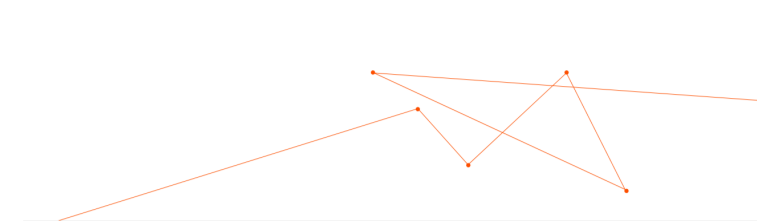


The background of the slide is a dark blue gradient. In the center, there is a faint, white fingerprint. Overlaid on the fingerprint and the background are several thin, orange lines that form a network or web-like structure. There are also some white, stylized 'L' shapes or corner brackets scattered around the fingerprint. In the top right corner, there is a small orange square with a white arrow pointing left.

A Short Introduction to Zero Trust John Kindervag ON2IT

Authentic Zero Trust

- It is a strategy designed to stop data breaches and other cyber-attacks by eliminating digital trust from systems.
- It leverages design principles proven to work over more than a decade
- It uses the standard 5-step methodology for implementing a Zero Trust architecture
- It provides demonstrable, positive security outcomes for companies who adopt Zero Trust



Some Zero Trust Misconceptions

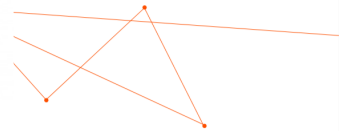
- Zero Trust means making a system trusted
- Zero Trust is about identity
- There are Zero Trust products
- Zero Trust is complicated

