cloud security alliance®

Searching for ZERO TRUST

Cloud Security Alliance

107,000+
INDIVIDUAL MEMBERS

100+
CHAPTERS

400+
CORPORATE MEMBERS

35+
ACTIVE WORKING GROUPS

Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

CSA cloud security alliance®

OUR COMMUNITY

2009
CSA FOUNDED

SEATTLE/BELLINGHAM, WA // US HEADQUARTERS

BERLIN // EMEA HEADQUARTERS

SHENZHEN // CHINA CSA NGO

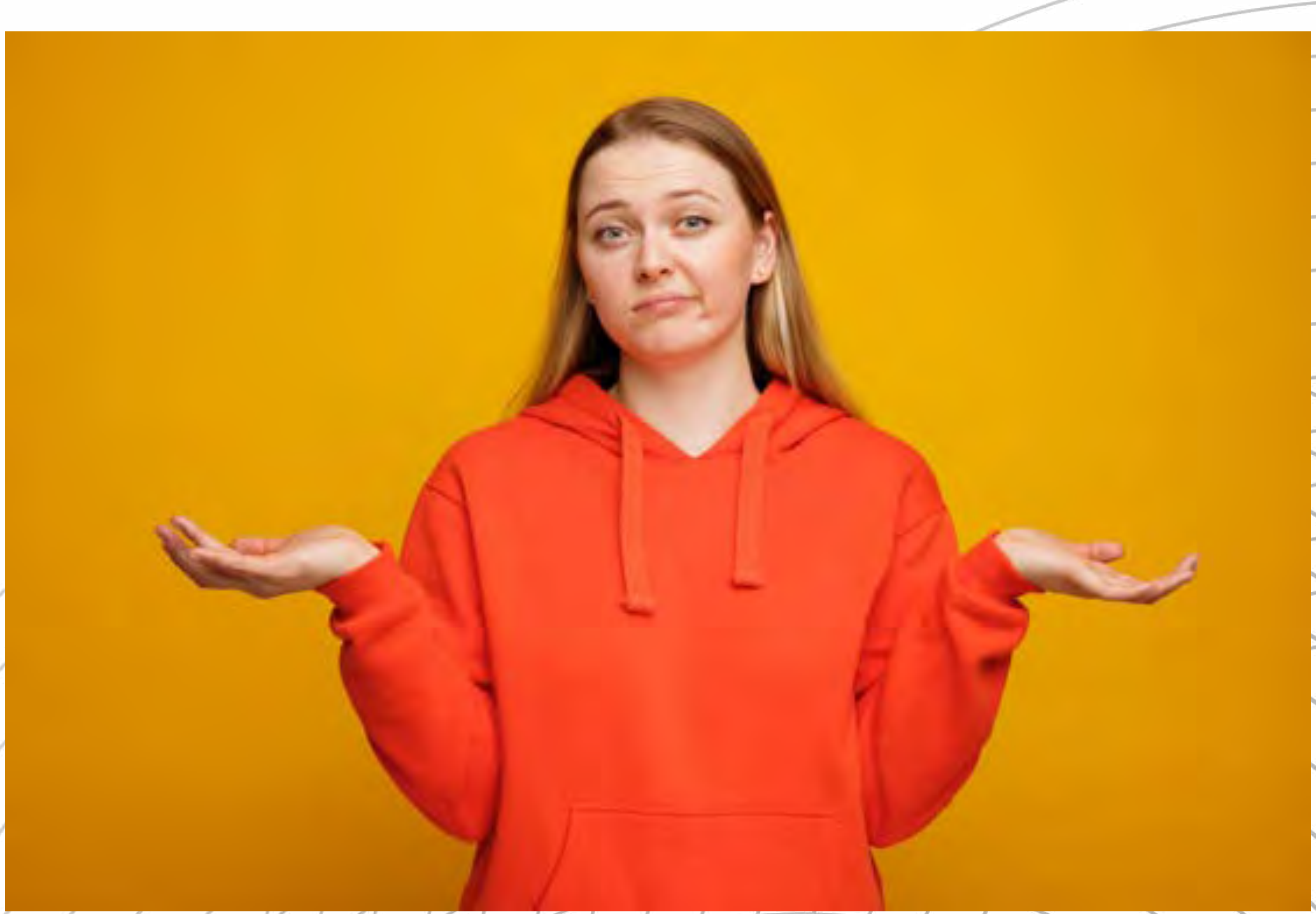
SINGAPORE // ASIA PACIFIC HEADQUARTERS

ZT: What is it?

Not a technology

ZT Definition

There’s no established definition, but a set of high level principles to guide a risk-based approach to cyber resources management in distributed organizations, with distributed supply chain and with distributed services.



It’s a philosophy

The definition CSA is using

Zero Trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified.

THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

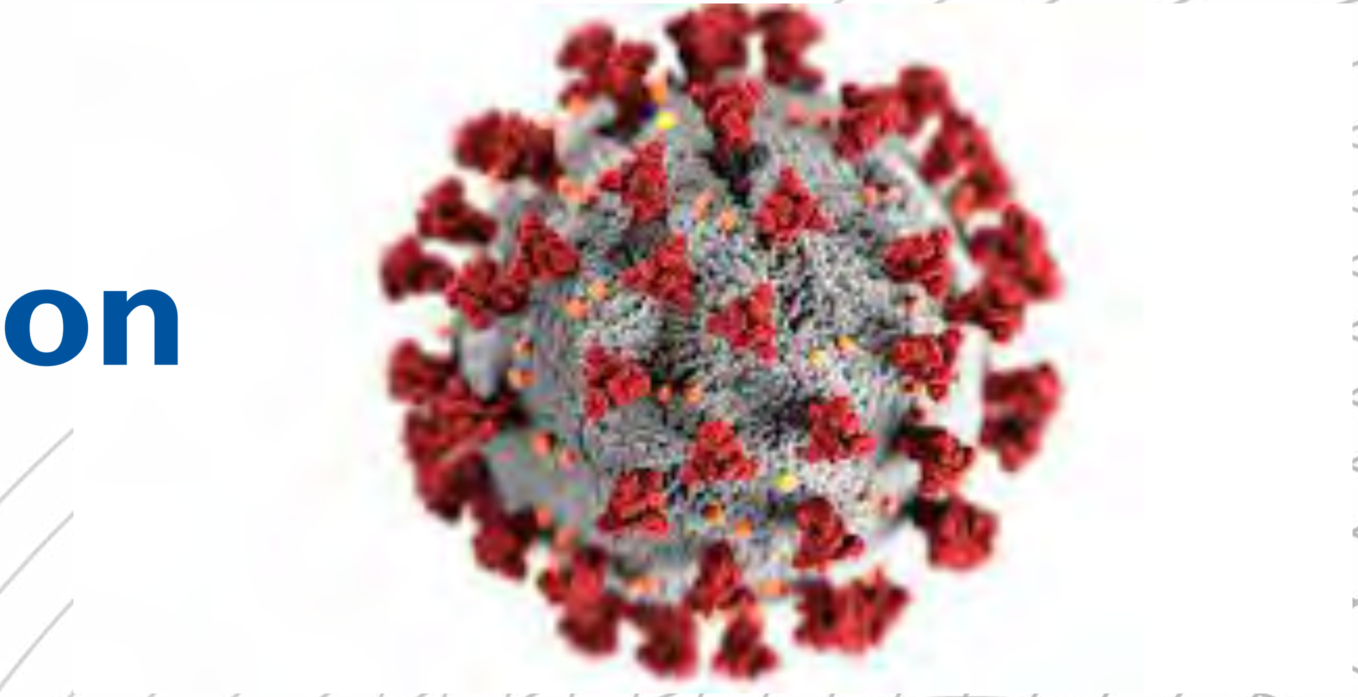
DRAFT REPORT TO THE PRESIDENT

Zero Trust and Trusted Identity Management

Context

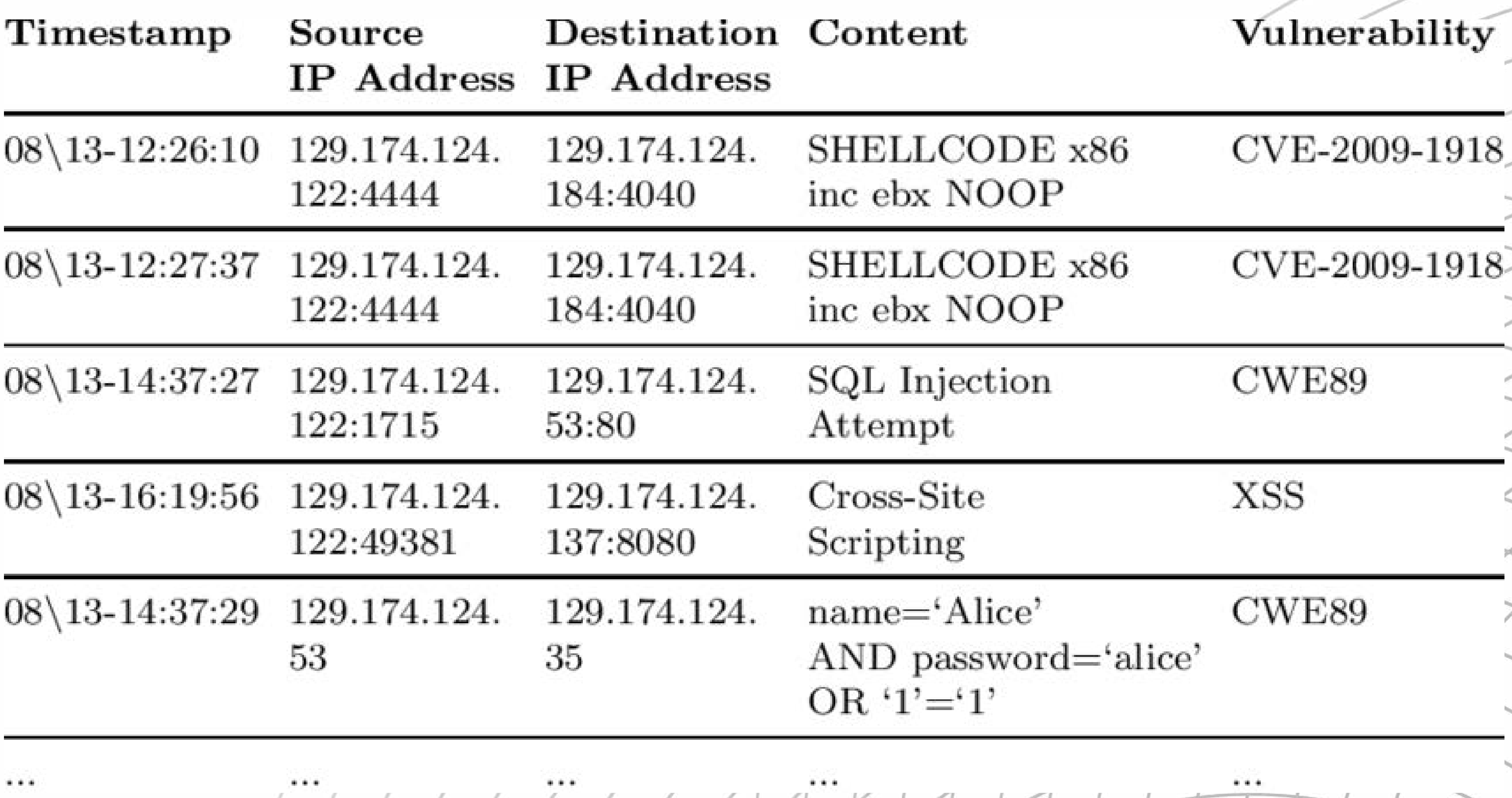
Complexity

Acceleration



Skepticism

Evidence Based Trust

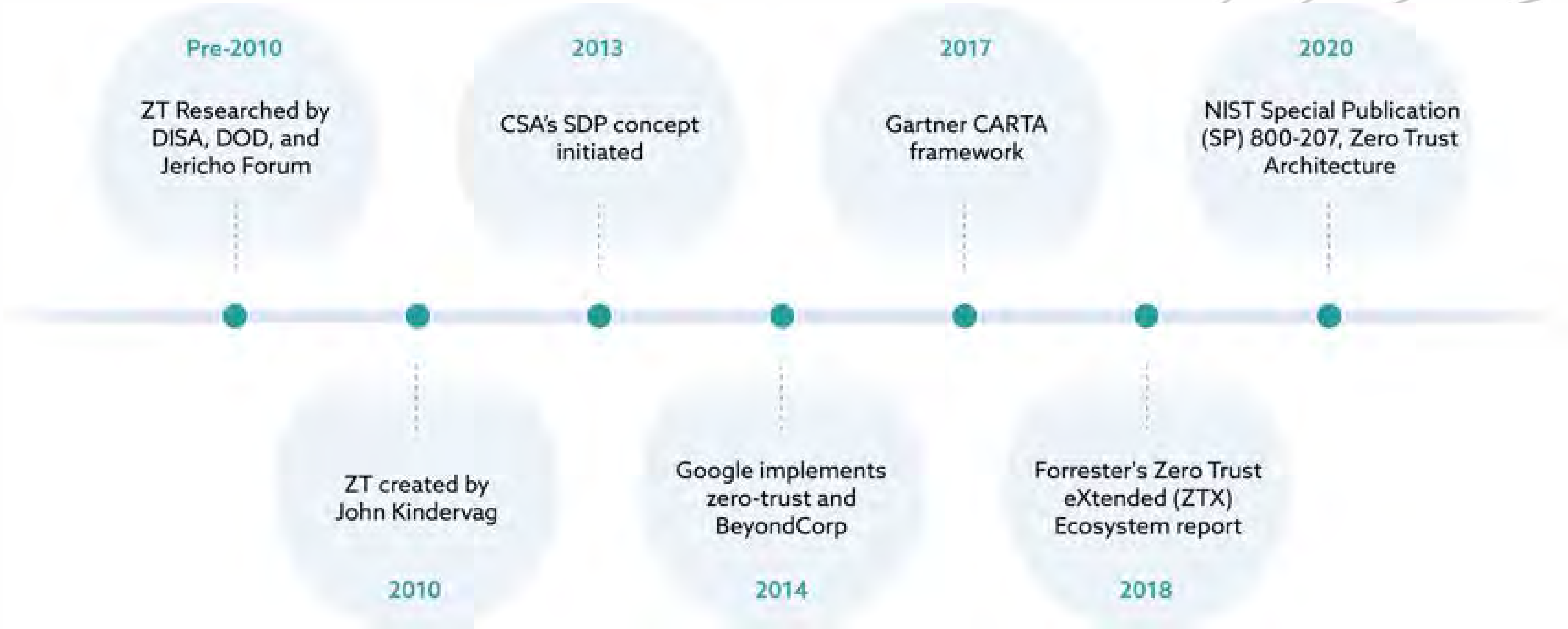


Timestamp	Source IP Address	Destination IP Address	Content	Vulnerability
08\13-12:26:10	129.174.124.122:4444	129.174.124.184:4040	SHELLCODE x86 inc ebx NOOP	CVE-2009-1918
08\13-12:27:37	129.174.124.122:4444	129.174.124.184:4040	SHELLCODE x86 inc ebx NOOP	CVE-2009-1918
