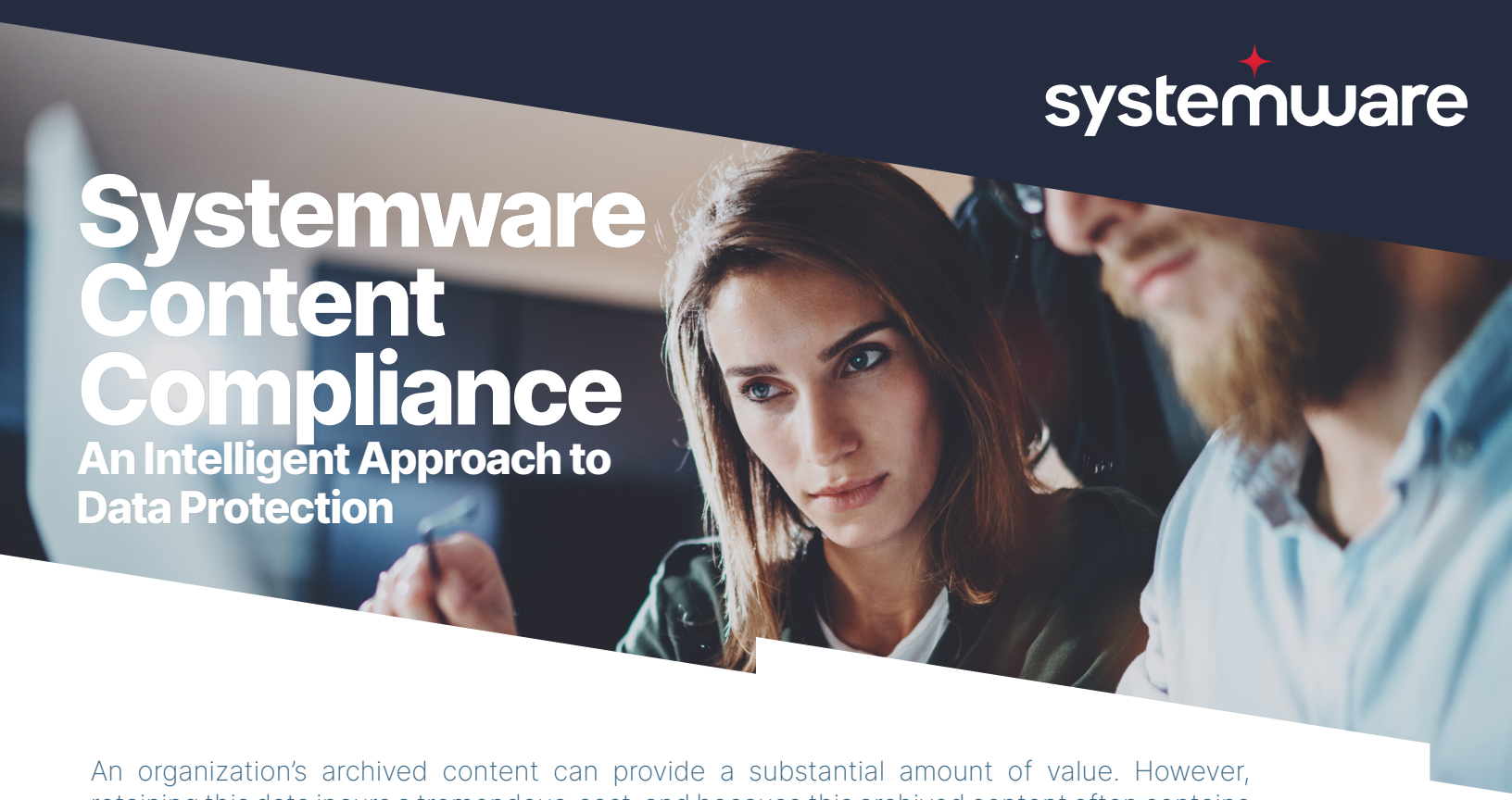
systemware

Systemware Content Compliance

An Intelligent Approach to Data Protection



An organization's archived content can provide a substantial amount of value. However, retaining this data incurs a tremendous cost, and because this archived content often contains personal customer information, it also introduces potential risks. That is why organizations must have a defined purpose for keeping any data, especially personal customer data.

