opentext™

Protecting customer data with OpenText Information Security Services

opentext™

Contents

Executive summary

Maintaining the security of OpenText services to ensure customer data is secure is of the utmost importance to OpenText.

OpenText uses industry best practice models, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001:2013 Information Technology Security techniques. In addition, OpenText incorporates the ISO 27002 information security control set within the context of an information security management system (ISMS) based on ISO/IEC27001.

The OpenText information security program ensures delivery of these best practice security controls by aligning control delivery through people, processes and technology.

To ensure best practice industry standards are continuously observed and reported, leading cybersecurity compliance attestations are available (as applicable to a service) for ISO 27001, ISO 27017, 27018, SOC 1 Type II, SOC 2 Type II, SOC 3, SOC 2 + HITRUST, PCI DSS, HIPAA, SWIFT, TISAX, CyberEssentials+, and FedRAMP.

Security services

OpenText Information Security Services include controls aligned to Governance & Risk, Compliance Attestation, Security Operations, Disaster Recovery and Business Continuity Planning and Access Control.

Governance and Risk

Governance and Risk is responsible for the overall strategy of the Information Security program and managing the cyber risk program. This includes development and management of an extensive information security policy library, which is based on and fully aligned to the ISO27001 control framework.

These information security policies create a baseline of security control standards to ensure OpenText meets its compliance attestation requirements and customer contractual obligations. The policies are openly accessible and disseminated to all teams at OpenText for awareness and observance.

OpenText conducts annual security awareness training for all staff and contractors to ensure that they are informed on the latest cyber risk trends (phishing, malware, etc.) and data protection strategies (protection of customer data, protection of Personally Identifiable Information). All associates acknowledge awareness of the OpenText Information Security policies and how to access the policy library.

A security awareness communications campaign is conducted periodically throughout the year to promote additional information security best practice awareness and risk avoidance.

The OpenText Information Security Risk Management Methodology is part of the company's overall risk management strategy and supports OpenText's ISO 27001:2013 Information Security Management System (ISMS) and other compliance attestation requirements. It applies standard risk management practices, including alignment to information security policies, identifying in-scope data assets, risk assessing applicable security controls and the effectiveness of security controls (based on threats/vulnerabilities) and determining the results.

Risk assessment results are reviewed and risk treatment remediation plans are developed and executed as applicable.

opentext™

Compliance attestation

The compliance attestation service supports the delivery of OpenText security certifications and attestation audit reports. These include leading cybersecurity compliance attestations, as applicable and available for a service, for ISO 27001, ISO 27017, 27018, SOC 1 Type II, SOC 2 Type II, SOC 3, SOC 2 + HITRUST, PCI DSS, HIPAA, SWIFT, TISAX, CyberEssentials+, and FedRAMP.

OpenText attestation reports evaluate multiple levels of service controls (application, infrastructure and data center) and the available reports provide an overview of the service, scope of control testing and control testing results.

Operations

Defense in Depth approach to security

The OpenText information security strategy provides multiple and redundant defense measures to ensure a robust security posture. Defense in Depth is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information. This multi-layered approach increases the security of a system and addresses many attack vectors. OpenText security services are provisioned in multiple layers to protect customer data and infrastructure assets.

Perimeter security

OpenText has configured advanced perimeter protection as a Unified Threat Management (UTM) System with:

- Daily threat signature updates.
- Perimeter firewalls controlling incoming and outgoing traffic.
- Distributed Denial of Service (DDOS) protection for all assets.
- VPN encryption.
- An Intrusion Protection System (IPS) that drops malicious traffic.
- An Intrusion Detection System (IDS) for passive protection.
- Load balancer/VLAN filter deployment to control network access.

Network security

Network security management ensures the protection of information and supporting information processing facilities. OpenText has adopted a network security design with numerous nodes divided into complex functional zones to prevent the propagation of attacks between zones and to minimize their potential impact.

- Segregation of networks based on risk, with access between network domains and segments restricted via firewalls and/or intrusion detection and prevention systems.
- Corporate and commercial networks are segregated from public networks by firewalls that employ intrusion detection and prevention systems.
- Network and associated devices are configured based on the principle of least privilege and disabling unrequired functionalities. Hardening measures include “deny all” defaults that require explicit privileges to be configured for firewall ingress and egress.

- Proxy and DMZ layers provide additional security to the organization's services so that only authorized parties can access what is exposed on the network.
- All OpenText workstation access to networks is controlled via 802.1x security certificates
- Remote access into networks from publicly accessible networks requires the use of virtual private network (VPN) and multi-factor authentication.
- Network DDOS services are provided by telco providers for OpenText hosted datacenters.

