



APPLICATION-CENTRIC FULL-STACK OBSERVABILITY

Observe Smarter. Perform Better.

uObserve™ resolves complex IT disruptions for enterprise organisations by correlating application and infrastructure performance — and it does it without agents.

Agentless

deployment

Minutes

to first insight

One console

app · network · compute · storage · VDI
· security

APAC AUTHORISED PARTNER



SECURE CENTRAL
A Pioneer Infotech Company

www.securecentral.com.au

What we will cover

A 20-minute walk-through for IT leadership, operations and security teams

01 The enterprise problem

Why disruptions still take hours to resolve

02 uObserve™ at a glance

Three capability pillars in one platform

03 How the tool actually works

Observe → correlate → analyse → act

04 Live product screens

Dependency maps, root cause, VDI, security

05 Architecture & deployment

Components, models and sizing

06 Command-centre operations

Video wall and shift workflow

07 Features, benefits & ROI

What the organisation gets

08 Customers & next steps

Proof and how to start

Enterprise IT is blind between the layers

Modern stacks are virtualised, hybrid and east-west heavy — but the tooling is still siloed

The war room

App, server, network, storage, desktop and security teams each bring a different tool and a different number. Hours are lost proving innocence instead of fixing the fault.

East-west darkness

Most traffic never crosses a physical tap. VM-to-VM and container-to-container conversations are invisible to perimeter tooling.

Agent fatigue

Classic APM needs code instrumentation and agents on every workload — change boards, licences and risk on production systems.

Unknown dependencies

Nobody has an accurate, current map of which service talks to what. Migrations, DR tests and change windows become guesswork.

The business cost

Every minute of degradation is revenue, reputation and regulator risk. Uila publishes an Incident Savings Calculator precisely because most organisations have never quantified what their unplanned downtime and troubleshooting hours actually cost — and what a correlated, agentless view saves.

Three pillars, one agentless platform

Everything below is delivered from the same metadata collection and the same console

Performance Observability

- 360° view of application, infrastructure, network and VDI user experience
- Root-cause isolation across compute, memory, storage and network
- AIOps-driven remediation actions
- Capacity planning & rightsizing

Application Dependency Mapping

- Automated, dynamic topology tracing of every tier and external service
- Accurate, always-current inventory of assets and their dependencies
- Change tracking and policy-violation detection on the live map
- Cloud migration & DR wave planning

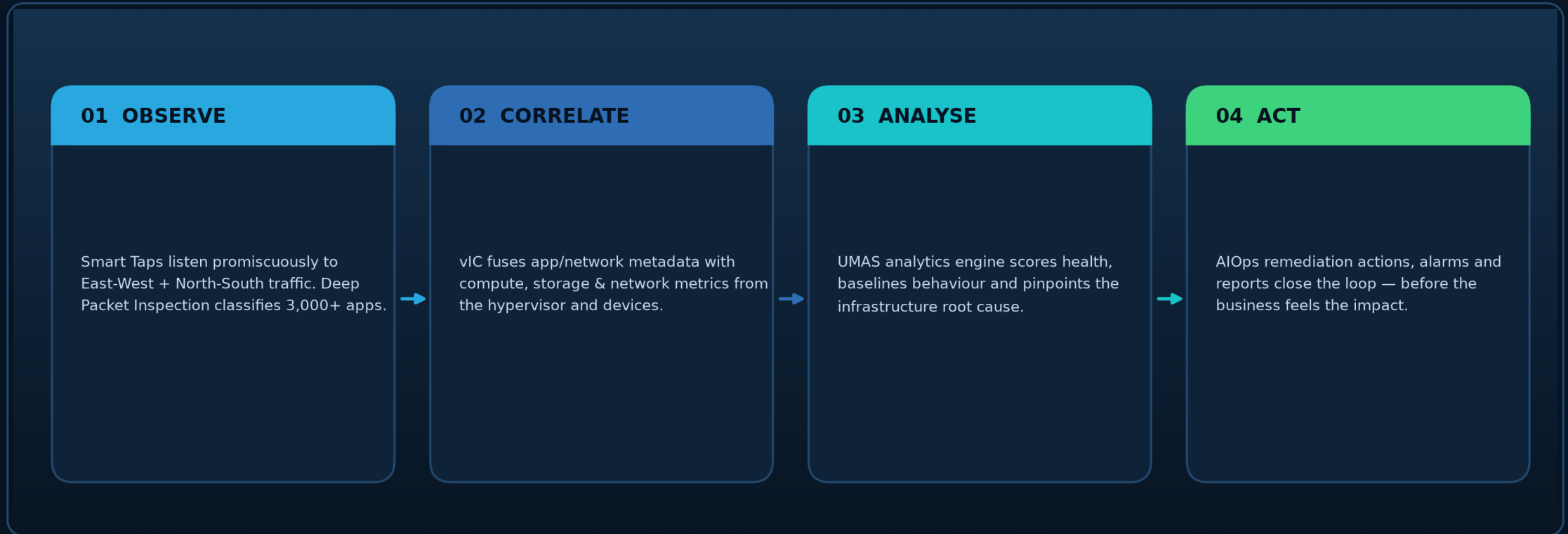
App-Centric Cyber Threat Protection

- East-west traffic inspection for lateral movement and stealth attacks
- Application behaviour anomaly detection
- Data-exfiltration and outbound country/destination insight
- Micro-segmentation planning & validation

