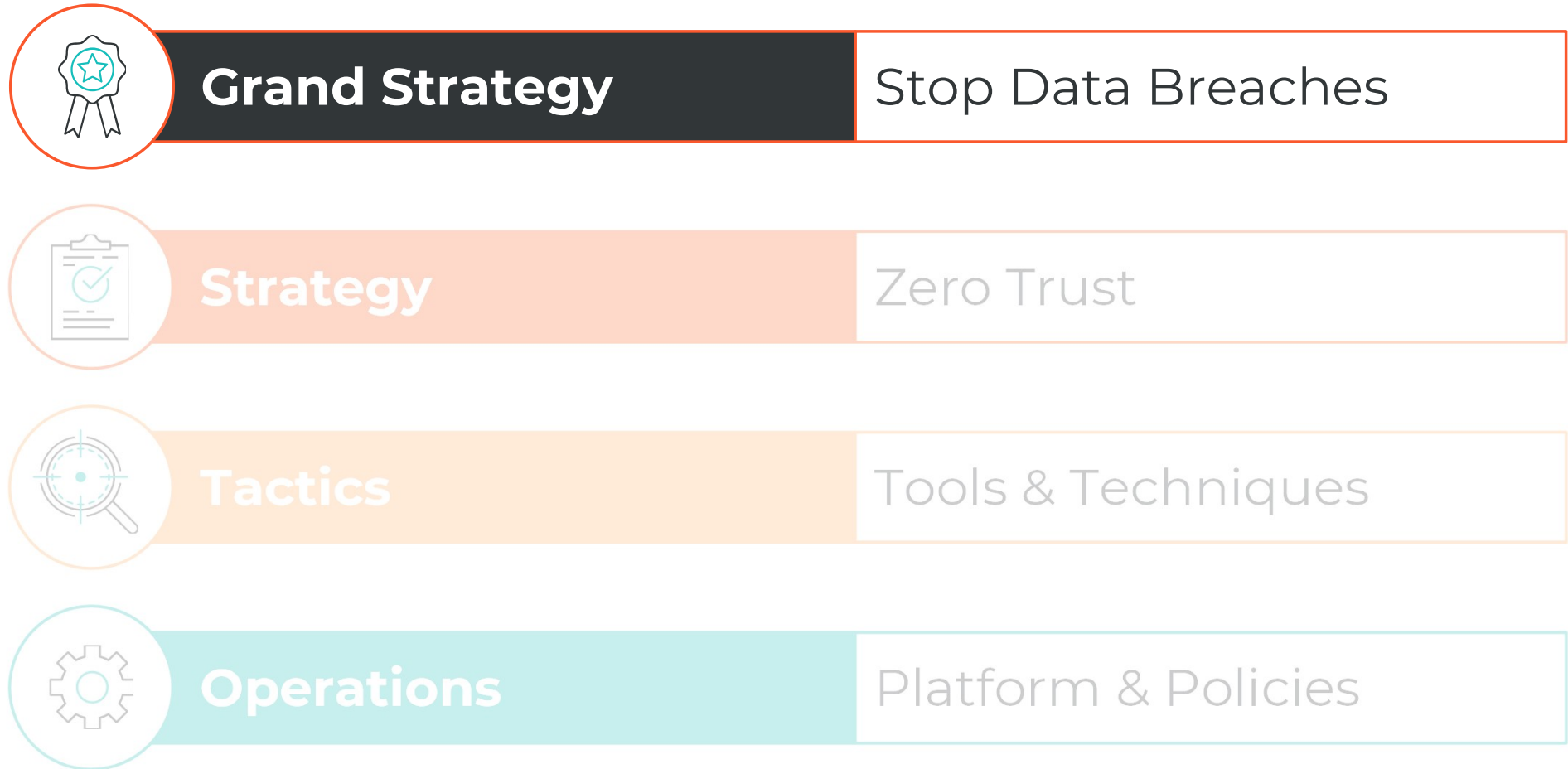
Zero Trust is complicated

# The Four Levels of Strategic Engagement





# The Four Levels of Cyber War





# Cyber Security Grand Strategy: Prevent Data Breaches

## THE WALL STREET JOURNAL.

BUSINESS

### Target Hit by Credit-Card Breach

Customers' Info May Have Been Stolen Over Black Friday Weekend

By *Robin Sidel, Danny Yadron and Sara Germano*

Updated Dec. 19, 2013 7:29 a.m. ET

BT

AT



# Cyber Security Grand Strategy: Prevent Data Breaches

The Washington Post  
*Democracy Dies in Darkness*

Federal Insider

## Hacks of OPM databases compromised 22.1 million people, federal authorities say

By [Ellen Nakashima](#) July 9, 2015 



Committee on Oversight and Government Reform  
U.S. House of Representatives  
114th C



The OPM Data Breach: How the Breach Affects  
National Security for Millions

Majority Staff

Hon. Jason Chaffetz, Chairman  
Committee on Oversight and Government Reform

Hon. Mark Mead, Ranking Member  
Subcommittee on Governmental Operations

Hon. Will Hurd, Chairman  
Subcommittee on Information Technology

September 7, 2016

[www.oversight.house.gov](http://www.oversight.house.gov)

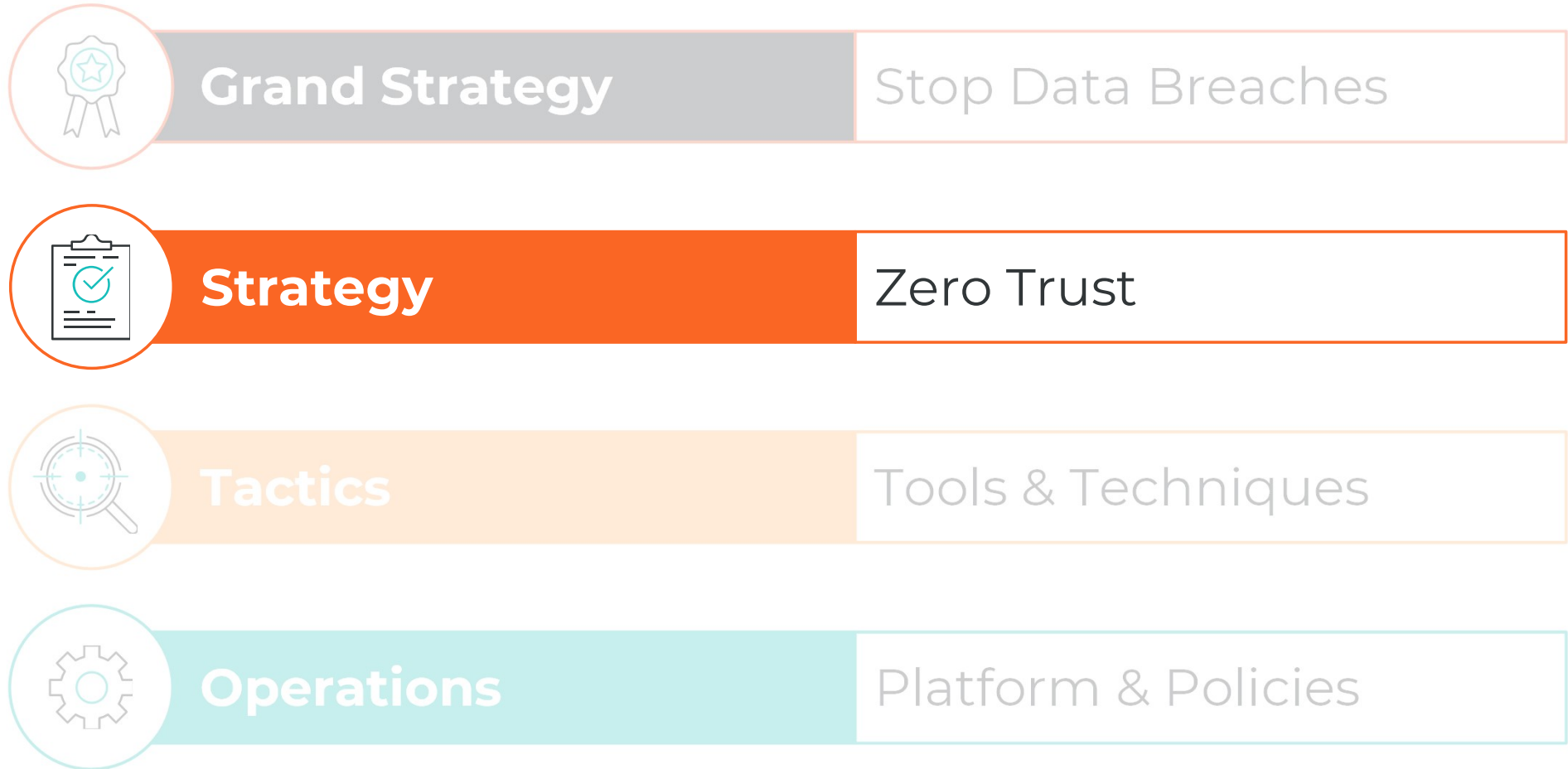
### Recommendation 2 – Reprioritize Federal Information Security Efforts Toward a Zero Trust Model

OMB should provide guidance to agencies to promote a zero trust IT security model. The OPM data breaches discovered in 2014 and 2015 illustrate the challenge of securing large, and therefore high-value, data repositories when defenses are geared toward perimeter defenses. In both cases the attackers compromised user credentials to gain initial network access, utilized tactics to elevate their privileges, and once inside the perimeter, were able to move throughout OPM's network, and ultimately accessed the "crown jewel" data held by OPM. The agency was unable to visualize and log network traffic which led to gaps in knowledge regarding how much data was actually exfiltrated by attackers.