Building a Structured Approach to Data Protection

Organizations must have a structured approach to adequately protecting customer data, even though relying on instinct when developing data protection and retention policies may be tempting. Beginning with an organized approach will provide a scalable solution that can be replicated across the entire organization. Content Compliance in Systemware Content Cloud offers simple, automated tools to make the process even easier.

Here are some questions to ask when building a data protection plan:

1. **Do you have a legal right to process the data?** Just because you can access the data does not mean you have a right to retain and use that information. Some personal data must be deleted immediately, while other information can be retained if the data is suitably protected.
2. **Do you have a regulatory obligation to retain** the data? If you have a regulatory requirement to keep the data, you should retain it only for as long as required and do so securely. Once the regulatory requirement is up, it is best to delete sensitive portions of the data promptly to prevent fines and other undue costs.
3. **Is there value within the data that can suitably be realized?** If not, simple archiving with basic indexing is enough. If so, more focused indexing can help you locate relevant data faster across multiple repositories.
4. **Do individuals accessing the content need to see the personal information?** If there is no regulatory requirement to keep data that is otherwise useful, organizations should ensure they are maintaining customer privacy. This security should be of primary importance. Even if you need to retain personal information for compliance, organizations should find a way to isolate personal information from other data.
5. **Is there a suitable method for reducing potential risk?** If you are not planning to remove the data for regulatory requirements or compliance reasons, perhaps look at other options to prevent the loss of personal information, such as data encryption, group or user-based access policies, data masking, or low-availability storage.

Handling Subject Rights Requests (SRRs)

Under laws like GDPR and CCPA, customers have the right to access their information (“right of access”) or be forgotten (“right of erasure”), amongst others. To fulfill these requests, organizations must be able to quickly locate relevant personal information and either package it up for delivery (for a right of access request) or delete it from the system (for a right of erasure request).

To handle these Subject Rights Requests (SRRs), you need to be able to perform a few vital functions:

IDENTIFY
Quickly locate, extract, and deliver relevant data across repositories and million-page reports

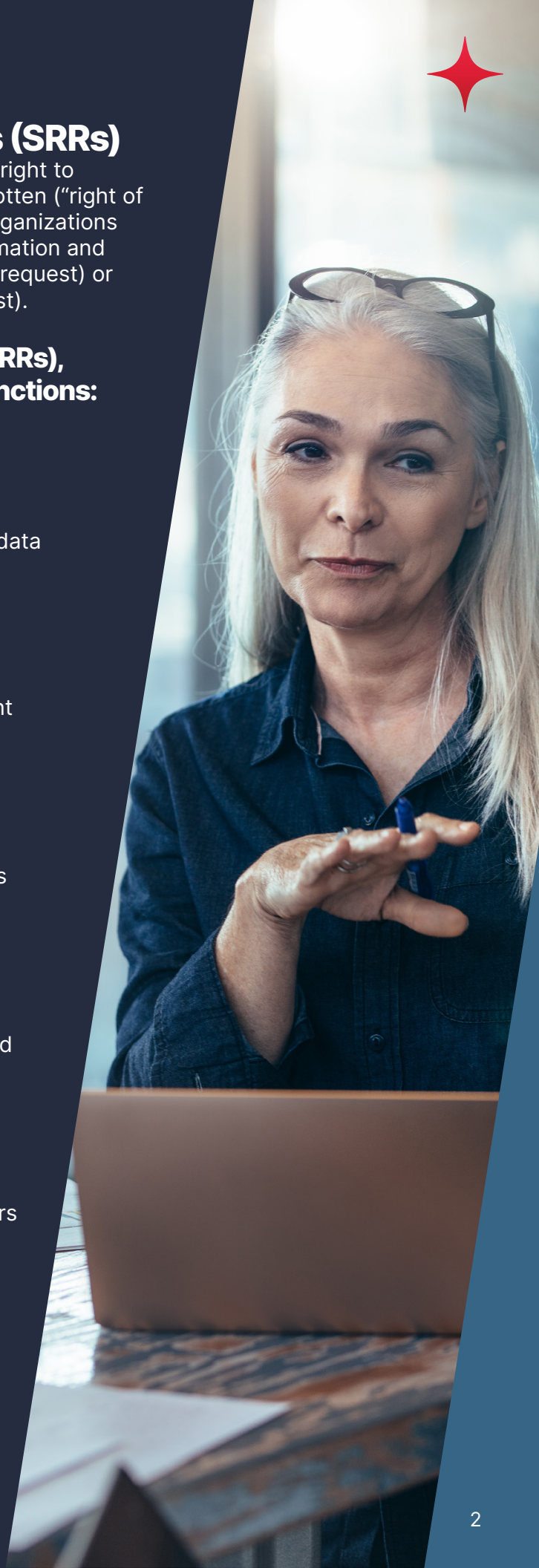
RETRIEVE & EXTRACT
Address the applicable portion of the content without compromising other data

