ZERO TRUST

A CUSTOMER AND PRACTITIONER’S PERSPECTIVE

Manoj Sharma

Global Head, Security Strategy

Symantec Enterprise Division, Broadcom

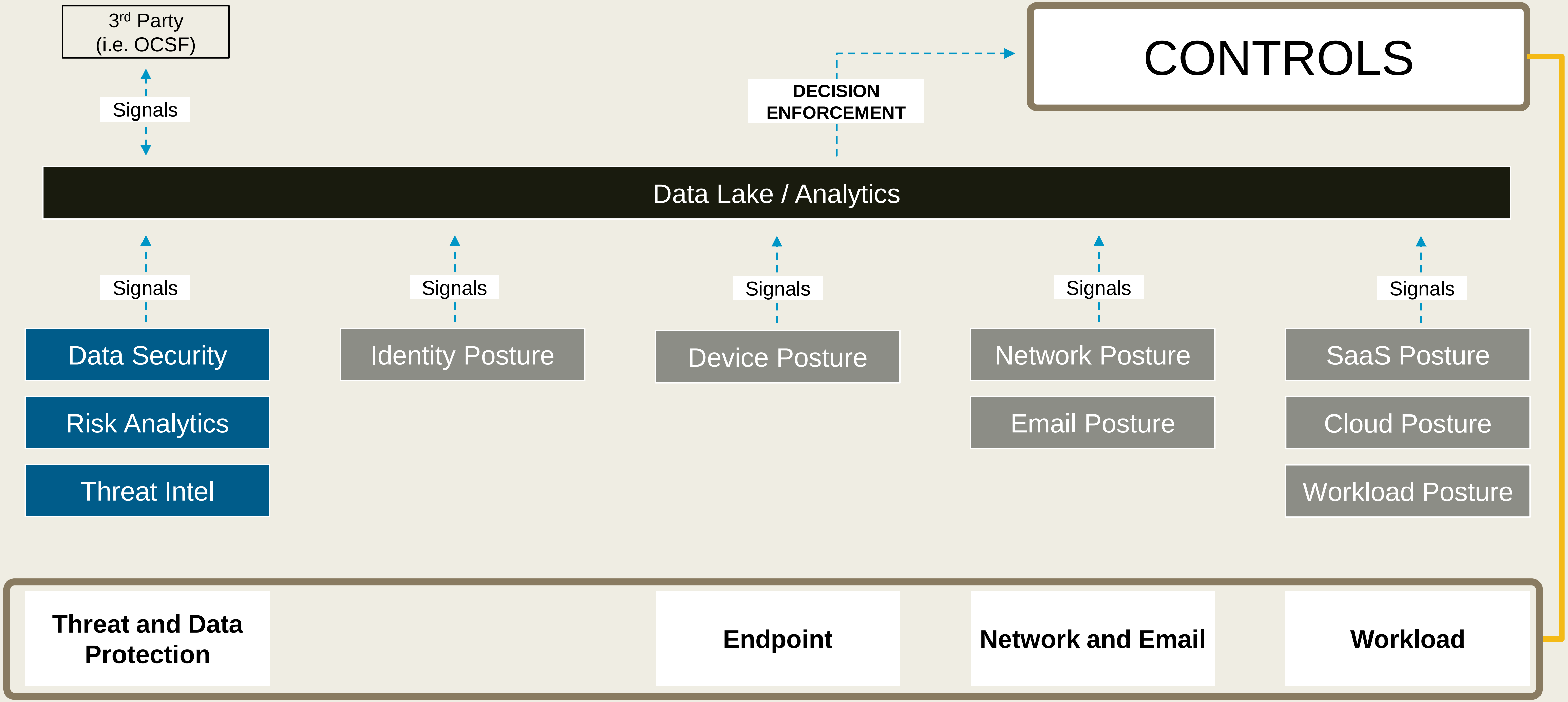
IDENTIFY → ASSUME BREACH → COTINUOUS VERIFICATION → PRINCIPLE OF LEAST PRIVILEGE

Zero Trust

Customer Acceptance v/s Adoption

- Accepted as a layered Security Framework
- Most FSI / Regulated Verticals consider ZT a true security (v/s compliance) framework
- Challenging Journey
  - *Is it going to disrupt my business continuity?*
  - *Common question: Where do we start? Micro-segmentation?*
  - *Common Answer: Let's start with ZTNA – Access centric ZT*
  - *Usually an afterthought: Data centric Zero Trust*
- Zero Trust as a design principle
- Real Time controls are challenged with evolving protocol landscape

A Vision of Zero Trust Architecture



Zero Trust: Evolving Use Cases

Software Supply Chain Security

- Zero Trust for Software Supply Chain Security
  - *How do you build trust with vendors?*

- Customers – Essential Services as asking for the SBOM before contracts are signed
  - How will this information be used?
  - Snapshot in time. How useful is it?
- Need an agreed upon template (standard?) for the information dispersion and ingestion
- (Opportunity) Bring continuous evaluation principle (ZT) into software supply chain security
  - Built-into build-pipeline v/s after the fact scanning
  - Attribution (software packages) & Tracking –not just one level – multi-level deep assessment
  - Continuous assessment – every build - every package - every time
  - Community-wide impact – Convergence & valuable outcomes

Thank you

Manoj Sharma
manoj.sharma@broadcom.com