To combat the advanced persistent threats seeking to compromise or exploit federal government IT networks, agencies should move toward a "zero trust" model of information security and IT

<sup>55</sup> Gov't Accountability Office, GAO-11-634, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (Oct. 2011) (stating the average CIO's tenure is two years).

# The Four Levels of Cyber War



# Not a Strategy

3-1 | Expense in depth isn't a strategy



John Kindervag  
@Kindervag

Most companies use HOPE as their risk mitigation strategy:  
(H)ead in the sand  
(O)bfuscate reality  
(P)oint the finger  
(E)mployment journey

RETWEETS 20 FAVORITES 7

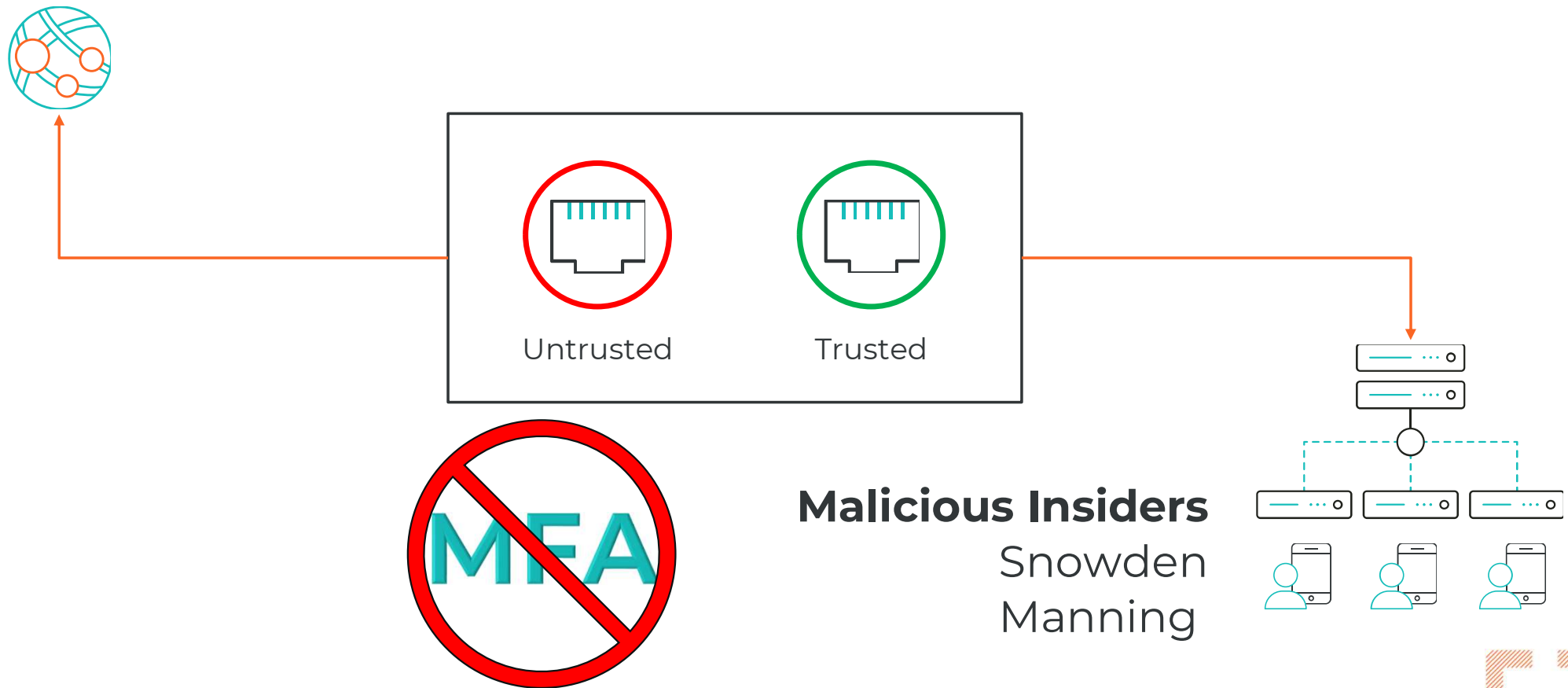


9:31 AM - 16 Dec 2014



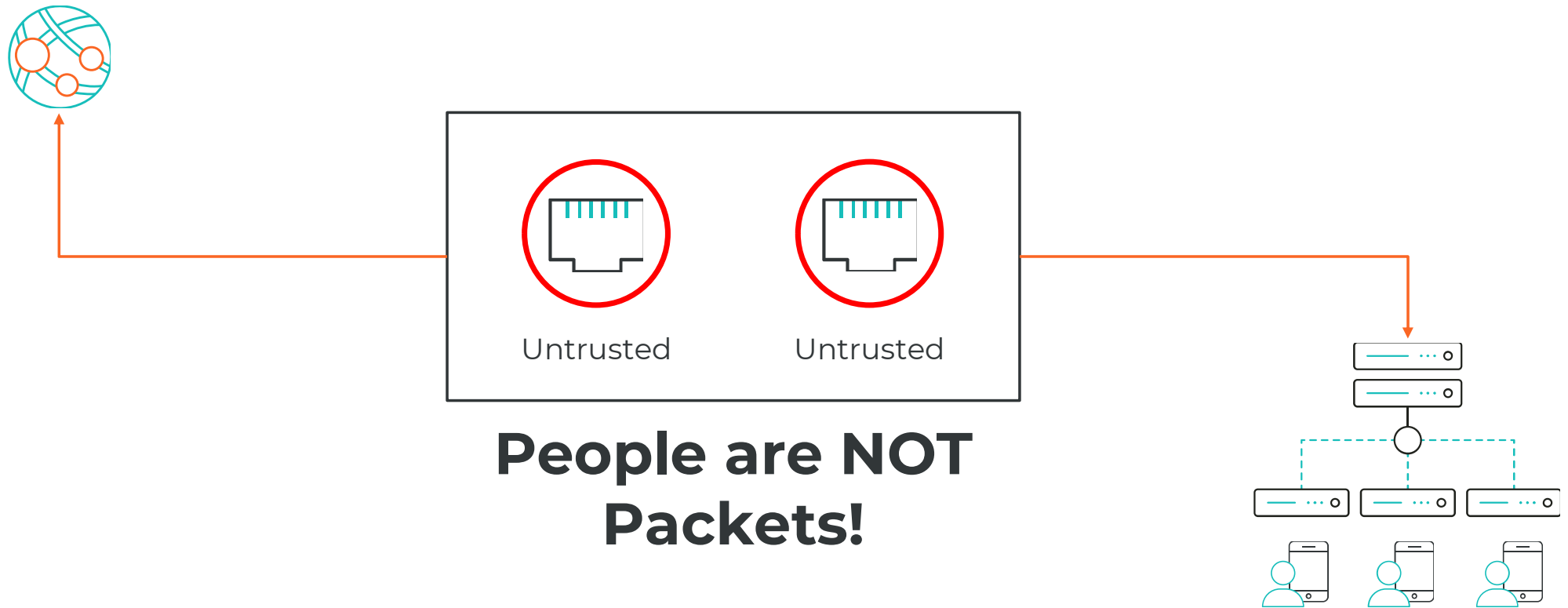
**Trust**  
**is a**  
**dangerous vulnerability**  
**that is exploited by**  
**malicious actors**

