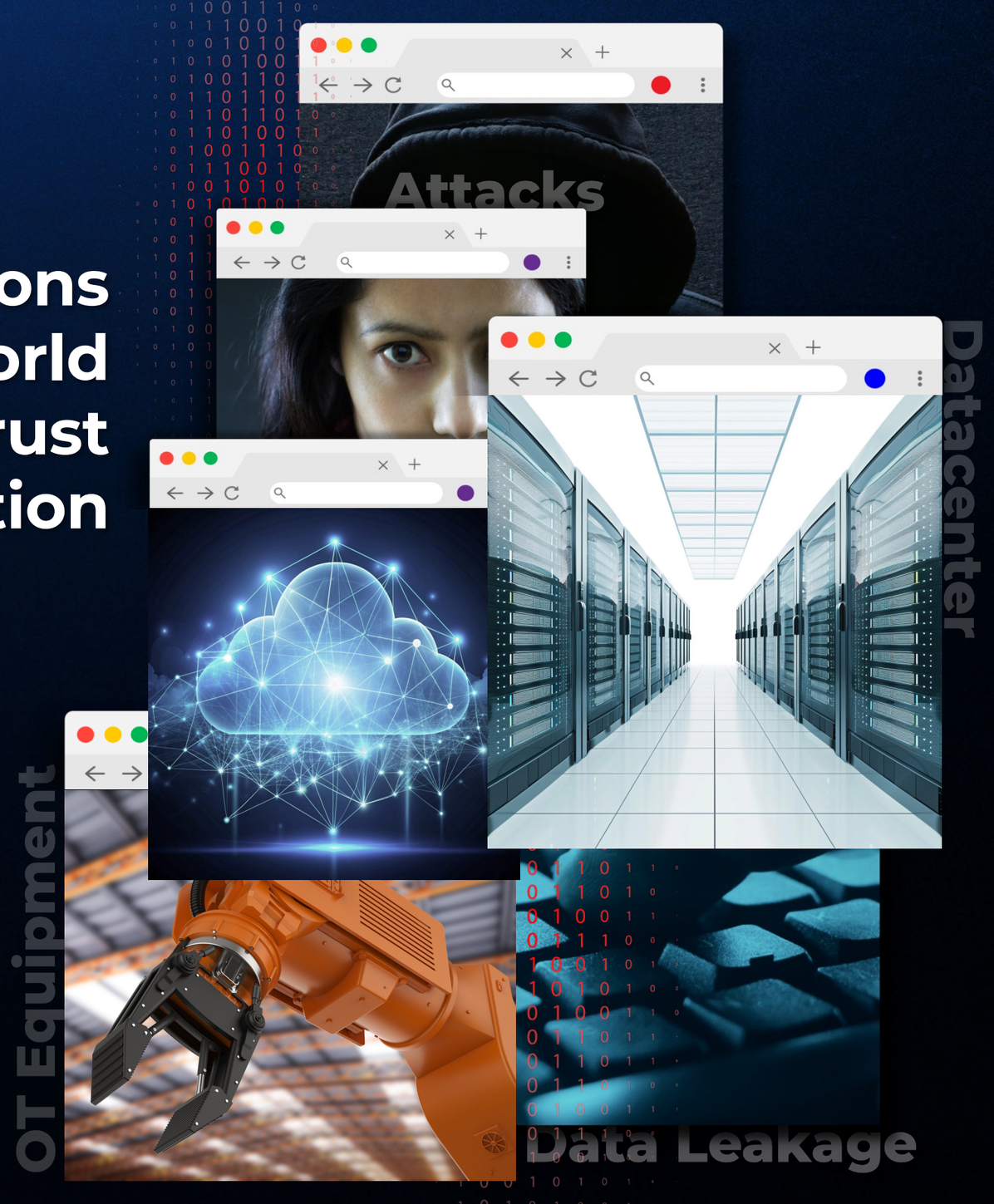
Practical Considerations for Real World Zero Trust Implementation