Delivered as self-hosted software or as a managed SaaS service — the same capability either way.

From metadata to answer in four moves

No code instrumentation, no agents on your production workloads



Deep Packet Inspection reads only the metadata — application identity, response time, network latency, retransmissions, transactions. No packet payload is ever stored, which removes the privacy and legal exposure that comes with full packet capture while still giving you packet-grade evidence.

Application Dependency Mapping

Auto-discovered, multi-tier topology with live health on every node and link



Tiers discovered automatically

Thin clients → connection server → VDI → load balancer → web → database → external services, grouped without any manual configuration.

Colour = health, not guesswork

Green / amber / red is driven by measured application and network response time, so the bottleneck tier is obvious at a glance.

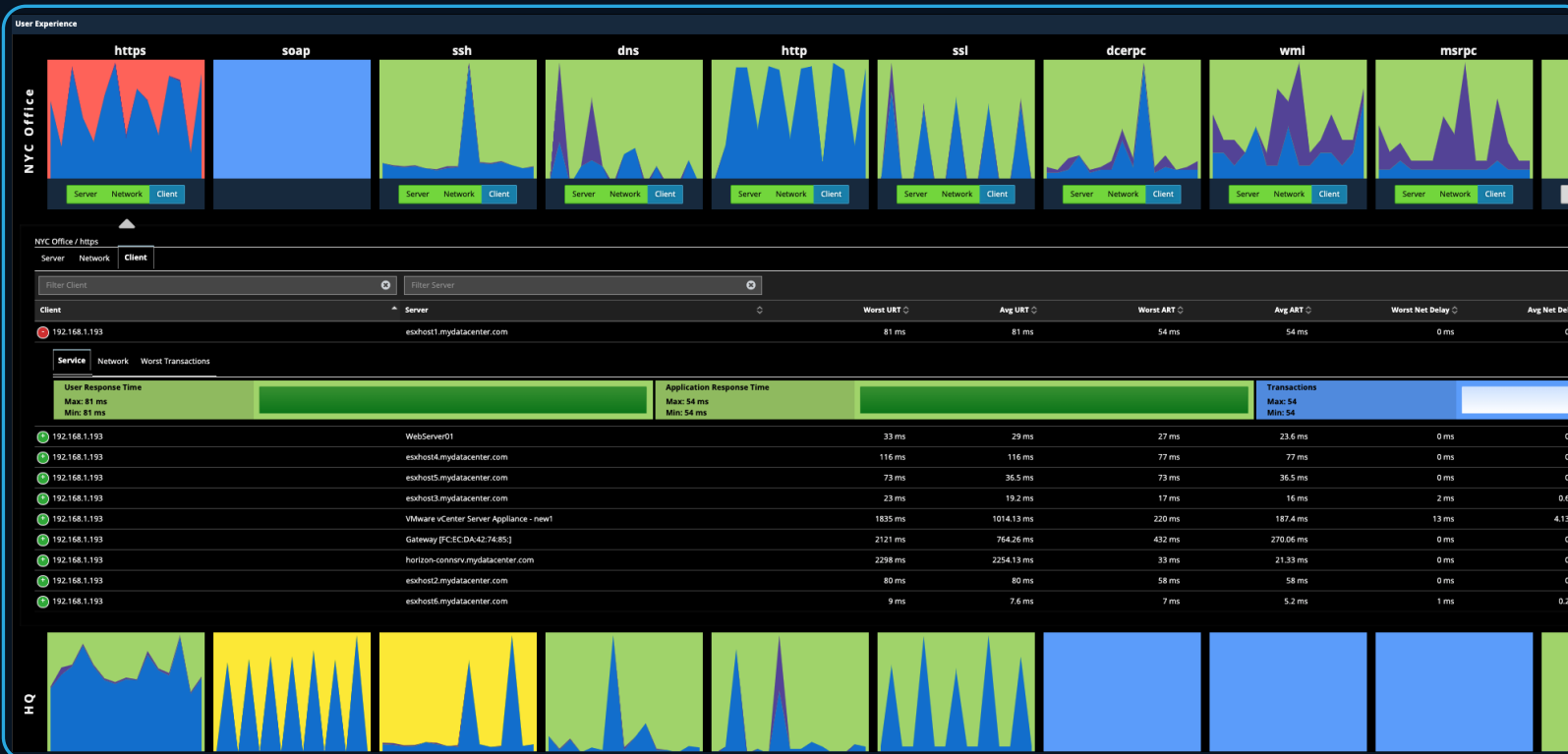
Click straight to root cause

Single-click drill-down from any node into the CPU, memory, storage or network evidence behind the issue.

