VIAVI Solutions

Application Note

StrataSync Security Overview

StrataSync™ is a cloud-hosted solution that provides asset and test results management for a wide range of VIAVI test instruments and systems. StrataSync improves technician efficiency and instrument usage, enabling automated job compliance and gives insights to performance issues with intelligent KPI aggregation and visualization.

Protecting the confidentiality, integrity and availability of customer information is paramount to maintaining trust and confidence in VIAVI. StrataSync uses a multi-layered approach to protect this key information and keep it highly available. This approach starts with a secure physical infrastructure for hosted data, strong network and application security, and redundancy within and across logical zones to ensure best-in-class service.

Secure Data-Center Infrastructure

StrataSync is supported by an industry-leading cloud infrastructure provider (AWS) with many years of experience in designing, constructing, and operating large-scale data centers worldwide. Physical access to the data centers is strictly controlled, monitored, and audited with:

- Professional security staff positioned at both the perimeter and at building ingress points
- Two-factor authentication required a minimum of two times to access data center floor space
- Logging and auditing of data-center access by authorized personnel
- Video surveillance throughout the facility and perimeter
- Physical intrusion detection systems

Power and environmental controls ensure a consistent and reliable environment that optimizes hardware performance with:

- Fully-redundant electrical power systems
- Uninterruptable power supply (UPS) units for back-up power in event of electrical failure
- Generators to provide longer-term back-up power in case of a catastrophic event
- Automatic fire detection and suppression equipment
- Climate and temperature control to maintain constant temperature for servers and other hardware

StrataSync

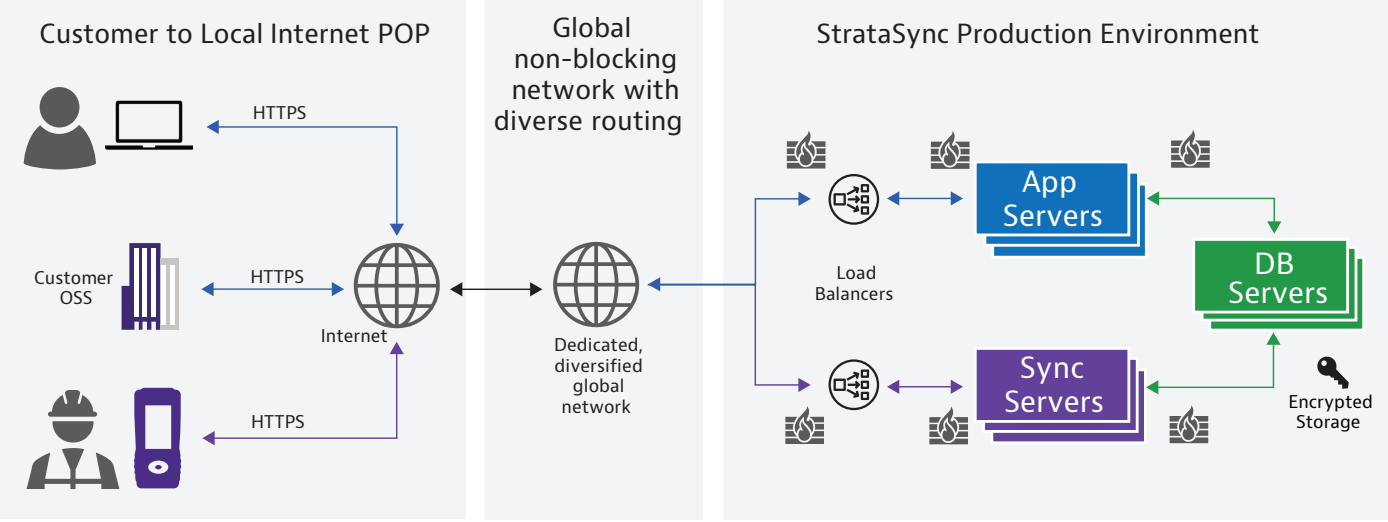
Security certification compliance includes:

- ISO 27001 certification of the information security management system (ISMS) covering infrastructure, data centers, and services
- SAS 70 Type II certified
- Federal Information Security Management Act (FISMA)
- Payment Card Industry Data Security Standard (PCI DSS)

Strong Network and Application Security

StrataSync is built from the ground up with security in mind: both network security and the logical security of the application architecture. For network security, StrataSync requires secure encrypted connections when data is in transit. This includes both the interface for the instrument syncing with the StrataSync sync server as well as the browser-based interface used by the supervisor or technician logging into the StrataSync application. Moreover, authentication methods at both the instrument and user login screen are required to gain access to StrataSync, ensuring that only the customer's instruments and the customer's users get access.