08\13-14:37:27	129.174.124.122:1715	129.174.124.53:80	SQL Injection Attempt	CWE89
08\13-16:19:56	129.174.124.122:49381	129.174.124.137:8080	Cross-Site Scripting	XSS
08\13-14:37:29	129.174.124.53	129.174.124.35	name='Alice' AND password='alice' OR '1'='1'	CWE89
...	...	...	...	...

Misnomer?

Memory Lane

ZT Timeline



Pre-2010

ZT Researched by DISA, DOD, and Jericho Forum

2010

ZT created by John Kindervag

2013

CSA's SDP concept initiated

2014

Google implements zero-trust and BeyondCorp

2017

Gartner CARTA framework

2018

Forrester's Zero Trust eXtended (ZTX) Ecosystem report

2020

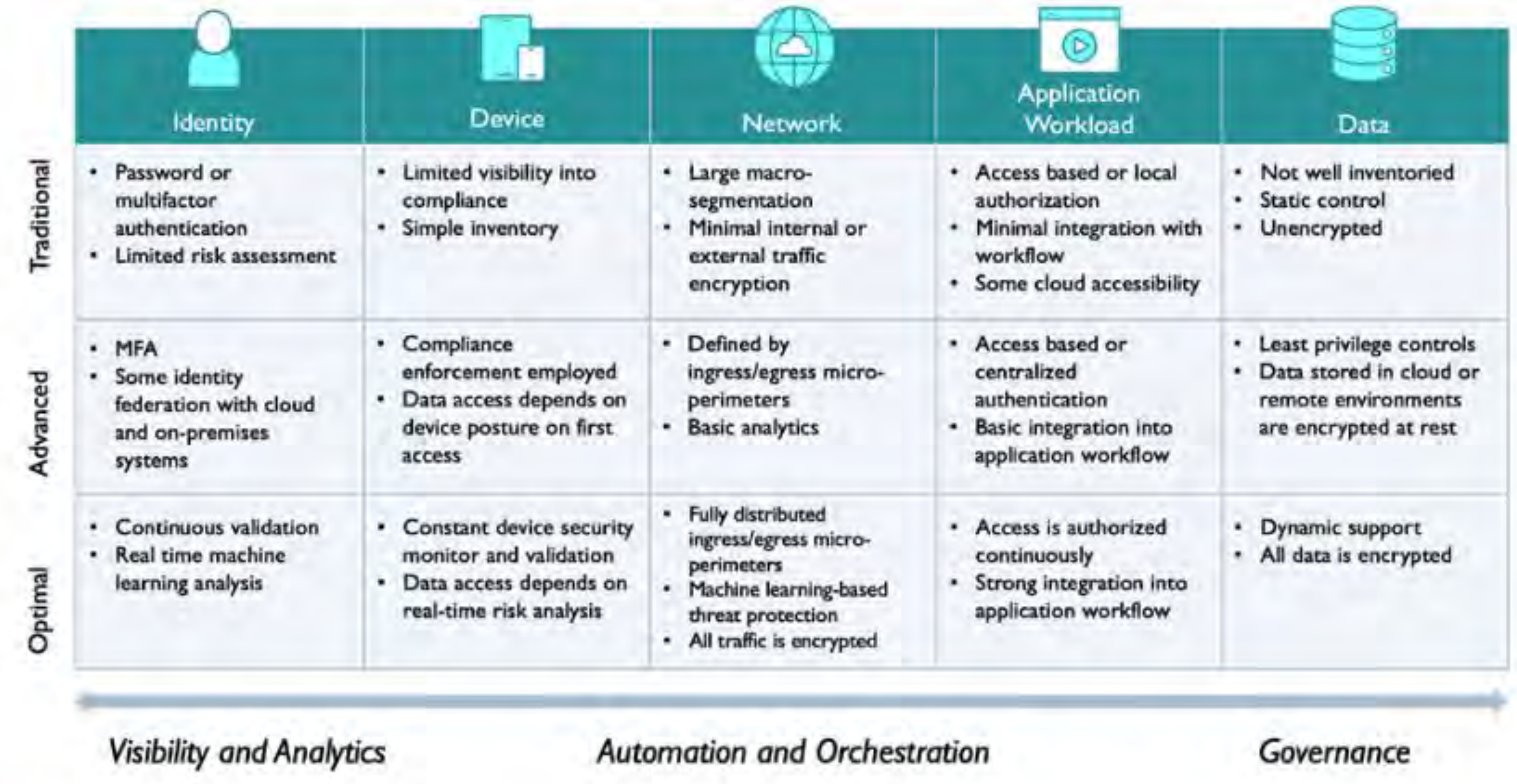
NIST Special Publication (SP) 800-207, Zero Trust Architecture

Principles

ZT Principles

- Design the system from the inside out, starting from the surface you want to protect.
- Trust no one and nothing, until validated and verified (make no assumptions, assume hostile environment, presume breach).
- Enforce the need to know and least privilege access principles.
- Define/Change access requirements and policies based on risk and context.
- Monitor (continuously) what’s happening.