Use it for: migration wave planning, DR runbooks, change impact analysis and accurate CMDB-grade inventory.

End-user experience & transaction analysis

Per-site, per-application response time broken into server, network and client contribution



Server vs network vs client

Each application tile splits the delay three ways. The argument about 'is it the network?' is settled before the bridge call starts.

Worst URT / ART, per site

User Response Time and Application Response Time ranked by client, server and site (HQ, branch, remote) with worst transactions listed.

4,200+ apps classified

Uila's DPI engine identifies HTTPS, SQL, DNS, SOAP, DCERPC, WMI, MSRPC and thousands more by behaviour.

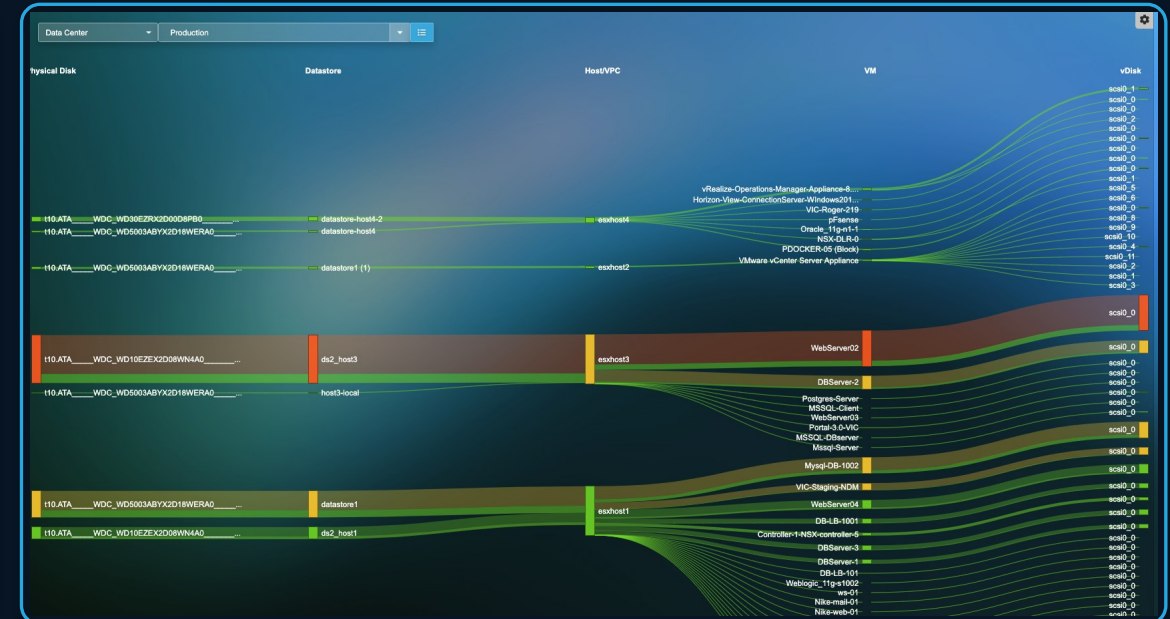
Infrastructure hot-spots & storage path analysis

Find the over-committed host or the slow datastore before users feel it



CPU circle-packing heat map

Data centre → cluster → host → VM in one picture. Size shows allocation, colour shows pressure. The red dot is the VM to look at.



Storage path Sankey

Physical disk → datastore → host → VM → vDisk. Trace a latency spike end-to-end and see exactly which workloads share the contended spindle.

VDI, GPU and hybrid-workforce experience

Agentless session analysis for VMware Horizon — logon duration, protocol latency, GPU and packet loss



Session-level truth

Per-user desktop, pool/farm, state, protocol (BLAST/PCoIP), logon duration, peak packet loss and round-trip time.