Mike Ichiriu
VP of Marketing and Product
Zentera Systems, Inc.
Nov 7, 2024



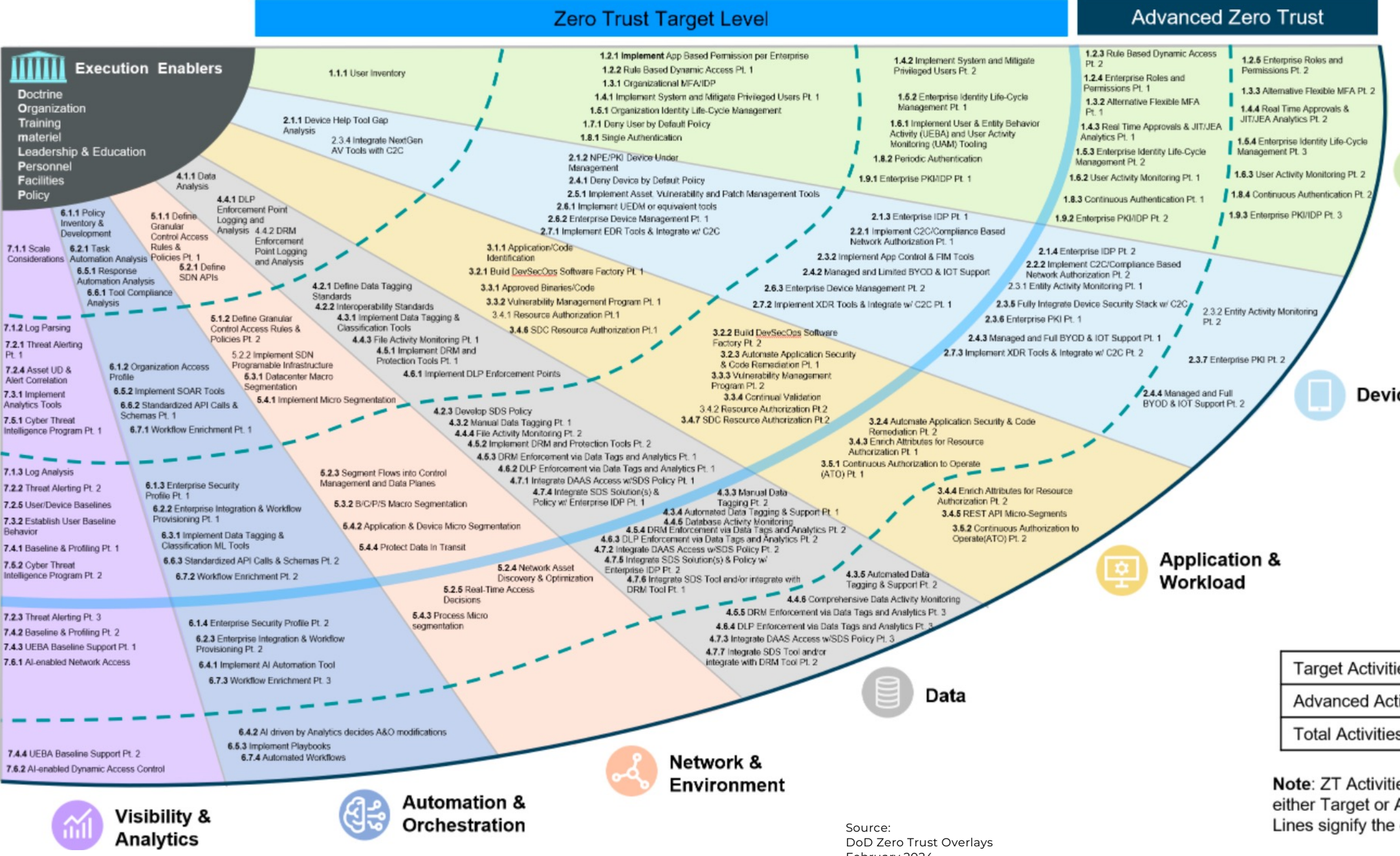
zentera™

What Does

Zero Trust

Make You Think Of?

zentera™



Target Activities	91
Advanced Activities	61
Total Activities	152

Note: ZT Activities are group as either Target or Advanced – Dotted Lines signify the original 5 phases

Source:
DoD Zero Trust Overlays
February 2024
v1.0

zentera™

”No plan survives first contact with the enemy.”

- Helmuth von Moltke the Elder

Source: Wikipedia

zentera™


”Everybody has plans until they get hit for the first time.”
- Mike Tyson

zentera™

Trusted by Major Enterprises to Secure Critical Applications and Data

2012
Year Founded

Silicon Valley-based
(Milpitas, CA)

12
Issued Patents

Global Customers

SIEMENS cādence® Capgemini DELTA

zentera™

What’s at the core of Zero Trust?

Never Trust, Always Verify

Assume Breach

zentera™

“[E]very application should be treated as internet-accessible from a security perspective.”

OMB M-22-09

or in other words

You should be able to open your network to the Internet and not worry about it

(“should be able”, not “should!”)

zentera™

Vision in M-22-09

- Agency systems are isolated from each other

Systems/resources – not networks or infrastructure - are what is protected and segmented

- Network traffic flowing between systems is encrypted

Communications is controlled by *policy*

- Staff have enterprise-managed accounts

User (and server) accesses are based on *identity*

- Security posture of devices is taken into account when granting access

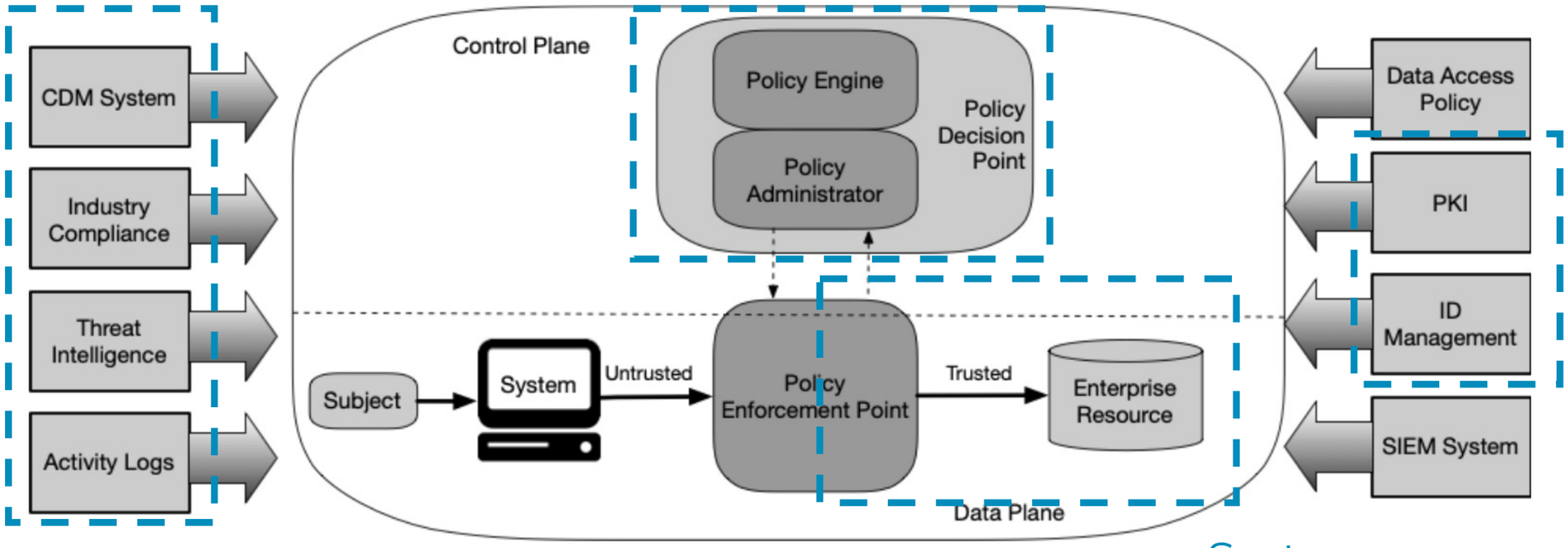
Access policies need to be context-aware