# Which One Goes to the Internet?

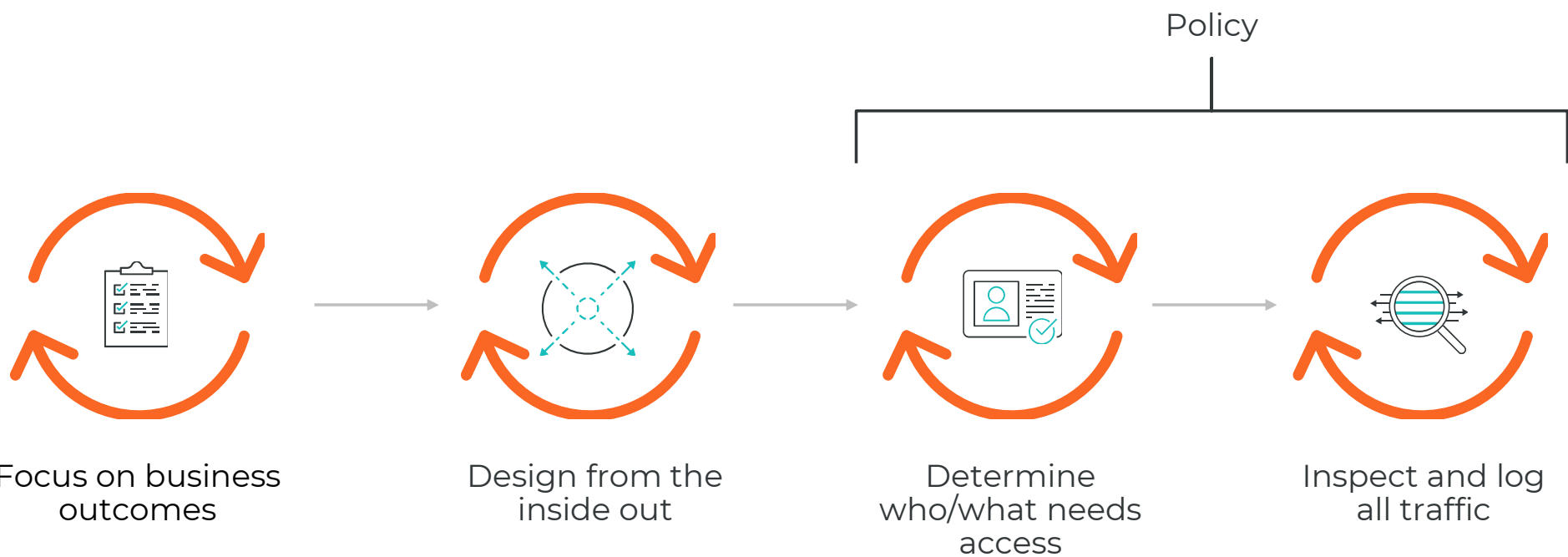




# Zero Trust



# Zero Trust Design Concepts



**JK0**

The segmented circles are an ON2IT logo feature that I incorporated into the slide. We need something else for this slide and the five steps slide

John Kindervag; 2023-10-10T13:54:40.254

**JK1**

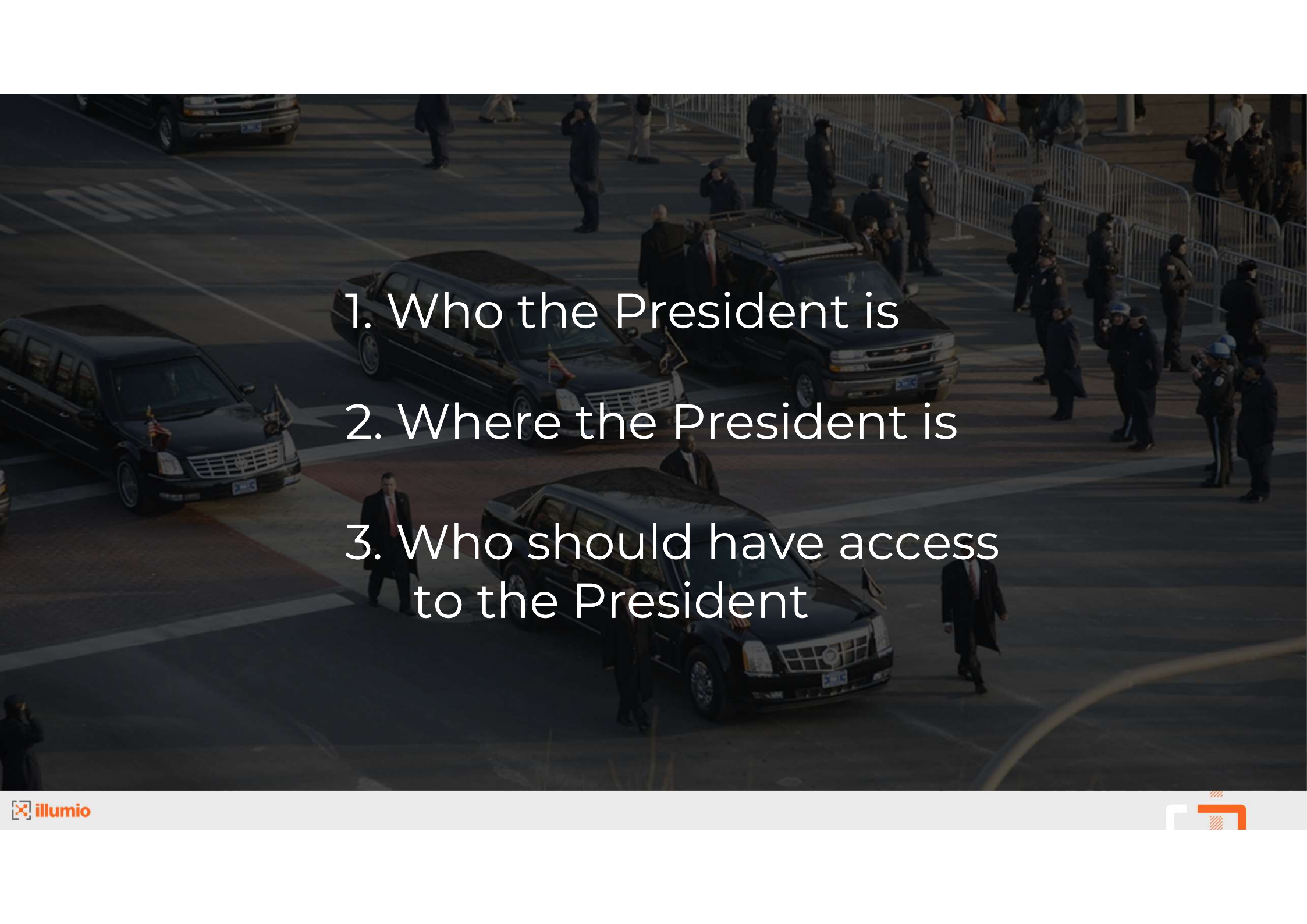
Can you replace the segmented circles from this slide and the 5 steps slide and replace them with the rotating circles from our Platform diagram. Please make the lines Illumio Orange