GPU observability

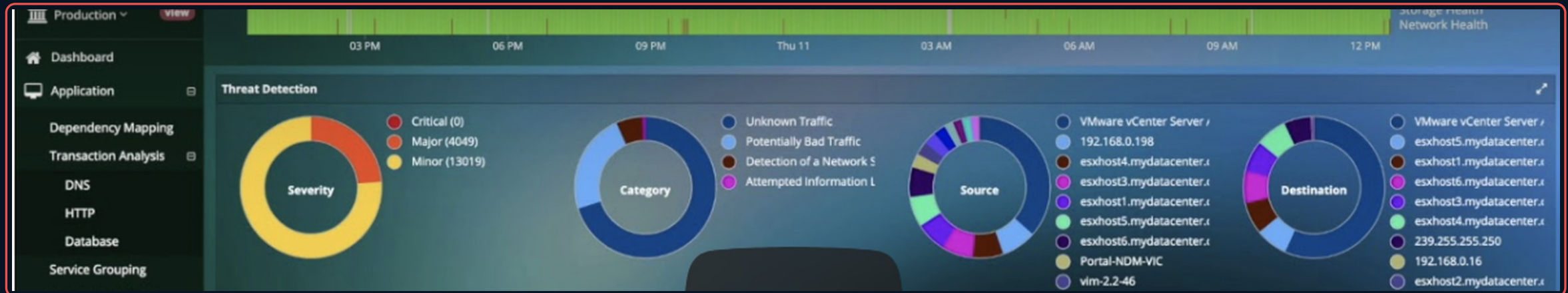
Frame buffer, encoder, decoder and GPU usage per host and per session — essential for designer, trading-floor and clinical workloads.

Ends the 'it's slow' ticket

Prove whether the cause is the endpoint, the WAN, the host or the application — without touching the desktop.

Cyber threat & application anomaly dashboard

The same east-west metadata that fixes performance also exposes lateral movement



Severity triage

Critical / major / minor volumes at a glance for the shift lead.

Category breakdown

Unknown traffic, potentially bad traffic, network scans, information leaks.

Source & destination

Which host or instance initiated it and where it went — internal or external.

Anomaly correlation

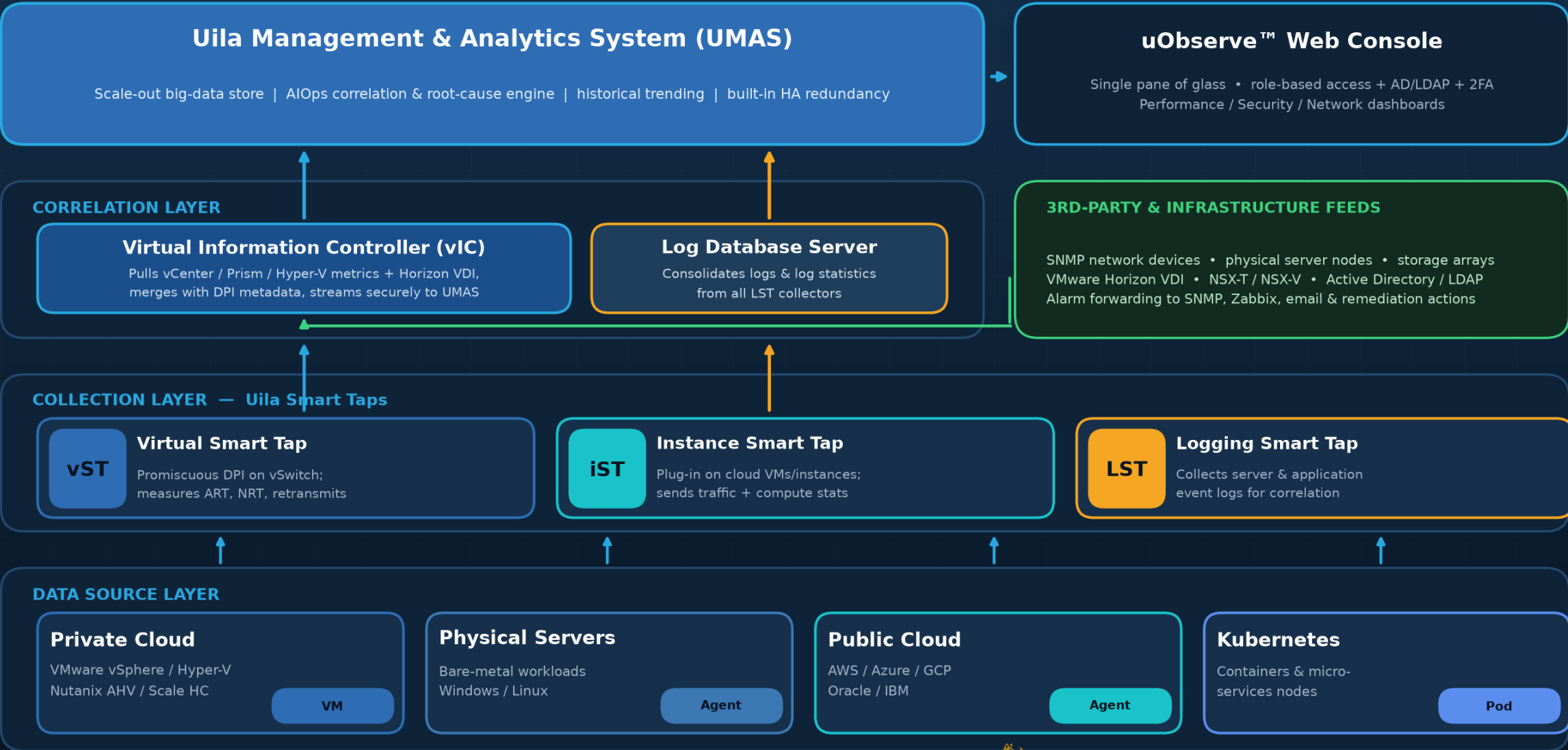
Deviation from the learned application map, plus outbound country insight.

