SDL SaaS Security
## Table of Contents

Introduction ........................................................................................................... 2  
SDL Cloud Operations .......................................................................................... 3  
Cloud Service Providers ....................................................................................... 3  
Access Control ..................................................................................................... 4  
SDL's Hosting Locations around the World ......................................................... 4  
Availability and Proactive Monitoring ................................................................. 5  
Physical Protection ............................................................................................... 5  
Logical Protection ............................................................................................... 5  
Business Continuity and Disaster Recovery ....................................................... 6  
Data Security ....................................................................................................... 6  
Security and Compliance ..................................................................................... 7  
Risk Assessment .................................................................................................. 8  
SDL Security Tools Capabilities ......................................................................... 8
Introduction

The security of our clients’ information is paramount to our business and we prioritize keeping their information secure.

SDL pledges to protect your business and data with industry-standard security tools that meet the highest levels of compliance with regulations, such as GDPR, PCI DSS, ISO27001 and SOC 2, among others. With special attention to regulated markets like the Finance and Life Science sectors, our security is tailored to provide a reliable service, maintain high availability and ensure quick recovery in the event of a disruption.

This brochure details how SDL manages security in day-to-day operations, including system administration, business continuity management, security and operations, data centers and privacy.

SDL’s Software as a Service (SaaS) environment consists of multiple products and capabilities, catering its services to over 600+ global clients, including 85 Fortune 100 companies.
SDL Cloud Operations

SDL Cloud Operations is ISO27001 certified for all of our hosted products.

SDL has achieved 100% compliance with the controls and objectives of SOC 2 Type 2 attestation. The SOC 2 Type 2 report helps our clients understand how security and compliance is implemented at SDL.

SDL’s Language Product TMS has been independently audited and complies with the requirements of the Life Sciences focused HITRUST Common Security Framework.

SDL is further specializing and tailoring security for its cloud services by implementing ISO27017 in 2020.

SDL plans to achieve ISO20000 certification for service management across its operations by Q1 2020.

Cloud Service Providers

SDL has contracted with leading third-party service providers to host SDL products. Included below are details about each service provider.

1. Amazon Web Services (AWS)

SDL partners with Amazon Web Services (AWS) to provide hosted deployment of SDL products. AWS maintains multiple certifications for security, the most relevant of which are ISO27001, CSA STAR and SSAE16, SOC 1, SOC 2 and SOC 3.

2. NTT Communications

SDL partners with NTT Communications to provide hosted deployment of SDL language and content solutions. SDL uses NTT public and private cloud data centers located in the UK, US, Europe and APAC regions. NTT Communications is ISO27001 certified for its data center operations and maintains SSAE16, SOC 1, SOC 2 and SOC 3 reports.

[nttict.com/services/managed-services/compliance/]

3. Alibaba Cloud

SDL partners with Alibaba Cloud to provide hosted deployment of SDL products. Alibaba Cloud maintains multiple certifications for security, the most relevant of which are ISO27001, ISO27017, CSA STAR and SSAE16, SOC 1, SOC 2 and SOC 3.
Access Control

Multifactor authentication (MFA) is enabled for the management of all cloud service provider infrastructures. Only authorized personnel have access to the cloud service providers’ management consoles and tools. All actions in the management console and tools are logged and stored centrally. Monitoring and review of these logs occurs periodically based on standard operating procedures.

SDL has a comprehensive hybrid cloud security framework for access controls, accountability, authorization and governance for any action undertaken by our personnel. Comprehensive security log aggregation and industry-leading tools ensure compliance and help identify threats. SDL has access control policies in place that apply to all operational personnel.

SDL collects, aggregates, indexes and analyzes access control log data to detect intrusions, threats and behavioral anomalies. As cyber threats become increasingly sophisticated, real-time monitoring and security analysis is needed for rapid threat detection and remediation. Our security experts provide monitoring and response capabilities, security intelligence and perform data analysis on access audit logs. SDL offers user productivity with Single Sign-On (SSO) and identity governance.

SDL policy in regard to access control is to provide the least possible access and a need-to-know basis.
Availability and Proactive Monitoring

SDL Cloud Operation Centers use a variety of tools to monitor responsiveness and availability of SaaS-based services. Application images and infrastructure are continually scanned for vulnerabilities and patched to protect against new exploits and ensure the highest possible security. Fault tolerance storage and redundant external connectivity and systems are used for distributed denial of service (DDOS) protection.

Physical Protection

The applications and services offered by SDL are hosted inside physical data centers and protected against various threats. SDL also operates a private cloud ensuring physical security needs are addressed according to international standards and best practices, including automatic fire prevention and power failure protections with an uninterruptable power supply (UPS). Other areas of vital importance are cooling systems and theft-prevention physical security such as CCTV, intrusion detection systems (IDS), security guards, gates and fences.