OVERSIGHT
Track who has accessed or edited all reports and other documents within the system

SECURE
Protect data from bad actors both at rest and in transit

MASK
Provide sensitive data to only privileged users without storing content twice

SIMPLIFY
Make routine tasks easier while preventing unprivileged users from viewing sensitive data



Managing Personal Data with Systemware Content Compliance

Systemware offers several capabilities to simplify content compliance and data protection management:

Identify Content with Intelligent Indexing

- Intelligently storing metadata about the document allows you to quickly identify data related to a specific account, day, location, etc.
- Indexing at the document, page, or line level, provides multiple ways to find and extract the specific content in question
- Package content together and deliver a single file quickly for an audit or customer request

Retrieve and Extract Content with Segmentation

- Content is virtually segmented using the indexed metadata allowing for quick content extraction down to the line-level while leaving the original data intact
- Quickly retrieve, package, and deliver portions of the overall document dynamically in a way that is seamless to the user
- Delete segments (in the case of a right of erasure request) of a report without affecting the surrounding content

Oversight

- Robust and configurable tracking of report access, edits, and more
- Track access using the same detailed search, line-level retrieval, and packaging as other content within the system

Secure Your Content with Data Encryption and Access Permissions

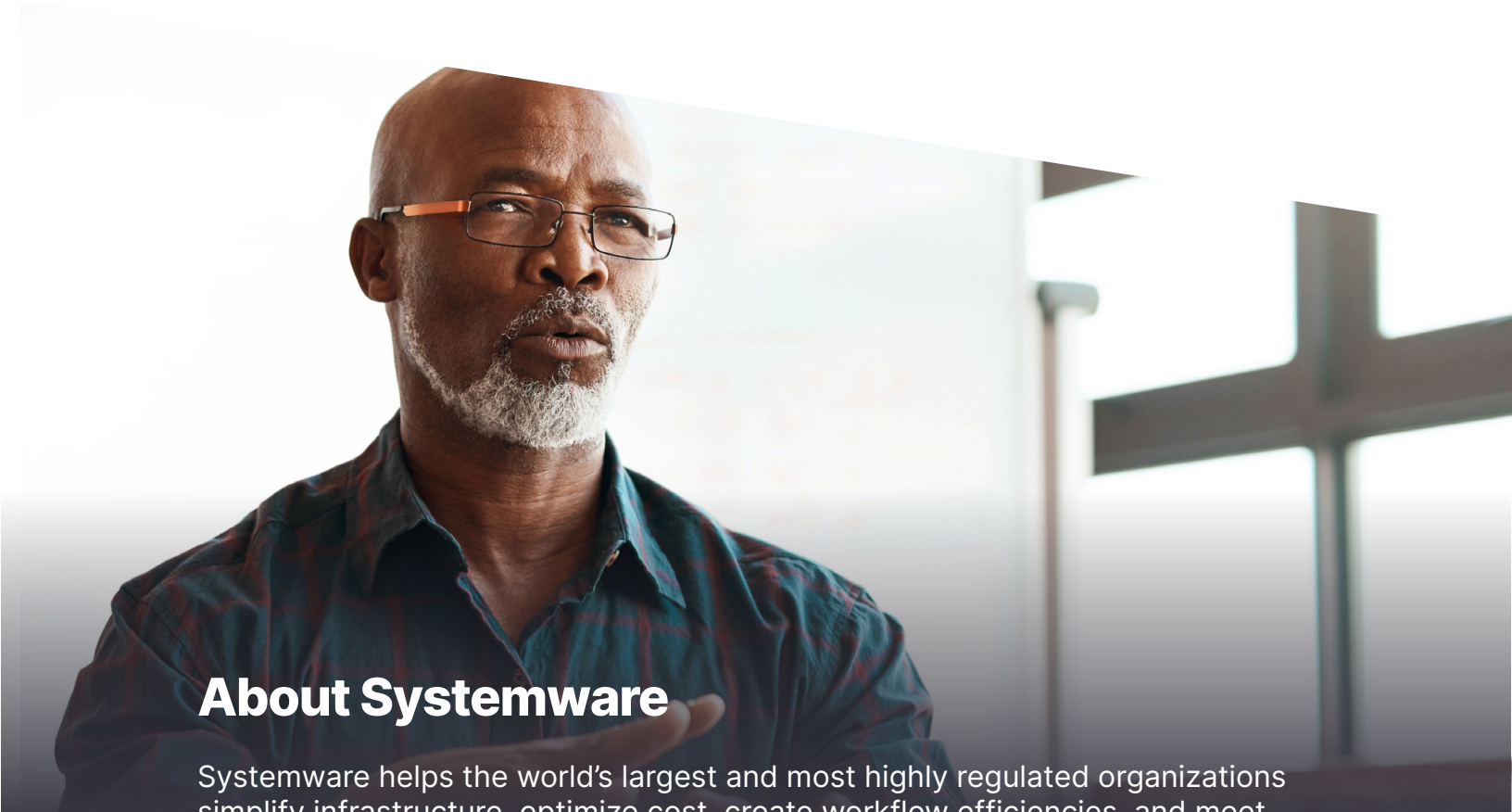
- Encrypt customer data both in transit and when stored
- Employ user, group, and role-based permissions to control and track access
- Ensure anyone other than permitted users cannot access the content

Mask Personal Information with Static and Dynamic Data Masking

- Dynamic data masking can permanently mask sensitive data upon access based on a user's security permissions
- Multiple levels of masking for different users and access requirements
- Whole screen masking is available based on user activity, preventing sensitive data leaks due to unattended workstations
- For content not covered by retention requirements but still valuable for use in analytics, organizations can re-capture masked data and delete the source data, providing anonymization through static data masking

Simplify with Workflows and Automation

- Using an "anonymization by design" approach, workflows pass data directly to algorithms that process the information automatically and then delete raw source data from the processing server. This approach prevents the exposure of sensitive data to those that do not need to access it
- Audit and SRR requests can be automated and easily replicated for quick responses to customer or regulatory requests



About Systemware

Systemware helps the world's largest and most highly regulated organizations simplify infrastructure, optimize cost, create workflow efficiencies, and meet information governance requirements. Our intelligent content services platform, Content Cloud, enables users to find and extract information wherever it is stored and transform and deliver it in the exact context needed for each business line. Content Cloud delivers optimized performance in public, private, hybrid, and IBM Z environments, as well as a fully hosted SaaS offering.