John Kindervag; 2023-10-17T17:14:06.105

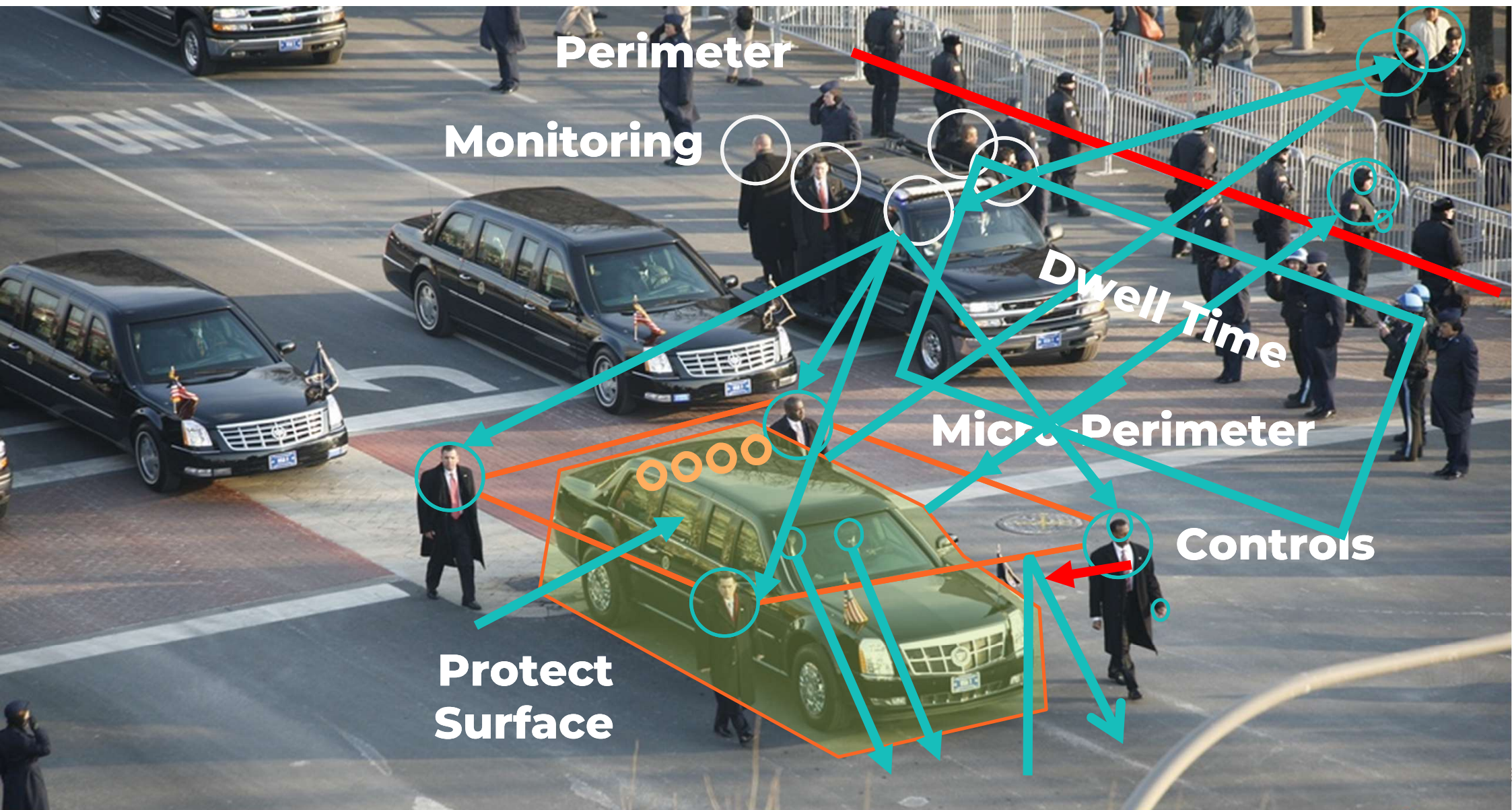
**JK1 0**

See the purple arrow on the image I overlayed on the right.

John Kindervag; 2023-10-17T17:15:21.357

- 
- An aerial photograph of a presidential motorcade. Three black limousines are visible on a city street, each with an American flag on the front. They are surrounded by a large number of police officers in dark uniforms, some standing and others in formation. The scene is set on a paved street with white lane markings. The text of the list is overlaid in white on the center of the image.
1. Who the President is
  2. Where the President is
  3. Who should have access to the President



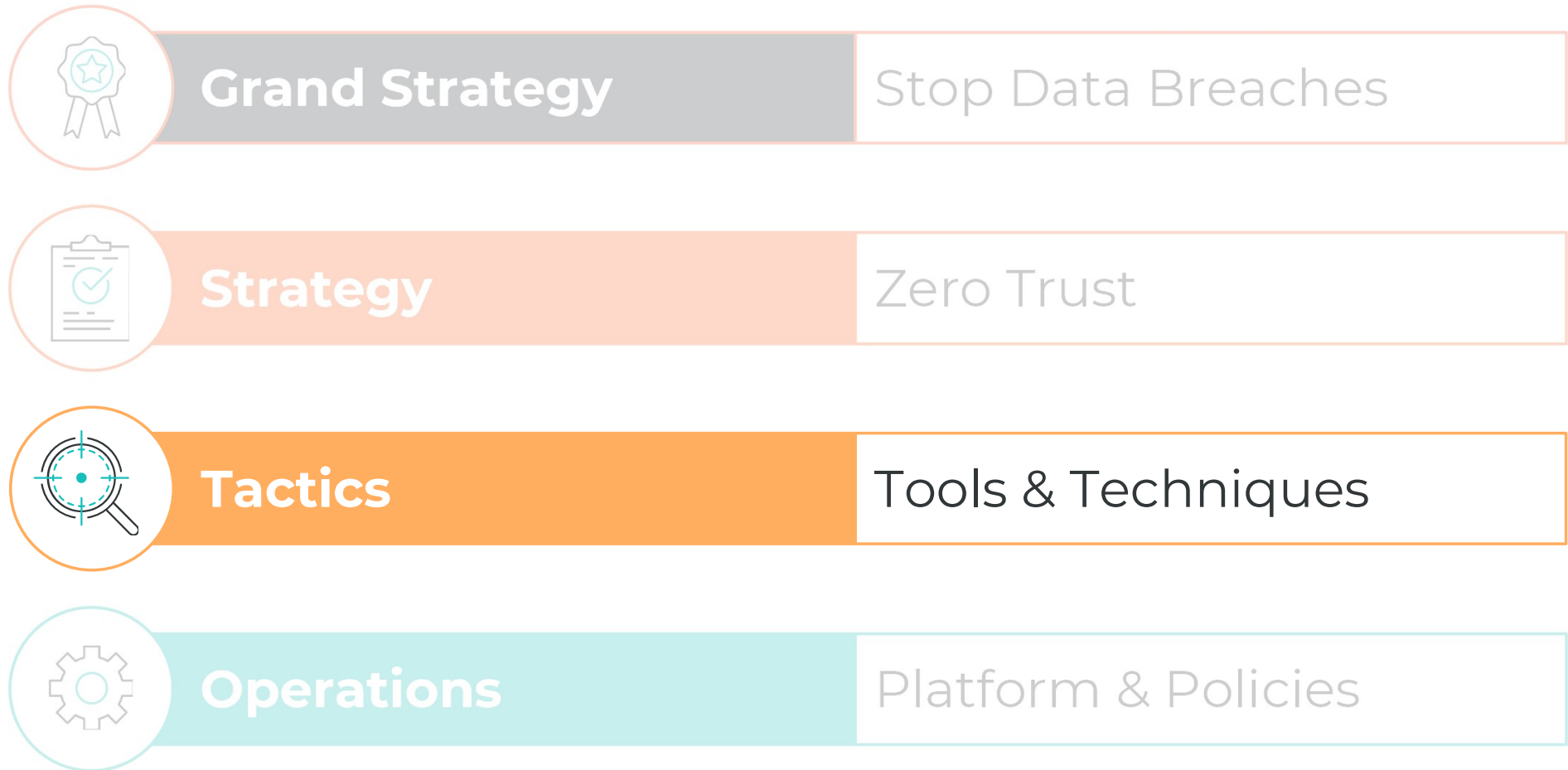


An aerial photograph of a presidential motorcade on a city street. Several black limousines are visible, with the President's car in the foreground. A police SUV is also present. Numerous police officers in riot gear are positioned around the vehicles, and a crowd of people is visible behind a metal barricade on the right. The text "ZERO TRUST" is overlaid in large white letters across the center of the image.

