



uObserve™

Application-Centric Observability

uObserve™ Core Value

Observe

End-to-end VDI user, Application, Infrastructure & Network Metrics & Log Analysis

Resolve

Reduce MTTR with Root Cause Isolation, Application-centric alerting & Automated Remediation Actions

Optimize

Right-size Infrastructure Resources

Secure

Intelligent Threat Detection on Application Workloads

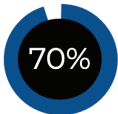
Enterprise Data center architecture has evolved dramatically in recent years, enabling it to effectively run large-scale, distributed, multi-tier applications across public, private and hybrid cloud environments. To support and ultimately ensure delivery of business-critical applications and services, an elastic data center architecture and agile development model has emerged to share workloads, data and resources across the multi-cloud environment. However, IT monitoring solutions have not kept pace with this new wave of multi-cloud dynamics and the agile DevOps model. Current tools have also reinforced the established silos that separate applications, virtual infrastructure, physical infrastructure and cloud resources, and failures could occur anywhere. Most enterprise organizations have also learnt that preventive security methods are not able to block all cyber attacks, so it has become critical for SecOps teams to prevent that network intrusion from becoming a data/financial/reputation loss. Based on Uila and other industry expert surveys:

- 2 out of 3 organizations do not have complete visibility into their assets and dependencies.
- 90% of organizations expect their IT team to resolve issues within 30 minutes.
- 2 out of 3 organizations would like to reduce their “tools overhead” to reduce MTTR and investment.
- Time it takes to determine root cause, accounts for over 70% of the time it takes to restore the service to normal operation.
- It takes over 280 days to identify and contain a security breach and the average cost/incident is almost \$4M.

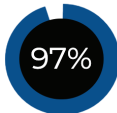
There is an expectation to optimize investment, avoid risks, maximize performance and most importantly streamline the IT operations through automation. This has led to organizations expecting a revolutionary shift in the way they monitor their critical applications and infrastructure.

Uila uObserve™'s Application-centric Performance & Security Observability Analytics to resolve Complex IT Disruptions

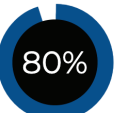
Uila uObserve™ provides Performance and Cyber Threat Observability Analytics & Logging, in a single pane of glass to help resolve complex IT disruptions for Enterprise IT across virtualized, containerized and physical server-based applications. With uObserve™, IT teams can visualize application workload dependencies across cloud platforms, rightsize infrastructure resources, troubleshoot disruptions for any onsite or remote VDI user due to application/network/infrastructure challenges, plan workload migration strategies for Cloud deployments and use AIOps to streamline troubleshooting and reduce MTTR with remediation actions . uObserve™ also allows security teams to combat advanced cyber threats, by providing comprehensive application-centric insights into cyber threats & Data Exfiltration activities. Organizations use uObserve™ to align themselves with their IT teams & cut MTTR from days to minutes to keep the end-user experience at peak performance & secure at all times across cloud boundaries.



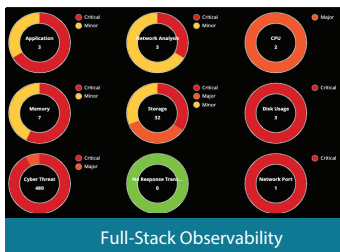
Reduction of Unplanned Downtime and Cost of Outages



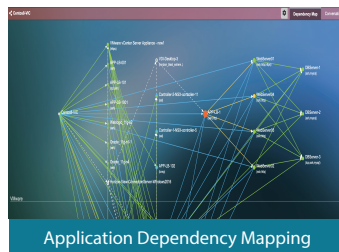
Reduction in time for Infrastructure & Application Discovery/Mapping Agentless and Automated