In addition to strong network security, StrataSync also employs the best practices associated with the logical security of the application architecture. The StrataSync application architecture uses a multi-tier model with firewalls between each tier to ensure that only traffic associated with specific ports and protocols are allowed to pass between the different tiers.



1689.900.1223

Figure 1. StrataSync security architecture

StrataSync network and application security features include:

- Secure encrypted connections between instruments and the StrataSync sync server as well as between the user and the StrataSync application
- All connections to StrataSync are via HTTPS using a minimum of TLS 1.2, ensuring a secure connection between the client (test instrument, customer user's browser or customer system) and their StrataSync environment
- Authentication methods are active at both instrument and user-login interfaces
- Strict user role-based access permissions and organizational visibility controls
- All passwords are stored in a database as salted, one-way hashes using best-practice implementations
- Session timeouts require re-authentication after periods of inactivity to ensure session security
- Single Sign-On (SSO) support via the OIDC protocol enables customers to use their own identity provider solution for consistent user authentication
- All customer data is logically separated by anonymized tenant IDs
- Perimeter firewalls allow only specific protocols and service ports and block all other unused protocols
- Application architecture uses a three-tier application security model (web, application, and database)
- Internal firewalls segregate traffic between web, application, and database tiers, allowing only specific ports and protocols to pass between tiers and blocking all other traffic
- Application firewalls on all servers ensure host-based security
- Security monitoring providing continuous threat and malware detection
- All database information is AES-256 encrypted at rest
- StrataSync is ISO27001-compliant

StrataSync's operational practices include:

- The VIAVI development, test and staging environments are hosted in separate VPCs from the StrataSync production systems, and hosted system administration interfaces are enabled with multi-factor authentication (MFA)
- Software composition analysis tool used for vulnerability detection when importing components during SW development
- Penetration testing tools used to evaluate vulnerabilities within operational staging and production environments for proactive remediation and fix verification
- All code and system configuration updates are peer-reviewed and tracked via configuration management

High-Availability Architecture

StrataSync is a cloud-based application and is architected to take full advantage of the availability and reliability associated with the cloud. It uses multiple techniques including server redundancy, server load balancing with auto-scaling, geographic diversity of server locations, and persistent-storage backups to ensure high-availability of the service.

High-availability architecture features include:

Redundant Servers — Redundancy at each of the tiers (e.g., web, application, and database tiers) ensures that a single server failure will not disrupt service. In case of a virtual server failure, StrataSync immediately fails over to the redundant server and spins up another server to be the new redundant server, ensuring that server failures have no impact on the StrataSync service. This contrasts with most non-cloud-based architectures that rely on a single server for each application and, as a result, experience significant down-time when the server associated with the application fails.

Server Load Balancing — Load balancing provides additional fail-over protection and enables spreading application traffic to ensure reliable performance of the service. In case of web-traffic spikes, auto-scaling provides additional servers that are added to the web load balancer to ensure reliable performance. Moreover, in case of a web-virtual-server failure, the server load balancer will divert traffic away from the failed server and move the traffic to the other web servers associated with the web-server load balancer.

Auto Scaling — The auto-scaling of web servers ensures consistent, reliable performance.

Logical and Geographic Diversity — StrataSync architecture spreads servers across multiple availability zones and maintains backups in geographically separate regions. This protects against service downtime due to power or network failures associated with a single location.

Persistent Storage Backups — This technique of maintaining independent copies of records ensures that customer data is always available.

Conclusion

StrataSync helps service providers increase operational efficiency by empowering their assets to tackle the major operational challenges of network testing in an efficient and effective manner. StrataSync provides automated asset management, configuration management, and test-data management of VIAVI instruments as well as asset tracking of non-VIAVI instruments. This gives service providers unprecedented levels of visibility into their assets and test data and delivers new levels of automation, control, and compliance auditability—increasing the operational efficiency of network testing and driving down associated operational costs.

StrataSync provides these valuable benefits while protecting the confidentiality, integrity, and availability of our customers' information. An architecture based on a multi-layered security approach protects key information and makes sure it is highly available. A secure physical infrastructure, strong network and application security, and redundancy within and across geographic regions ensures best-in-class service.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

stratasync-an-tfs-tm-ae
30173354 901 1123