



— WEBINAR SERIES —

Sandy Serkes
Co-Founder & CEO

Jennifer Nelson
VP Strategic Solutions

Beyond Keywords: How AutoClassification Transforms Enterprise Search (and enables trusted AI)



Webinar Series



www.ValoraTech.com



ROT Remediation:
File Share Clean-up
January 21



How AC Transforms
Enterprise Search



Letting the Robots
Classify: Automating IG
February 18



Managing Data Privacy &
While Managing Records



AutoClassifying the 3 Rs:
ROT, Records & Retention
March 18



From Observational to
Operational InfoGov



Structured Data
Management & Disposition
April 15



AI: What Happens when
the Model Collapses



10 Ways AutoClassification
Can Impact AI
May 13



AutoClassification & AI
Trends in Enterprise

About Valora



- AutoClassification platform for Information Governance
- Automates **discovery**, **identification**, **classification** & defensible disposition
- Trusted by IG teams, Records & IM teams, Legal, Compliance, IT teams
- Brings **multiple enterprise repositories** into a single view, and **multiple IG use cases** under one umbrella



Poll Results

Who's here today
& what are your interests?



Who you are & what your challenges are



Who You Are

Records / Information Management

Knowledge Management

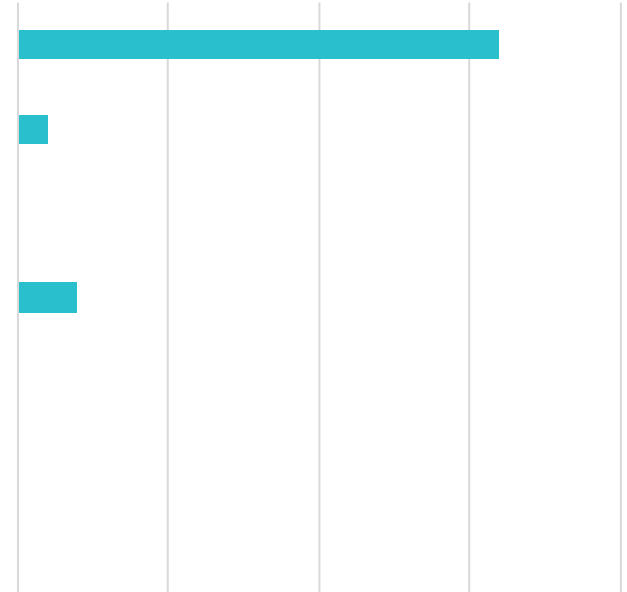
Legal

Compliance

IT

Data Privacy / Security

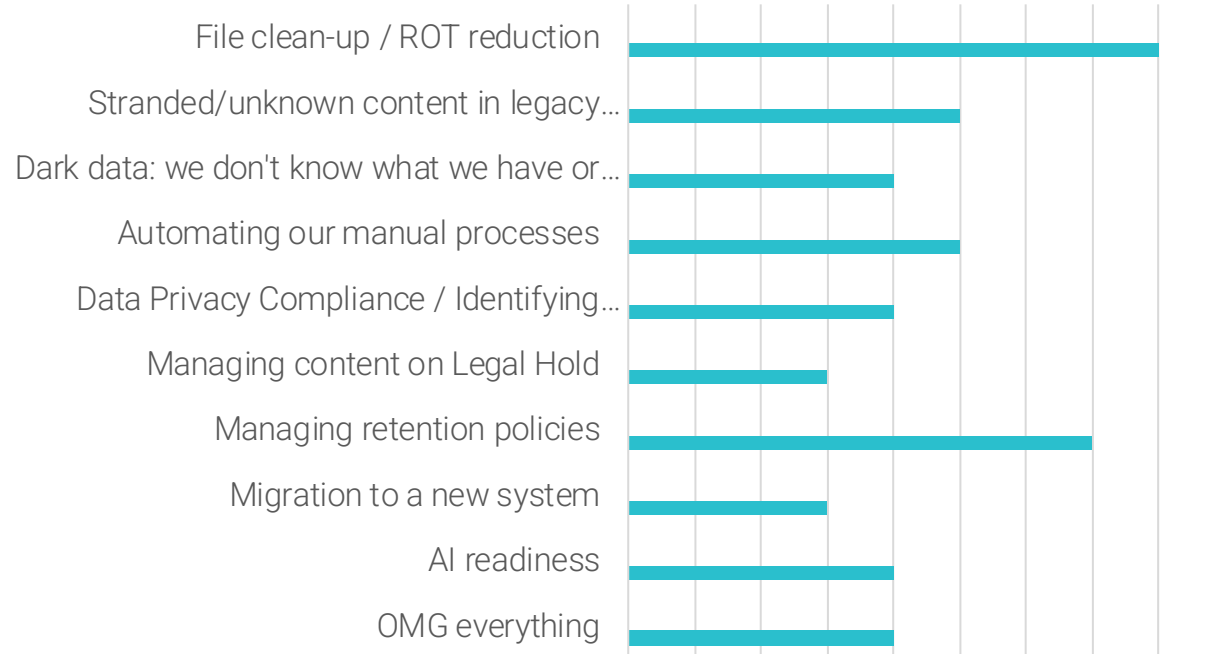
Other



Who you are & what your challenges are



Your RIM &
IG Challenges



Housekeeping



Q&A



Recording



Slides



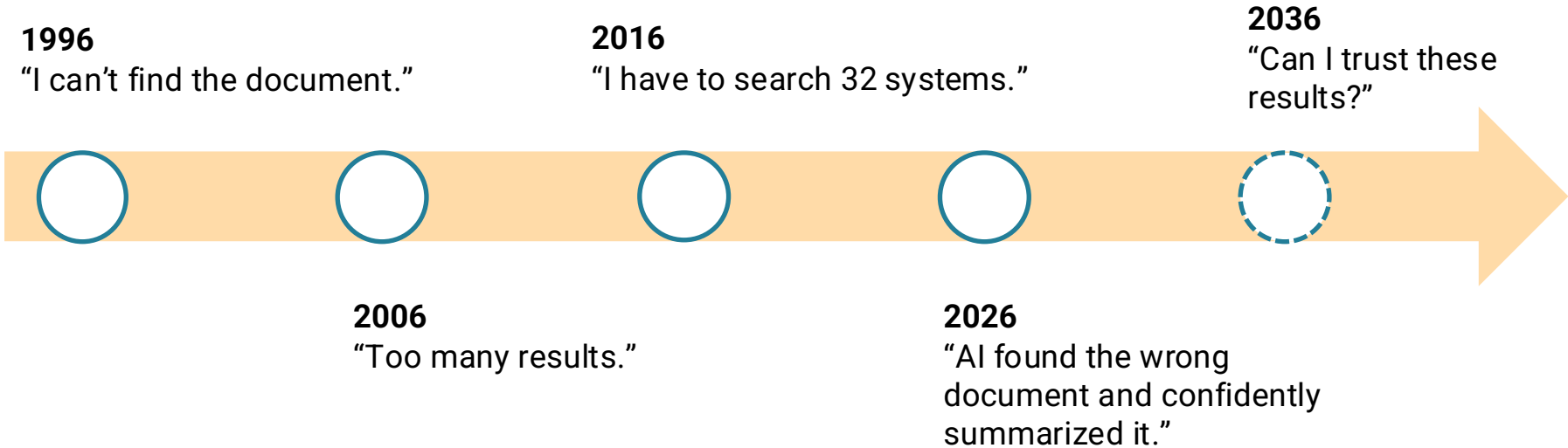
Feedback

Agenda



- Why enterprise search is struggling
- Why AI alone doesn't solve the problem
- What AutoClassification adds
- Use cases
- Search + AI + Classification Together
- Q&A

The Evolution of Search



Enterprise Search has a context problem

Search Is Everywhere

- Microsoft 365
- SharePoint
- Google Workspace
- File Shares
- ECM Platforms
- Knowledge Bases
- AI Assistants



Enterprise Search has a context problem

Search Is Everywhere

- Microsoft 365
- SharePoint
- Google Workspace
- File Shares
- ECM Platforms
- Knowledge Bases
- AI Assistants