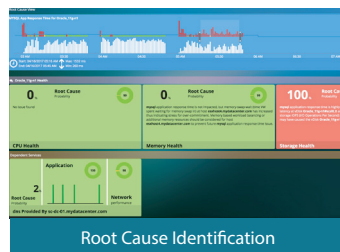
Faster Detection and Troubleshooting of Issue with Full-Stack Root-Cause Analysis



Full-Stack Observability



Application Dependency Mapping



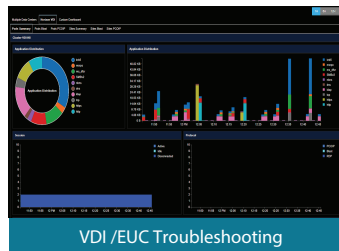
Root Cause Identification



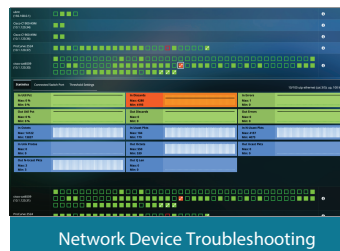
Threat Detection



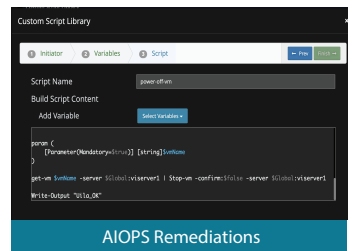
Infrastructure Analysis



VDI /EUC Troubleshooting

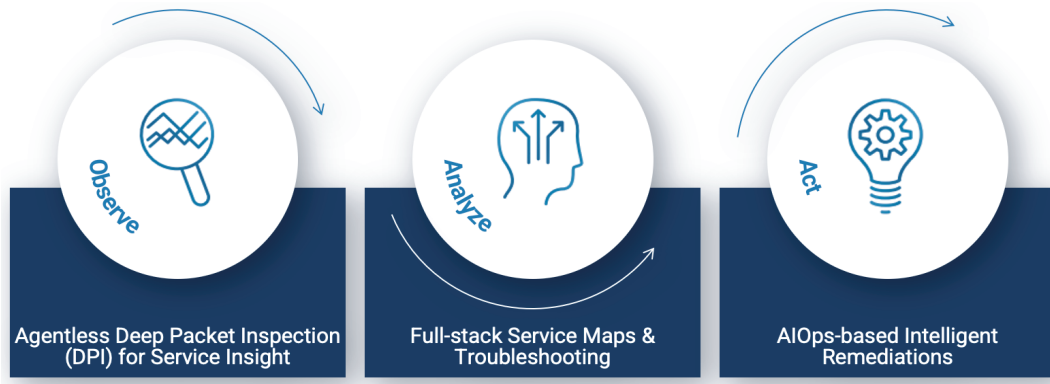


Network Device Troubleshooting



AIOps Remediations

Feature Highlights



Performance Observability & Automated Remediations

Agentless and Scalable Architecture with Deep Packet Inspection Insights

- Agentless architecture to monitor across the full-stack. This allows you to monitor your application workloads without any special approvals from application owners or suffering from complex, tedious & expensive rollouts.
- Monitor and resolve downtime and slowdowns for more than 4,200 applications, including Web, Databases, ERP, Healthcare (EPIC, HL7, Dicom), Financial (FIX), Industrial (Scada), SaaS (Office 365, Zoom, Webex, Teams, Google) and many more.
- Monitor VMware, Nutanix, Microsoft Hyper-v, AWS, Azure, GCP, Kubernetes deployments & Physical Servers in a single interface

Full-Stack Monitoring to isolate Root-Cause for outages and performance challenges before End-user Impact

- Built-in Expert system gives IT teams a 1-click access to root cause from the Dependency Maps and remediation steps for unplanned business service outages or performance degradations.
- Pinpoint root cause behind unplanned downtime or slowdowns, including application, infrastructure & virtual/physical network challenges in a single unified view.
- Solve problems from the end-user's perspective in addition to proactive monitoring to solve problems before they occur.
- Utilize Continuous Machine Learning (ML) & Behavior Learning algorithms to identify anomalies from performance baselines instead of manual guesstimates to provide unprecedented level of accuracy.
- Centralized & Correlated Infrastructure & Application Log Analytics to investigate and resolve any performance issue.

