Overview

Syncron ServiceCloud™ Security

syncron ServiceCloud™

Syncron ServiceCloud™
Security Overview

At Syncron, we guarantee the highest SaaS security standards possible, ensuring world-class security procedures for the sensitive data of our customers.

The security of our customers' data is vital to our business and your sensitive data is our priority. Through vetted application, physical, and information security systems, along with industry-leading business continuity, operational security and customer support, we make sure to guard your data with the best virtual and physical protection possible.

Syncron's security can be categorized into four areas:
Application, Physical, Information and Business Continuity

Application Security

Syncron's services employ application-only access and role-based access control (RBAC), so users of the application can only access the application features, not the underlying database or infrastructure components. Additional application security features include:

- Single tenant application, one customer per installation.
- Robust configurable password policies.
- Supported SSO through SAML v2.
- Audit trails for sensitive entities such as user, role, permission, etc. (configurable for other entities).
- All logins are recorded (both successful and un-successful).
- IP address restrictions (possible to whitelist IP addresses with application access).

Syncron ServiceCloud™
Responsible for security **IN** the Cloud

Amazon Web Services (AWS)
Responsible for security **OF** the Cloud

Physical Security

Syncron utilizes ISO 27001-certified Amazon Web Services (AWS), the world's leading Infrastructure as a Service (IaaS) provider, to deliver its cloud-based services quickly from region to region, ensuring the highest levels of physical security.

Amazon Web Services (AWS)

Syncron leverages AWS as part of its service delivery platform. AWS has an ISO 27001 certification and is SOC 2 Type II audited, and organizations like Nasdaq, NASA and Siemens trust these services.

Data Centers and Regions

- The Syncron services are delivered either from the EU (Ireland region), Asia (Tokyo region) or the U.S. (Northern Virginia region). Each region consists of multiple data centers.
- The data centers are state-of-the-art and employ the latest fire detection and suppression, power, cooling, monitoring and surveillance technologies.
- Data never leaves the region where the application is located.

Secure Hardware Decommissioning

- All hardware passes through a decommissioning process described in DoD 5220.22-M *(National Industrial Security Program Operating Manual)* or NIST 800-88 *(Guidelines for Media Sanitization)* to securely destroy data.

Information Security

Syncron encrypts data at every stage, and performs industry best-practice vulnerability testing on a regular basis to ensure your data is secure.

Data Encryption

- All data at rest is encrypted, using customer-specific encryption keys, via the AES-256 encryption algorithm. All data in transit to and from Syncron services are encrypted using either HTTPS, SFTP or IBM WebSphere MQ.
- Networks are segmented and secured by firewalls, network ACLs and proxy servers.

Regular Testing

- A third-party security firm performs annual penetration testing on Syncron-developed applications.
- Quarterly vulnerability scans performed on all internet-facing services.
- Compliance with EU Data Protection Directive.

ISO Certification

- Syncron is running an ISO 27001 compliance project and aims for compliance by year-end 2017. The next step after achieving compliance is certification.

Business Continuity, Operational Security and Customer Support

Syncron leads the industry in system uptime and reliability, with service levels higher than 99.5%, ensuring that business-critical applications are always there when you need them, and we've put the processes and people in place to maintain the utmost levels of both security and usability.

Data Backups

We ensure a minimum of two live copies of database-stored data, in separate data centers, with automated failover. Encrypted backups are stored in three data centers, providing over 99% durability.

