

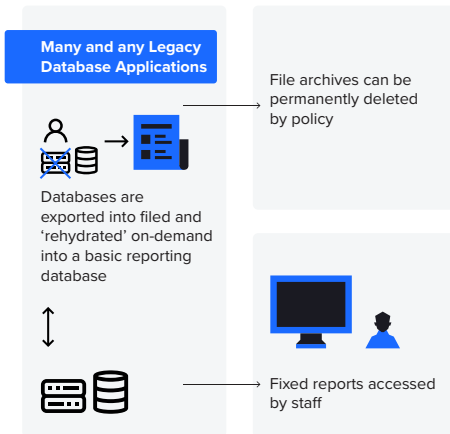
Voltage Data Privacy and Protection Professional Services Quick-Start Offerings

This flyer outlines the OpenText Cybersecurity Professional Services quick-start offerings available to help Customers and Partners get started on solutions for the Voltage Data Privacy and Protection pillar.

Application Retirement

Overview and Solution

Application Retirement solves the Customer's need to save money by "retiring" or "archiving" expensive legacy applications, but keeps the data available for infrequent ad-hoc reporting. This solution sets up an archive of the information such that the systems can be archived, but remain available for common reporting needs (for example, for audits or ad-hoc questions). This solution is repeatable, so many legacy applications can be closed and placed into the archive. This increases the return on investment and becomes a valuable resource for many departments.



Services Offering

10-days kick-start support:

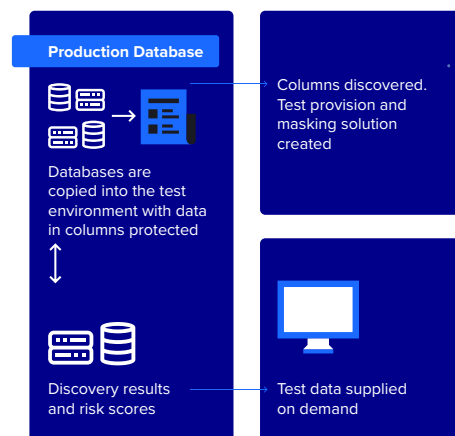
- Delivery of a half-day workshop to decide what is needed for setup.
- Installation and documentation of the solution into a development environment.

- Connection to a JDBC-compliant legacy application.
- Extraction of the complete data schema into the archive.
- Delivery of a half-day workshop showcasing how to set up ad-hoc reporting.
- Any remaining time will be used to mentor the Customer or Partner on key aspects they would like to become familiar with.

Test Data Management

Overview and Solution

Test Data Management (TDM) is the process of checking and testing a "production-ready" copy of the software before it is released into production. However, this practice is now considered high risk because these copies can contain sensitive information and are being placed into a less secure location where access rights are higher than usual to support testing activity. If the



information is compromised, the organization is at risk of fines and loss of reputation. The solution, therefore, is to create a TDM library of protected production data sets that are refreshed consistently and automatically.

Services Offering

10-days kick-start support:

- Delivery of a half-day workshop to decide what is needed for setup.
- Installation and documentation of the solution into a development environment.
- Connection to a JDBC-compliant legacy application.
- Carry out discovery on the database for up to 50 tables, using the out-of-the-box grammars.
- Set up a test data flow from Production to Test, showing how sensitive data can be anonymized following the results from discovery.
- Delivery of a half-day workshop showcasing how to expand on this solution.
- Any remaining time will be used to mentor the Customer or Partner on any key aspects they would like to become familiar with.

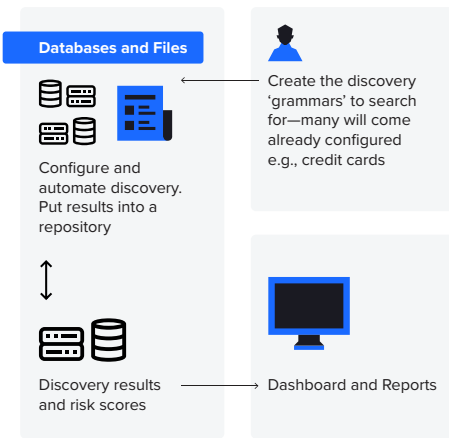
Sensitive Data Discovery

Overview and Solution

Sensitive data discovery is a common need that answers the requirement to understand where the high-risk information resides in a company. The personas involved include the Chief Information Security Officer (CISO), the Chief Data Officer (CDO), and the Governance, GDPR, Testing, and Applications

Support teams. In the past, data security was a low priority and data became siloed and stockpiled. However, recent legislation regarding how data should be kept and protected has made it an essential area of focus, with companies putting in place measures to avoid fines and damage to their reputation.

The OpenText solution provides functionality that automatically discovers and categorizes data. Discovery can be in files and databases; the solution can simply connect to a repository and look for a predefined set of definitions of what is considered sensitive. The results are provided in a dashboard, which can then be used to classify and act, such as deletion, quarantining, or encryption.