# ZERO TRUST



# The Four Levels of Cyber War



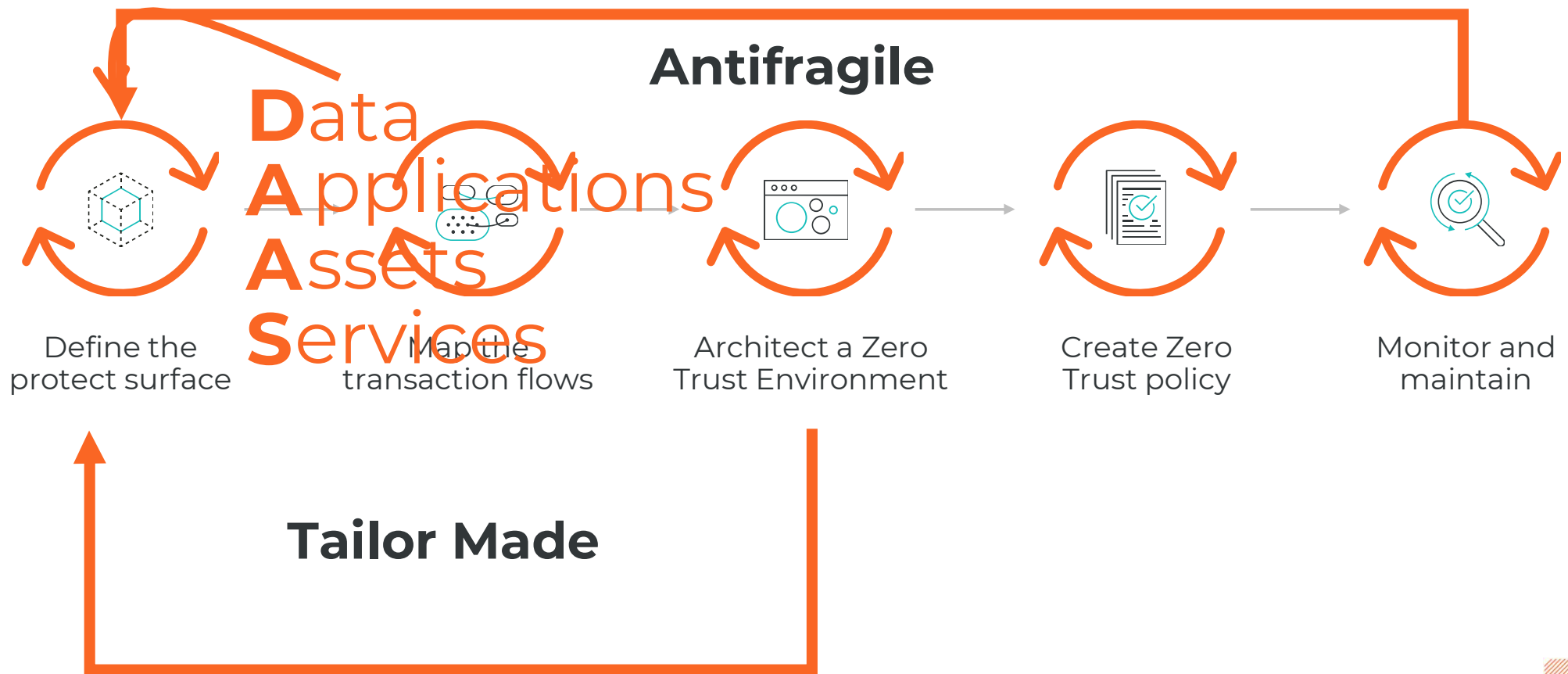




# Start Your Zero Trust Journey with the First Step

Flørli stairs in  
Lysefjorden, Norway

# 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



November 5, 2010

## Build Security Into Your Network's DNA: The Zero Trust Network Architecture

by John Kindervag  
for Security & Risk Professionals





# Segmentation is Key to Zero Trust

“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.<sup>2</sup> 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.<sup>2</sup> Therefore, new ways of segmenting networks must be created because all future networks need to be segmented by default.



# New NSA Cybersecurity Information Sheet

## Advancing Zero Trust Maturity Throughout the Network and Environment Pillar



### Advancing Zero Trust Maturity Throughout the Network and Environment Pillar

---

#### Executive summary

After gaining access to an organization's network, one of the most common techniques malicious cyber actors use is lateral movement through the network, gaining access to more sensitive data and critical systems. The Zero Trust network and environment pillar curtails adversarial lateral movement by employing controls and capabilities to logically and physically segment, isolate, and control access (on-premises and off-premises) through granular policy restrictions.

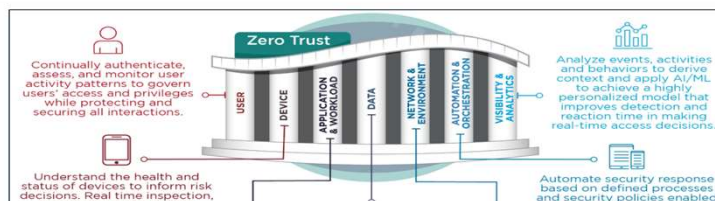
The network and environment pillar works in concert with the other Zero Trust pillars as part of a holistic Zero Trust security model that assumes adversary breaches occur inside the network, and so limits, verifies, and monitors activities throughout the network.

The concepts introduced in this cybersecurity information sheet provide guidance on enhancing existing network security controls to limit the potential impact of a compromise through data flow mapping, macro and micro segmentation, and software defined networking. These capabilities enable host isolation, network segmentation, enforcement of encryption, and enterprise visibility. As organizations mature their internal network control, they greatly improve their defense-in-depth posture and, consequently, can better contain, detect, and isolate network intrusions.



# New NSA Cybersecurity Information Sheet

## Advancing Zero Trust Maturity Throughout the Network and Environment Pillar

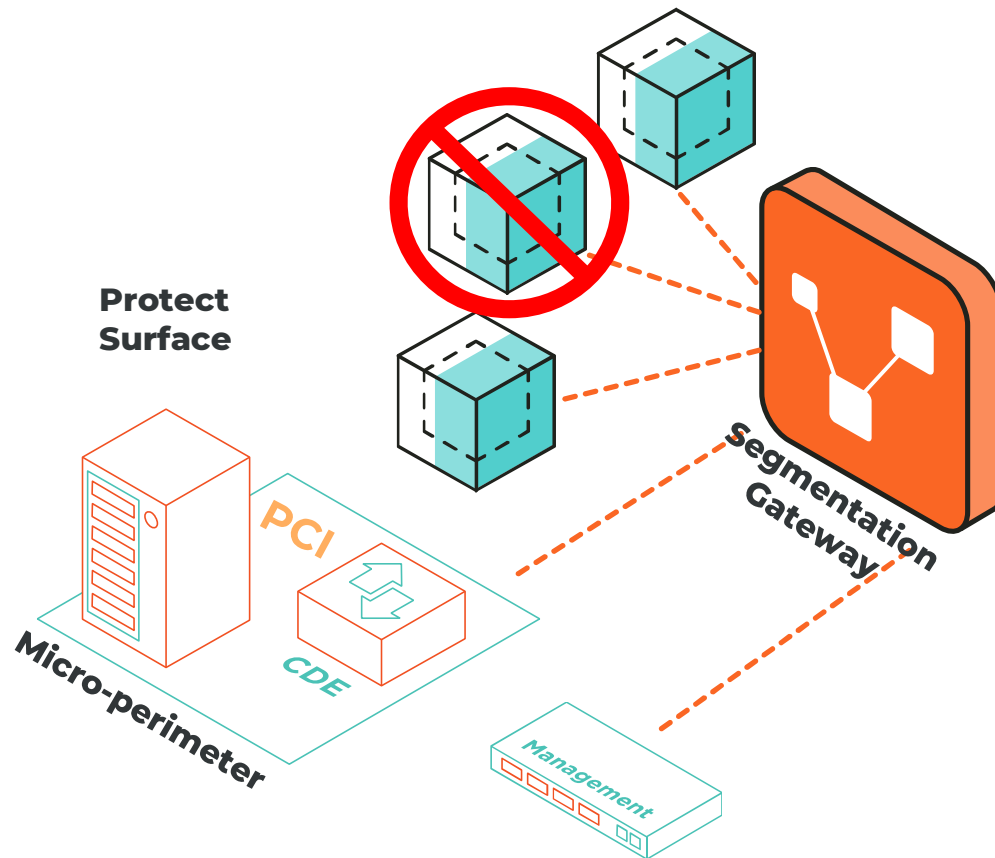


### Network and environment pillar

While a network is the connectivity of hardware and software, the cybersecurity environment as defined in the DoD CSRA and NIST SP 800-207 is the digital ecosystem encompassing all of the network components, non-person entities, and protocols for inter-communication. [5], [6] The ZT maturity model delivers a network secured in-depth through several key functions of each of the four networking and environment pillar capabilities:

- Data flow mapping
- Macro segmentation
- Micro segmentation
- Software Defined Networking