Deep Insights into Infrastructure, Virtual/Physical Networks & Applications

- Visualize compute performance impact on application performance with metrics like CPU swap wait, CPU Ready, Utilization & tie to Application Response Time.
- Visualize performance (memory usage, swap rate, swap wait times) of all memory arrays in your hosts.
- Visualize trending performance issues on Read/Write latencies and IOPS across VMs, vDisk and Data Stores. Get alerted to disk capacity challenges.
- Virtual East-west Network flow analysis reveals network issues and stress impacting application servers, plus see anomalous traffic between VMs. .
- Monitor network device configuration settings, health, availability and bandwidth usage, as well as various other network parameters for traffic statistics including errors, discards, etc. and visualize impact of network on application performance.
- End user response time tracking proactively alerts IT to service degradation from the user's perspective before user and revenue impact.
- Deep Application Intelligence with Application Transaction Analysis.
- Visualize under-provisioned hosts or instances leading to performance issues, and over-provisioned resources wasting precious investment.
- Up/Down status and process level monitoring for servers.

Kubernetes Observability

- Automated Application-centric Kubernetes Observability for infrastructure and application teams to rapidly identify and resolve operational complexities.
- Up-to-date container topology for Kubernetes-orchestrated microservice applications with automated & dynamic Application Dependency Mapping.
- Unparalleled insights into end-to-end workload dependencies that exist across containerized infrastructure and existing VM infrastructure.
- Real-time discovery metrics across every microservice, pod, cluster and node for faster troubleshooting and futureproofing of resource management/provisioning.
- Single click root-cause analysis to resolve any application outage or slowdown with full-stack visibility.
- Identify most common Kubernetes issues impacting application performance, including failing pods, pod evictions due to resources, crash errors, etc.

Automated IT Operations with Intelligent Remediations

- AIOps to streamline troubleshooting and reduce MTTR with remediation actions across the infrastructure, including VDI.
- Intelligent Alert-based triggers and Manual triggers provide complete control in proactively preventing issues as well as streamlining problem resolution.
- Increase IT team efficiency by automating repetitive tasks and helping them focus on issues that matter.
- Actions include Power off/Suspend/Reset/Power On VMs, logging off VDI users, Updating VMware tools, Restart Guest OS, Kill process running on a VDI desktop, etc.
- Fully customizable PowerShell scripting for VMware vCenter and Horizon VDI to provide full remediation & configuration control for your entire-stack.

Centralized Log Analysis for Multi-Cloud deployments

- Instant and automated access to out-of-box correlated and contextualized logs from multiple systems including Windows (Event and Active Directory), IIS servers, Zscaler, Cisco, Barracuda, F5, Checkpoint, Juniper, etc. and applications like Microsoft SQL server, VMware Horizon, IBM MQ, Oracle, Office 365, and much more
- Contextualized querying and filtering within logs for accelerated troubleshooting and infrastructure management.
- Intelligent full-stack Observability context in a unified console that combines metric and log data to improve IT team efficiencies. No need to dig through logs in a separate tool and correlate with metric data.