FALSE

FALSE

FALSE

FALSE





TRUST

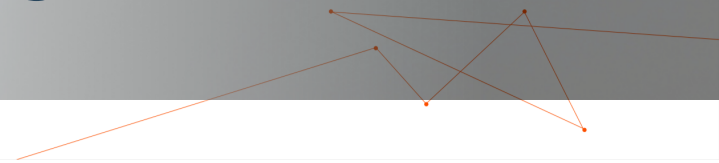
is a dangerous

VULNERABILITY

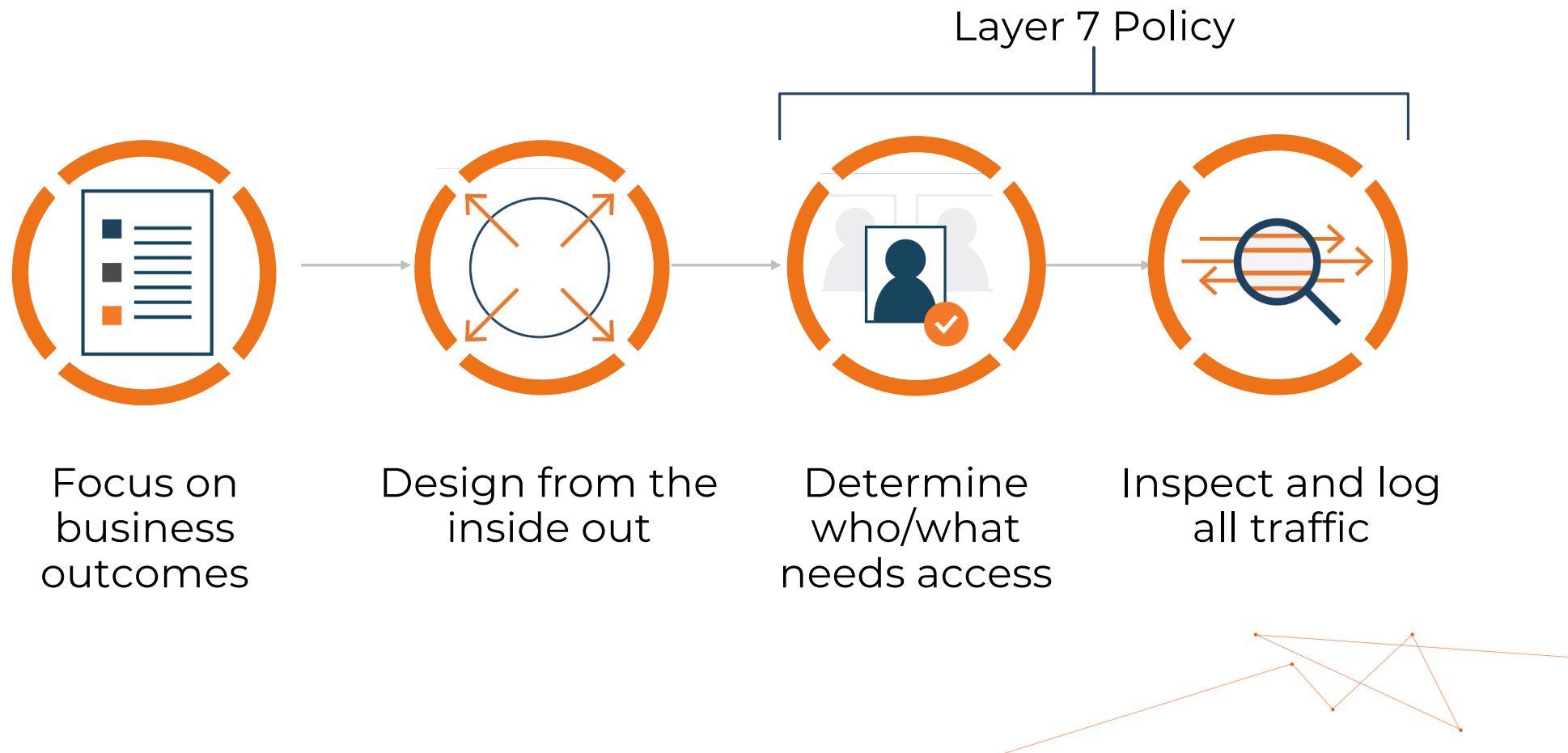
that is