zentera™

M-22-09 Definition Aligns to NIST SP800-207

Context-aware

Policy-Driven



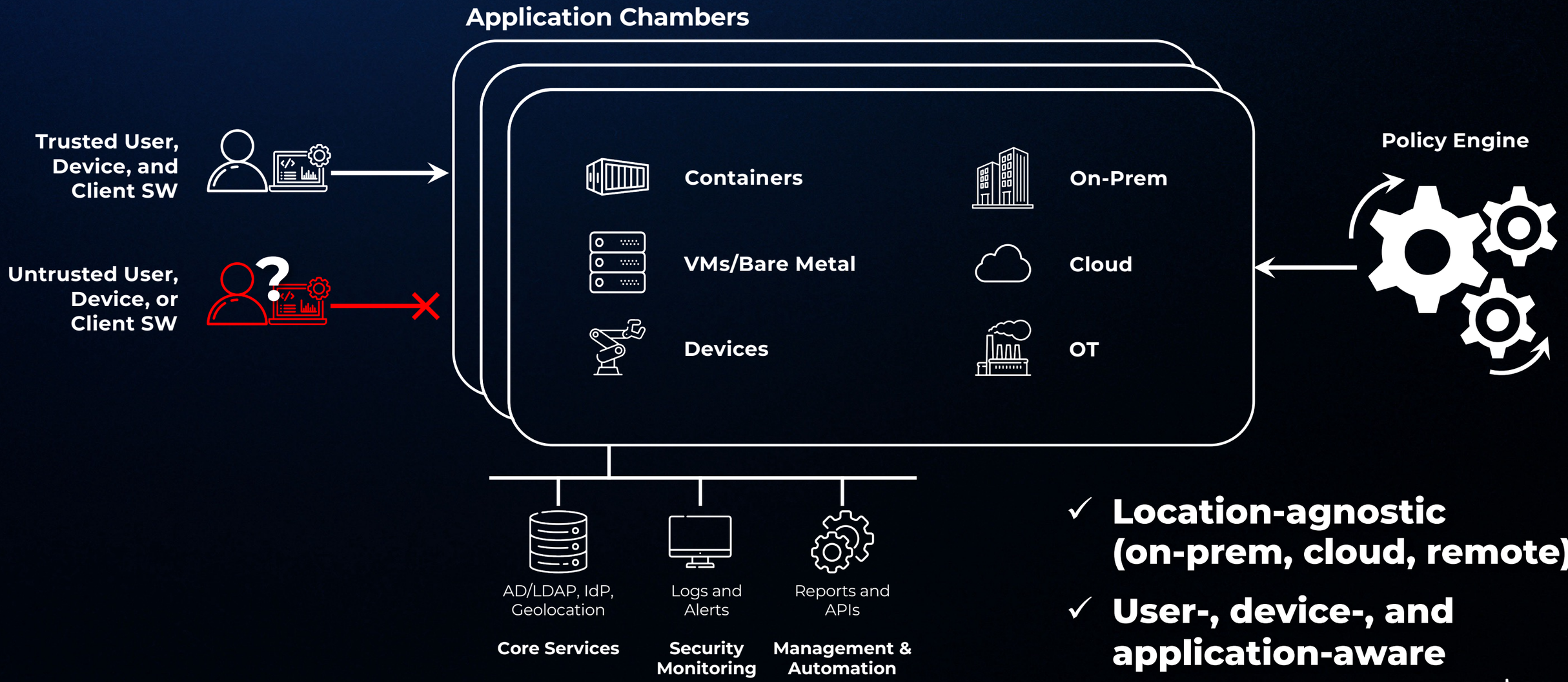
Identity-based

Figure 2: Core Zero Trust Logical Components

System + segmentation boundary

zentera™

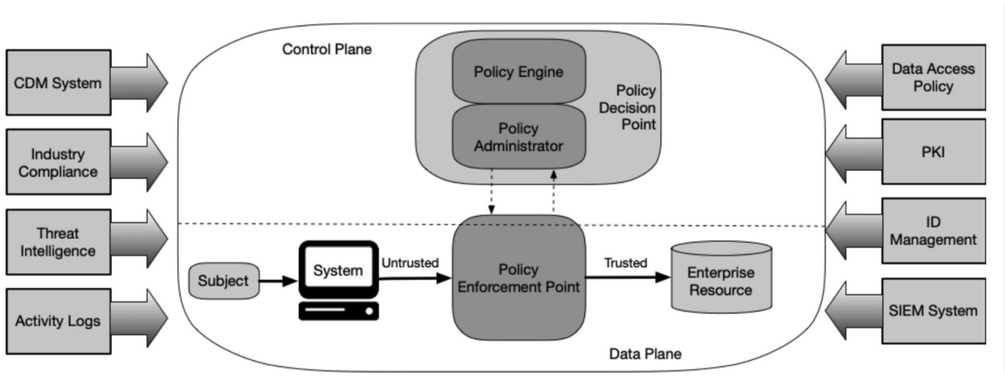
The *Application Chamber*: A Useful Mental Model

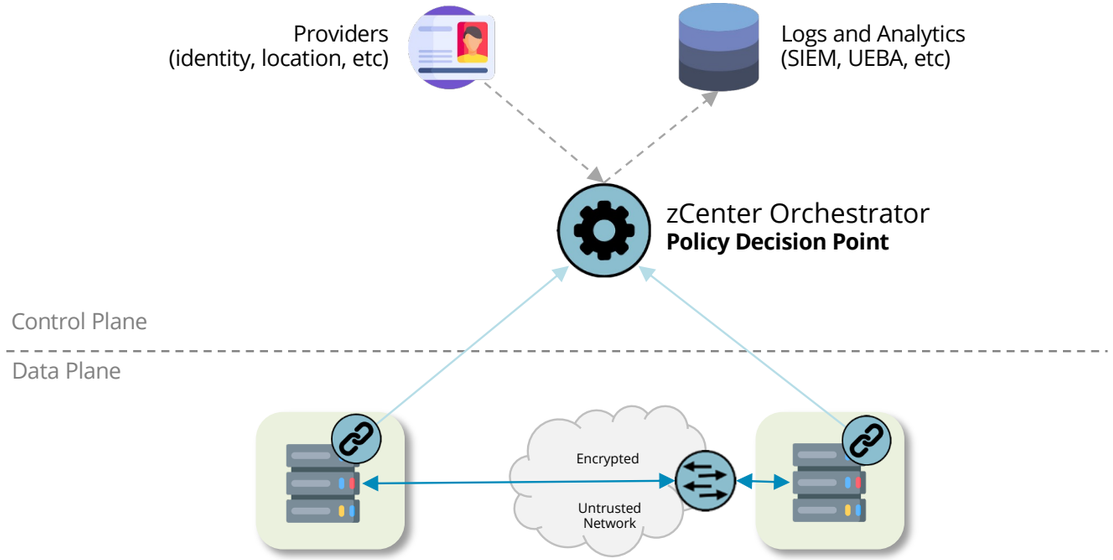


- ✓ **Location-agnostic (on-prem, cloud, remote)**
- ✓ **User-, device-, and application-aware**

zentera™

Mapping to NIST SP800-207 – Resource to Resource





- Policy enforcement at source and destination
- Micro-segmentation and ZTNA natively integrated
- Overlay network allows authorized traffic without opening physical ports
- Avoids “boil the ocean” infrastructure upgrade

zLink Agent
Policy Enforcement Point
ZNS
Overlay Network Switch (optional in LAN)
Virtual Chamber
Implicit Trust Zone