Users still say:

“I know it exists...I just can't find it”



Why keyword search falls short

Keyword search relies on:

- Exact words
- File & path names
- User-applied tags
- User knowledge



Why keyword search falls short

Keyword search relies on:

- Exact words
- File & path names
- User-applied tags
- User knowledge

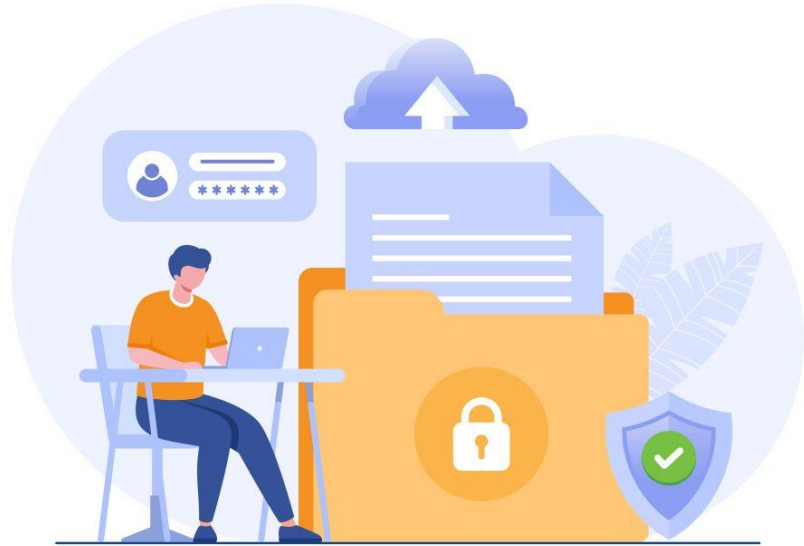
But business questions are about meaning:

- Which documents contain personal information?
- Records are subject to retention?
- Contracts are active?
- Policies are authoritative?

Search is now a risk management issue

Growing Pressures:

- Privacy regulations
- FOIA requests
- Litigation
- Cybersecurity incidents
- Compliance obligations



Search is now a risk management issue

Growing Pressures:

- Privacy regulations
- FOIA requests
- Litigation
- Cybersecurity incidents
- Compliance obligations

Organizations must:

- ✓ Find information quickly
- ✓ Demonstrate completeness
- ✓ Defend search results
- ✓ Reduce review effort

The AI question everyone is asking

“Can’t AI just find what I’m looking for?”

Fair question.

- ✓ AI can read documents
- ✓ AI can summarize content
- ✓ AI can answer questions
- ✓ AI can search across repositories



The AI question everyone is asking

“Can’t AI just find what I’m looking for?”

Fair question.

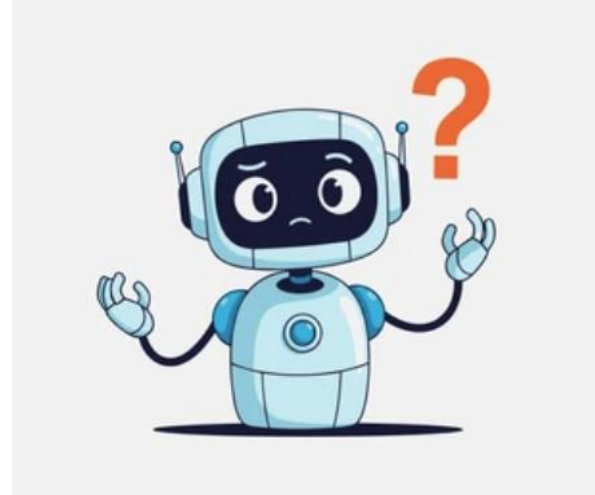
- AI can read document documents
- AI can summarize content
- AI can answer questions
- AI can search across repositories

So why do we still need
AutoClassification?

AI has the same problem search has

AI can read information,
but can it determine:

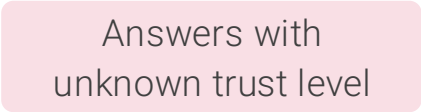
- Which version is current?
- Document is authoritative?
- Content is obsolete?
- Records are sensitive?
- Information should be excluded?