Pillars and Maturity Model



	Identity	Device	Network	Application Workload	Data
Traditional	• Password or multifactor authentication • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based or local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based or centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analysis	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted

Visibility and Analytics *Automation and Orchestration* *Governance*

Figure 1.5.1: *CISA High-Level Zero Trust Maturity Model*[18]

Objectives and Benefits

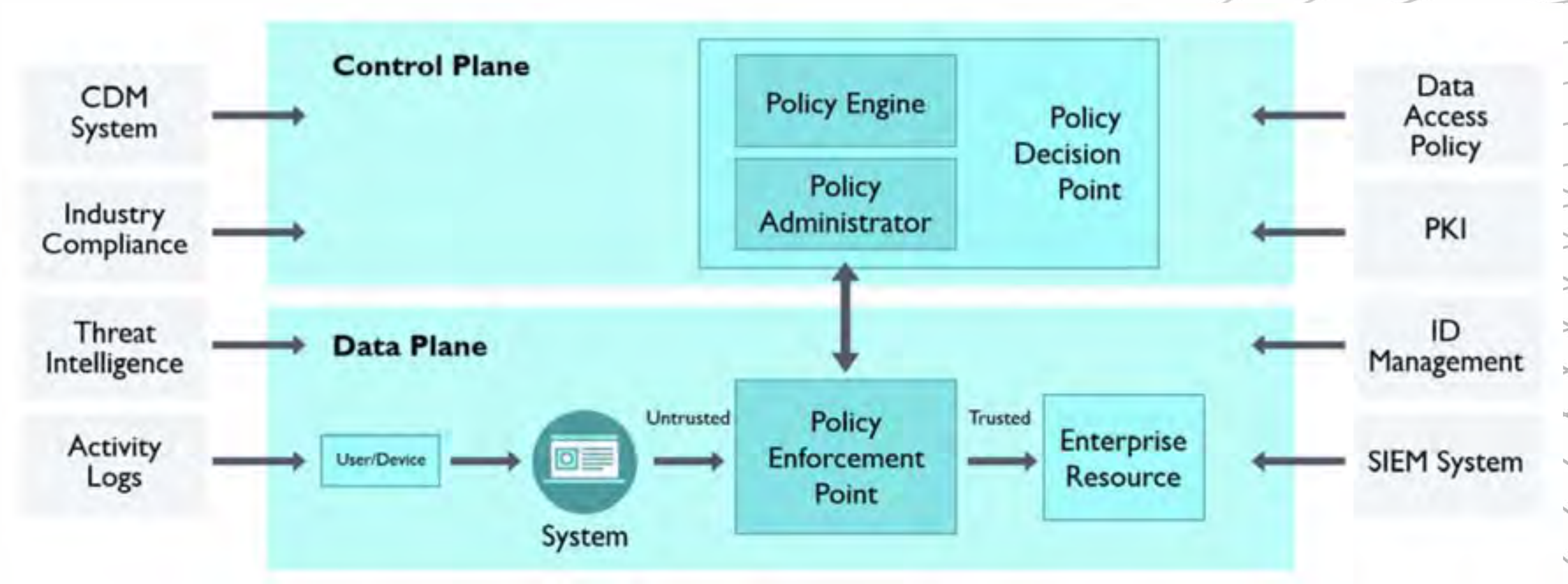