# Zero Trust Defines Network Segmentation

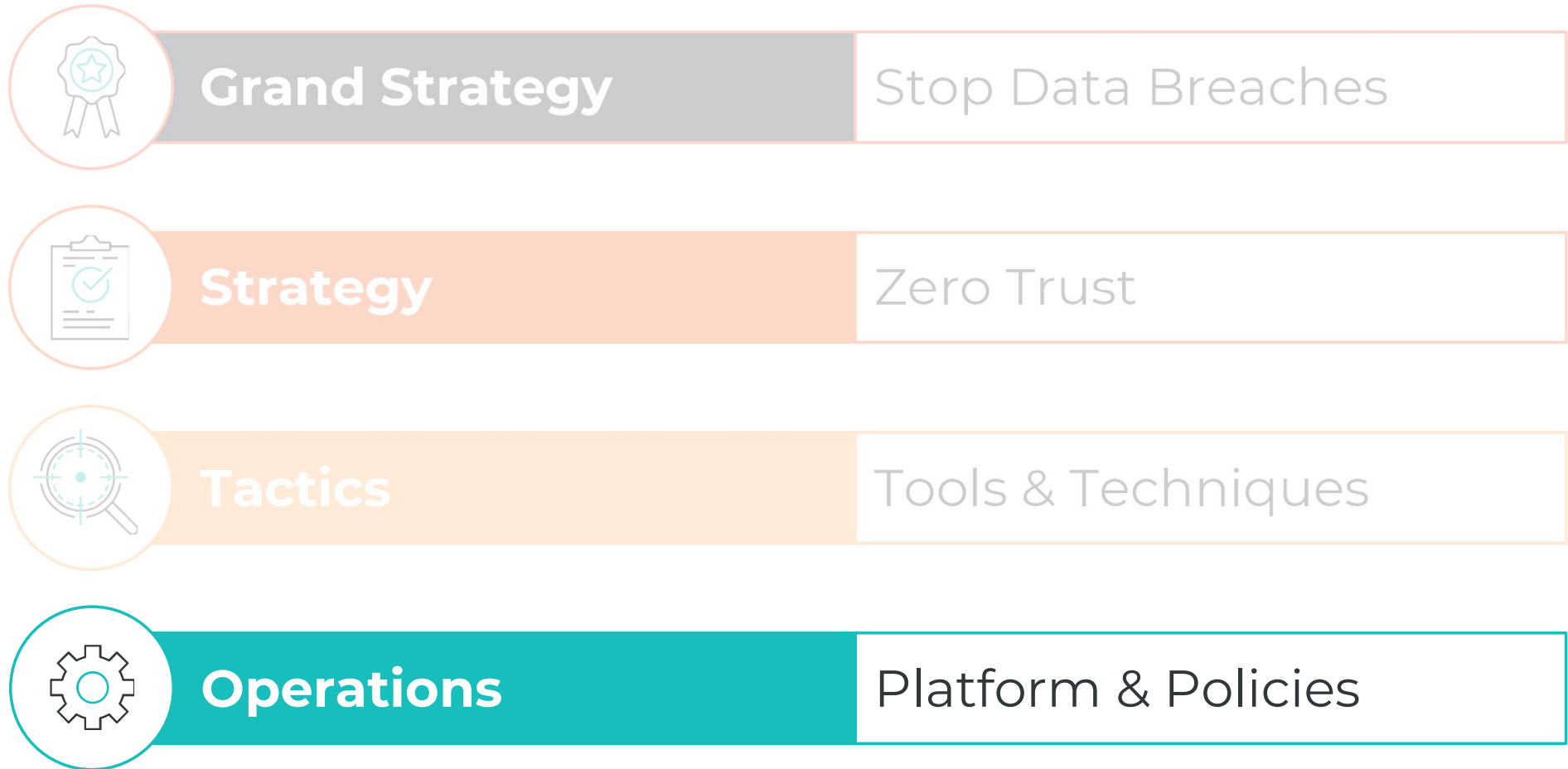


1. Why are you segmenting?
2. How are you enforcing Segmentation?





# The Four Levels of Cyber War



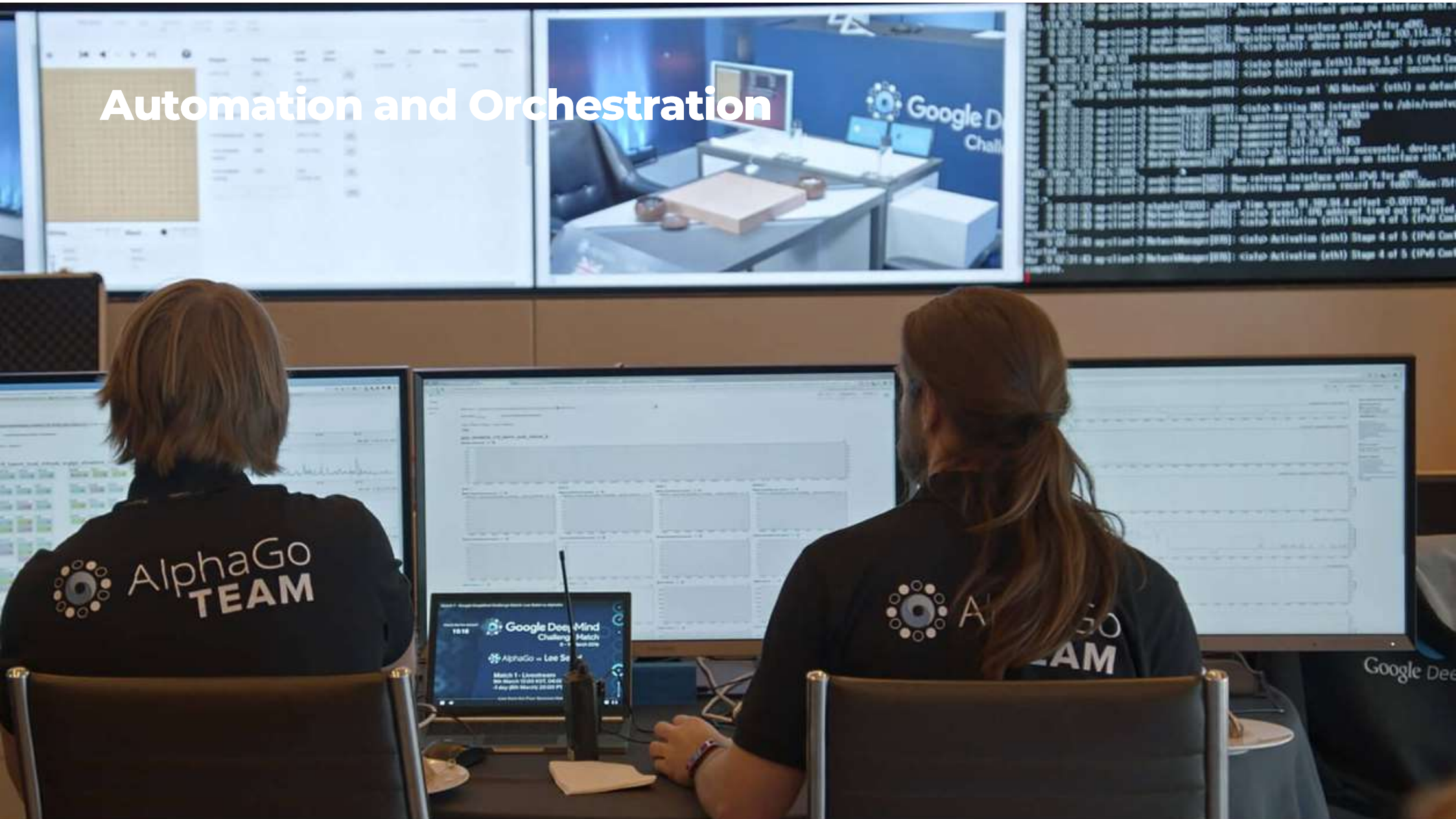
# Automation and Orchestration

Google DeepMind  
Challenge Match  
8 - 15 March 2016