VDI/EUC End-to-end Mapping & User Session Analysis

- Reduced time to value with Automated discovery and mapping of VDI Components (end-to-end from user clients to virtual desktops to backend application and connection servers) and all interdependencies for VMware Horizon and Citrix deployments.
- Troubleshoot issues proactively directly from the Dependency Map down to the Application, Network or Infrastructure.
- Insights into detailed user sessions for VMware Horizon deployments, including metrics on active, idle, disconnected states.
- Visualize username, associated virtual desktop VM, session start time, pool or farm information, etc.
- Measure time for every stage in the logon process like broker duration, agent duration, app launch duration, etc. and isolate issues leading to failed or slow logons.
- Visualization of Blast Extreme and PCOIP RX and TX Packet Loss, Round-Trip Time, User session latency, bandwidth, etc.
- Insights into Application traffic from VDI desktop as a client connects to application servers (e.g. Zoom, ERP, Databases, EHR, Financial, web, etc.)
- Full visibility into the associated alarms, conversation, infrastructure resources, applications in use and process level information.
- Visualize session data for your entire VDI deployment or customize views for your Pools, Pods or Sites.
- Intelligent NVIDIA GPU metrics using the NVIDIA System Management Interface (NVSMI) to allow desktops teams to provide the maximized performance for GPU-enabled virtual desktops.

Application Dependency Mapping

Agentless, Automated Mapping of Applications and Infrastructure

- Automated visualization of all virtual, physical and cloud assets and their interdependencies at the application level.
- Visualize Application and Infrastructure Dependencies across all Clouds, Containers and On-Premise to pinpoint areas of fixing and investment.
- Automatically generated and updated in real-time for all applications.
- Create and customize multi-tier application groups based on your requirements.
- Single-click identification of root cause in Application performance down to Application, Infrastructure & Virtual/Physical Network bottlenecks from the map.
- Take Back Control of Your Changes & Identify Policy Violations with visualization into additions, deletions and modifications for any asset and dependency.
- Plan your organization's Migration Strategies with Agentless Pre-Migration Assessments and Export results to Excel or CMDB systems.

Cyber Threat Monitoring

Classify and Identify Lateral Movement & Anomalous behavior of Malicious Cyber Threats

- Comprehensive visibility into lateral (east-west) movement traffic patterns to identify custom backdoors and compromised systems.
- Classify normal network traffic and application behavior and highlight anomalous traffic and dependencies.
- Real-time Signature & Anomaly-based Threat Identification for all business-critical applications and resources across cloud boundaries.
- Visualize deviation (unauthorized VMs/connections/external internet connections) from baseline security policy.
- Map Outbound Traffic from your Data Center to the Internet to reduce risk associated with general Internet connectivity.
- Chain of Evidence for quick and effective response to any threat with comprehensive application transaction data, infrastructure status and network traffic data before, during and after an attack.

Uila Testimonials

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

- Harris County Clerk's Office

"The product was well thought out and fairly intuitive. We are very pleased with this product and what it does for us."

- BYU Hawaii

"Uila has provided us with the tools to maintain or exceed those service levels, while also giving us the capabilities to proactively tune our applications and determine the optimal system upgrades."

- The Myers-Briggs Company



"Whenever there's a performance issue now, we can go in to Uila and it's much easier to find out why."

