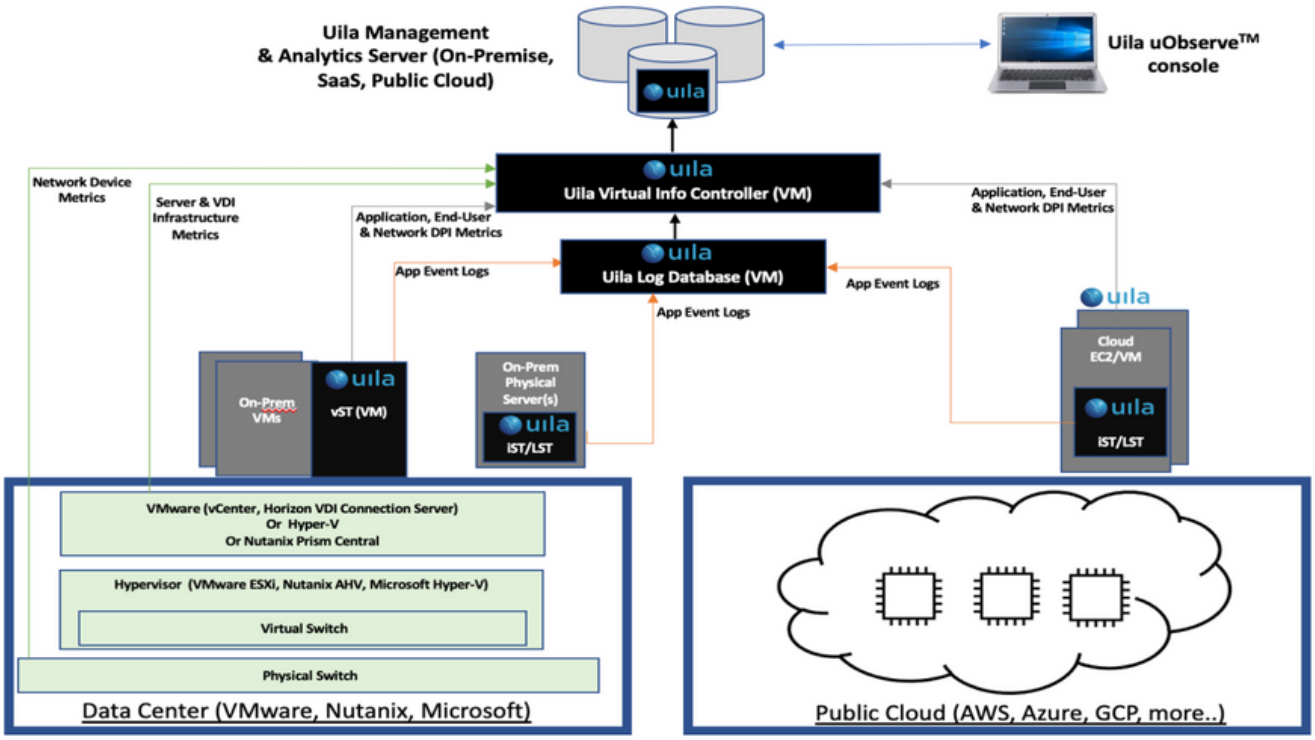
Uila SaaS Cloud Security & Compliance

INFO@UILA.COM WWW.UILA.COM +1-408-400-3706

INFO@UILA.COM WWW.UILA.COM +1-408-819-0777

Uila Architecture and Data in Uila SaaS Cloud



Uila Virtual Smart Tap (vST): It is deployed in a distributed manner across the data center or the Public Cloud. The vST installs in the host (Private Cloud) or VM/instance (Public Cloud) as an efficiently designed guest Virtual Machine where it promiscuously listens to all traffic from the virtual switch or getting traffic from Uila's Instance Smart Tap (iST) that traverses the virtual networks (North-South and East-West).