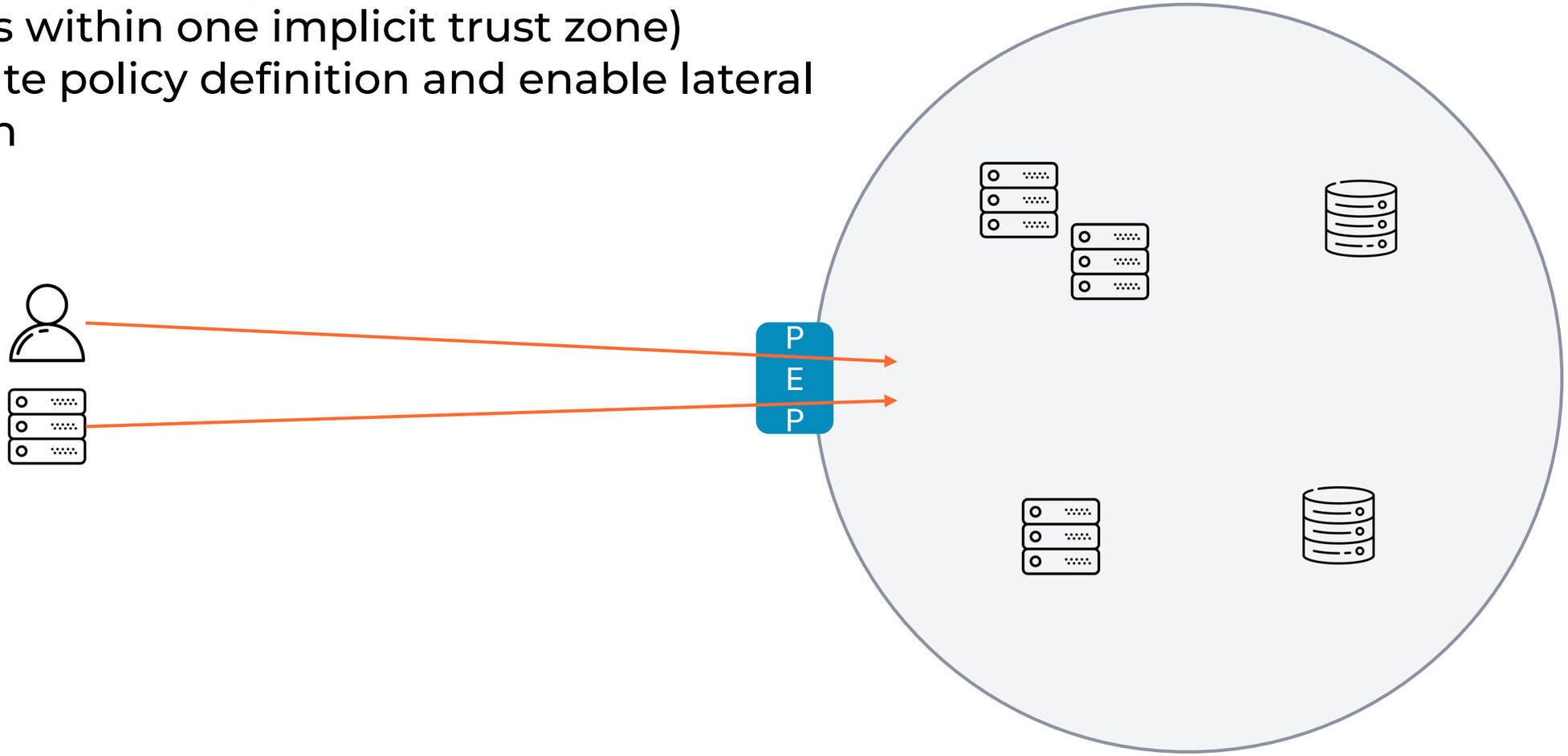
Practical Consideration 1

- How big should each chamber (implicit trust zone) be?

zentera™

How big should each chamber be?

A: Large chambers (groups of dissimilar resources within one implicit trust zone) complicate policy definition and enable lateral migration

