CITRIX CLOUD SOLUTIONS — UBERAGENT

uberAgent — See Everything. Fix It Faster. Keep It Secure.

Citrix

Most monitoring tools tell you that something is slow. uberAgent tells you exactly why — from the precise second a logon started, through every application call, network hop, and process event, all the way to the user's actual experience score. One lightweight agent. Two powerful engines. Complete visibility across every physical, virtual, and Citrix endpoint in your environment.

- User Experience Monitoring (UXM)
- Endpoint Security Analytics (ESA)
- MITRE ATT&CK Framework
- Less than 0.5% additional CPU load
- Citrix, Windows and macOS

OAS · Protect. Detect. Recover.

Prepared 11 September 2026

ONE AGENT, TWO INTELLIGENCE ENGINES

Built Around Two Integrated Engines

uberAgent is built around two integrated engines that work from the same single lightweight agent — delivering user experience insight and security analytics together, from every endpoint, without duplicating infrastructure or management overhead.

UXM — PERFORMANCE · RELIABILITY · PRODUCTIVITY

User Experience Monitoring

UXM answers the question your helpdesk hears every day: "why is it slow?" It captures granular data from every layer of the user's experience — boot duration, logon stages, application launch time, browser performance, and network quality — and distils it all into a single Experience Score that makes health visible at a glance. - Boot and logon duration — broken down stage by stage - Application unresponsiveness detection and alerting - Network reliability — latency, jitter, and packet loss per app - Process startup duration and CPU/RAM per application - Browser performance and web app metrics - Application usage metering for licence audit - Deep Citrix session and VDA insights

ESA — THREAT DETECTION · COMPLIANCE · RISK

Endpoint Security Analytics

ESA turns every endpoint into a security sensor. It monitors process call chains, network connections, registry changes, DNS queries, and file activity in real time — feeding a sophisticated threat detection engine that catches risky behaviour using MITRE ATT&CK rules, Sigma rules, and uberAgent's own uAQL query language. - MITRE ATT&CK framework — comprehensive threat coverage - Sigma rule and Sysmon rule compatibility - DNS query monitoring and hash calculation - Registry and file activity monitoring - Authenticode signature verification - Endpoint security and compliance rating - Graphical rule editor with uAQL query language

WHY IT MATTERS

Four Numbers That Capture the Value

uberAgent consolidates what typically requires multiple separate tools — performance monitoring, security analytics, licence auditing, and capacity planning — into a single agent with a minimal footprint and an outsized return on investment.

<0.5%

Additional CPU Load

The uberAgent endpoint agent is engineered for minimal footprint. Despite the volume of data it collects, it adds less than half a percent of additional CPU load — invisible to users, transparent to performance.

3–5×

Tools Replaced by One Agent

Organisations typically replace three to five separate monitoring, security analytics, and audit tools when deploying uberAgent — reducing vendor sprawl, licensing cost, and management complexity in a single move.

100%

Physical, Virtual & Citrix Coverage

One agent covers every endpoint type — physical Windows PCs, Windows Servers, macOS devices, Citrix VDA sessions, Microsoft AVD, and Windows 365 Cloud PCs — from the same deployment and management model.

Real-time

Threat Detection & Response

ESA processes call chains, network connections, and file events as they happen — detecting risky behaviour and threat indicators in real time, not after the fact. Every event is traceable back to the originating user, process, and network target.

CORE CAPABILITIES

What uberAgent Monitors and Detects

Six UXM capabilities that give your team the data to diagnose performance problems before users raise a ticket — and six ESA capabilities that give your security team the visibility to catch threats before they cause damage.

UXM — USER EXPERIENCE MONITORING

Boot & Logon Duration Analysis

uberAgent captures every stage of the Windows boot and user logon process — from power-on through Group Policy processing, profile load, logon script execution, and application readiness. When logon times creep up, the data shows exactly which stage is responsible and on which machines, without requiring manual investigation.

STAGE-BY-STAGE BREAKDOWN

UXM — USER EXPERIENCE MONITORING

Application Responsiveness & Crash Detection

uberAgent detects application hangs, crashes, and unresponsiveness events across every managed endpoint — including which specific version of which application is failing and how frequently. This makes it possible to correlate a sudden spike in helpdesk calls with a specific application update or configuration change.