Uila Virtual Information Controller (vIC): The vIC can be installed in either the Private and Public Cloud. In the Private Cloud, Virtual Information Controller (vIC) is the integration conduit to the data center Virtualization Management System e.g. VMware vCenter. The vIC collects network, storage and compute performance metrics that are maintained by vCenter and combines it with the application and network metadata from all deployed vSTs. In the Public Cloud, the vIC collects the Instance & VM level networking, application, compute statistics from the vSTs.In both cases, the vIC securely transmits it to the Uila Management and Analytics System, either on-premise or in the cloud.

Uila Instance Smart Tap (iST): It is deployed as a plug-in in a distributed manner across the Public Cloud on the VMs or Instances running the application workload. It collects traffic as well as VM and Instance level Compute statistics and sends it to the vST for Deep Packet Inspection.

Uila Management and Analytics Server (UMAS): UMAS, the core of the Uila virtual infrastructure architecture is a big data store and analytics engine that is designed from ground up to scale-out to accommodate large data center deployments with thousands of servers, to scale-in to record data in high resolution, maintain historical data while maintaining real time responsiveness. Built-in redundancy offers high availability, mitigates downtime, and reduces maintenance overhead.
Uila offers 3 distinct models for the deployment of the critical Uila Management and Analytics Server (UMAS). UMAS can be installed On-premise (of the user), Public Cloud (AWS, Azure, etc.) or Uila's SaaS Cloud.

Uila logging Smart Tap (LST): The Uila Logging Smart Tap (LST) is deployed as a plug-in in a distributed manner across the Data Center on VMs/Physical Servers and Public Cloud in the VMs or Instances. It collects logs from the server and/or application and sends it to the Uila logging server for further analysis.

Uila Log Database Server: The Uila Log Database Server can be installed in either the Private or Public Cloud. The Uila Log Database Server collects and consolidates logs and log statistics from multiple Logging Smart Taps (LST). The Uila uObserve web console requests the log data from Uila vIC, which in turn queries the Log Database Server and delivers it back to the Uila UMAS server.

How does Uila Cloud ensure data captured by vST agent is not compromised during transmission to the Uila Cloud?

First, the data transmission between vST and Uila Cloud is using Secure Shell (SSH), an encrypted network protocol. Second, we added another security layer by using digital signed certification to ensure the true identity of the vST agent loaded in your server.

How does Uila Cloud ensure no business critical information is captured and stored in the cloud?

Although vST can capture and see the network traffics, it only analyzes the packet header to identify unique application and its response time. vST keeps both application response time and network response time for performance analysis.

However, when an application exhibits slow performances, vST will capture small portion of the transaction data, e.g. IP addresses to allow application developer to analyze application issue that might be the cause of slow response time. If capture partial data is prohibited by your company's security policy, we recommend that you select the On-Prem deployment option.

Uila SaaS Cloud Physical Security

Security Officers

While most data centers outsource their security personnel, Uila's hosting company directly employs experienced security officers at their facilities, adding a layer of accountability to the protection of our mission-critical business applications. Security personnel receive rigorous annual training and are required to pass certification. The security officers are on-site around the clock, every day of the year to protect the Uila IT infrastructure.

IP-DVR Cameras & Perimeter Fencing

The facility is secured by 8’ perimeter fencing as well as 360 degree view IP-DVR cameras.

Biometric Scanners & Card Readers

Most main entrances and many locations throughout the data centers require the use of a personalized security badge and biometric scanner.

Mantrap Entries

Facility employs mantrap or double mantrap entries in order to strictly maintain the flow of people through the entry points at our data centers.

Locking Cages & Cabinets

Cages and cabinets are key locked and monitored by video.

Uila SaaS Cloud Data Center Compliance

All compliance examinations and assessments at the hosting company facility are conducted by Schellman & Company, LLC, an independent CPA firm, a globally licensed PCI Qualified Security Assessor, an ISO Certification Body, HITRUST CSF Assessor, and a FedRAMP Third Party Assessment Organization (3PAO).