uObserve™ Reference Architecture



Agentless metadata collection • no packet payload stored • scale-out big-data analytics

UMAS deploys on-premises, in Uila SaaS Cloud, or in your public cloud



What each component actually does

Four software elements — all virtual appliances or plug-ins, nothing to rack

vST

Virtual Smart Tap

Guest VM on the host (private cloud), VM/instance (public cloud) or Kubernetes node. Listens promiscuously to the virtual switch for north-south and east-west traffic, applies DPI, and emits application + network metadata only — never payload.

1 vCPU · 2 GB RAM · 4 GB disk

iST

Instance Smart Tap

Lightweight plug-in distributed across public-cloud VMs and instances. Collects traffic plus instance-level compute statistics and forwards them to the vST for deep packet inspection.

t2.large (AWS) · D2s v3 (Azure)

vIC

Virtual Information Controller

The integration conduit to vCenter, Hyper-V, Nutanix Prism, OpenStack and VMware Horizon. Pulls network, storage and compute metrics, merges them with DPI metadata from every vST, and securely streams the result to UMAS.

4 vCPU · 24-48 GB RAM

UMAS

Management & Analytics System

The brain: a scale-out big-data store and analytics engine with built-in redundancy. Correlates application behaviour to infrastructure metrics, pinpoints root cause, retains high-resolution history and drives the console.

On-prem, Uila SaaS or public cloud

Three deployment models, one sizing model

Pick the model that fits your data-sovereignty and operating preference — capability is identical

SAAS / MANAGED

- UMAS hosted in the Uila Cloud
- You deploy only vST + vIC on-site
- Fastest time-to-value — minutes
- Ideal for lean teams & pilots

SELF-HOSTED ON-PREM

- UMAS + vIC inside your data centre
- Metadata never leaves your estate
- Suits sovereign / regulated workloads
- Full control of retention policy

PUBLIC / HYBRID CLOUD

- UMAS & vIC in AWS / Azure / GCP
- iST plug-ins on cloud instances
- Single console across on-prem + cloud
- Ideal for migration programmes

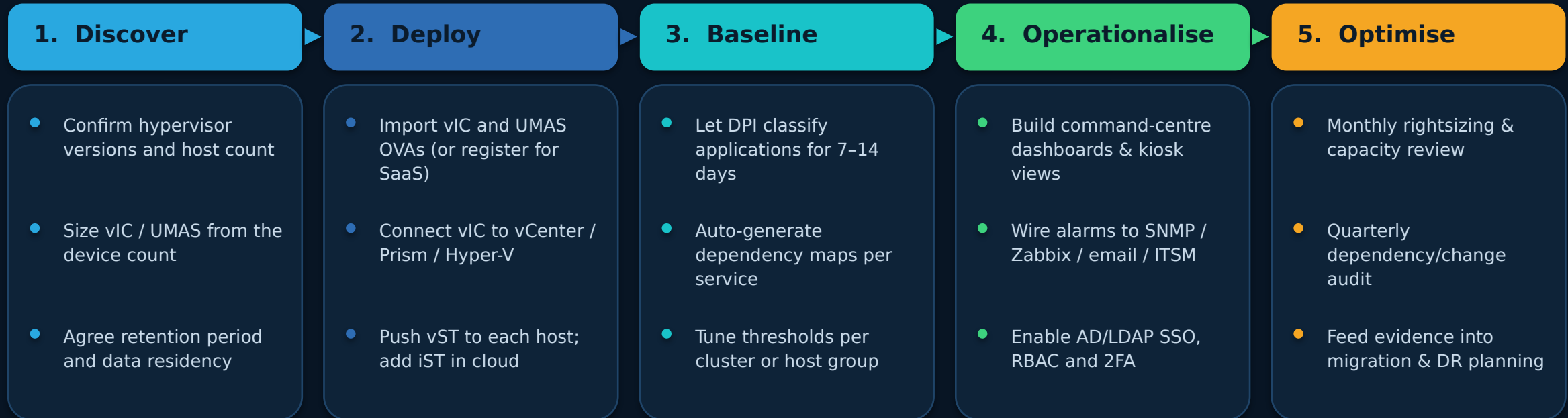
DEPLOYMENT SIZING GUIDE (VMware reference — source: Uila published system requirements)

