CTB Overview

cisco *Live!*

Telemetry Streams
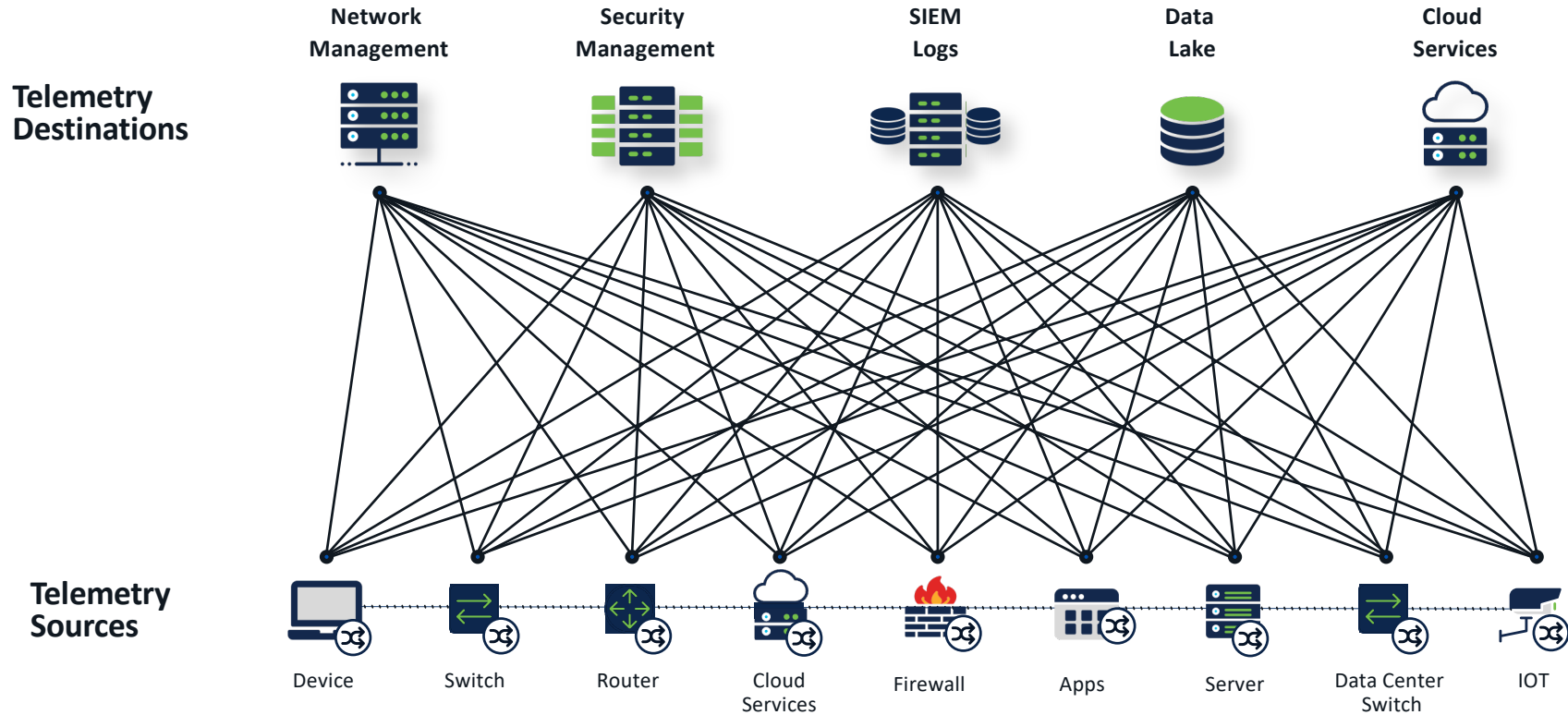
Telemetry Streams – AFTER CTB

Network Management   **Security Management**   **SEIM / Logs**   **Data Lake**   **Cloud Services**