SOC 1 Type 2 and SOC 2 Type 2

Each year, an external auditing firm completes System and Organization Controls (SOC) 1 Type 2 and SOC 2 Type 2 reviews of the data center facilities.
SOC 1 and SOC 2 are attestation standards issued by the American Institute of Certified Public Accountants (AICPA). The SOC 1 report is intended to meet the needs of user entities' management and auditors as they evaluate the effect of a service organization's controls on the user entity's financial statement assertions. The SOC 2 report is intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. The hosting company's SOC 2 reports include the security and availability Trust Services categories.

ISO 27001

The hosting company has achieved the International Organization for Standardization certification (ISO 27001) covering both corporate policies and procedures, as well as the operating data center. The ISO/IEC 27001:2013 certification is one of the most stringent certifications for information security controls, and confirms the information security controls and other forms of risk treatment are in place to detect and defend against potential data system vulnerabilities.

NIST 800-53

Each year, an independent Third Party Assessment Organization (3PAO) firm completes an external assessment to validate the hosting company's strict adherence to the National Institute of Standards and Technology Publication Series 800-53 (NIST 800-53) high-impact baseline controls and additional Federal Risk and Authorization Management Program (FedRAMP) requirements. The scope of assessment includes a subset of control families applicable to colocation services. The utilization of the high-impact baseline controls for NIST 800-53 reflects commitment to successfully delivering the most rigorous compliance standards to support customers' Federal Information Security Management Act (FISMA) and FedRAMP compliance efforts.

PCI DSS

Each year, a Quality Service Assessor (QSA) completes an external assessment to validate hosting company's compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) as a "Level 1" service provider for our colocation services. The scope of assessment includes physical security and related policies at the data center.

HIPAA

HIPAA requires that covered entities take strong measures to protect the privacy and security of electronic protected health information (ePHI). By attaining HIPAA validation through an external attestation, the hosting company provides assurance to healthcare providers and other related enterprises that its national platform of multi-tenant data centers conforms to a high standard of data security and provides a secure environment for customers' sensitive and confidential data.

Uila SaaS Cloud Power & Cooling

Airside Economization

Air-side economizers pull colder outside air into the facility for cooling purposes, rather than using recirculated mechanically-cooled air from inside the data center.

Hot/Cold Aisle Containment

The company deploys cabinet lineups in hot- and cold-aisle configurations so that hot exhaust air and cold intake air remain isolated from one another.

Uila Information Management & Governance

Security Ownership

Uila has an authorized individual with security responsibilities who is responsible for information security, security program ownership, responsibilities and accountabilities.

Destruction of Physical Data

All physical data will be shredded using cross-cut shredders by 3rd party Data destruction organizations upon contract termination. All electronic data will be erased based on industry-based data destruction standards.

Export of Data

Uila will not allow use or disclosure of customer data or hardware to third parties without first receiving approval from customer.

Infrastructure Resources for Application and Database

Uila logically segregates data for individual customers. Uila does not share any data with 3rd party without prior approval from the customer.

Secure Coding Practices

Uila implements and documents secure coding practices within the organization that are consistent with Industry Standards and are otherwise sufficient to protect the Software and Database from security risks as a result of development work.

Secure System & Network Configurations

Uila ensures that all systems that are used to provide the Services are configured and managed in accordance with a recognized and current standard for operating system, application server, database, client, and network security.

All Systems Access Privileges Cease When User Terminates

Uila ensures that access to the customer's information is promptly terminated at the time that any personnel ceases to provide services to the customer. Uila implements its own employee confidential agreements to support this requirement.

Vulnerability Management Practices

Uila has security controls in place to mitigate the risk from security vulnerabilities in a measurable time frame that balances risk and the business/operational requirements. This includes any and all patches needed to support platform operating system, desktop operating system, applications and the IT infrastructure (i.e. switches, firewalls, etc.). Uila keeps all infrastructure software and software necessary to the support the customer's instance updated to supported software versions.

For more details contact sales@uila.com