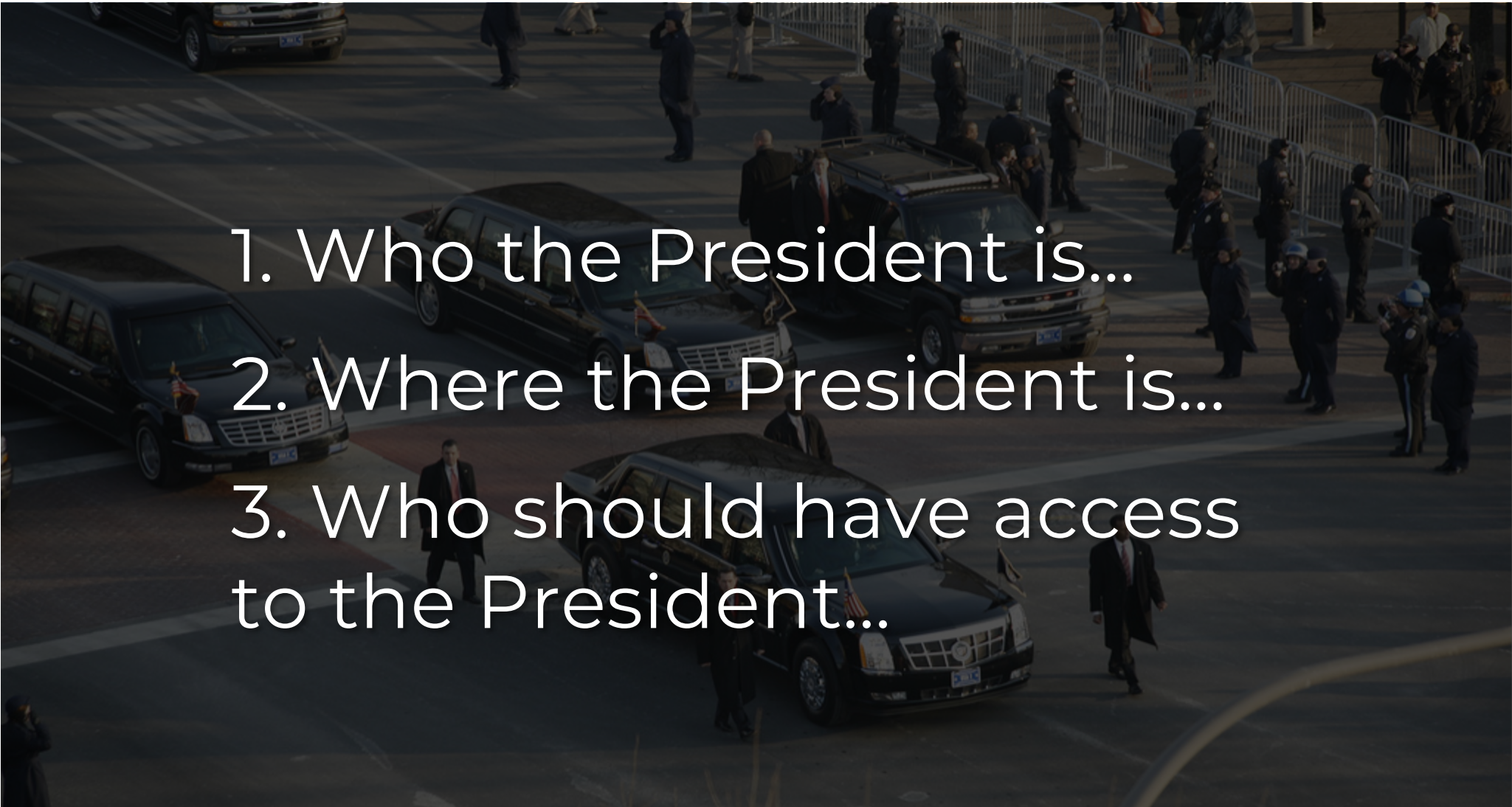
EXPLOITED

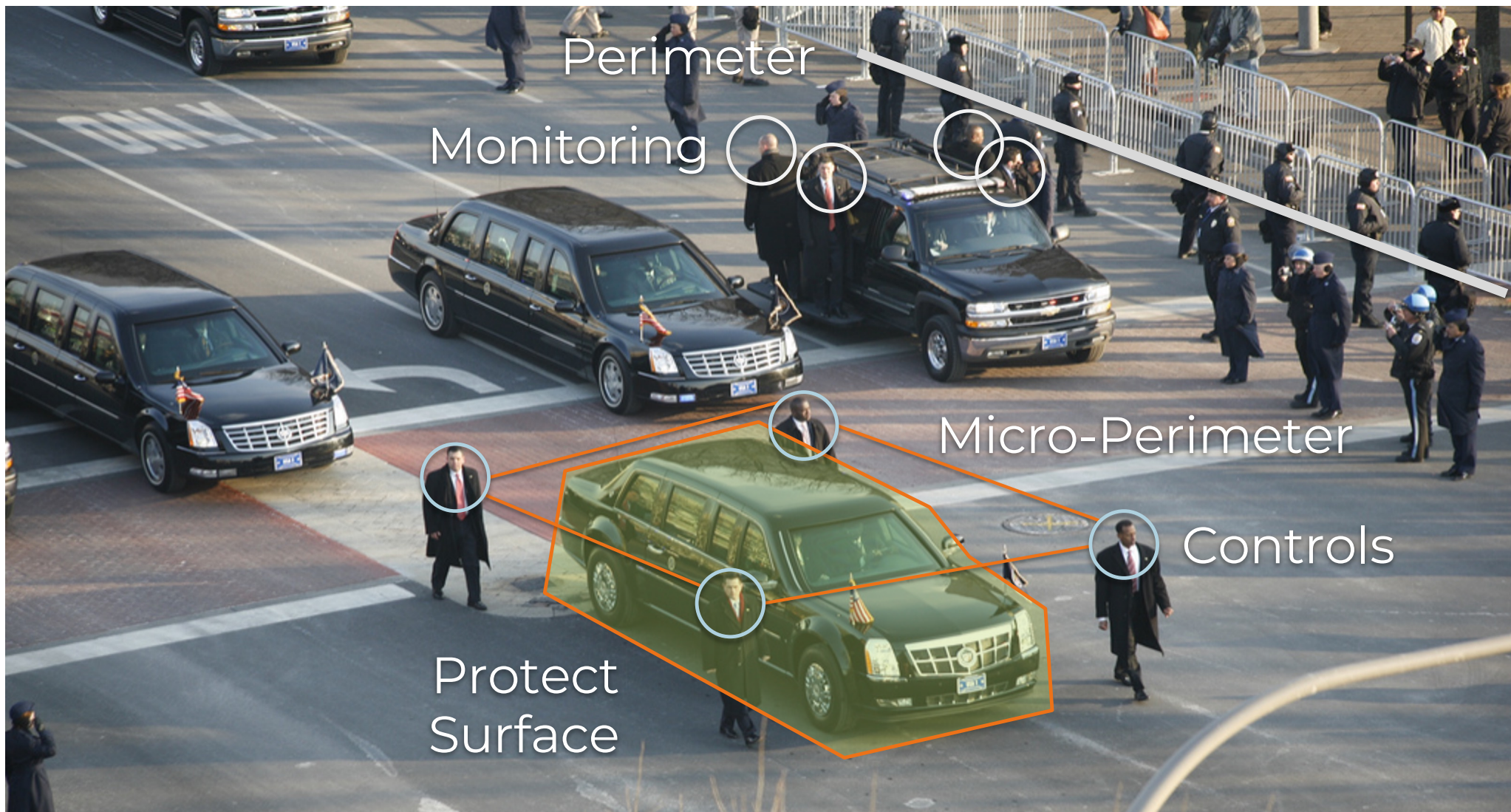
by **MALICIOUS** actors



Zero Trust Design Concepts



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