- Quarles & Brady

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

- City of Sioux Falls

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

- Baron Capital

System Requirements

Instance/VM Type		CPU	Memory & Storage
Virtual Smart Tap (vST) for On-premise		1 vCPU (1 Core)	1 GB virtual memory 2 GB virtual storage, local
Virtual Smart Tap (vST) in Public Cloud	t2.large for AWS D2s v3 for Azure	For latest Kubernetes requirements, visit: https://www.uila.com/products/uila-system-requirements	
Virtual Information Controller (VIC) for On-premise		4 vCPU	Small VIC 24 GB RAM allocated*, 12GB RAM reserved, 50GB storage, thin provisioned: <1000 VMs, less than 200 Network Monitoring ports, less than 100 nodes for server monitoring Medium VIC 32 GB RAM allocated* , 16GB RAM reserved, 100GB storage, thin provisioned: 1000~2000 VMs, 200~400 Network Monitoring ports, 100~200 nodes for server monitoring Large VIC 48 GB RAM allocated* , 24GB RAM reserved, 200GB storage, thin provisioned: 2000~5000VMs, 400~600 Network Monitoring ports, 200-400 nodes for server monitoring
Virtual Information Controller (VIC) in Public Cloud	AWS t2.medium (<500 Instances) t2.large (500-1000 Instances) r4.large (1000+ Instances) Azure B2S (<500 VMs) D2s v3 (500-1000 VMs) A2m v2 (1000+ VMs)		* Additional 6GB RAM needed per Horizon Connection Server when using VMware Horizon VDI integration
Uila Management & Analytics System (UMAS) for On-Premise		1 vCPU (4 Cores)	For small scale deployment (under 1000 devices including VM and external device): One-box UMAS (1 VM to host UMAS) with 4 vCPU, 48GB RAM allocated and 32GB reserved, 1TB for 1 month data retention For medium scale deployment (1000~2000 devices including VM and external device) One-box UMAS (1 VM to host UMAS) with 4 vCPU, 64GB RAM allocated and 48GB reserved, 2TB for 1 month data retention For large scale deployment (2000~5000 devices including VM and external device) Web UMAS: 4 vCPU, 48GB RAM allocated and 32GB reserved, 800GB DB UMAS: 4 vCPU, 48GB RAM allocated and 32GB reserved, 5TB For super-large scale deployment (greater than 5000 devices), contact Uila
Uila Management & Analytics System in Public Cloud	r4.xlarge for AWS E4 v3 for Azure		
Browser	Windows: Firefox, Edge, Chrome	OS X: Safari, Firefox, Chrome, Opera	Linux: Firefox, Chrome
Hypervisor	VMware ESXi/NSX, Nutanix AHV, KVM (OpenStack)	vSphere ESXi 6.0 or higher; vCenter Server 6.0 or higher; VMware NSX 6.2, or higher Nutanix Prism Central pc.2021.8 or PC.2022.6.0.1 and AHV 20201105.2096 OpenStack vQ or higher; Nova Node OS versions: Ubuntu 16/Centos 7; OpenStack Virtual Switch & Linux bridge	
Uila Log Database Server		8 Cores	8 GB RAM, 250 GB SSD

System SKUs

Description	Remark
Uila uObserve Software incl. Cyber Threat , AIOps, Log Analysis, Subscription License/pCPU socket Uila CIPM Annual Subscription License for # of VM/Instance for Cloud	Includes software updates and support (Refer to www.uila.com/support)
Uila uObserve Perpetual License/pCPU socket Uila CIPM Perpetual License for # of VM/Instance for Cloud	Software update and support purchased separately
Annual Support for Uila uObserve Perpetual License/pCPU socket Annual Support for Uila CIPM Perpetual License for # of VM/Instance for Cloud	Includes software updates and support (Refer to www.uila.com/support)
Uila Network Device Monitoring Annual Subscription License for x Ports Uila VDI Session Monitoring Software Annual Subscription License based on x number of active sessions	Includes software updates and support (Refer to www.uila.com/support)

About Uila

Uila uObserve resolves Complex IT Disruptions for Enterprise Organizations with its Intelligent Application-Centric Full-Stack Observability Platform, that correlates Application and Infrastructure Performance to isolate and remediate issues before business impact. With Uila, IT teams can visualize application workload dependencies across cloud platforms, rightsize infrastructure resources, troubleshoot disruptions for any onsite or remote VDI user due to application/network/infrastructure challenges, plan workload migration strategies for Cloud deployments and use AIOps to streamline troubleshooting and reduce MTTR with remediation actions. Uila also allows security teams to combat advanced cyber threats, by providing comprehensive application anomaly insights, cyber threats & Data Exfiltration activities. Organizations use Uila to align themselves with their IT teams and cut MTTR from days to minutes to always keep End-User Experience at peak performance & secure, across cloud boundaries.

Uila, Inc.
2975 Scott Blvd.,
Suite 110
Santa Clara CA 95054
USA

www.uila.com
+1-(408) 400-3706
sales@uila.com & support@uila.com