COMPONENT	SMALL (<1,000 devices)	MEDIUM (1,000-2,000)	LARGE (2,000-5,000)
Virtual Smart Tap (vST)	1 vCPU • 2 GB RAM • 4 GB disk, one per host		
Virtual Info Controller (vIC)	4 vCPU • 24 GB RAM • 50 GB	4 vCPU • 32 GB RAM • 100 GB	4 vCPU • 48 GB RAM • 200 GB
UMAS (self-hosted)	4 vCPU • 48 GB RAM • 1 TB	4 vCPU • 64 GB RAM • 2 TB	2-box: Web 800 GB + DB 5 TB
Log Database Server	8 cores • 8 GB RAM • 250 GB SSD		

Retention shown for 1 month. >5,000 devices = custom sizing. vST scales linearly: add a tap as you add a host.

A typical enterprise rollout

Concrete steps — sequence them to suit your change calendar



Prove it first

Uila offers a 21-day free trial and an interactive demo. A sensible pilot is one production cluster plus one business-critical service — enough to show real dependency maps and at least one root-cause win.

Built for the 24x7 Command Centre



NOC + SOC + Service Desk working from one correlated source of truth

VIDEO WALL — SUGGESTED 6-PANEL LAYOUT

Service Health Grid

Business-service RAG status
for every critical application

Application Dependency Map

Live topology + tier-to-tier
response times

Infrastructure Hot-Spots

CPU / memory / storage latency
circle-pack heat map

End-User & VDI Experience

Logon duration, protocol latency,
GPU & session state by site

Threat & Anomaly Feed

East-West anomalies, severity
mix, source/destination pairs

Capacity & Trend Board

Rightsizing, reclaimable capacity,
30/90-day trend lines

Tier-1 NOC

Triage & first response

Tier-2 / SRE

Root-cause & remediation

SOC Analyst

Threat & lateral movement

WHY IT SUITS COMMAND CENTRE OPS

● Glance-able health

Colour-coded RAG across app,
compute, network, storage & VDI.

● Zero-agent rollout

No change windows on production
workloads to gain visibility.

● Single source of truth

NOC, SOC and app owners read the
same correlated evidence.

● Full-screen kiosk mode

Dashboards designed for large-format
wall displays and dark rooms.

● Shift-ready alarms

Thresholds, baselines and alarm
forwarding to SNMP / Zabbix / email.

● Historical playback

Rewind to the incident window for
post-incident review and reporting.

One platform, role-based views — no tool-swivel, no finger-pointing between teams.

How a shift actually runs on uObserve™

From alarm to closure without leaving the platform

T+0 min

Alarm fires

Threshold or baseline deviation raises an alarm on the wall and to SNMP/Zabbix/email.

T+1 min

Triage on the map

Tier-1 opens the dependency map; the degraded tier is already amber/red.

T+3 min

Root cause

Drill into the node: CPU ready, memory swap, storage IOPS/latency or network retransmits.

T+5 min

Scope the blast radius

See every dependent service and user session affected before you communicate.

T+8 min

Remediate

Apply the AIOps remediation action or hand a precise ticket to the owning team.

Post

Review

Replay the incident window from retained history for the post-incident report.

