fuse analytics

about fuse

Due to expanding compliance regulations, it is increasingly challenging for companies to retire legacy applications with sensitive data.

Fuse is designed to secure sensitive data in the cloud allowing organizations to save up to 90% of legacy systems cost, maintain enterprise access features and decrease privacy risk exposure while managing complex retention policies both across the organization and the globe.

qualification questions

- **Are you changing systems and applications currently or do you have plans this year to make changes to your enterprise landscape?**
- Do you have existing, aging systems that may have outdated security protocols that need retirement?
- Do you have ongoing legal or compliance concerns related to Labor data and systems? (EEO, Wage hour, FLSA, FMLA etc). Or do you have any other litigation matters complicating retention?
- Is the organization facing remediation needs for breaches or data privacy incidents?
- Are there mergers or acquisitions where systems consolidation and overhead reduction may be requirements?

differentiators

- Cross-application enterprise integration experience and migration knowledge and resources.
- Network of system implementers with transactional system experience and knowledge (SAP, Oracle, PeopleSoft, Workday, ADP, Microsoft, Accumatica, etc)
- Highly scalable, 100% cloud based platform and tools for acquiring and storing massive amounts of enterprise data and documents with features covering data privacy, data sovereignty and security controls to allow customers to manage organizational data history responsibly “up and out”.
- Expert input on building and managing Privacy and Data Sovereignty architectures and applications.

business cases

- Licenses / Maintenance eliminated
- People skills and knowledge can be reallocated (business user + IT)
- Hardware repurposing and elimination
- Reduce Privacy, Compliance & Audit Risk to Personal data (Data Subjects)
- IT support effort and costs elimination (ticketing, maintenance and support)

buyer roles

- CIO, VP IT
- CHROs
- Legal & Compliance
- Data Privacy Officers

FUSE
ANALYTICS

common objections

We will just build something in-house.

- loss of functionality in data access, security
- insecure and fragmented solutions like SQL databases, CSV, XLS for sensitive data
- more than just structured data (think documents, web pages, reports, etc)
- temporary solution and not scalable
- deconstructed data won't be directly usable by the business

GDPR doesn't affect us

- How will you deal with Data subject rights, Data Sovereignty, and Personal Access data controls as well as evolving national privacy laws beyond just the EU? For example China, Brazil, and even the US.
- North American states like CA and NY have already passed new privacy regulations and many more are in draft form, most are modeled after GDPR.
- Many other countries are applying pressure to cover their citizen's data no matter where they work and live.
- Avoidance risks creating an organizational strategy that is reactive and fragmented as opposed to proactive and controlled.

Why wouldn't we use a generic archiving solution for all enterprise data (not a stand-alone platform)

- A Very high IT cost option.
- Data Governance functionality gets lost- Personal data treatment is central.
- The majority of data (in terms of size) is often semi-structured and unstructured (documents, pages, reports) not neatly packaged CSVs and tables.
- Creating order in a data lake is a purely custom effort and security difficult to manage across business functions and users..

We will look at archiving after the conversion is completed to our new system.

- Approaching it as an afterthought means ***paying twice*** for similar work; these are typically highly redundant efforts
- Often resulting in companies dragging down new system ROI's by never removing applications from the landscape.

We probably don't have that much data we need to keep around (at least not for more than a year or two).

Most organizations currently hold 10-20x the data typically required for "current business operations.

- Retention of various datasets and documents is complex especially in the HR and Payroll space due to labor laws, wage hour laws, EE0, OSHA and many other regulations. The scope ranges from 2-3 years minimum to 30+ years retention.
- Transactional enterprise systems are 100x the weight of the data required for retention. A typical ERP system for HR may have 3000 database tables, only 300 of which are *NOT* system or configuration tables. Of these 300 data tables the ones that remain after dropping unused data tables and fields can often be reduced to 30-40 flattened datasets. There is a massive reduction in the footprint.

- Business user access needs often increase over time for the first 3-5 years because a repository becomes the only point of reference. They will typically access this data for the first 3-5 years an average of 100-200 times per calendar year and more depending on the size of the organization and needs related to legal and compliance inquiries, audits and subpoenas.