The hidden risk of Enterprise AI

ENTERPRISE CONTENT

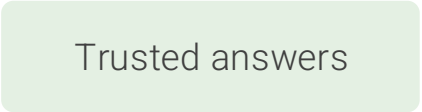
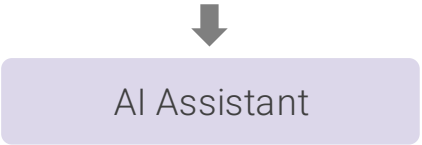
- Current policies
- Duplicate files
- Contracts
- Outdated policies
- Sensitive Information
- Email archives
- Draft Documents
- Personal Information
- Shared drives



- Is it accurate?
- Is it current?
- Is it approved?
- Is it safe?

CLASSIFIED ENTERPRISE CONTENT

- Current/approved policy
- Draft Documents
- Obsolete policy
- Active contracts
- Duplicate copies
- Expired contract
- Official procedures
- Old versions
- Sensitive data



- Authoritative
- Current
- Relevant
- Governed

AutoClassification creates trusted data for AI

AutoClassification Identifies:

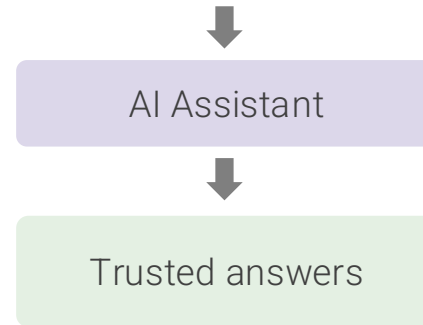
- Authoritative content
- Obsolete content
- Sensitive information
- Record categories
- Business context
- Regulatory classifications

Result:

- ✓ AI learns from better information.
- ✓ AI retrieves better information.
- ✓ AI delivers better answers.

CLASSIFIED ENTERPRISE CONTENT

- Current/approved policy
- Draft Documents
- Obsolete policy
- Active contracts
- Duplicate copies
- Expired contract
- Official procedures
- Old versions
- Sensitive data



- Authoritative
- Current
- Relevant
- Governed

An effective information ecosystem



Search answers :

“What contains these words?”



AutoClassification
answers :

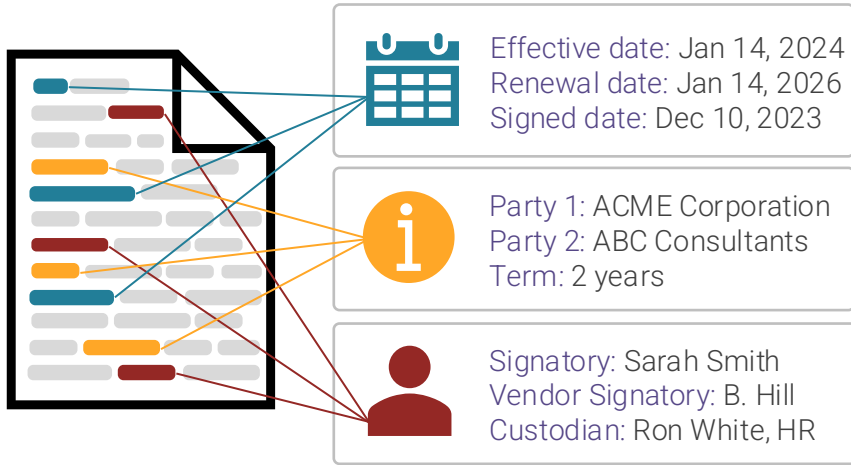
“What is this information?”



AI answers :

“What does this information mean?”

What is AutoClassification?



