opentext™

Data sheet

OpenText™ Axcelerate™ Security in the Amazon Web Services (AWS) cloud

Maximum security, availability and peace of mind for sensitive eDiscovery, regulatory compliance and investigation projects

OpenText Information Security Program

OpenText Infrastructure Security

Axcelerate Application Security and Scalability

AWS cloud Security

List of associated OpenText products the component works with

- **Axcelerate OnDemand**
- **Axcelerate Private Cloud**

As timelines continue to compress and cyberattacks continue to rise, it is more important than ever that legal teams can reliably and securely access critical data whenever, wherever they need to. OpenText Axcelerate, deployed in the Amazon Web Services (AWS) cloud, provides reliability, security protocols and processes designed to reduce risk, ensure maximum security and availability, and give legal teams peace of mind knowing that their sensitive legal data is secure and accessible, 24/7.

Axcelerate OnDemand and Private Cloud deployments reduce risk by centralizing Axcelerate hosting and providing access for all counsel and service providers leveraging AWS's state-of-the-art facilities. With regional isolation and multiple availability zones, AWS minimizes downtime and ensures that data is accessible 24/7, 365 days a year.

OpenText Information Security Program

At OpenText security is in our DNA, starting with the OpenText Security Awareness Program which employs generally accepted security practices as outlined in guidelines such as the FFIEC Handbook for Financial Institutions and the ISO 27001:2013 standard (which is validated by an independent third party). OpenText Security Awareness fosters a culture of sensitivity and security in all offices and all personnel are subject to stringent background checks (i.e., criminal records, credit references, drug testing, education and professional references, etc.) in accordance with local laws. OpenText personnel undergo mandatory security awareness training during on-boarding and annually thereafter. As for access to data, OpenText applies the principles of least privilege (POLP) to restrict access to client data to only those personnel who require it as part of their role. User access reviews are conducted quarterly to verify access needs and to validate the accuracy of user permissions.

OpenText Infrastructure Security

To ensure that customer data is protected from external threats, OpenText employs multi-layered defense at the infrastructure, application, network and physical security layers. Annual vulnerability testing is conducted to test key administrative and technical controls. Axcelerate security infrastructure employs the following security protocols and certifications:

- Axcelerate/AWS ISO 27001 certified to be compliant (information security standard).
- Axcelerate/AWS VPC isolation - no cross-communication/peering between virtual private networks (VPCs). See AWS section below.
- Axcelerate/AWS: SentinelOne anti-virus/anti-malware based on behavior-based static AI engine to proactively identify and isolate/quarantine threats on machines that handle client data. This prevents replication of malware across environments and prevents any viruses or malware from getting on local machines or networks. Unlike other virus detection software, SentinelOne doesn't require virus signature updates to effectively protect information assets.

OpenText regularly achieves third-party validation for thousands of global compliance requirements that AWS monitors to meet security and compliance standards across various industries.

opentext™

Axcelerate Application Security and Scalability

For two decades, the Axcelerate platform has been trusted by major government agencies, a majority of Fortune 100 companies, the world's largest tech companies, and 15 out of 20 of the world's largest law firms to handle the most sensitive legal data.

Axcelerate's robust infrastructure, application security and scalability ensure that teams have secure, reliable access to critical data and even assists teams with protection of sensitive data. Axcelerate employs instance level virtual firewall and data encryption in-motion and at-rest. Redundant internal safeguards are hard-coded into the application that restrict server-to-server communications. Where data is transferred within the perimeter, it is encrypted and unreadable to anyone on the network without the appropriate key. Clients have the option to retain their own data encryption key.

Where Axcelerate features in-platform integration with third party software, additional security measures are employed. For example, Veritone aiWARE for text-to-text translation extracts only the text from selected documents that is securely transferred to Veritone's translation engine and back; native files stay within the Axcelerate environment.

To ensure rapid scalability within the AWS ecosystem to match project demands Axcelerate employs elastic-aware architecture that dynamically provisions resources as needed without waiting for manual changeovers or approvals.

Axcelerate's security features also extend to functionality that assists legal teams to identify and protect sensitive client data. Technology-assisted review (predictive coding) based on continuous machine learning ensures higher accuracy and reduces risks of inadvertently exposing privileged or sensitive data. Additionally, Axcelerate features automated data detection, in-place and bulk redaction (PII, PCI, PHI, etc.), self-triggered quality assurance (QA) checks, and automated identification and redaction of names via Magellan text analytics.

AWS cloud Security

AWS provides the world's most comprehensive and broadly adopted cloud platform. The AWS cloud infrastructure is trusted by government agencies like NASA and financial regulators like FINRA. The pairing of Axcelerate and AWS provides a secure and scalable environment for eDiscovery and investigation, regardless of the size of the data set, the number of users, the geographic locations of the users and the sensitivity of the data. Specific AWS features include:

- Security certifications - AWS Assurance Programs are well-accredited with dozens of certifications, frameworks and international legal compliance programs, including SSAE, SOC and ISO. In fact, AWS supports more security standards and compliance certifications than any other offering. These include PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.
- Data encryption - All data in the AWS cloud is encrypted at rest. To protect local storage and NAS data, OpenText encrypts all data on AWS EBS volumes using an OpenText managed key, which is created and managed using the AWS KMS service. Additionally OpenText can optionally encrypt internal network communication between servers and devices in the VPC. Any network communication outside of the VPC is always encrypted.
- Regional isolation - Each AWS region is designed to be completely isolated from other Amazon EC2 regions to achieve the greatest possible fault tolerance and stability. AWS employs multiple availability zones within each region, each designed as an independent failure zone (all redundantly connected to multiple Tier-1 transit providers).

Axcelerate in the AWS cloud provides maximum security and availability to ensure that you can deliver on your most pressing and sensitive projects.