CRASH & HANG MONITORING

UXM — USER EXPERIENCE MONITORING

Network Reliability — Per Application

Most monitoring tools measure network performance at the interface level. uberAgent captures latency, jitter, and packet loss per application and per network connection — making it immediately clear whether a slow application is caused by a network issue, and which network path is responsible.

LATENCY · JITTER · PACKET LOSS

UXM — USER EXPERIENCE MONITORING

Browser & Web App Performance

As more business applications move to the browser, measuring performance inside the browser becomes critical. uberAgent monitors browser activity and web app response times — identifying slow SaaS applications, measuring page load performance, and tracking which browser extensions are consuming resources.

BROWSER METRICS

UXM — USER EXPERIENCE MONITORING

Citrix Session & VDA Insights

uberAgent automatically detects Citrix Virtual Delivery Agent (VDA) and Delivery Controller environments and activates Citrix-specific metrics — session ICA latency, machine registration status, licence usage, published application inventory, and Machine Catalogue health — giving a complete picture of your CVAD site from a single tool.

CITRIX CVAD INTEGRATION

UXM — USER EXPERIENCE MONITORING

Application Usage Metering & Licence Audit

uberAgent tracks exactly which applications are used, how often, and by which users — across every managed device. This provides the data needed for software licence audits, right-sizing purchasing decisions, and identifying shelfware. Organisations commonly discover 15–25% licence cost savings from the usage data alone.

LICENCE OPTIMISATION

ESA — ENDPOINT SECURITY ANALYTICS

MITRE ATT&CK Threat Detection Engine

ESA's threat detection engine uses the MITRE ATT&CK framework to classify and detect adversary tactics and techniques in real time. It supports Sigma rules — the open standard for security detection — and Sysmon rules, with a graphical rule editor so your team can customise detection without writing XML. The uAQL query language makes rules precise and readable.

MITRE ATT&CK · SIGMA

ESA — ENDPOINT SECURITY ANALYTICS

Process Call Chain Analysis

ESA traces every process launch back through its parent chain — making it possible to see not just that a suspicious process ran, but exactly what caused it to run, in what sequence, and under which user context. This is the data that separates a meaningful threat alert from noise, and makes investigations conclusive rather than speculative.

PROCESS TRACING

ESA — ENDPOINT SECURITY ANALYTICS

DNS Query Monitoring & Network Connections

ESA monitors every DNS query made from every endpoint — per user, per application, and per process — detecting DNS-based C2 communications, tunnelling attempts, and connections to known-malicious domains. Network connections are tracked by user, application, and network target, making lateral movement and data exfiltration visible.

DNS · NETWORK VISIBILITY

ESA — ENDPOINT SECURITY ANALYTICS

Registry & File System Monitoring

ESA tracks registry modifications and file system events across endpoints — detecting persistence mechanisms, malicious registry writes, and suspicious file creation or modification patterns. Hash calculation enables file integrity verification, and Authenticode signature checking flags unsigned or incorrectly signed executables before they cause harm.

REGISTRY · FILE INTEGRITY

ESA — ENDPOINT SECURITY ANALYTICS

Endpoint Security & Compliance Rating

ESA conducts periodic security configuration checks across endpoints — verifying that line-of-business applications, operating system settings, and security controls meet defined standards. Results are presented as a compliance rating per endpoint, with the ability to create custom checks against your own security policies and regulatory requirements.

COMPLIANCE · CONFIG CHECKS

ESA — ENDPOINT SECURITY ANALYTICS

SOC & EDR Augmentation

ESA is designed to complement, not replace, existing EDR and XDR solutions. The granular data it provides — particularly on Citrix and virtual endpoints that many EDR tools cover poorly — feeds SOC workflows via Splunk, Elasticsearch, or other SIEM platforms. ESA extends detection coverage to environments that existing tools may miss entirely.

SIEM INTEGRATION

THE EXPERIENCE SCORE

Three Scores. One Clear Picture of Your Environment.

uberAgent's Experience Score dashboard distils the volume of raw performance data into three composite scores — giving IT teams an instant read on overall environment health, and a clear starting point for drilling into the detail when something needs attention.