Services Offering

10-days kick-start support:

- Delivery of a half-day workshop to decide what is needed to be for setup.
- Installation and documentation of the solution into a development environment.
- Connection to a JDBC-compliant legacy application.
- Carry out discovery on the database for up to 500 tables, using the out-of-the-box grammars.

- Delivery of a half-day workshop showcasing how to expand on this solution.
- Any remaining time will be used to mentor the Customer or Partner on any key aspects they would like to become familiar with.

Data Encryption

Overview and Solution

In order to protect sensitive data that a company holds, data encryption is essential. However, most companies have so many IT systems that they haven't reached this position of safety, leaving much of their data unprotected. Data repositories include databases, applications, and file stores (such as email, SharePoint, and filesystems). The type of encryption is also important. For example, if you encrypt an email addresses within an application, the address must remain looking like one; otherwise the IT systems might break. The final need is to encrypt consistently across many systems; otherwise, related applications might also fail if they use different encryption values.

The solution is to provide a consistent, format-preserving, global-strength enterprise encryption engine—one that can interface with many systems and be incorporated into many products and areas of the company. This is what OpenText provides and our OpenText™ Professional Services group is here to help Customers or Partners get started.

Services Offering

5-days kick-start support:

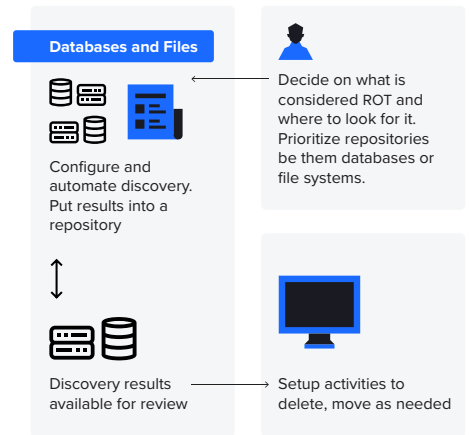
- Delivery of a half-day workshop to decide what is needed to for setup.
- Installation and documentation of the solution into a development environment.
- Delivery of online virtual workshops with the Customer for a tour of the product features, aligned to how they want to use it moving forward.

- Delivery of an online workshop showing how encryption can be customized and interfaced with.
- Delivery of a report comprising the options discussed and decisions made during the workshops.
- Any remaining time will be used to mentor the Customer or Partner on any key aspects they would like to become familiar with.

Save Money: Removing Duplicate or Outdated Data

Overview and Solution

Removing duplicate or outdated data can save a company a lot of money. This is known as Redundant, Obsolete, and Trivial (ROT) Management. Purging a legacy of ROT and regularly removing it saves on storage costs. It can also be carried out before initiatives such as a cloud move, sensitive data discovery, and encryption programs. The solution is to analyze the data repository and, from the results, act on it through deletion or archival. OpenText provides a solution that can do this on file repositories such as email, SharePoint, and file systems; it also works on databases. This scenario is easy to establish, as most ROT parameters are pre-loaded, such as duplication detection or age discovery.



Services Offering

5-days kick-start support focusing on file repositories or database systems:

FILES

- Delivery of an online workshop tour of the SaaS FAS product, focusing on the ROT functionality.
- Delivery of a report of options and decisions made during the workshop.
- Connection to a filesystem of up to 500 GB to carry out ROT analysis.
- Review of the results and advice on next steps (delete, encrypt, move).
- Any remaining time will be used to mentor the Customer on how to adopt solution configuration and how the usage can be expanded.

DATABASES

- Same as the list above for files, but also includes an installation of the database tooling.
- Ensure that the Customer understands the functionality of the tool.
- A small database will be installed (or provided by the Customer) to experiment with approaches for ROT management, for example, modeling and deletion of outdated data.

Service Implementation

Work will be carried out remotely. If this isn't possible, travel expenses will be billed to the Customer. All hardware required will be based on minimal requirements and are expected to be provided by the Customer.

Service Planning and Deployment

The OpenText Security Services Specialist will schedule the delivery of this service at a time mutually agreed and shall be during local standard business hours, excluding holidays (or unless otherwise agreed by OpenText). Any services provided outside of standard business hours will be subject to additional charges.

OpenText will provide resources with the following skill set(s) to work at the direction of Customer:

- Ability to perform installation, configuration, and troubleshooting of the OpenTextSecurity software.
- Ability to perform evaluation of the current security configuration and implementation of OpenText Security products.
- Ability to provide overall expertise and planning knowledge in the deployment of OpenText Security products.

Service Eligibility

The Customer must provide timely access to key stakeholders for facilitating the work required. Typical stakeholders will include the Executive Sponsor, Project Manager, Security Operations Manager(s), Security Operations Analyst(s), Incident Responder(s), Chief Security Officer, Audit & Compliance Officer(s).

Learn more at

www.microfocus.com/en-us/cyberres/data-privacy-protection

SKU PS-AA715—Data Security (5-day)

Connect with Us
www.opentext.com