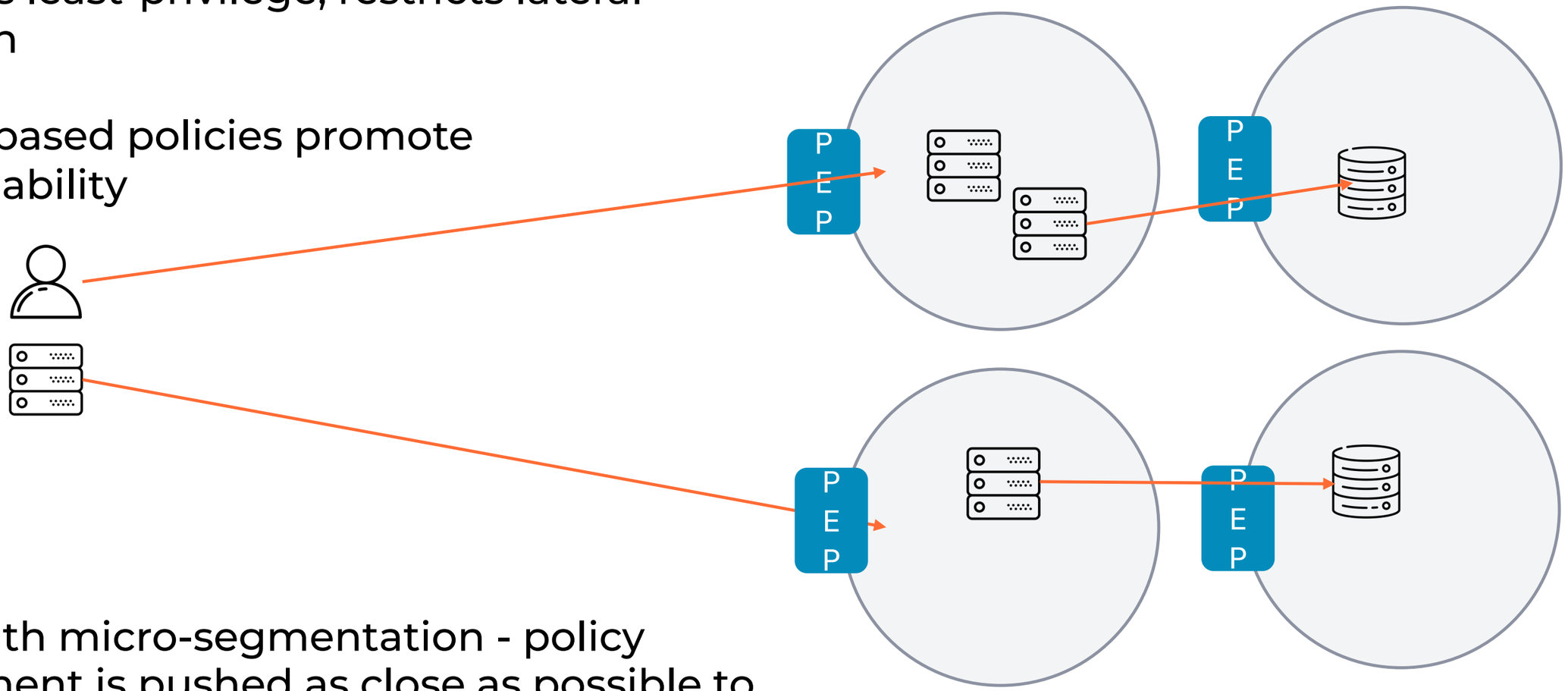


zentera™

How big should each chamber be?

Small chambers grouped into like functions promotes least-privilege; restricts lateral migration

Identity-based policies promote maintainability



Aligns with micro-segmentation - policy enforcement is pushed as close as possible to the workload

zentera™

Practical Consideration 2

- My application already supports a modern ICAM. Don’t I already have Zero Trust?

zentera™

My application already supports a modern ICAM…

A: No.

You wouldn’t put an application on the Internet without a firewall? Treat the internal network like the Internet.

zentera™

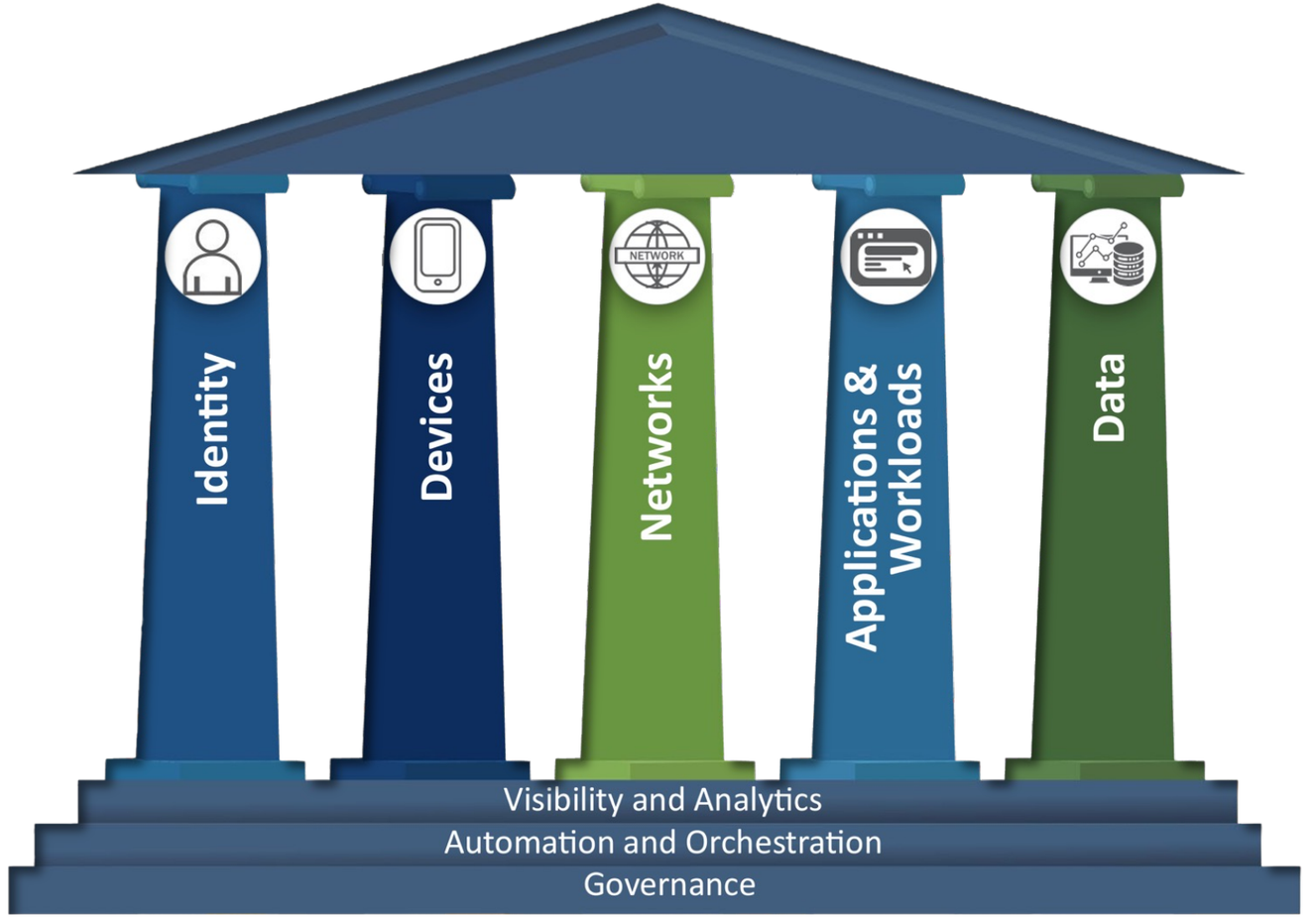
Practical Consideration 3

- What kinds of context do I need in my policies?

zentera™

What kinds of context do I need?