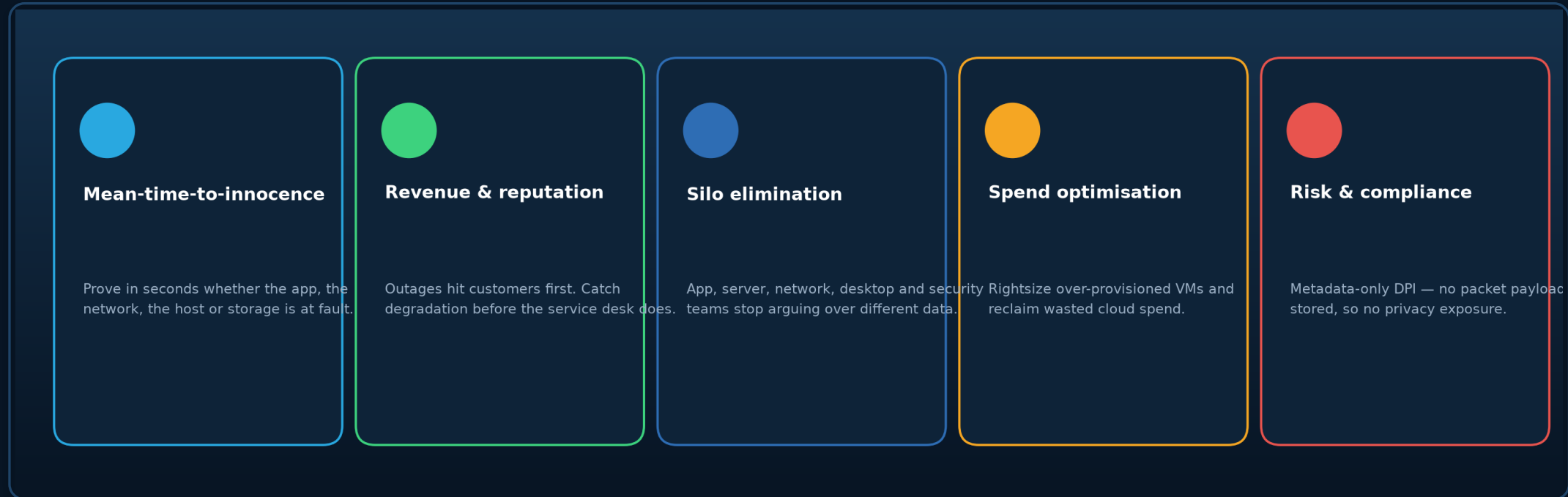
What it does — and what the organisation gets

Mapped from capability to measurable business outcome

CAPABILITY	BENEFIT TO THE ORGANISATION
Agentless DPI collection	Visibility in minutes with no code change, no agents on production workloads and no change-board battle
Application ↔ infrastructure correlation	One correlated answer replaces five siloed tools; mean-time-to-innocence collapses
Automated dependency mapping	Accurate, always-current service inventory for migration, DR, audit and change control
Full-stack root-cause analytics	Shorter MTTR, fewer escalations, less unplanned downtime and fewer repeat incidents
VDI / EUC & GPU observability	Hybrid-workforce productivity protected; desktop tickets resolved with evidence
East-west threat & anomaly detection	Lateral movement and data exfiltration surfaced without endpoint security agents
Capacity planning & rightsizing	Reclaim over-provisioned VMs and cut wasted on-prem and cloud spend
Metadata-only, no payload storage	Packet-grade evidence without the privacy, legal or storage burden of full capture

Why an enterprise needs this tool

The reasons IT teams give for keeping uObserve™ in the critical path



- **Accelerate incident resolution**

Correlated evidence instead of five dashboards

- **Maintain revenue & reputation**

Catch degradation before customers report it

- **Rapid time to value, low TCO**

Virtual appliances; no professional-services marathon

- **Optimise IT spending**

Rightsize what is over-provisioned, on-prem and in cloud

- **Maximise IT productivity**

Silo elimination across ops, network, desktop and security

- **Nullify legal & privacy issues**

Metadata only — no packet payload retained

Organisations that run on Uila

A selection of publicly referenced customers across government, finance, healthcare, legal, education and service providers

Harris County

US county government

City of Sioux Falls

Municipal government

Baron Capital

Investment management

**First Tech Federal
Credit Union**

Financial services

Migdal Group

Insurance & finance

Quarles & Brady LLP

Legal services

**The Myers-Briggs
Company**

Assessment & publishing

GDS

Data centre service provider

**Lake Emergency
Medical Services**

Healthcare / emergency

**Bay Area Community
Health**

Healthcare

Wurth Industry

Industrial distribution

Security Central

Monitoring services

BYU Hawaii

Higher education

**Boston Architectural
College**

Higher education

**Netcor (German
insurer)**

MSP / insurance

Also: a US multinational telecommunications R&D division, an APAC government industrial ministry, and a global wine producer.

“We have been able to solve all the complaints that have been directed towards my team for infrastructure-driven application complaints.”

Mark Martinez — IT Director, Harris County

In their own words

Published customer testimonials and review-site feedback

"Uila's ability for virtual environment visibility is something I have not seen in any other product."

Henry Mayorga — CSO & VP of Infrastructure, Baron Capital

"We were able to trace back all the conversation flows, and identify problems that we didn't even know existed in our environment that was dragging us down."

Brandon Morris — Lead System Administrator, City of Sioux Falls

"In 1 second we were able to tell the Application guys that there is nothing wrong with the Infrastructure... I was able to tell them which server, which port had the issue."

Snir Hoffman — Migdal Group

"We can take proactive steps using Uila to mitigate issues, whereas before we just had to wait for that magical call."