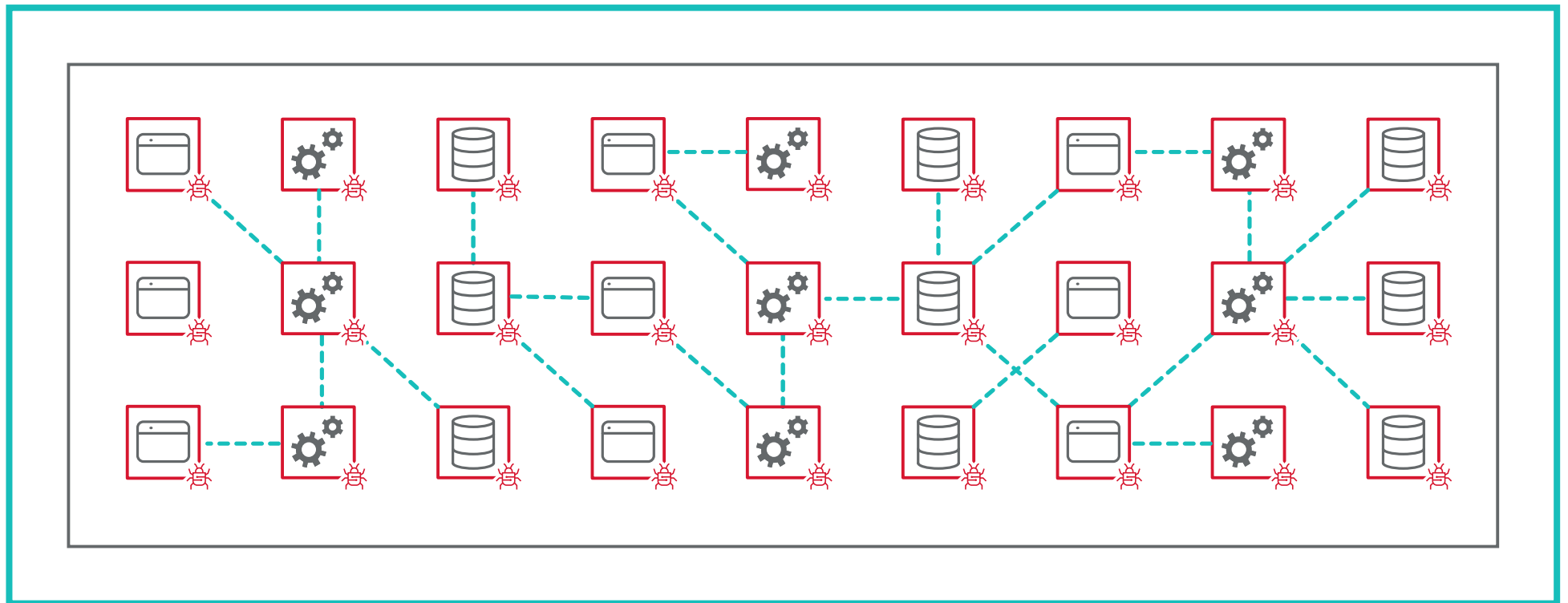
AlphaGo



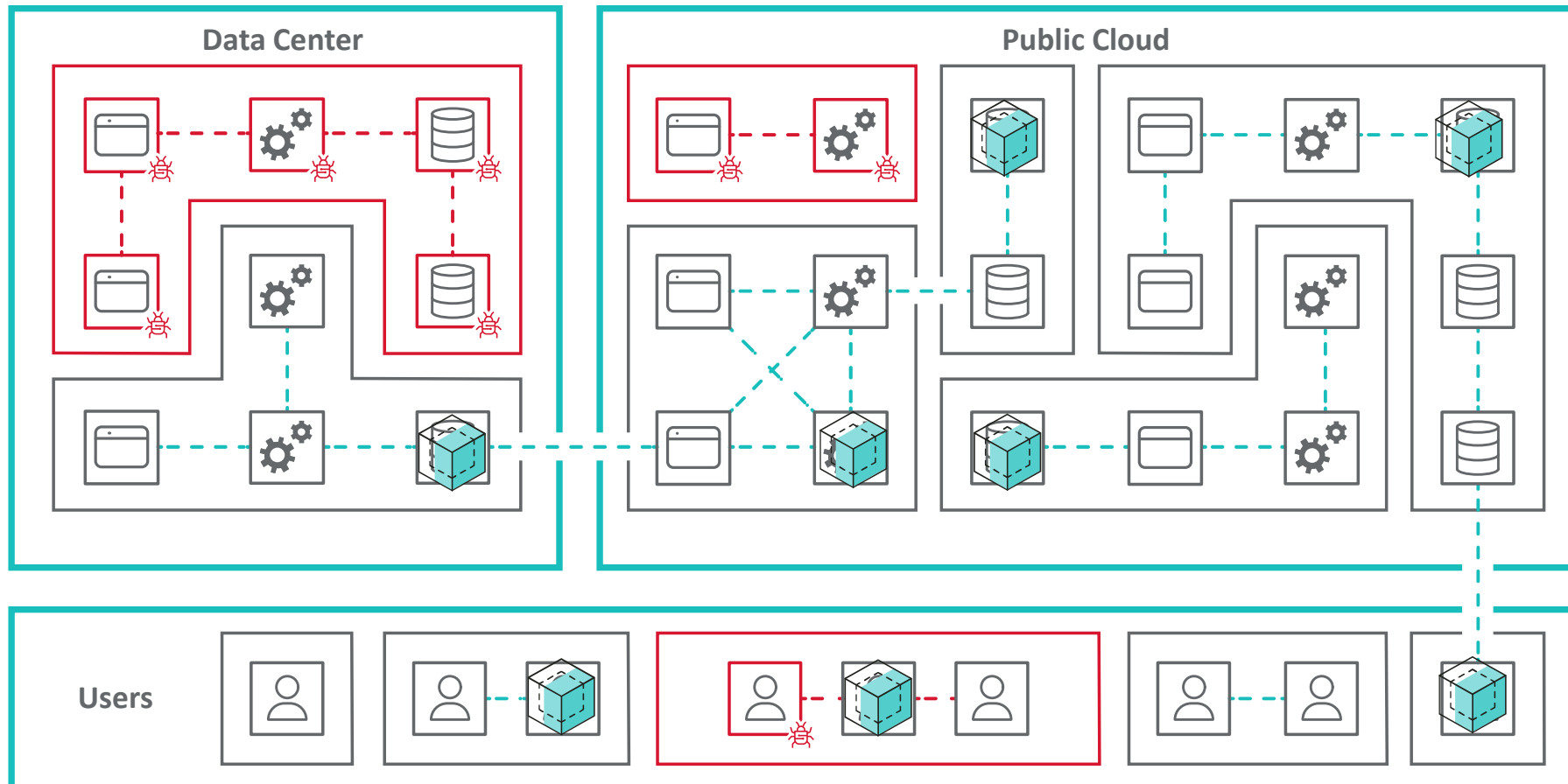
# Automation and Orchestration



# Flat Networks Are Dangerous



# Zero Trust Segmentation Creates Protect Surfaces



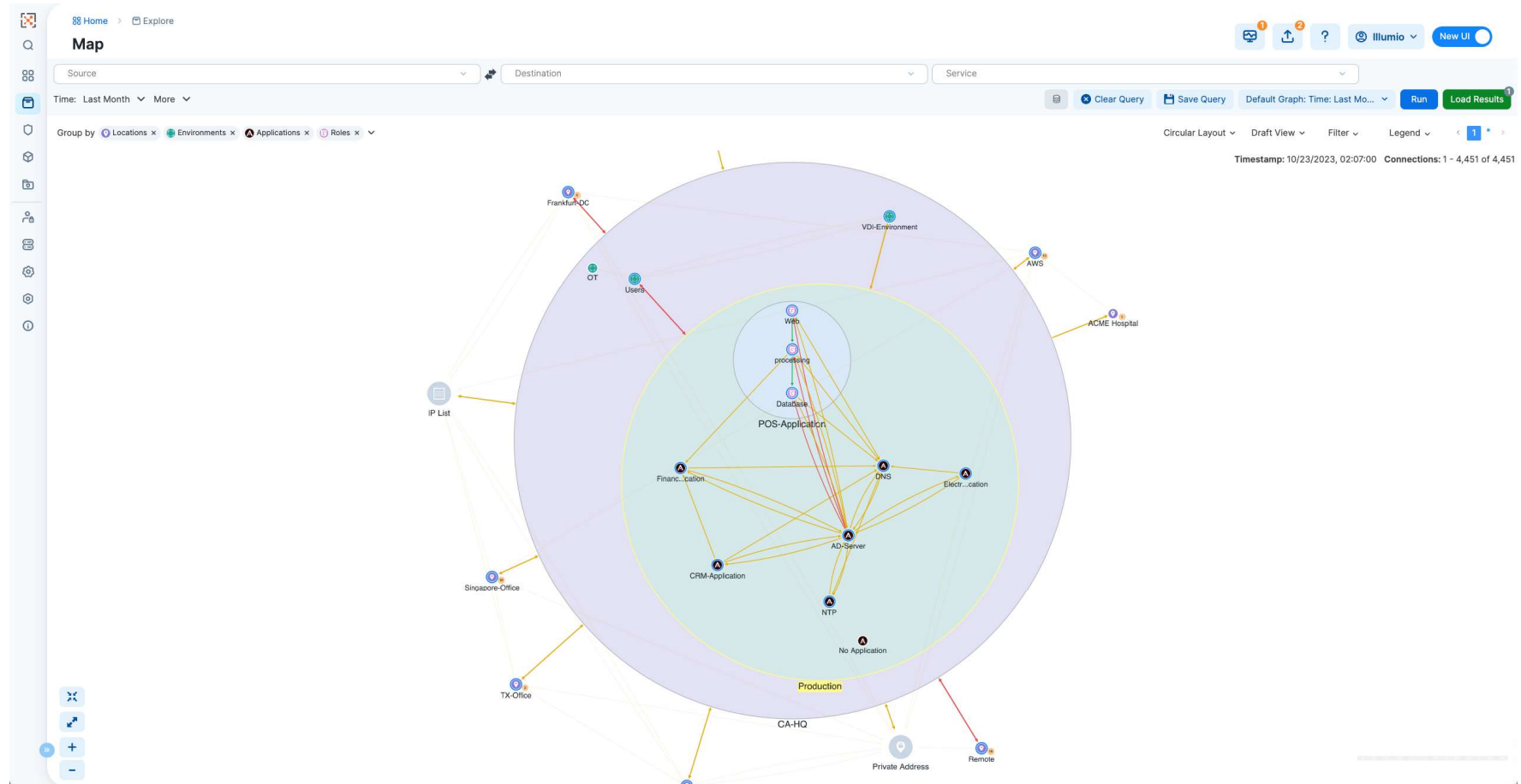
# The Kipling Method of Zero Trust Rule Writing