The CISA ZTMM

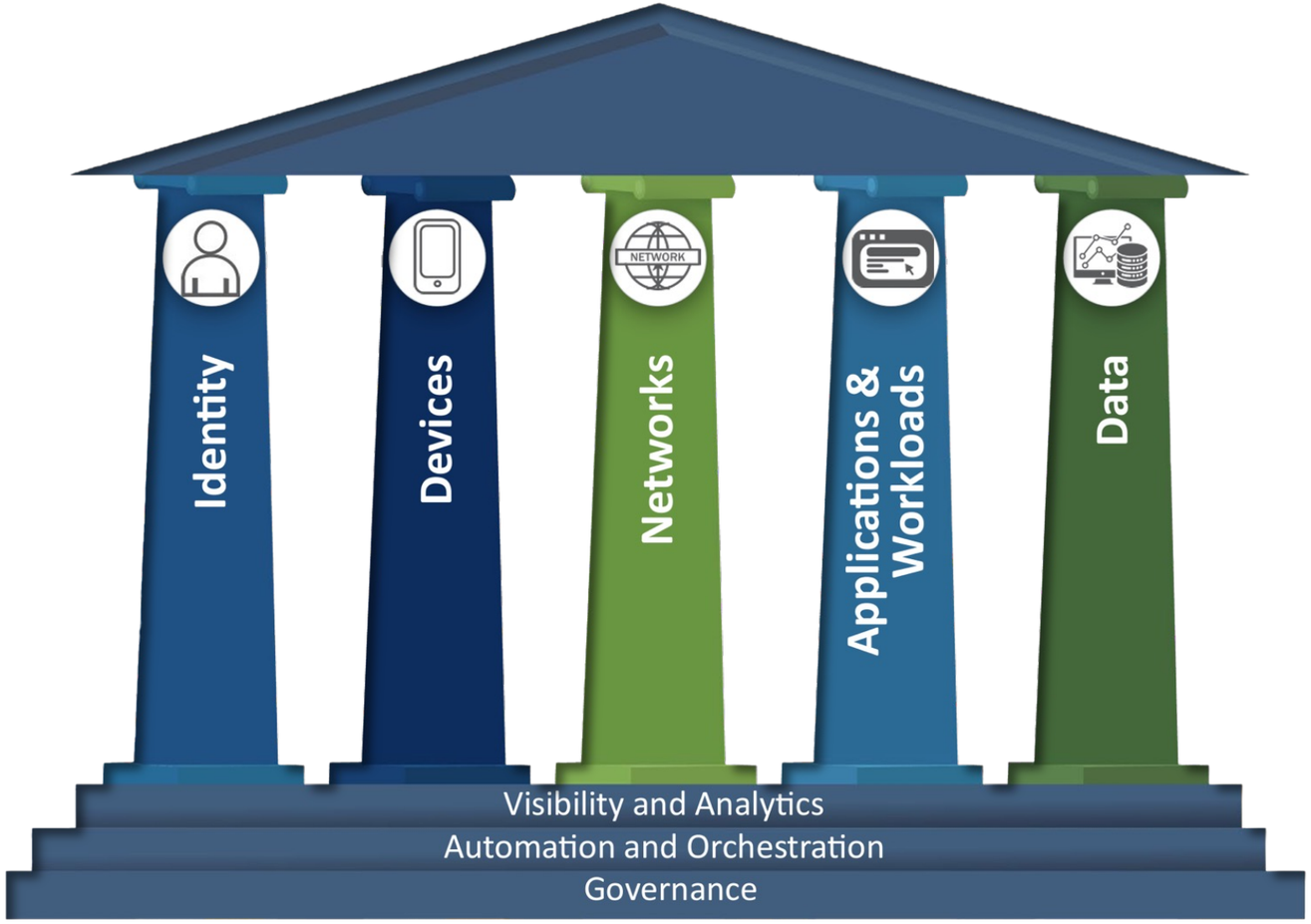


zentera™

The Pitfalls of Pillar Thinking

"Each pillar can progress at its own pace… [but] coordination can only be achieved with capabilities and dependencies compatible with one another and the enterprise-wide environment."

- CISA Zero Trust Maturity Model v2.0, April 2023



zentera™

What kinds of context do I need?