Art Piwcio — Director of Infrastructure & Applications, Security Central

"Uila went from being a need, to a pilot, to a critical piece of our virtualised infrastructure in a matter of weeks."

Jim Root — CIO, Lake Emergency Medical Services

"Very high-end monitoring system with a very cheap price comparing to existing products in the market."

ShuChung Chang — Director of IT, Bay Area Community Health

Who uses it, and for what

Industry-aligned use cases and the roles that live in the console every day

BY INDUSTRY

Finance

Trading latency, branch experience, regulated change control

Healthcare

Clinical system uptime, EMR response, imaging storage paths

Government

Citizen services, sovereign deployment, cyber threat visibility

Telecom / MSP

Multi-tenant service assurance and SLA evidence

Education

Campus VDI, enrolment peaks, lab capacity

Retail

POS and e-commerce transaction performance at peak

BY ROLE

CIO

Service health and spend in one report

IT Architect

Dependency truth for migration and DR design

IT / Network Operations

Fast triage and root cause on shift

Cloud Engineer

Hybrid workload visibility and rightsizing

CSO / Security Engineer

East-west anomaly and lateral movement

Desktop Engineer

VDI and end-user experience evidence

Why uObserve™ instead of more of the same

How the approach differs from classic APM, NPM and infrastructure monitoring

Classic APM

- Agents / code instrumentation on every app
- Blind to infrastructure root cause
- Licensing scales painfully with hosts

Classic NPM / flow

- Sees north-south, misses east-west
- Flow records lack application context
- No compute or storage correlation

Infra monitoring

- Green dashboards while users suffer
- Resource metrics with no app meaning
- Separate tool per silo

Uila uObserve™

- Agentless DPI across east-west and north-south
- Application ↔ infrastructure correlated in one engine
- Performance, dependency and security in one console

The one-line version

Uila is the only layer that sees the conversation AND the infrastructure carrying it — which is why it can tell you the cause, not just the symptom.

Uila, delivered locally by SecureCentral

Enterprise software, delivered with expertise you can trust — www.securecentral.com.au

Value-Driven Technology Partnership

We take enterprise software vendors to market across Asia Pacific — recruiting, contracting and activating the right reseller network in each country.

Solution Consulting

Certified pre-sales architects who scope, demonstrate and prove Uila alongside your team — including proof-of-value deployments.

SECURECENTRAL IN APAC

12+ years in APAC distribution

8 markets served

5 delivery countries: AU · NZ · SG · MY · ID

Managed Support

Regional first-line and second-line support in local time zones, escalating to the vendor only when it is genuinely needed.

Marketing & Demand Generation

Co-branded campaigns, localised collateral and lead generation that partners can run out of the box.

What this means for your Uila deployment

● Local contracting

Buy in-region, in your currency, under APAC terms

● Deployment expertise

Sizing, vST/vIC/UMAS rollout and dashboard design done with you

● Local-hours support

First and second line in your time zone before vendor escalation

● Broader stack fit

Integrated with ITSM, ITAM, cyber and remote-support practices



NEXT STEPS

See it on your own infrastructure.

1

Interactive demo

A guided walk-through of the live console — no install.

2

21-day free trial

Deploy vIC + vST in your lab or a production cluster.

3

Infrastructure & performance assessment

Uila-led assessment producing a dependency map and hot-spot report.

4

Design workshop

Agree model, sizing, retention and command-centre dashboards.

YOUR APAC AUTHORISED PARTNER



Licensing, deployment, enablement and local first- and second-line support for Uila across Asia Pacific.

Web www.securecentral.com.au

Email info@securecentral.com.au

Phone +61 424 135 693

Markets AU · NZ · SG · MY · ID

SecureCentral Global Pty Ltd · A Pioneer Infotech Company

Sources & assumptions

So every claim in this deck can be traced

Product capability, pillars and positioning	uila.com — Performance Observability, Application Dependency Mapping, Cyber Threat Protection pages
Architecture and component roles	uila.com/products/how-it-works and the uObserve User Guide (vST, iST, LST, vIC, Log DB Server, UMAS)
Sizing figures in the deployment table	uila.com/products/uila-system-requirements (VMware reference, 1-month retention)
Customer names and quotations	uila.com/products/customer-testimonials and published success-story PDFs
Platform support (vSphere 8, Horizon, NSX-T/V, Nutanix, Hyper-V, Scale)	Uila press releases and technology-partner pages
Screenshots	Product screens published on uila.com; cropped for legibility, otherwise unmodified
SecureCentral partner details, markets and practice areas	securecentral.com.au — home page, Uila partner page and business registration footer

Assumption: the command-centre video-wall layout and the five-stage rollout plan are Uila-informed recommendations by the author, not vendor-published artefacts.