Who	What	When	Where	Why	How
Resource Validation	Application Validation	Time Limitations	Location	Environment	Flow Validation
Ex -Identity Attributes	Application Name	Ex -Working Hours	Workload Location	Protect Surface	Workload Metadata
Ex -Workload Name	Ex -AD	Ex -Anytime	Ex -New York	DAAS Element	Metadata Analysis
Ex -OT Asset Name	Ex -AD_Port Range		Ex -Azure	Ex -Test Environment	
Ex -Endpoint Name	Ex -AD Process ID		Ex -Remote	Ex -SCADA	

IF Who = AD\_Admins, What = AD\_App\_Validation, When = Anytime, Where = Domain Controller (On Prem or Cloud), Why = Protect Surface Tag, How = AD\_Meta, THEN Allow.



# ZTS Makes Zero Trust Easy to Consume

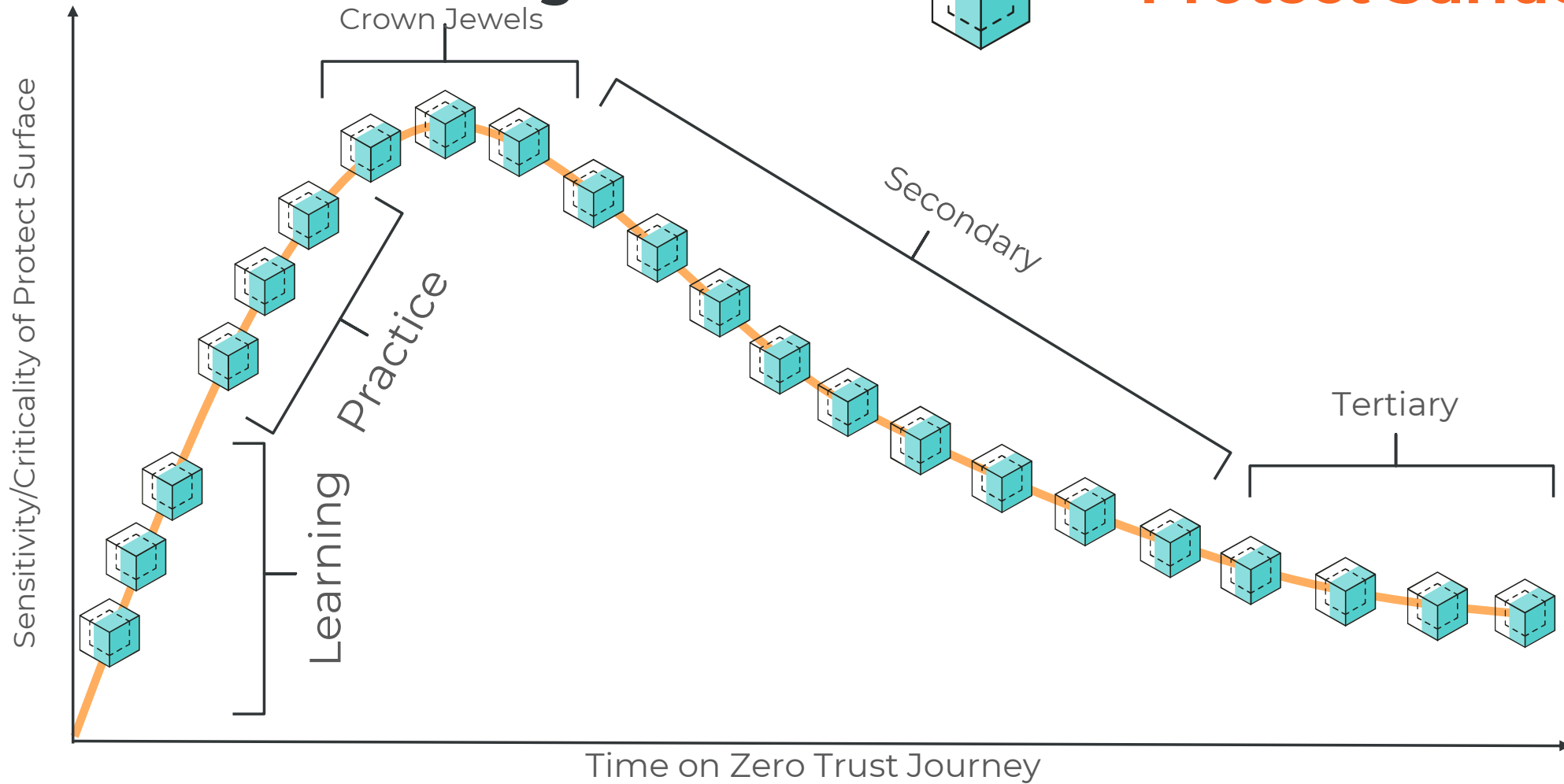




# Zero Trust Learning Curve








= **Protect Surface**



# Zero Trust Maturity Model

DAAS Element \_\_\_\_\_  
Protect Surface \_\_\_\_\_

	Initial	Repeatable	Defined	Managed	Optimized
 1. Define your Protect Surface	1	2	3	4	5
 2. Map the Transaction Flows	1	2	3	4	5
 3. Architect a Zero Trust Environment	1	2	3	4	5
 4. Create Zero Trust Policy	1	2	3	4	5
 5. Monitor and Maintain the Network	1	2	3	4	5

Total Score \_\_\_\_\_



# Zero Trust Is The World's Only Cybersecurity Strategy



“Zero trust would have profoundly limited the attacker’s ability to move within OPM’s network and access such sensitive data.”

**Source:** Adopting a zero trust cyber model in government: <http://federalnewsradio.com/commentary/2016/09/adopting-zero-trust-cyber-model-government/>





KEEP IN TOUCH

## John Kindervag

[zerotrust@illumio.com](mailto:zerotrust@illumio.com)

[twitter.com/kindervag](https://twitter.com/kindervag)



- JK0** Can we get a proxy email account like zerotrust@illumio.com  
John Kindervag; 2023-10-19T20:49:57.609
- JK0 0** [@Raghu Nandakumara] any thoughts  
John Kindervag; 2023-10-23T18:57:56.371
- RN0 1** John, yes we can get IT to setup one for us.  
Raghu Nandakumara; 2023-11-05T17:59:36.016
- JK0 2** What's the process for this?  
John Kindervag; 2023-11-06T15:32:45.881
- RN0 3** I have raised a ticket to create zerotrust@illumio.com and have You, Trevor, Christer and me as recipients.  
Raghu Nandakumara; 2023-11-07T19:21:01.428
- JK0 4** Thanks Raghu  
John Kindervag; 2023-11-07T21:06:08.346
- JK1** Need to know what phone number to put here.  
John Kindervag; 2023-10-19T20:50:18.245
- JK1 0** [@Raghu Nandakumara]  
John Kindervag; 2023-10-23T18:58:05.637
- RN1 1** Do you need a phone number?  
Raghu Nandakumara; 2023-11-05T17:59:44.907
- JK1 2** I don't know. Who would monitor it? What are your thoughts?  
John Kindervag; 2023-11-06T15:31:37.051
- RN1 3** No, we don't need a phone number.  
Raghu Nandakumara; 2023-11-07T19:20:25.866





# Thank you