Limited Access

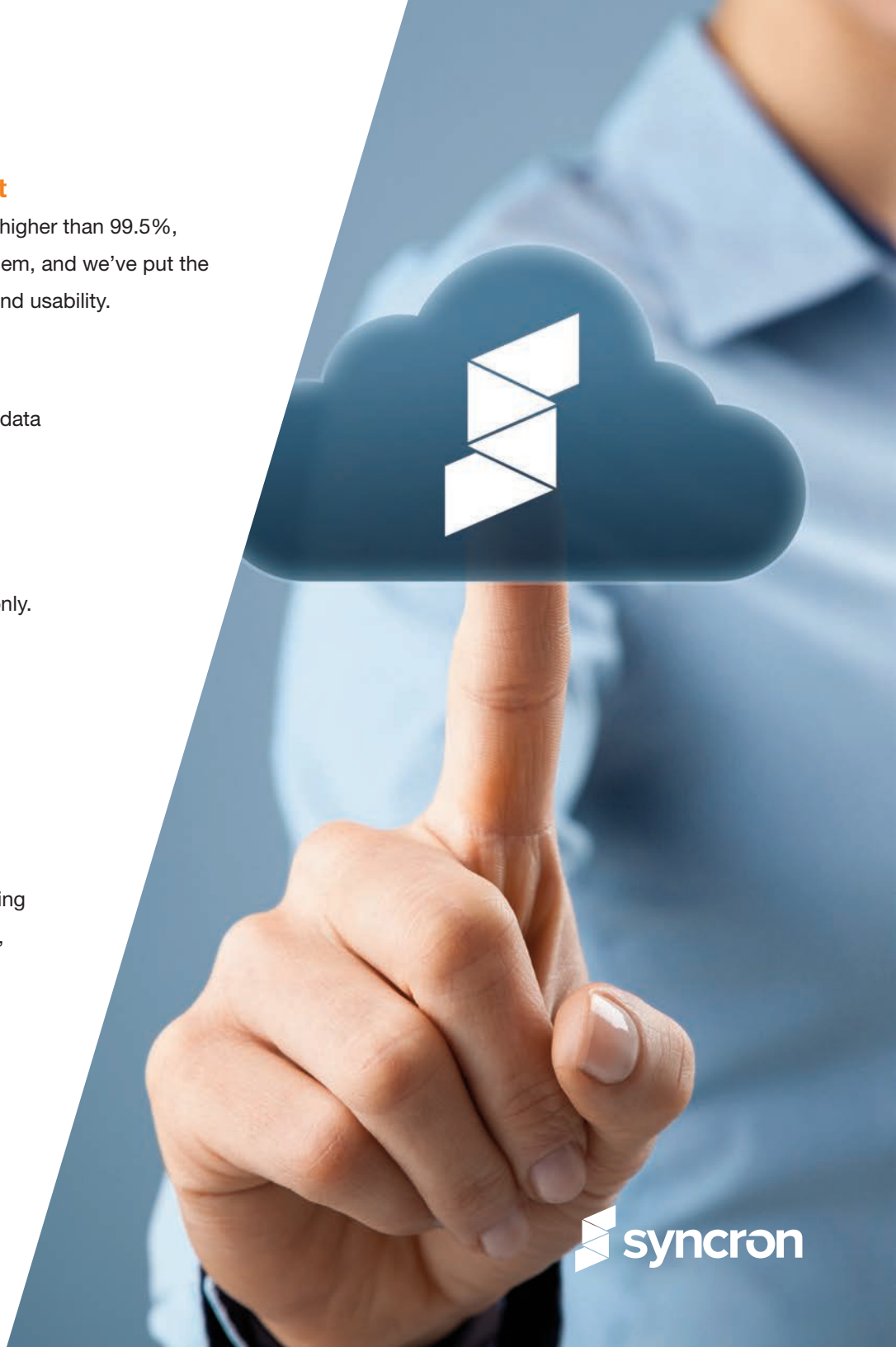
- Syncron's access to customer data is limited to the required personnel only. Access requires a two-level approval process.

Continuous Monitoring

- Monitoring covers networks, systems, applications and logs.

Support and Alerts

- The support desk is staffed 24/7/365.
- A central log server allows for central log monitoring and automatic alerting
- All alerts go through an automated workflow with multiple alert channels, priorities and escalations.



syncron

Empowering Exceptional After-sales Service.™

Syncron.com