APP — APPLICATION PERFORMANCE & RELIABILITY

Application Score

Synthesises application launch time, crash rate, and unresponsiveness events into a single score per application — making it immediately visible which applications are degrading the user experience and how significantly.

SESSION — SESSION & LOGON QUALITY

Session Score

Captures boot duration, logon duration, network quality, and session stability into a score per user session — highlighting which users are consistently receiving a poor experience and whether the cause is machine-specific, network-related, or environmental.

MACHINE — MACHINE HEALTH & RESOURCE USAGE

Machine Score

Tracks CPU, memory, disk, and overall machine responsiveness into a per-machine score — surfacing machines that are chronically under-resourced, approaching capacity limits, or generating disproportionate helpdesk contact before they become critical problems.

THE EXPERIENCE SCORE

Resolving Issues at Scale

Identifying one slow machine is straightforward. uberAgent's value is in finding correlations across hundreds or thousands of endpoints simultaneously — making it possible to identify that a specific application update, Group Policy change, or network configuration is affecting a defined subset of machines, without manually reviewing individual tickets.

BACKEND & INTEGRATION FLEXIBILITY

Splunk — The Reporting Engine of Choice for uberAgent

uberAgent feeds data into the monitoring platforms your team already uses, with no requirement to replace existing investments. uberAgent is a data collection and analysis platform — it needs a backend to store and visualise what it captures. Splunk is the primary reporting tool, and the one for which uberAgent ships over 60 fully built dashboards out of the box. Other backends are supported, but dashboards are only available for Splunk.

RECOMMENDED

Splunk Enterprise / Splunk Cloud

Full dashboard suite — 60+ out-of-the-box reports for UXM and ESA. Splunk AI integration for automated process detection and risk analysis. Supports on-premises and cloud deployment. Separate Splunk licence required.

Elasticsearch & Kibana

Raw uberAgent data can be forwarded to Elasticsearch. Custom Kibana visualisations can be built, but no pre-built dashboards are included. Suited to organisations with an existing ELK stack.

Azure Monitor

Data can be forwarded to Azure Monitor / Log Analytics for organisations using Azure as their primary observability platform. No pre-built dashboards — visualisations built via Azure Workbooks.

Apache Kafka

For organisations routing telemetry through a Kafka pipeline to a custom SIEM or data lake. uberAgent functions as a high-volume, structured data producer in this architecture.

BACKEND & INTEGRATION FLEXIBILITY

Splunk Licensing and Breadth of Deployment

Splunk Enterprise or Splunk Cloud acts as the central intelligence platform — receiving data from uberAgent agents across every endpoint, indexing it, and presenting it through a rich set of pre-built dashboards. Each dashboard is searchable, filterable by time range, machine, user, or application, and fully responsive across screen sizes.

It is important to understand that Splunk carries its own licensing cost, separate from uberAgent. Splunk is licensed on a data ingestion volume basis — the more endpoints you monitor and the more metrics you collect, the more data is indexed per day. OAS advises on the right Splunk sizing and licensing model for your environment to ensure uberAgent delivers its full value without unexpected cost surprises.

Where uberAgent really earns its place is in breadth of deployment. The same single agent that monitors your Citrix VDA servers and user sessions can be extended to any other Windows or macOS endpoint in your organisation — application servers, domain controllers, physical PCs, executive laptops — giving your IT team one unified view of the entire estate rather than separate tools for each workload type.

SPLUNK DASHBOARDS

60+ Dashboards Included Out of the Box

uberAgent ships three Splunk app packages — the UXM app, the ESA app, and the Helpdesk app. Together they provide over 60 pre-built dashboards covering every aspect of user experience, endpoint performance, and security analytics. Here are ten of the most important, covering both the UXM and ESA sets.