How it works:

- Full text analysis determines **rich metadata** attributes
- Recognition algorithms determine **document type**
- Disposition algorithms determine **rules & actions**

Automatically assigns:

- Records categories & record classes
- Privacy indicators & sensitivity labels
- Retention metadata & event triggers
- What is appropriate for AI use / what is not

Results:

- ✓ Consistent
- ✓ Defensible
- ✓ Context

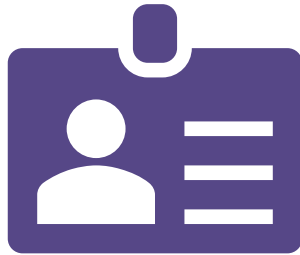
Search before vs. Search after

Search Alone	Search + AutoClassification
Keywords	Keywords + Context
Large result sets	Precise result sets
High review burden	Reduces review burden
Inconsistent metadata	Consistent metadata
Limited confidence	Greater confidence

Use Case: DSAR & Privacy Requests

Challenge:

Find all personal information associated with an individual.



AutoClassification adds:

- ✓ Personal information detail
- ✓ Sensitive data categories
- ✓ Context awareness
- ✓ Faster response

Use Case: Breach Response

Challenge 1:

What sensitive information was exposed?



AutoClassification identifies:

- ✓ PII, PHI, PCI
- ✓ Financial Data
- ✓ Confidential information
- ✓ Regulated records

Use Case: Breach Response

Challenge 2:

Why did you still have the data?



AutoClassification identifies:

- ✓ Collection basis
- ✓ Opt-in, opt-out status
- ✓ Legitimate non-disposition (ex: holds)
- ✓ Opportunities for data minimization

Use Case: Investigations & eDiscovery

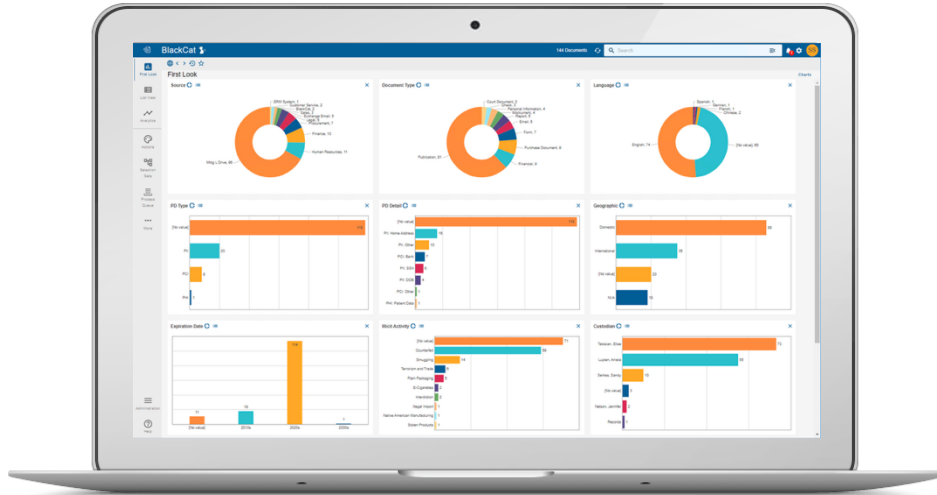
- Goals:
- Reduce collection volume
 - Pinpoint relevance & privilege
 - Accelerate review
 - Improve defensibility



AutoClassification provides:

- ✓ Reduced master corpus
- ✓ Targeted collection
- ✓ Context before review begins
- ✓ Reusable metadata

Quick demo



DSAR search of a former employee



Breach report of comprised repository



eDiscovery search

Search + AutoClassification + AI



Search finds information



AutoClassification adds context



AI generates insight



Users get trusted answers

Key takeaways



- ✓ Search Without Context **Produces Noise**
- ✓ AI Without Context **Produces Risk**
- ✓ AutoClassification **Provides Context**

Resulting in:

- ✓ Better Search
- ✓ Better Compliance
- ✓ Better Investigations
- ✓ Better AI Outcomes
- ✓ Greater Trust



www.valoratech.com



Book a Demo



Webinar Series



[/valora-technologies](https://www.linkedin.com/company/valora-technologies)

Q&A

Thank you



Sandy Serkes
President & CEO
sserkes@valoratech.com



Jennifer Nelson
VP Strategic Solutions
jnelson@valoratech.com