Policies Should Orchestrate Across All Pillars

User/Service Acct — `apache`

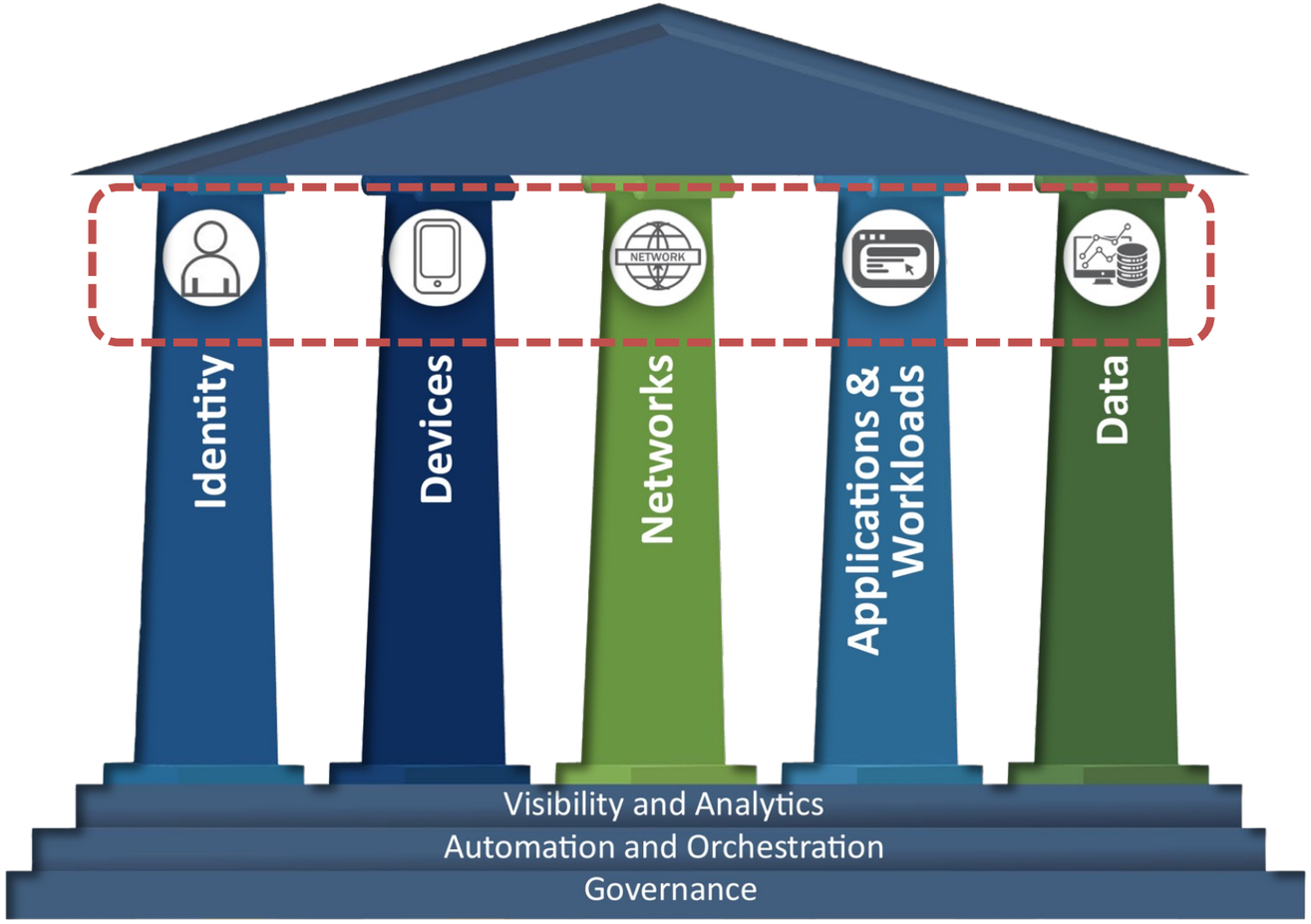
Running On — `Webservers`

Using application — `/usr/bin/java`

To Access — `MySQL Servers`

Containing data — `ERP`

ALLOW AND ENCRYPT IN TLS 1.3
DEFAULT DENY FOR EVERYTHING ELSE



zentera™

Practical Consideration 4

- How do I handle hybrid environments?

zentera™

How do I handle hybrid environments?

A: This is important; the scope of your ZT control must follow the resource and its mission environment.

For example, cloud-based ZT is great, but does not apply to on-prem or OT.

Ideal: look for PDP and PEP solutions to orchestrate across all of your environments so you can use the same ops methodology everywhere.

zentera™

Practical Consideration 5

- What are the limits of a centralized PDP?

zentera™

What are the limits of a centralized PDP?

A: Generally, a centralized PDP is preferred provides a single point for policy definition and management. But it is not always the best solution.

Examples:

- Resources need to be managed by separate commands
- DDIL conditions

Practical Consideration 6

- How can I perform continuous validation without slowing down application performance?

zentera™

How can I perform continuous validation without slowing down application performance?

A: Continuous validation does not require every packet to be validated.

Validate the flow, then move to fast path

Monitor for changes that might invalidate the flow (e.g., policy changes, *Zero Trust factor* changes)