| Dashboard Name | Category | What It Shows |

| --- | --- | --- |

| Experience Score Overview | UXM | The entry-point dashboard. Calculates and visualises composite experience scores across the entire endpoint fleet — broken down by user, application, and machine — with drill-through to any component where scores are degrading. |

| Logon Duration Analysis | UXM | Breaks down every user logon into its component stages — Group Policy processing, profile load, folder redirection, logon scripts, and application readiness — showing exactly which phase is causing slow logons and on which machines or user groups. |

| Application Performance & Errors | UXM | Tracks application launch times, crash events, hang detection, and error rates per application across the entire estate — identifying which application versions are behaving poorly and correlating issues with recent changes. |

| Network Reliability Drill-Down | UXM | Shows network latency, jitter, and packet loss per application, per network target, and per endpoint — enabling precise identification of whether a performance complaint originates from the network path rather than the application or server. |

| Machine Performance & Inventory | UXM | Displays CPU, memory, disk, and overall machine health across the endpoint fleet. The inventory view shows OS versions, hardware specs, and installed applications across all monitored machines — essential for capacity and upgrade planning. |

| Application Usage Metering | UXM | Tracks which applications are actively used, by which users, and for how long — across every managed endpoint. Provides the data needed for software licence audits, identifying shelfware, and planning application rationalisation projects. |

| Citrix Session Insights | UXM | Delivers deep visibility into Citrix CVAD environments — ICA session latency, bandwidth usage, protocol encoding settings, VDA machine registration status, licence consumption, and published application inventory per site. |

| Threat Detection & Risk Analysis | ESA | The primary ESA security dashboard. Displays detected threat events mapped to MITRE ATT&CK technique IDs, categorised by severity, application, and endpoint — giving SOC teams an immediate view of risky activity across the fleet. |

| Process Tree & Call Chain | ESA | Visualises the full parent-child process hierarchy for any detected event — showing what spawned a suspicious process, under which user context, with command-line arguments and process lifetime. Transforms a security alert into a complete investigation chain. |

| DNS Risk & Network Connections | ESA | Dedicated DNS monitoring dashboard tracking all DNS queries per user, process, and network target — detecting DNS tunnelling, C2 beacon patterns, and connections to known-malicious domains. Network connection data is visualised per user and per application. |

In addition to the UXM and ESA dashboard apps, uberAgent ships a separate Helpdesk Splunk App — a streamlined view of the uberAgent dataset designed specifically for first-line support staff. It surfaces the most relevant metrics for per-user and per-machine troubleshooting in a simplified interface, without requiring helpdesk technicians to navigate the full UXM dashboard suite.

INDUSTRY COMPARISON

uberAgent vs Cisco ThousandEyes — Different Tools, Different Answers

Cisco ThousandEyes is an excellent and widely respected platform — but it answers a fundamentally different question from uberAgent. Understanding the distinction helps organisations choose the right tool for their monitoring challenge, or recognise when they need both.

Citrix uberAgent

- Primary focus: what is the user actually experiencing? uberAgent monitors the endpoint — what the user sees, what applications are doing, how the machine is performing, and whether the environment is secure.
- Monitoring approach: agent installed on every endpoint — collects real data from actual user sessions, real applications, and real network connections made by real users in real time.
- Application visibility: deep per-application data — launch times, crash rates, resource usage, process call chains, network connections per app, browser performance, and usage metering. Works with every application automatically.
- Citrix & VDI environments: native Citrix integration — auto-detects VDA and Delivery Controller roles, monitors ICA session metrics, logon stages, machine catalogue health, and Citrix licence consumption. Optimised for virtual desktop environments.
- Security analytics: full ESA engine — MITRE ATT&CK threat detection, process call chain analysis, DNS monitoring, registry and file monitoring, compliance rating, and Sigma/Sysmon rule support. Endpoint security is a core capability.
- Network visibility: per-application network metrics captured from real user connections — latency, jitter, packet loss, and DNS queries as experienced by the actual user and application. Covers internal and internet-bound traffic.
- External internet monitoring: monitors what internet-connected applications experience from the endpoint — surfacing issues with specific