Perimeter
Monitoring

Micro-Perimeter

Controls

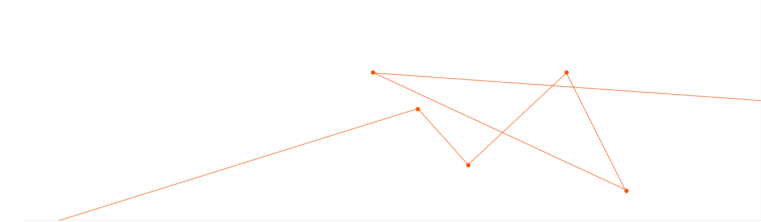
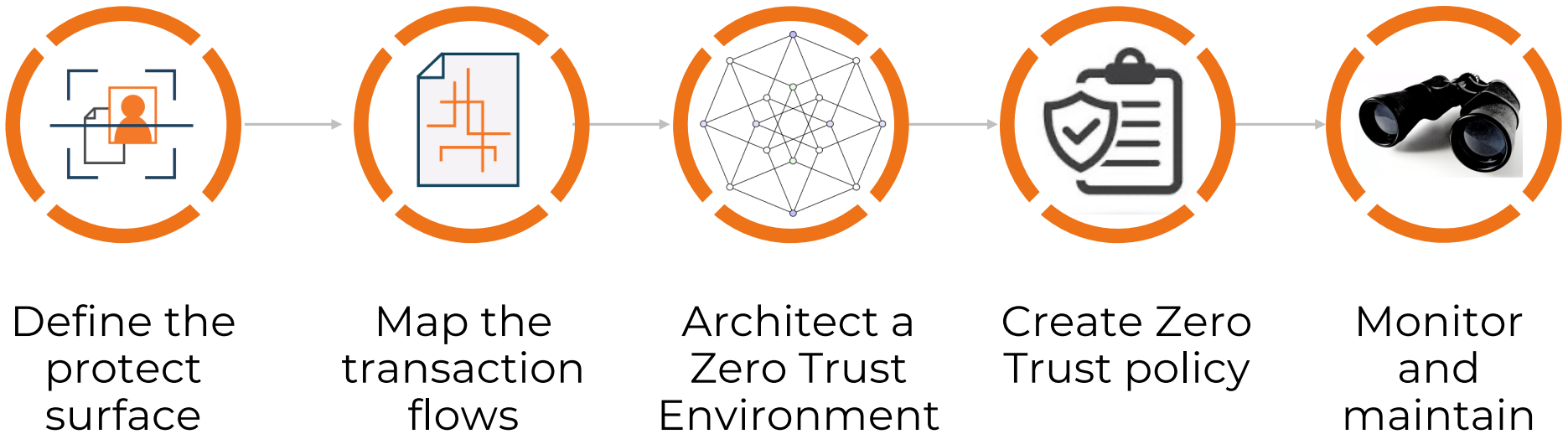
Protect
Surface