Logical Protection

Logical security measures are also implemented. Through backups and exports to alternate data centers, fault-tolerant storage solutions protect client data against loss or corruption. Full and differential backups are also used to safeguard client data for up to four weeks. If customers require additional security, our solutions are fully redundant and guarantee a high degree of data integrity.

Virtualization is managed by the cloud service provider and ensures elasticity, rapid deployment of servers and rapid migration to other hardware or data centers. Networks are segmented so only web servers are exposed to the internet, decreasing the footprint for attacks and increasing detection possibilities.
Business Continuity and Disaster Recovery

Our multi-cloud strategy focuses on multiple service providers. This approach protects SDL and its customers from catastrophic failures due to natural disasters and major disruptions impacting individual service providers while satisfying the most complex regulatory compliance requirements.

SDL Cloud Operations provides services specifically tailored to guarantee high availability (HA) to our client’s services and data, including:

- Resilient devices for hardware, network failures and power loss
- Regular back-up and secure offsite storage
- Routine security patching and updates to protect against viruses or malicious attacks

HA is configurable using Active-Active and Active-Passive clustering methods.

Data Security

For most applications, client data is stored in databases. Depending on the SDL hosted product and specified needs, the database is single instance or multi-tenanted. All SDL personnel working on cloud operations must pass strict background and criminal records checks. Upon clearance the required access to the applicable cloud-hosted environments is provided. Any personnel that do not pass the background checks are terminated with immediate effect.

All of SDL’s external office network communication to and from the internet is checked by security appliances and screened for viruses. SDL personnel’s access to the hosted environments is only permitted from within SDL’s office networks.
Security and Compliance

Clients send their information to SDL SaaS applications, making security one of our top priorities. To maintain integrity and confidentiality, SDL ensures only authorized personnel have access to the information.

All SaaS applications are hosted in highly-secured third-party data centers. SDL’s data center and cloud providers must meet the highest standards of physical and logical security and industry-standard compliance. All suppliers have been evaluated against strict security standards as part of SDL’s vendor selection and management policy.

SDL’s security tools work with payment processing companies and financial institutions to meet Payment Card Industry Data Security Standard (PCI DSS) requirements. Security tool reports and dashboards fulfill this requirement, as well as other regulations (e.g. GPG13 or GDPR). Details on how SDL employees handle personal client information are published in security policies and procedures. These documents are classified as SDL internal classification level and only available to SDL representatives. The Privacy Policy for cloud services about collecting, processing or handling personal information can be found on SDL’s corporate website.

sdl.com/aboutus/privacypolicy.html

The SDL Cloud Security Operations team consists of multiple security engineers located in different geographical locations covering 24/7 security activities. The team uses multiple tools to monitor the state of the hybrid cloud environment from all security aspects.

SDL Cloud Security Operations team members must complete annual online security awareness refresher training. This training includes general awareness about employee responsibilities and information security.

New hires are made aware about information security policies and their obligations towards information security during induction training. New hires must complete code of conduct, information security awareness and data protection training on an in-house online training tool within 30 working days of their start date.
Risk Assessment

SDL has documented a comprehensive risk assessment plan consistent with the ISO 27001:2013.

SDL Cloud Operations Managers perform risk assessment for their respective processes with the assistance of the SDL Cloud Security Operations Team. These teams are responsible for regularly reviewing the risk management framework to assess, analyze and manage risks to the lowest acceptable level for the system environment and effectiveness of controls. Based on the assessment, the SDL Cloud Security Operations Team prepares a risk register with risk treatment plans for identified issues. Factors such as fraud and theft are also considered while performing risk assessment.

SDL Security Tools Capabilities

- SDL uses leading industry applications, infrastructure, log management and event management monitoring tools to perform anomaly detection on server access, application authorization and to prepare error report logs.
- SDL has implemented perimeter firewalls and integrated Network Threat Protection (NTP) with anti-virus to monitor network traffic and prevent intrusions. The NTP is automatically updated with signatures from the vendor as soon as they are released.
- The Cloud Operations Center team operates 24/7 to support real-time event management activities.
- SDL uses industry recommended tools for threat visibility and ensures compliance of our client’s cloud footprint by combining threat detection, predictive analytics, security configuration management and automated incident response.
- SDL has configured an industry-leading vulnerability and penetration security testing scanner to conduct periodic automated scans on its infrastructure.
- SDL security tools provide capabilities for security analytics, log data analysis, intrusion detection, vulnerability management, configuration assessment, security incident response, file integrity monitoring and cloud security monitoring services.
- An IT Infrastructure Library (ITIL) compliant ticketing tool is used for incident management (including security incident management), request fulfillment, service level management, problem management and change management.
- The security team is part of the Change Advisory Board (CAB) to review all changes from a security perspective.
In summary, SDL is able to provide the most extensive security operations suitable for highly regulated industries and the most demanding customers. Beyond this, SDL is able to provide security services as needed based on customer requirements.