VERSATILITY

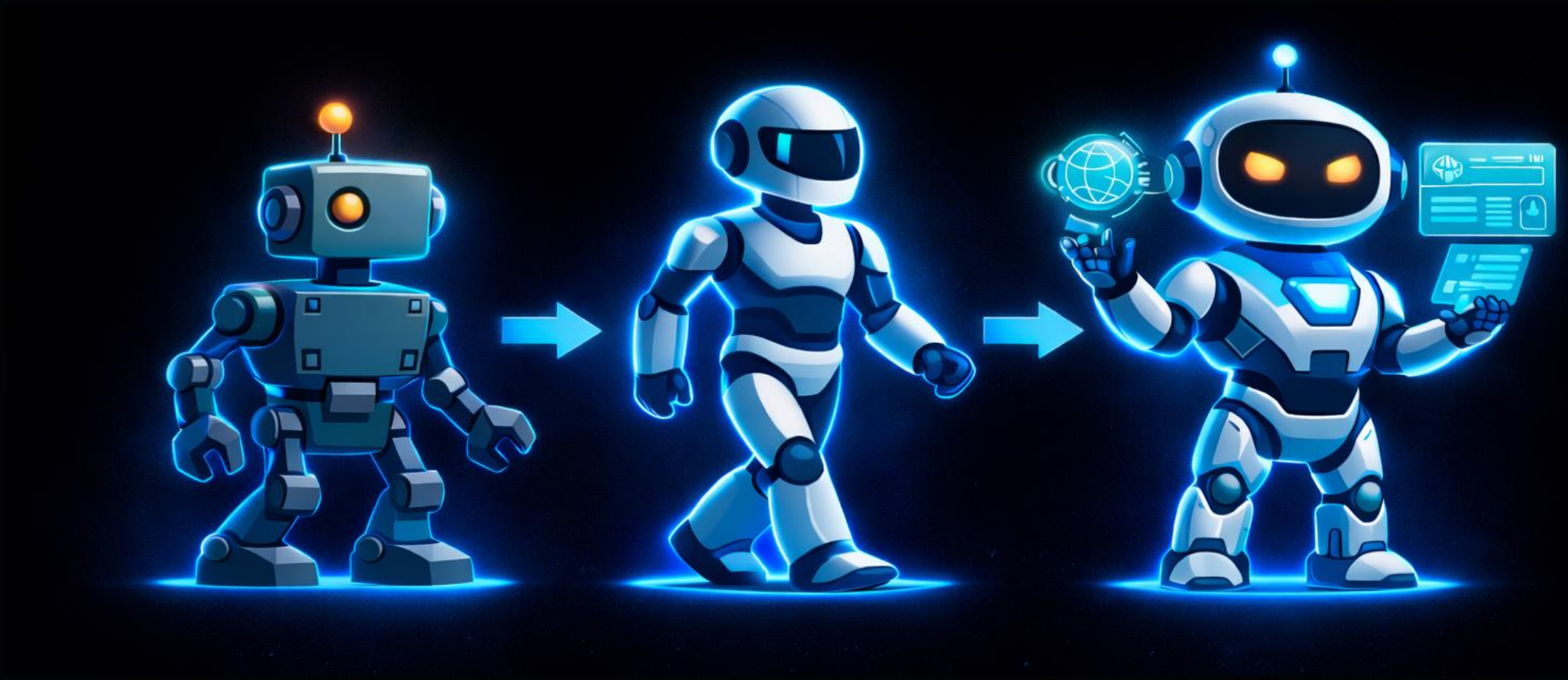
Zero Trust AI-Ops:

How Versa's MCP Architecture Secures AI-Driven Ops

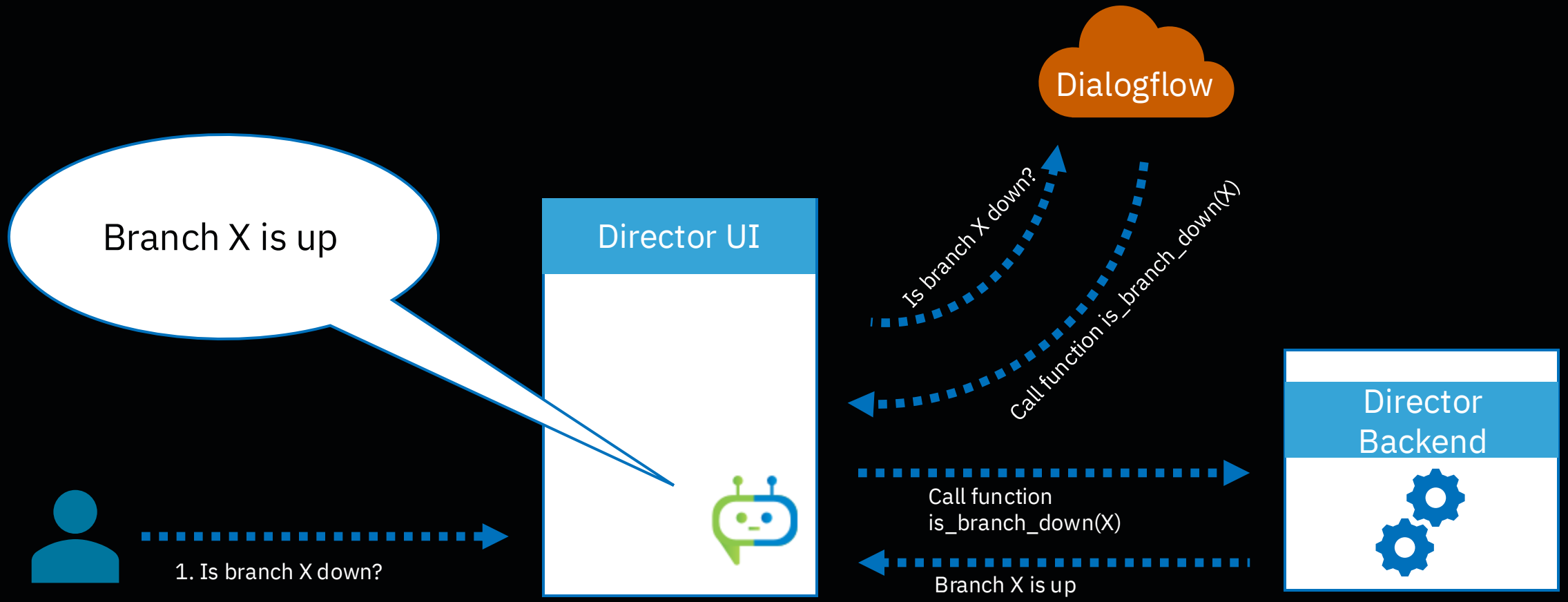
Sridhar Iyer

Sr Director, ML/AI

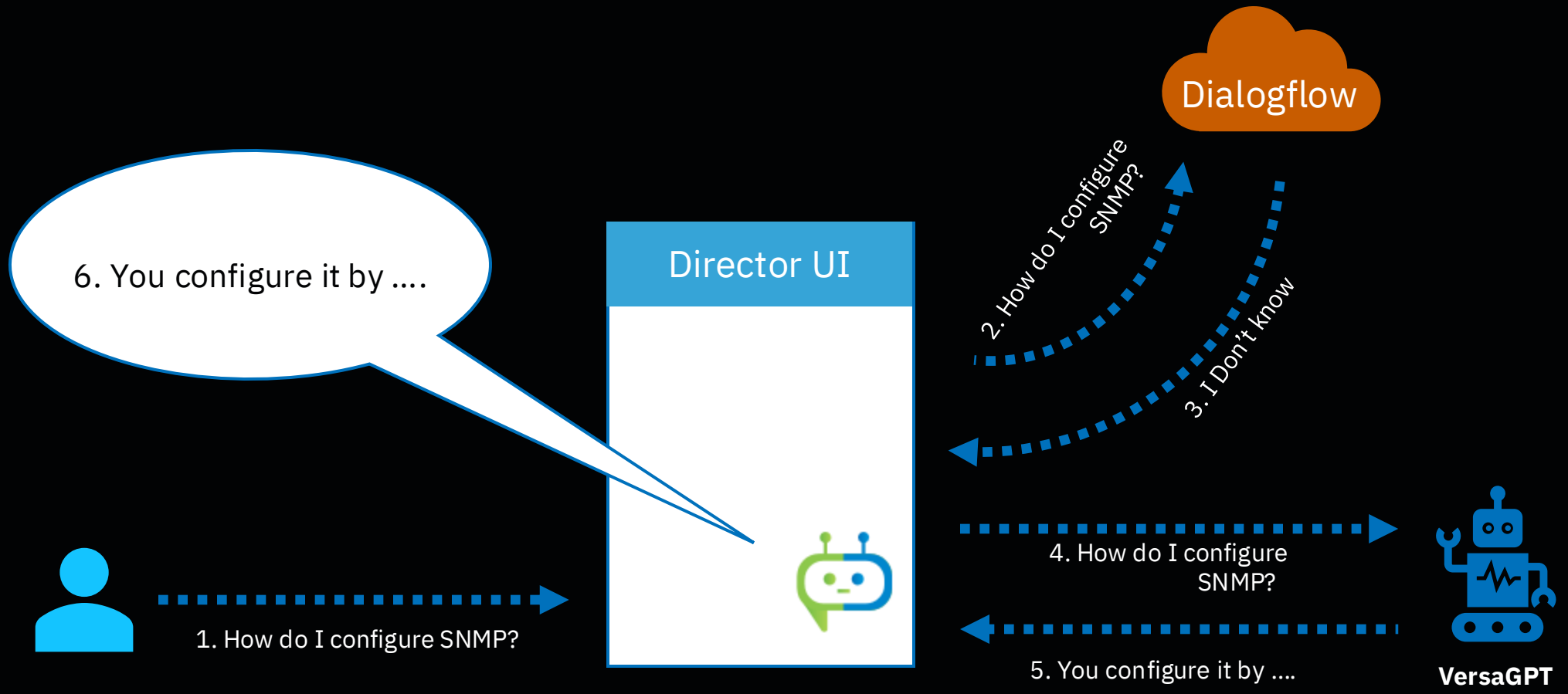
Evolution of Verbo



Release 1

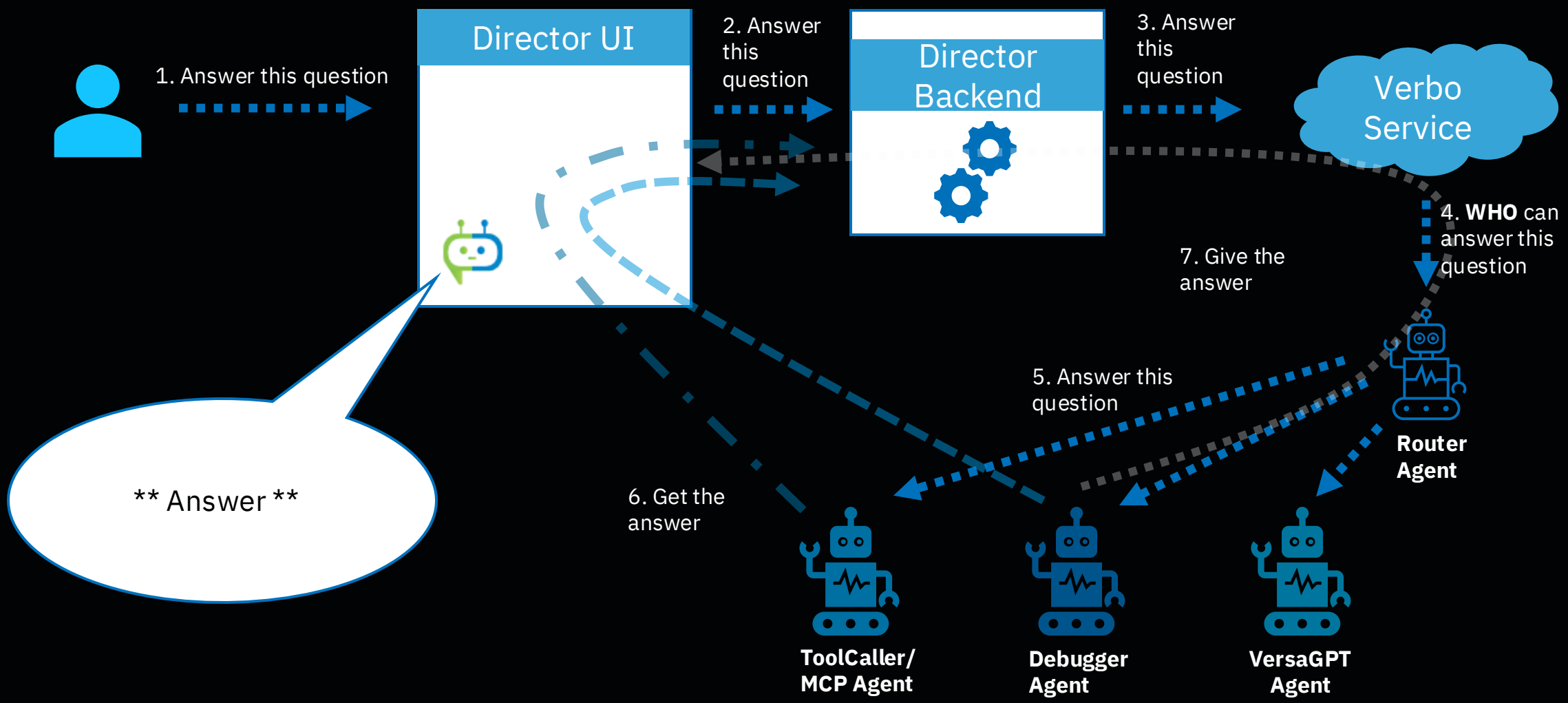

Dialogflow
Branch X is up
Director UI
Is branch X down?
Call function is_branch_down(X)
Director Backend
Call function
is_branch_down(X)
Branch X is up
1. Is branch X down?

Release 2



VERSATILITY

Release 3



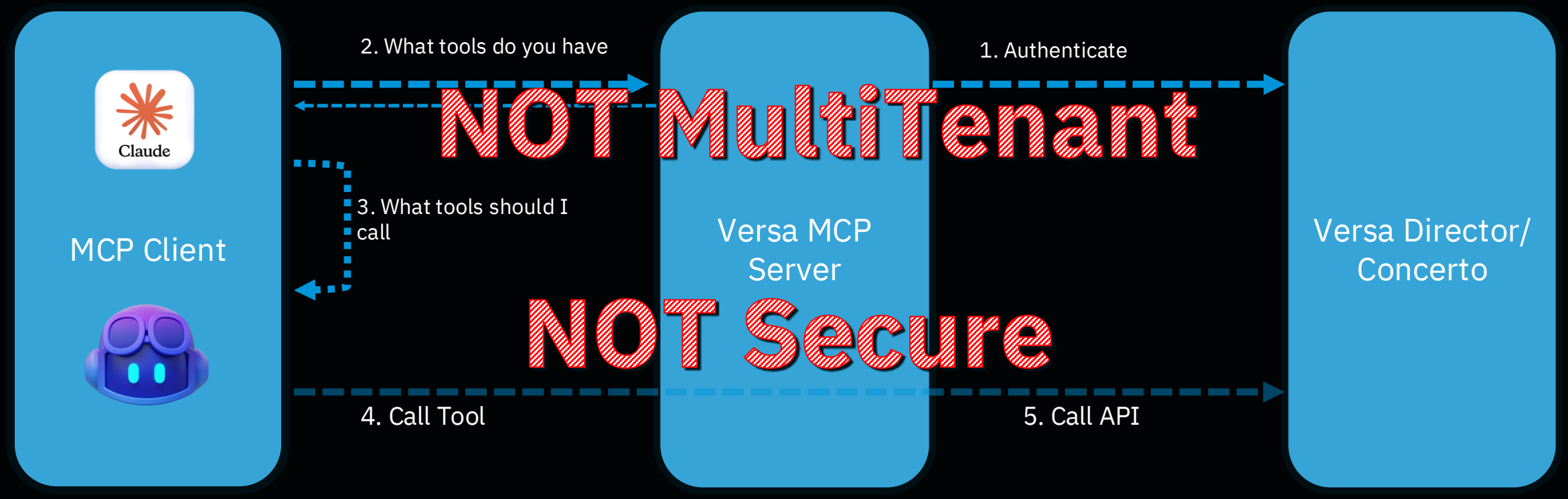
VERSATILITY

MCP Server

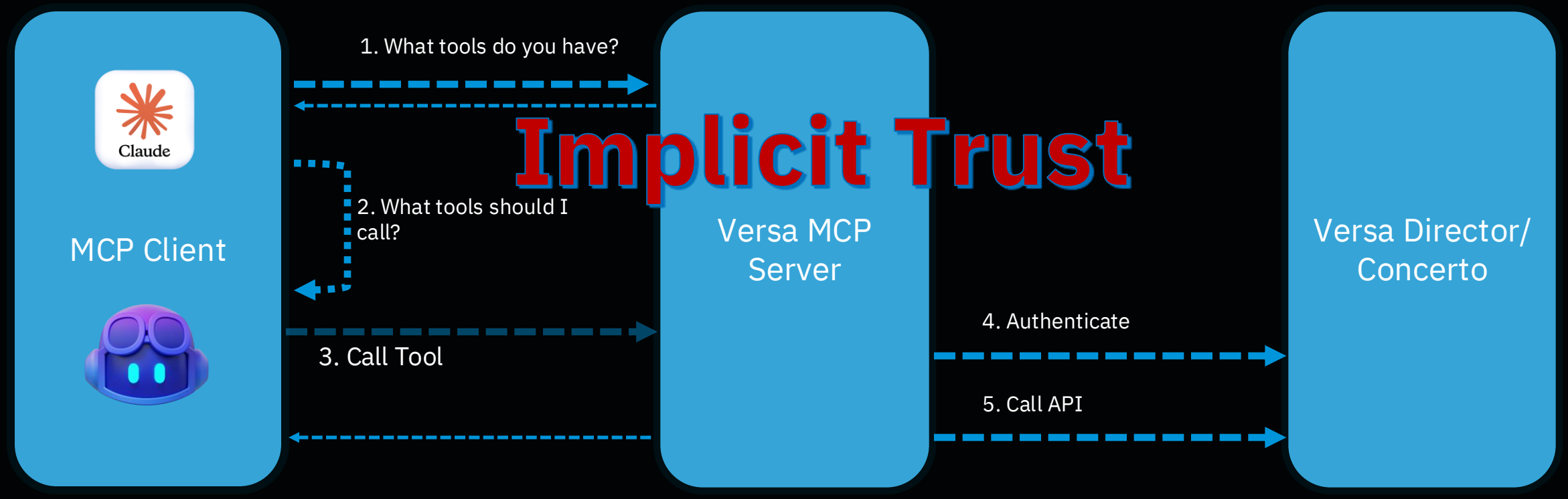
The Ugly, The Good & The Best

VERSATILITY

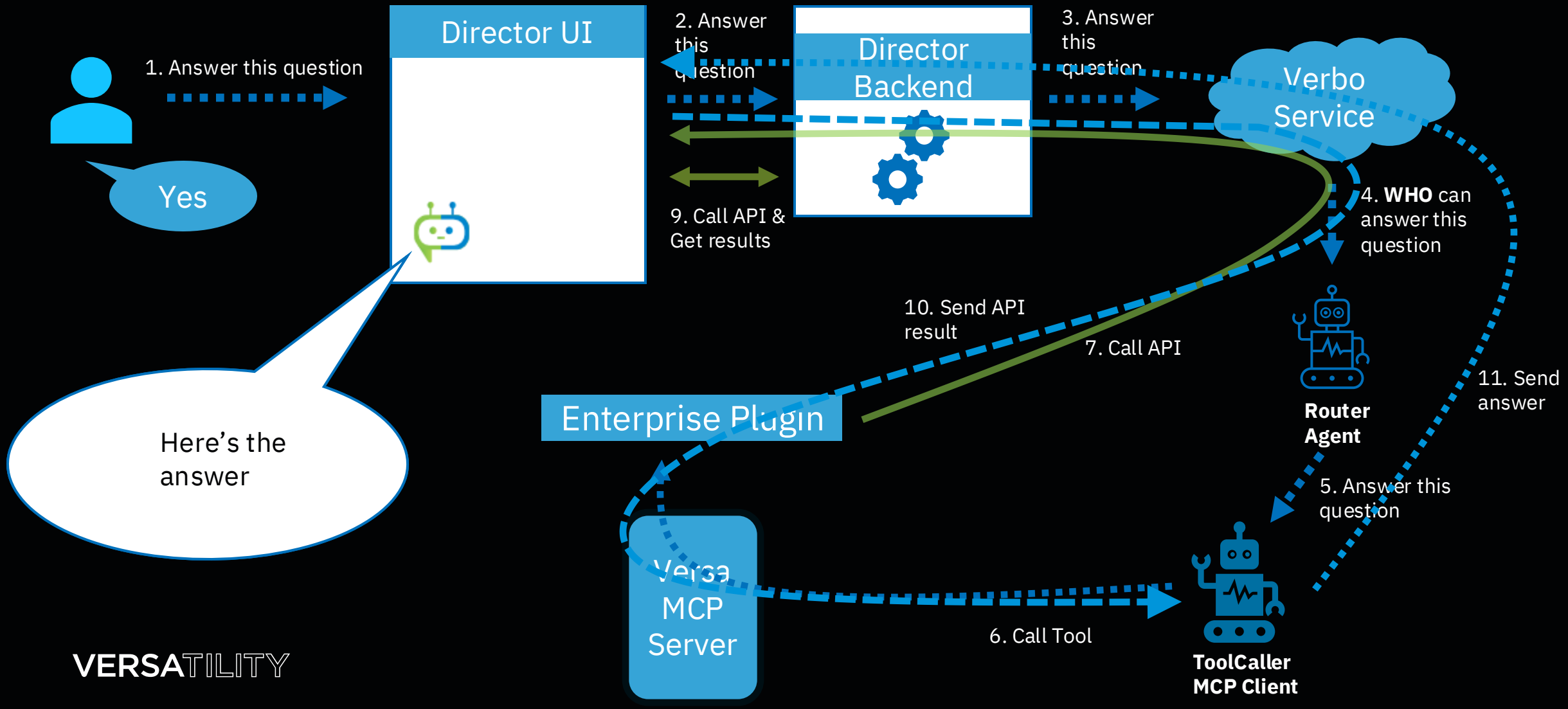
Basic MCP server



Secure MCP server



Zero Trust MCP by Versa



VERSATILITY

Compatibility Matrix

Supported Platforms & Versions

Platform	Version	Server
Director	22.1.4+ (Next hotfix)	Versa MCP Server V1
Director	23.1+	Versa MCP Server V2
Concerto	12.2+	Versa MCP Server V1
Concerto	13.1+	Versa MCP Server V2

Tool Coverage at a Glance

72 Tools Across 12 Categories

Category	#	Highlights
Analytics (SDWAN/NGFW/alarm/SASE/threats)	7	MOS, SLA, link usage, firewall, IDP/AV/CASB/IoT
DEM Analytics	7	User experience, app experience, geo map
Network Health	5	Device counts, transport quality, security overview
Monitoring	8	System alarms, dashboard, audit logs
Appliance Info	15	Details, health, sync, violations, config export
Routing	6	BGP, OSPF, ping, route counts
Layer 2	4	MAC table, LLDP topology
Service Config	7	CGNAT, NGFW policies, VPN, policy rules