zentera™

Master the Mission…

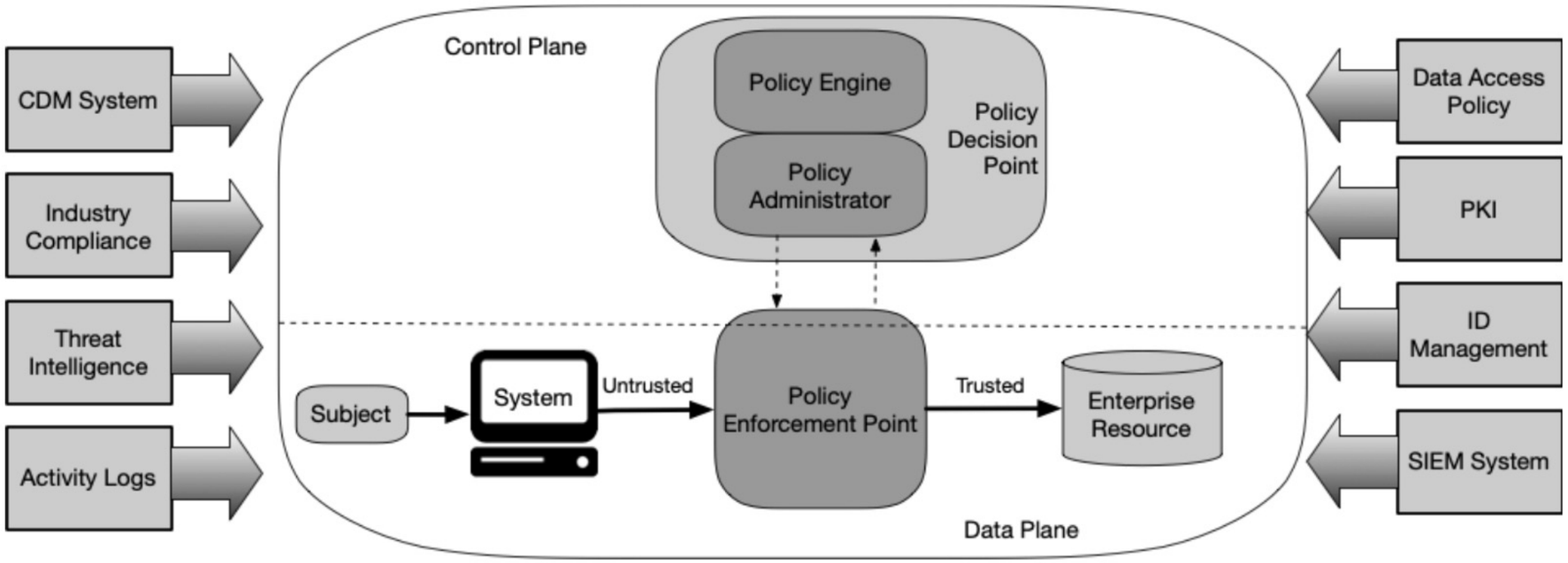


Figure 2: Core Zero Trust Logical Components

zentera™

Master the Mission… Manage the Details

Supported via integration with existing enterprise tools

User	**1.1** AD/ADFS + zCenter	**1.2** zCenter Policy Engine	**1.3** zCenter + IdP	**1.4** zCenter Policy Engine	**1.5** zCenter + IdP	**1.6** zCenter logging + UEBA	**1.7** zCenter Policy Engine	**1.8** zCenter + zLink	**1.9** Enterprise ICAM + zCenter
Device	**2.1** zCenter + zLink	**2.2** zCenter + zLink + EDR	**2.3** zCenter + zLink + EDR	**2.4** zCenter + ZNS + zLink	**2.5** zCenter + zLink + EDR	**2.6** zCenter + UEM/MDM	**2.7** zCenter + EDR/XDR		
Application & Workload	**3.1** zCenter + zLink	**3.2** zCenter Policy Engine + Chamber	**3.3** zCenter + CI/CD	**3.4** zCenter + CI/CD	**3.5** zCenter				
Data	**4.1** Data Catalog + zCenter Policy Engine	**4.2** Data Tagging + zCenter Policy Engine	**4.3** Data Tagging + zCenter Automation	**4.4** zCenter Policy Engine + Chamber	**4.5** CoIP AppLink + 3rd Party Disk Encryption	**4.6** CoIP DLP	**4.7** CoIP Data Policy		
Network & Environment	**5.1** zCenter + zLink Learning	**5.2** CoIP Overlay	**5.3** zCenter + CoIP Virtual Chamber	**5.4** zCenter + CoIP Virtual Chamber					
Automation & Orchestration	**6.1** zCenter	**6.2** zCenter UI / APIs + RPA	**6.3** zCenter	**6.4** zCenter	**6.5** zCenter Logging + SOAR	**6.6** zCenter API	**6.7** zCenter		
Visibility & Analytics	**7.1** zCenter	**7.2** zCenter + SIEM	**7.3** zCenter + SIEM	**7.4** zCenter	**7.5** zCenter + SIEM	**7.6** zCenter + External Tooling			

zentera™

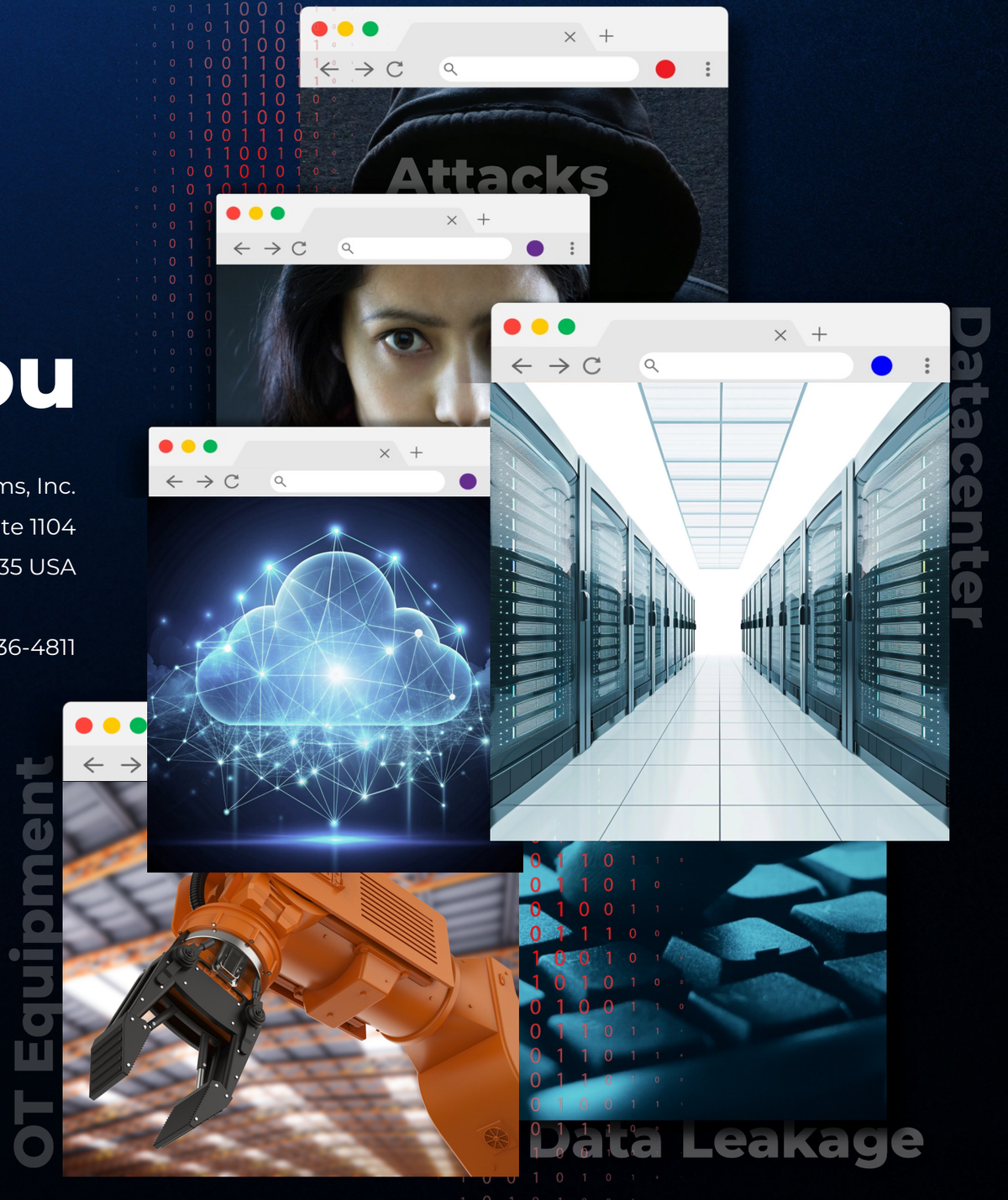
Questions?

zentera™

Thank You

Zentera Systems, Inc.
1525 McCarthy Blvd., Suite 1104
Milpitas, CA 95035 USA

tel: +1 (408) 436-4811



zentera™