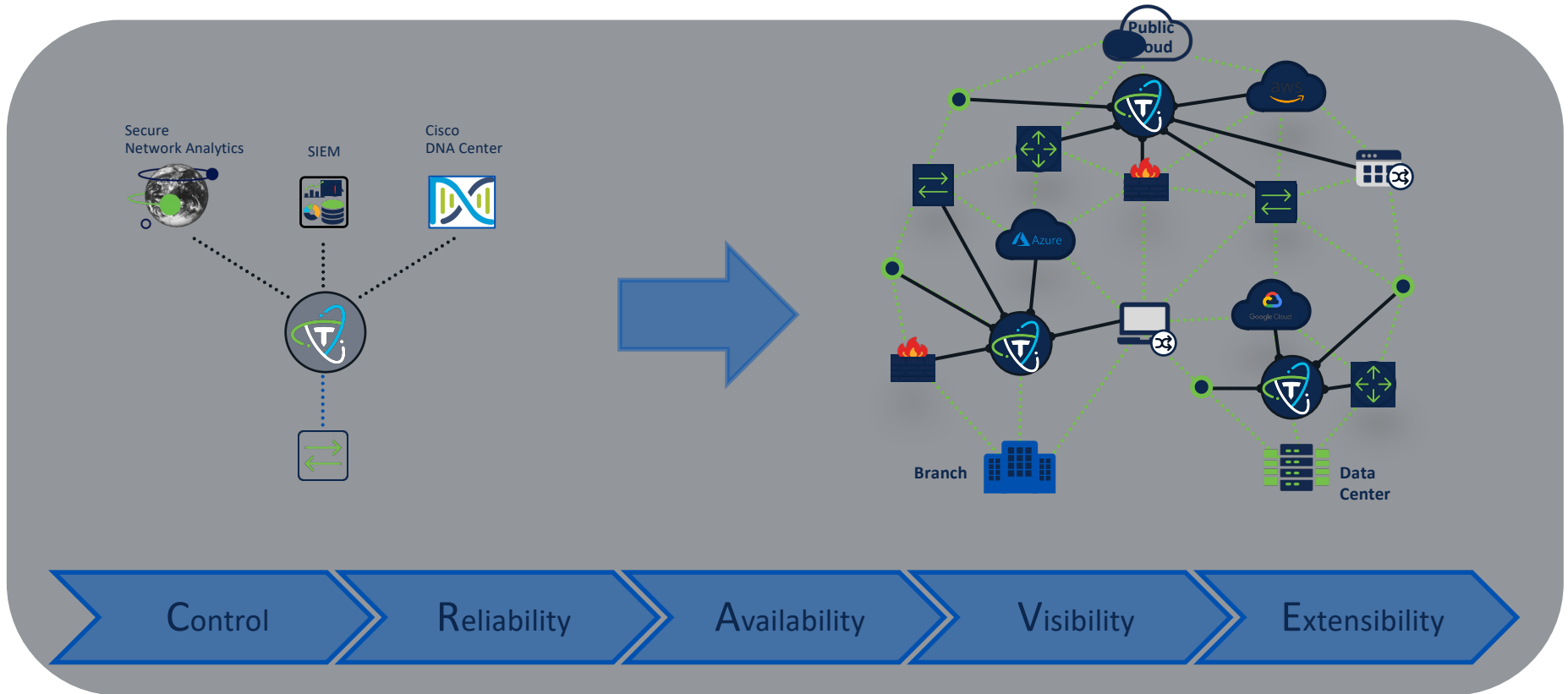As a producer of telemetry, I want to send to a single target regardless of how many consumers exists

As a consumer of telemetry, I want to treat all of my telemetry sources as code via an API

Device   Server   Switch   Router   Cloud Services   Apps   Firewall   Data Center Switch   IOT
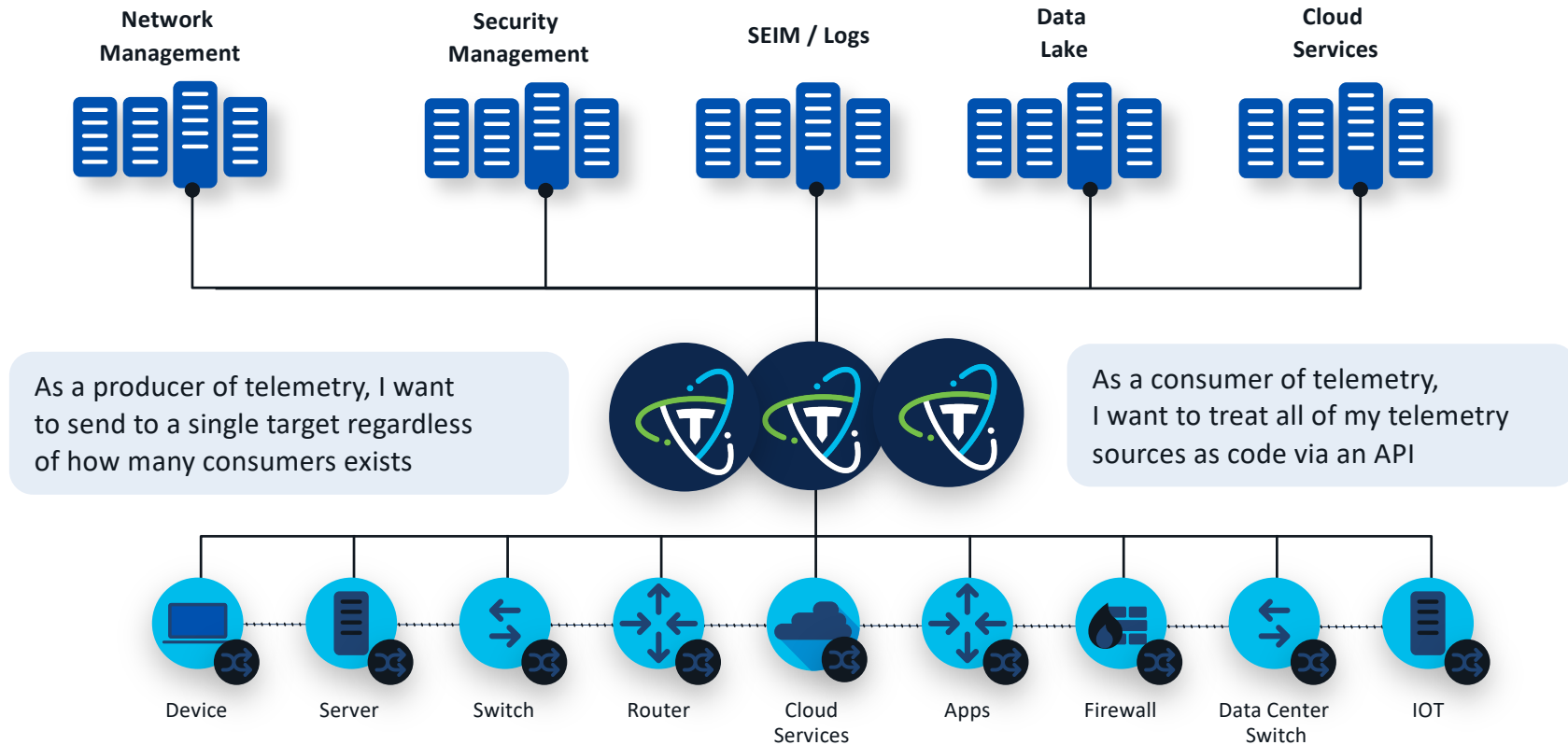
Intelligent Telemetry Plane (ITP)

Secure Network Analytics

SIEM

Cisco DNA Center

Public Cloud

Azure

Google Cloud

aws

Branch

Data Center

| Control | Reliability | Availability | Visibility | Extensibility |

Cisco Telemetry Broker Democratizes Telemetry Data

Brokering

The ability to route and replicate telemetry data from a source location to multiple destinations

Filtering

The ability to filter data being replicated to enable fine grain control over what destinations ingest and analyze

Transforming

The ability to transform data protocols from the source to the destinations protocol of choice

Brokering

Replicate Telemetry (20x perf improvement over UDP Director)	>>>>>	Quickly enable PoV/onboarding of non-incumbent tools
Route Telemetry (Cloud, On Prem, Container, Serverless)	>>>>>	Let teams run the tools of their choice without deploying new agents/collectors

Filtering

Filter to Drop & Segment	>>>>>	Control Costs: Pay Splunk to only index high value data
		Compliance: Keep low value data in low-cost storage

Transformation

Protocol Transformation	>>>>>	Increased visibility of legacy sources, and into cloud sources
Data Transformation	>>>>>	Aggregate data, transform fields, add context
Anonymize PII	>>>>>	GDPR compliance to all downstream tools

Telemetry Exporters

- Netflow / sFlow
- Syslog
- App. Exporters (NVM)
- SNMP Trap
- AWS/Azure Logs
- Proxy logs
- Generic Inputs

Exporters = Network, Application, or Cloud provider points of telemetry egress.