Templates	5	Listing, workflow, device associations
VOS Commands	3	FTS5 search, CLI execution
Monitor Tab	3	Summary dashboard, appliance list/detail
Other	2	Health check, pagination

+ 70 Analytics Proxy endpoints across 20 features (SDWAN, NGFW, SFW, SECACC, SYSTEM, THREATS, IDP, ATP, AV, DOS, DNSF, URLF, CASB, IPF, RBI, IOT, SASEWEB, CGNAT, PCAP)

VERSATILITY

Quick-Win Use Cases

Highest-Value Day-1 Scenarios

1. **Morning health check**
   Device counts, status breakdown, top sites by bandwidth (< 5 sec)

2. **Alarm triage**
   Severity breakdown (donut chart), critical alarm log with timestamps (13K+ events)

3. **Compliance audit**
   Traffic by country (166 countries), zone segmentation, GenAI detection (1.3M hits)

4. **Security posture**
   Active threats, firewall allow/deny breakdown (226M+ flows)

5. **DEM user experience**
   KPI cards, worst-user rankings, app performance scores

6. **MOS voice quality**
   Per-site/circuit MOS scores, SLA compliance tracking

7. **Incident investigation**
   Alarm timeseries for spike detection, before/after comparison

Test Results Summary

Validated at v1.8.54

46
Tests Executed

87%
Pass Rate

96%
Tool Selection Accuracy

0%
Hallucination Rate

Category	Tests	Target	Result
Tool Confusion	30 designed / 20 run	≥ 80%	**~90%**
Parameter Hallucination	25 designed / 7 run	≥ 90%	**100%**
Edge Cases	20 designed / 5 run	≥ 95%	**100%**
Multi-turn Scenarios	30 designed / 6 run	Complete w/o errors	**Pass**

Deployment Modes

ENTERPRISE Mode

SaaS + On-Prem with Enterprise Plugin

- MCP → WebSocket → verboService → Browser → Director
- No credentials on MCP server
- Requires verboService + MongoDB

SaaS model

– Versa-hosted Verbo service
– Enterprise Plugin integration

On-Prem model

– Self-hosted Verbo + Enterprise Plugin
– Customize models/agents as needed

MCP ONLY Mode

On-Prem Only

- MCP server connects directly to Director
- User authenticates via browser OAuth
- Tokens stored in-memory (ephemeral)
- No Verbo service or Enterprise Plugin required
- Free & open source
- Simplest setup for on-prem environments

Demo

Thank You

VERSATILITY