All internal OpenText access to commercial services and data is via a Security Clean Room Gateway

- Application virtualization software for Data Loss Prevention (DLP)
- Security session tracking
- Key stroke logging
- Prevention of any customer data exfiltration – no cut, paste, copy or egress path for customer data

Endpoint protection

OpenText uses an advanced threat protection (ATP) service, which provides prevention and detection of viruses, malware and threat attacks across all endpoints (workstations, servers and other infrastructure assets).

The ATP monitors and responds to malicious activities or processes occurring on end user workstations or servers. It extends detection and response capability across multiple security layers to defend the entire technology stack with rapid identification and elimination of threats via fully automated response capabilities to stop attacks in progress.

The ATP also provides Extended Detection and Response (XDR) capabilities that bring visibility and context into threats and automated response for all endpoints. XDR uses advanced machine learning algorithms and behavior-based artificial intelligence (AI), cloud-based reputation feeds and custom threat hunting alerts to detect zero day/realtime threats as they develop.

Hardening

All infrastructure assets (servers, applications, operating systems, database and network) configurations are hardened according to vendor recommendations and Center for Information Security (CIS) benchmarks, along with some additional OpenText requirements. Hardening best practices adopted at OpenText include changing default passwords, automatic installation of service packs, encryption of resources, limiting privileges, denial of all traffic to certain ports and proactive threat and vulnerability scans.

Threat and Vulnerability Management (TVM)

OpenText follows NIST National Vulnerability Database (NVD) guidance and Common Vulnerability Scoring System (CVSS) to assess the severity of vulnerabilities and determine the handling priority based on the rating of vulnerability exploitation risks.

Vulnerabilities are patched on a monthly cadence as patches are released by manufacturers or vendors. Critical vulnerabilities are patched as soon as possible. Applications are patched via standard quarterly product release cycles unless criticality requires an urgent resolution.

Application security

OpenText employs a Product Security Assurance Program with a goal to incorporate security at the earliest possible phase of the product lifecycle. Requirements are derived from industry standard best practice guidelines such as the OWASP Development Guide and Security Cheat Sheet Series projects.

Threat modeling is performed during the initial design phase of any new application or feature. It is used to identify and understand where threats to the application are most likely to come from and prepare mitigation strategies to protect against them. The process is also used to identify test scenarios to test security requirements.

OpenText follows secure development principles throughout the entire product lifecycle. These include minimizing risk by reducing the attack surface area of an application, establishing secure default standards to ensure the application is secure by default, employing principles of least privilege access and applying defense-in-depth strategies to control risks.

Application testing standards include, but are not limited to:

- Static application security testing (SAST) – mandated to routinely incorporate SAST activities into development procedures.

- Dynamic application security testing (DAST) – mandated to routinely incorporate DAST activities (application layer vulnerability testing) into quality assurance and regression testing procedures.
- Direct application security vulnerability assessments and penetration tests.

Vulnerability scanning

OpenText vulnerability scanning is executed monthly using industry standard tools and is performed by authorized information security personnel or approved security vendors.

- Vulnerability scanning is conducted across the entire commercial environment. Scanning occurs within the internal network infrastructure and externally from the internet.
- Scans follow a cadence of reoccurring schedules, allowing for retesting of remediated vulnerabilities.
- Scan results are collected, analyzed, prioritized and assigned by system to owners for remediation.
- Tracking, reporting and metrics provide the current security posture in applications and network/infrastructure.
- Ad hoc scans may also be conducted due to publicly announced security vulnerabilities require immediate analysis.