Cisco ThousandEyes

- Primary focus: what is the network doing? ThousandEyes monitors paths, routes, and connectivity — ISPs, cloud providers, SaaS reachability, and internet infrastructure — from synthetic vantage points.
- Monitoring approach: synthetic monitoring from cloud and enterprise agents — simulates user requests to test reachability and performance of URLs, APIs, and network paths from defined vantage points.
- Application visibility: HTTP/HTTPS layer testing for web applications and APIs. Strong for SaaS availability and page load testing. Limited visibility into installed desktop application behaviour or virtual desktop session performance.
- Citrix & VDI environments: can monitor the network path to Citrix infrastructure from enterprise agents. Does not monitor what is happening inside the Citrix session, on the VDA, or within the virtual desktop environment itself.
- Security analytics: network-layer security visibility — BGP routing anomalies, DNS hijacking, internet outages, and path-level threat intelligence. Not designed for endpoint threat detection or process-level security monitoring.
- Network visibility: unmatched network path visibility — BGP routing, ISP performance, CDN health, and internet backbone analysis from 193+ global vantage points. The authority for internet and WAN infrastructure monitoring.
- External internet monitoring: industry leader for external internet and SaaS monitoring. Provides ISP-level path analysis, cloud provider health

destinations, DNS resolution failures, and connection drops per user and per app.

- Deployment model: lightweight agent on managed endpoints — Windows and macOS, physical and virtual. Included in Citrix UHMC subscription. Requires Splunk or alternative backend for dashboards.

tracking, and internet outage detection at a global scale unavailable to any agent-based tool.

- Deployment model: cloud-based SaaS platform with enterprise agents deployed at network vantage points. Endpoint agents available for end-user monitoring. Priced per test and agent volume — typically a significant separate investment.

INDUSTRY COMPARISON

The Practical Conclusion

If your challenge is understanding why users in a Citrix or virtual desktop environment are experiencing slow logons, crashing applications, or inconsistent performance — and whether endpoints are secure — uberAgent is the right tool. If your challenge is understanding why your organisation cannot reach a SaaS provider, which ISP is causing packet loss on your WAN, or how internet routing affects application delivery globally — ThousandEyes answers those questions. For organisations that need both layers of visibility, the two tools are complementary rather than competing.

HOW IT'S DELIVERED

Delivered as a Managed Service by OAS

uberAgent is powerful out of the box — but its real value is realised when the data is being actively reviewed, acted on, and used to drive continuous improvement. OAS manages the full lifecycle on your behalf.

Deployment & Agent Rollout

OAS deploys the uberAgent endpoint agent across your entire estate — physical, virtual, and Citrix — using group policy, SCCM, or your existing software distribution tooling, with Citrix-specific configuration applied automatically on VDA and Delivery Controller hosts.

FULLY MANAGED ROLLOUT

Dashboard Configuration & Alerting

OAS configures the Splunk or Elasticsearch dashboards, tunes alert thresholds for your environment's baseline, and sets up automated notifications for Experience Score degradation, security events, and capacity warnings — so issues surface before users complain.

ALWAYS ON

Security Rule Management

OAS maintains and updates the ESA threat detection rule set — incorporating new Sigma rules, refining MITRE ATT&CK coverage, and tuning detection thresholds to reduce false positives while ensuring genuine threats are not missed. Custom compliance checks are created to match your specific policies.

ONGOING TUNING

Reporting & Capacity Reviews

Regular reports covering Experience Score trends, top-impacted users and machines, application reliability statistics, security event summaries, and capacity utilisation — providing the data for informed infrastructure decisions and the documentation required for POPIA compliance evidence.

POPIA READY

THE CITRIX SOLUTION SERIES

Citrix provides a comprehensive, secure and high-performance digital workspace platform for any industry. uberAgent is the observability layer that answers the question every IT team faces daily: how is the environment actually performing for real users, and is it secure? Acquired by Citrix from vast limits GmbH in 2024, uberAgent is now fully integrated into the Citrix platform — included in the Citrix Universal Hybrid Multi-Cloud and Citrix Platform License subscriptions.

Citrix DaaS **Secure Private Access** **NetScaler** **XenServer**

Stop Guessing. Start Knowing.

Speak to an OAS consultant about deploying uberAgent across your Citrix and endpoint environment, or follow the official Citrix PoC guide to evaluate it yourself in your own lab.

TELEPHONE

+27 11 485 3454

EMAIL

info@oas.co.za

WEB

https://www.oas.co.za

OFFICE

25 Durham Street, Raedene Estate, Johannesburg

Request a demo: https://www.oas.co.za/contact/demo

Open Architecture Systems — Protect. Detect. Recover. Citrix Platinum Partner since 1987.