CTB Distributed Nodes

VPP Powered

Telegraf Powered

- Broker
- Transform
- Filter
- ITP: CRAVE
- Custom I/O, Transforms
- API

Telemetry Consumers

- **Cisco Secure Analytics** (SNA, SCA)
- Cisco On-Prem Platforms (DNA Center, Tetration)
- 3rd Party On-Prem (Home grown Data Lakes, Live Action, SevOne)
- **Cisco XDR**
- 3rd Party Cloud Services (SIEM/Datadog/ServiceNow)
- **OTel**

...and more

Available now | Available 2025

CTB Components

- CTB Manager node:
  - Only one manager is deployed and can manage multiple Broker nodes*
  - Maintains the policy/rules for the broker nodes enabling central management from one view
  - If the manager goes down, broker nodes continue to process telemetry
  - Backup configurations are created for recovery

- CTB Broker node:
  - Where the telemetry brokering work occurs
  - Can be deployed closest to telemetry sources

Manager

Broker Node

Broker Node

Broker Node

Broker Node

Management Network

Monitoring Network
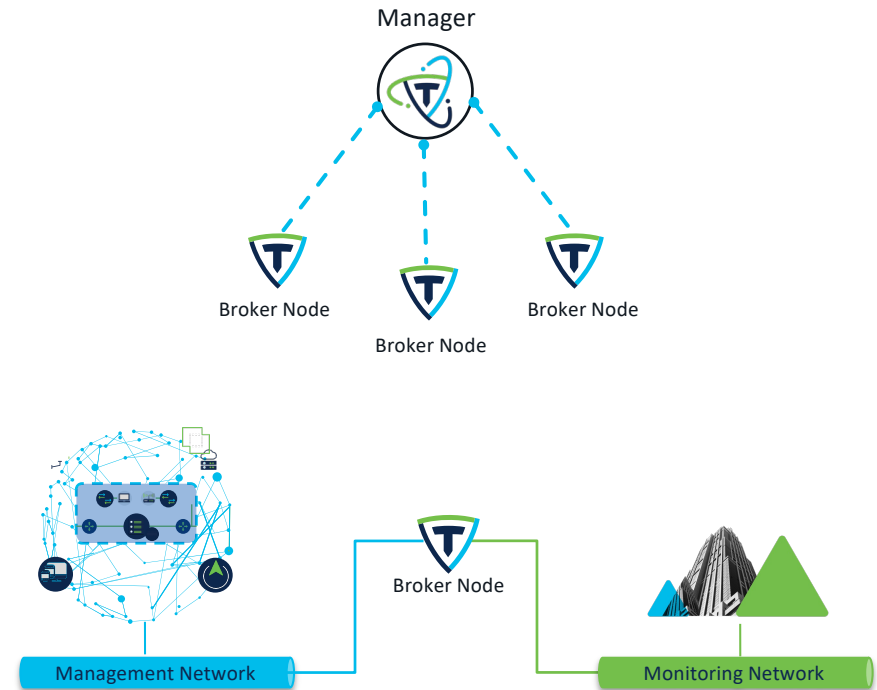
*A single Manager supports up to 10 Broker nodes

Deployment specifications

Minimum requirements for a
CTB Manager:

- CPU: 4 cores
- Memory: 8 GB
- Storage: 100GB

vmware vSphere

Versions
7.0, 6.7 or
6.5

KVM

Minimum requirements for a
CTB Broker Node:

- CPU: 8 cores
- Memory: 12 GB RAM
- Storage: 60 GB

TB2300 now available (Broker Node only)

CTB Network Design (Basic)

- The Manager node has a single interface
  - Dedicated for management traffic only

- Broker nodes have two virtual interfaces
  - One dedicated for management (and TCP traffic)
  - One dedicated for monitoring UDP traffic

- For smaller deployments that do not have a segmented management network all exporters of telemetry are sent to the Broker Node on the management/monitoring network

- The Broker Node must have two IPs (v4 or v6) for Management and Monitoring interfaces

Manager

Management Interface

Management/Monitoring Network

Single Management-monitoring Network

On-Prem Networks

Management Interface

Monitor Interface

Broker Node