Penetration testing

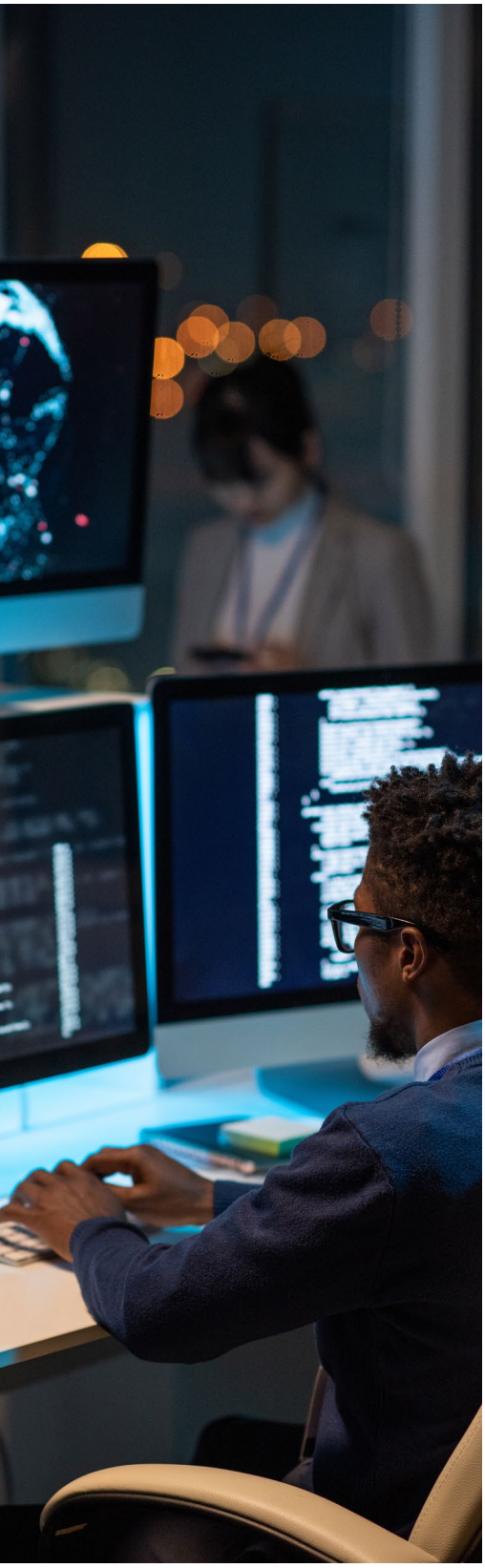
OpenText engages well-qualified independent third parties to perform penetration testing of its networks, systems, hosted solutions and web applications as needed (no less than annually).

- Application penetration testing is performed against externally (internet) facing applications.
- An annual penetration test is conducted across the entire OpenText global network infrastructure.
- Automated and manual penetration testing techniques are used to produce detailed and summary reports of vulnerabilities found.
- Penetration test results are collected, analyzed, prioritized and assigned by system to owners for remediation.
- Tracking, reporting and metrics inform the current security posture in applications and network infrastructure.

Security Information and Event Management (SIEM)

OpenText uses a security information and event management (SIEM) system, which collects, aggregates and analyzes activity from commercial environment assets across commercial infrastructure. The SIEM manages security log aggregation, assessment, event correlation, triage and event identification.

Identified events are reviewed in real time by the Cyber Response Center (CRC), a 24×7 team responsible for monitoring, detecting, assessing and responding to cybersecurity threats and incidents.



It is critical to ensure detection of threats, behaviors and activities that put information assets at risk are logged. At a minimum all logged events include the following information:

- Nature of the activity (e.g., connection attempt, login)
- Status or result of the activity (e.g., success, failure, error messages or IDs)
- Time of the activity based on a consistent and reliable time source (e.g., NTP)
- Source of the activity (e.g., IP, account, host)
- Destination or target of the activity (e.g., IP, account, host)
- Log collection and correlation engine

All logs are stored on a secured server for 12 months.

Threat intelligence and threat hunting

Proactive analysis and research of emerging or existing threat actors and threats from several sources enables OpenText to deploy preventative measures in advance before threats can impact business.

OpenText security researchers examine security threats that "exist in the wild." A combination of industry alerts and intelligence reports are used to identify threats that require investigation. The research includes information about threats, indicators and analysis of internal data to prioritize responses to the threats.

Security Honeypots are also in place to assist security researchers in identifying potential attacker behavior patterns.

Active threat hunting is conducted to proactively examine OpenText services for any indication of compromise (IOCs) from identified threats,

Security incident response process

This service monitors, detects and responds to security incidents or breaches. The NIST Computer Security Incident Handling Guide—preparation, detection and analysis, containment eradication and recovery and post incident activity is the model used for this process. The process uses playbooks for scenario-based response and for any required collaboration with internal staff and law enforcement authorities, should the need arise.

This process ensures that the right steps are taken and information is documented in the event of a security incident. OpenText will notify the Customer without undue delay of any security incident that impacts the Customer's data. If the Customer suspects a vulnerability or incident, it can submit its concerns to OpenText via the incident reporting process, or as a technical support request.

All pertinent information related to the event is stored in a digital forensics platform to ensure nonrepudiation of the information.