ZTA Objectives and Benefits

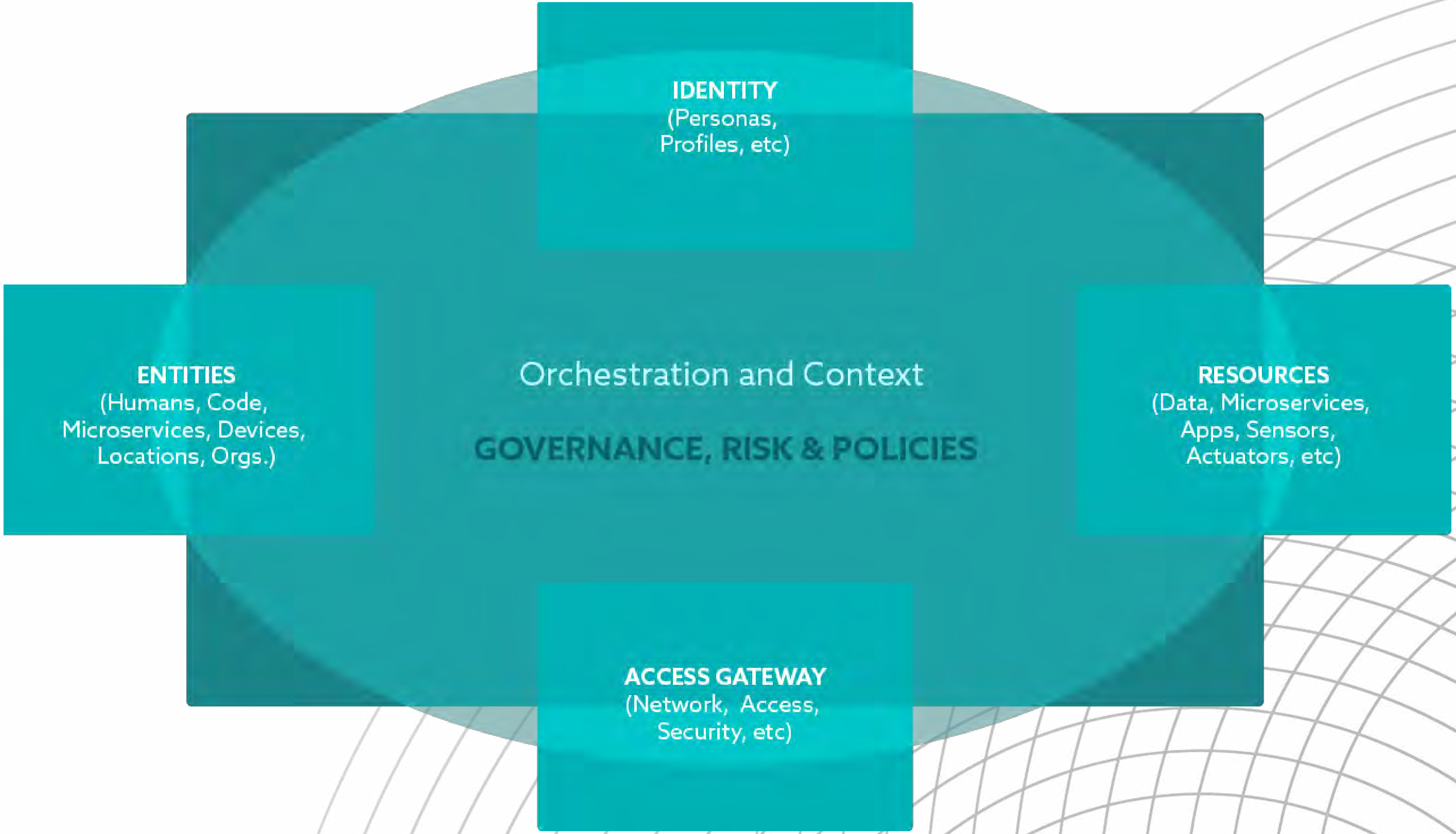
- Reduce Risk
- Improve Organizational Accountability
- Establishing a Protective Framework
- Simplify User Experience
- Reduce Attack Surface
- Reduce Complexity

- Enforce the Least Privilege and Need to Know Principles
- Improve Security Posture & Resilience
- Improve Incident Containment & Management
- Improve Compliance Management

Logic and Models

Logical Components / NIST





IDENTITY
(Personas, Profiles, etc)

ENTITIES
(Humans, Code, Microservices, Devices, Locations, Orgs.)

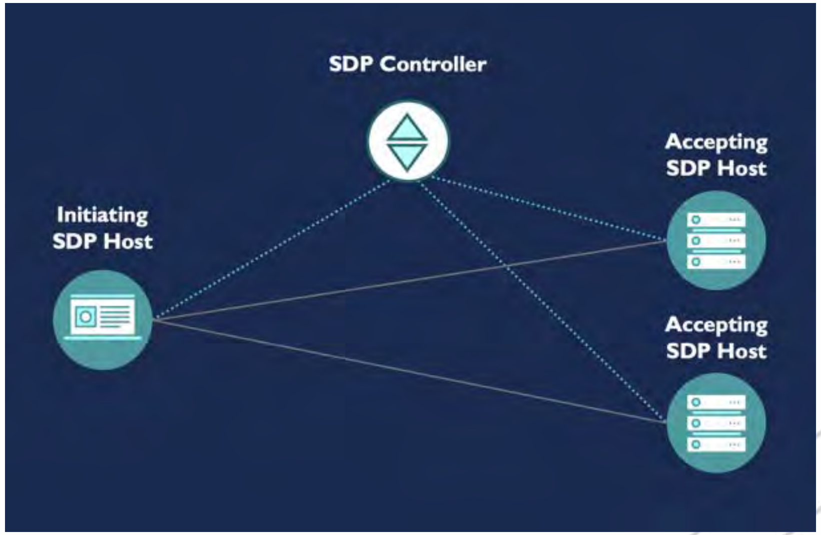
Orchestration and Context

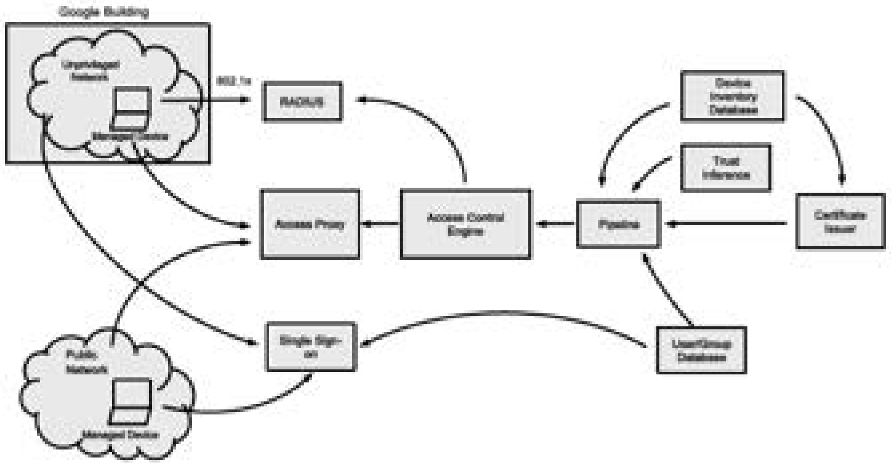
GOVERNANCE, RISK & POLICIES

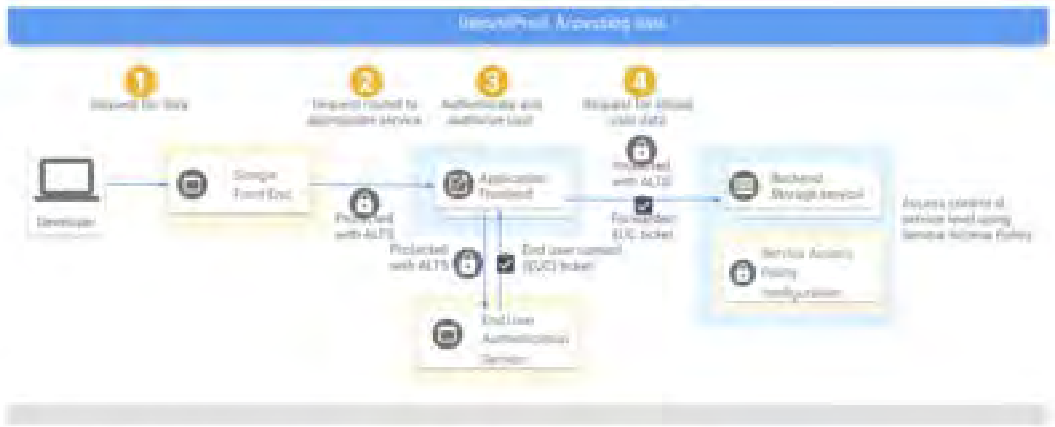
RESOURCES
(Data, Microservices, Apps, Sensors, Actuators, etc)

ACCESS GATEWAY
(Network, Access, Security, etc)

Implementation Models



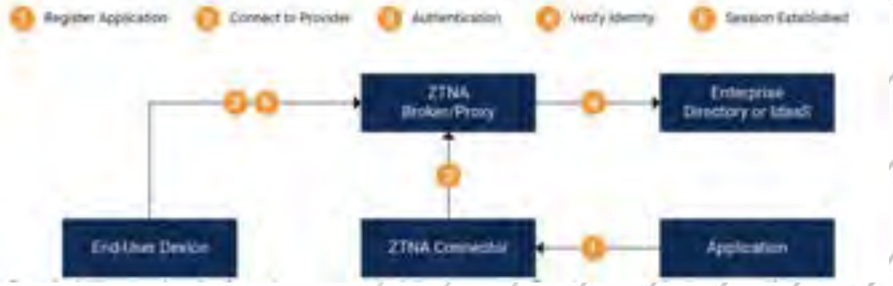




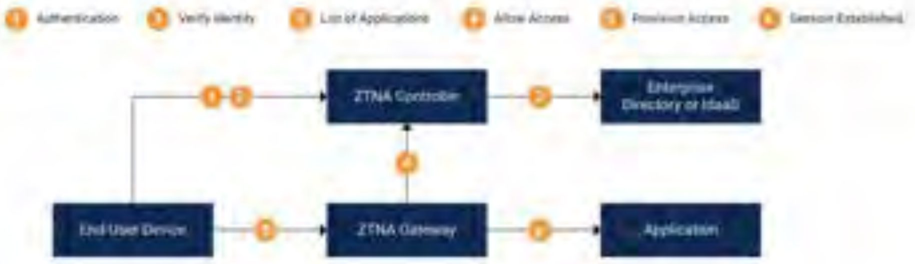
Request for data
Request routed to application service
Authenticate and authorize user
Request for stored user data
Developer
Google Front End
Protected with ALTS
Application Frontend
Protected with ALTS
End user context (EUC) ticket
Protected with ALTS
Forwarded EUC ticket
Backend Storage service
Service Access Policy
End User Authentication Service
Access control at service level using Service Access Policy

Figure 1: Google's cloud-native architecture security controls —accessing user data

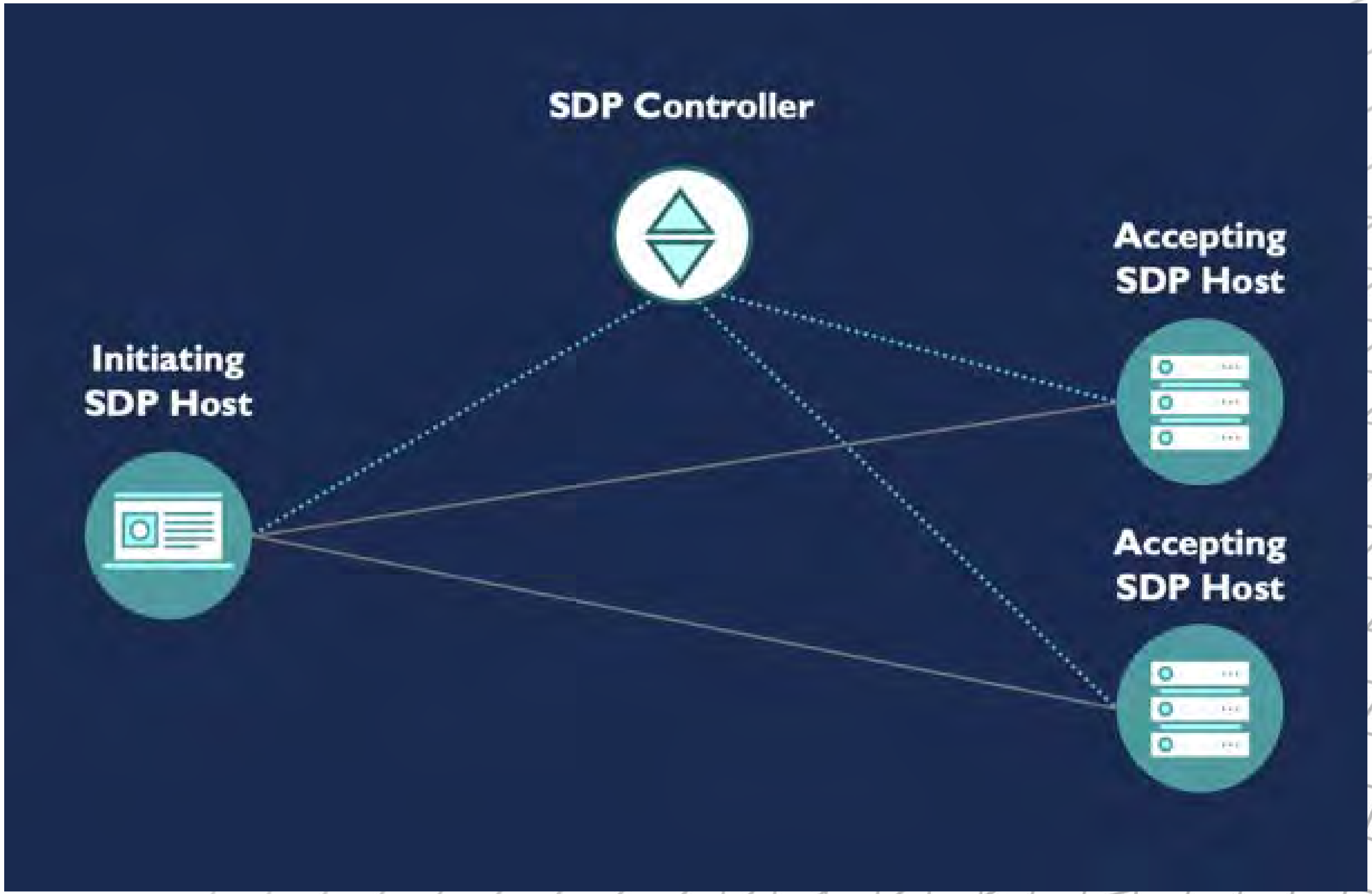
Conceptual Model of Service-initiated ZTNA



C



Implementation Models: Software Defined Perimeter



Strategy & Planning

Strategy and Planning

- It is primarily about risk management
- Understand your needs, your current state and define the goals (use cases)
- Determine which assets (data/services/etc.) are involved / what do you need to protect?
- Determine which entities (humans and non) are involved
- Define/Refine the IAM approach

- Select the service architecture / What are the data flows?
- Select the ZT implementation model and approach
- Define your policies
- Select the technology
- Monitor and review based on the risk and context

BE AGILE!

ZERO TRUST

Advancement Center

Collective knowledge guiding zero trust implementation

CSA cloud security alliance®
CROWDSTRIKE
okta
zscaler

Questions?

Contact

Links to the CSA's work on ZT and SDP can be found in the Attachments section.

Research

https://cloudsecurityalliance.org/research/

CSA STAR
https://cloudsecurityalliance.org/star/#_overview

Cloud Controls Matrix
https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_downloads

Training
https://cloudsecurityalliance.org/education/

Membership
https://cloudsecurityalliance.org/membership/

Daniele Catteddu, Chief Technology Officer, CSA

dcatteddu@cloudsecurityalliance.org

ZT@cloudsecurityalliance.org

Cloudsecurityalliance.org/ZT