ZERO TRUST

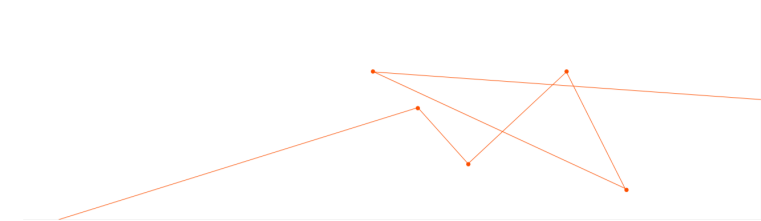
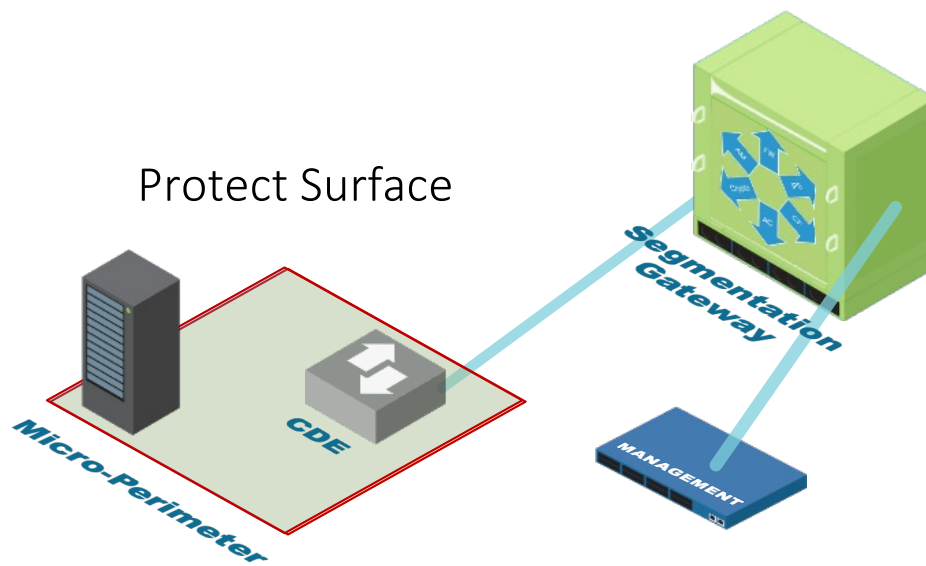


The 5-Step Methodology for Deploying Zero Trust Guides Your Journey



Zero Trust Defines Network Segmentation

1. Why are you segmenting?
2. How are you enforcing segmentation at Layer 2-7?



The Kipling Method of Zero Trust Rule Writing

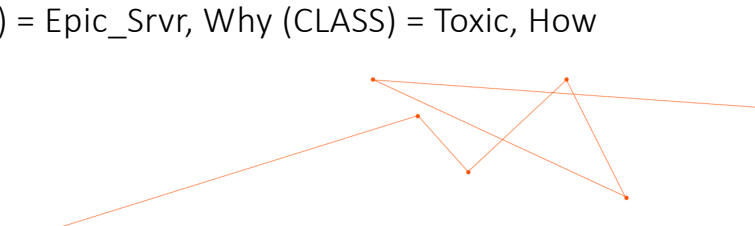
Who	What	When	Where	Why	How
User ID	Application ID	Time Limitations	Device ID	Classification	Content ID
Auth type			System Object	Data ID	Threat Protection
			Workload		SSL Decryption
			Geolocation		URL Filtering
					Wildfire

Cloud:

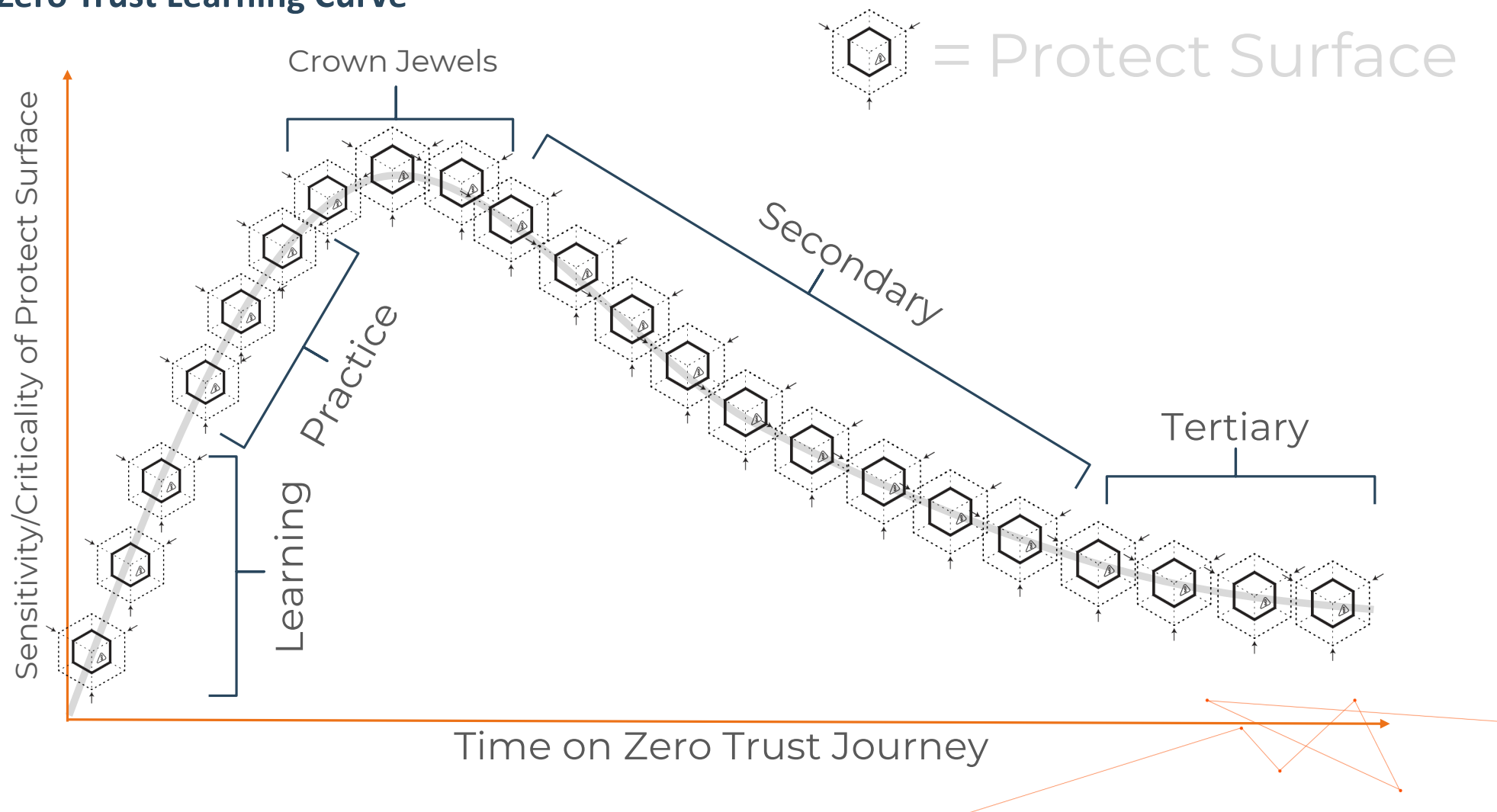
IF Who (UID) = Sales, What (AID) = Salesforce, When (TOD) = Working Hours, Where (LOC) = US, Why (CLASS) = Toxic, How (CID) = SFDC_CID, THEN Allow.

On Prem:

IF Who (UID) = Epic_Users, What (AID) = Epic, When (TOD) = Any, Where (LOC) = Epic_Srvr, Why (CLASS) = Toxic, How (CID) = Epic_CID, THEN Allow.








Zero Trust Learning Curve



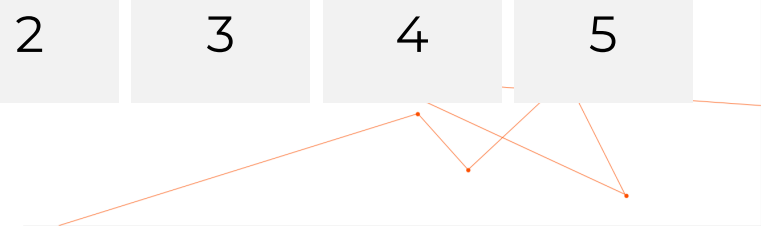
Zero Trust Maturity Model

Protect Surface _____

DAAS Element _____

	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 _____





STAY IN CONTACT



John Kindervag



info@on2it.net



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



ON2IT.net



ABOUT ON2IT:

Easily embrace the protective power of Zero Trust security through ON2IT's Zero Trust-as-a-Service. ON2IT applies Zero Trust, as defined by Creator of Zero Trust and ON2IT SVP, John Kindervag, to your cybersecurity in a convenient and comprehensive managed security services model. ON2IT safeguards your environment through the innovative AUXO™ Zero Trust platform and a team of seasoned cybersecurity analysts with 24x7 eyes-on-glass, who continuously monitor your network, act proactively, and execute threat countermeasures in real-time.