A forensics report will be provided to the Customer detailing root cause forensics analysis. During a security incident post-mortem period, customers will be provided with updates as soon as new information is available or OpenText will respond reasonably to information requested about the security incident by the Customer.

This process is tested by a third-party security firm via an annual tabletop exercise.

Data security

All data in OpenText commercial environments is classified as “secret” under ISO27001 and protected with the following control principles:

- Encryption of data-in-transit and data-at-rest, based on agreed contract terms.
- Access control/user authentication via multi factor authentication.
- Shielded (secured) replication of date to remote site for Disaster Recovery synchronization.
- To protect data in transit and provide secure communication in transit, OpenText offers TLs 1.2, VPN, SFTP, SSH, FTPS, HTTPS, AS2 or AS3, as agreed in the customer cloud contract, which enables authentication through certificates, session encryption and/or file level encryption.
- End user sessions for internet browsers to portal applications are encrypted with HTTPS.
- OpenText issued workstations have hard drive encryption by default.
- Any authorized destruction of data follows follow NIST 800-88 or Department of Defense 5220.22-M standard protocols.
- All mobile devices are managed via Mobile Device Management software.
- Wireless access to commercial environments is not permitted.

Disaster recovery and business continuity planning

OpenText deploys high availability configuration options across its environments.

The disaster recovery testing service confirms that recovery plans are documented and effectively tested to ensure continued availability and that services can be restored with minimal disruptions. Service recovery plans are designed to accommodate traditional industry standard metrics of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as defined below:

- **Recovery Time Objective (RTO)** – The elapsed time between declaration of a service-impacting event and the time production services are restored.
- **Recovery Point Objective (RPO)** – The maximum amount of data, in minutes, that might be lost if a catastrophic event occurs.

Disaster recovery testing service and designed RTO and RPO times are specific to each commercial service and subject to contractual requirements and definition.

The OpenText business continuity program follows the ISO 22301:2012 International Standard. Its key goal is to ensure prioritized business function recovery, reduce impacts (financial, operational, reputational/customer, legal and regulatory) and deliver organizational resiliency.

Maintaining business operations is vital to delivery of services. Comprehensive risk assessment (RA) and business impact analysis (BIA) are used to determine the needs of each facility and business function. These steps assist in determining criticality and recovery timeframe requirements. Continuity plans are subject to annual quality assessments, checks, reviews, approvals, tests and audits.

Playbooks, policies, procedures and plans address various scenarios including Pandemic Plan, Emergency Management Plan, Crisis Management Policies, Call Trees and Recovery and Communication processes.

opentext™

Access control

All access to information and systems by OpenText personnel is enforced through a least privileged access policy and a full, role-based lifecycle for identity access management processes, as well as a regular cadenced review and validation of all access privileges. Workforce members are only granted rights to access those assets needed to fulfill job functions.

All access is via multi factor authentication: a User ID assigned to a named individual, a password and/or a security token.

Physical access control

Data center facilities are designed to physically protect equipment and other critical resources from unauthorized access and environmental hazards.

- Access to all information processing facilities is physically restricted.
- Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
- Limited access is maintained for all areas except public entry lobbies, washrooms, lounges, food areas and all areas outside of the outermost security perimeter.
- Personnel must use company issued badges to enter secured areas in buildings or facilities.
- All visitors must show government issued photo identification and sign in prior to gaining access to restricted areas. Visitors to company sites are always escorted by authorized personnel.

Logical access control

Employee access rights are granted following the least privilege access principle, on a need-to-know basis and with a legitimate business need.

All access requests are validated by information security personnel and approved by management.

Authentication credentials must not be shared or disclosed to any third party. It is a breach of policy for any user to use another user's authentication credentials or misuse their own.

Access to production environments by OpenText support personnel is controlled via secure logical access gates and requires multi-factor authentication. Recording of support activities on production systems is done through keystroke logging by deploying software on the access gates.

Information security personnel and functional managers regularly validate access privileges to control moves, adds or changes to privileges and accounts.

opentext™

Security validations

This service is responsible for the management, validation, provisioning and deprovisioning of all access credentials

- The provisioning, revoking and review of access to the OpenText network and privileged accounts are performed in support of compliance activities.
- All access that is granted is role based and aligned to least privilege access principles.
- All access for all employees is reviewed on a quarterly basis.
- Security also performs quarterly firewall rule reviews, which includes ensuring rules are provisioned correctly and correcting any anomalies. All unused or duplicate firewall rules are removed.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn