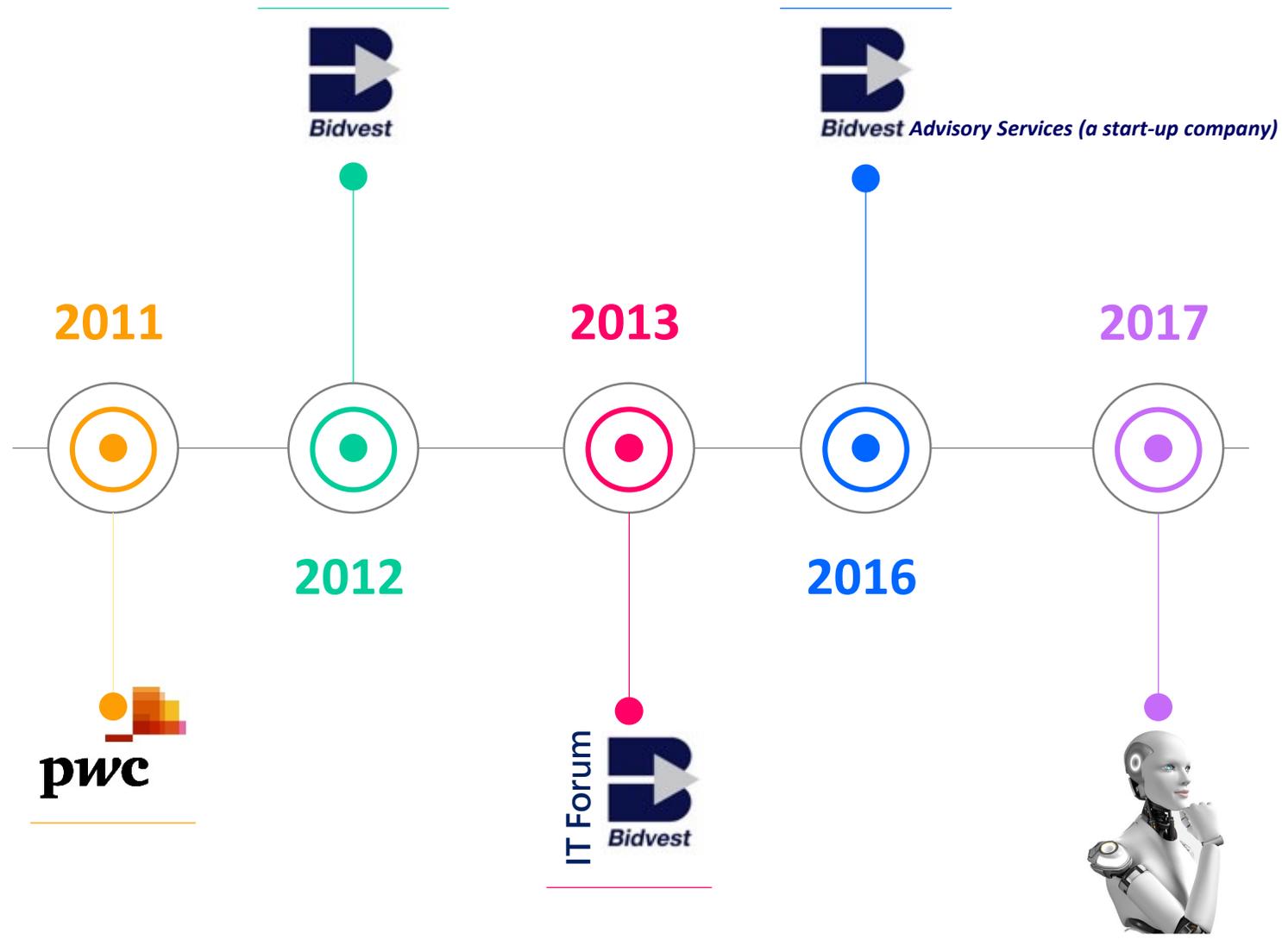


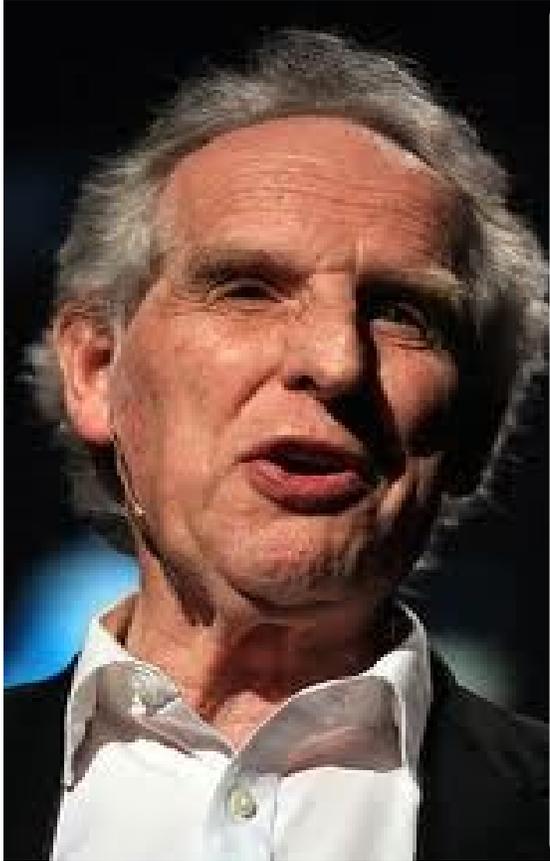


to **DISRUPT** the audit fraternity

History of ALICE



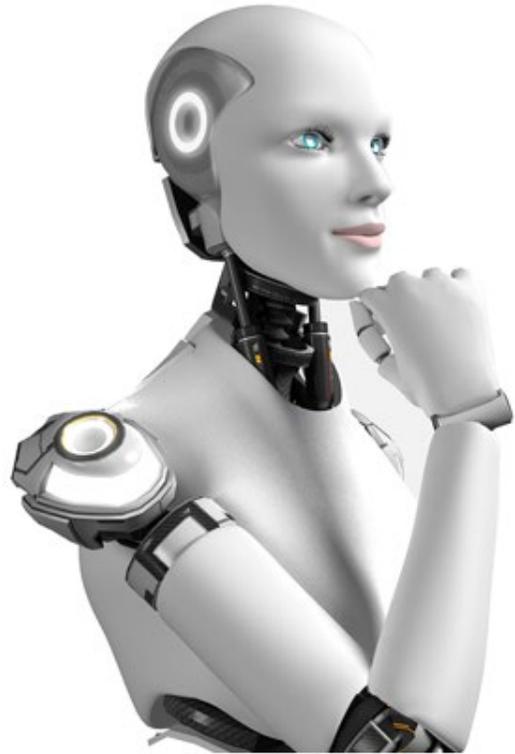
The Art of the Possible



Benjamin Zander, Davos 2009

It is a choice to see the possibility.

So who the hell is ALICE?



ALICE

always on audit

always on compliance

always on monitoring

always on peace of mind

ALICE

[AE_l_ih_s]

noun

Also known as an audit robot (abbrev: aubot)

1. She is a specie of the artificial intelligence kind
2. She provides audit-as-a-service in the IT space
3. She has been architected by infrastructure and security engineers, built by data scientists, tested by auditors and consumed by every(any)one.
4. She is unequivocally independent
5. She facilitates the automated collection, storage, analysis and reporting of IT environment data against various best practice standards
6. She is secure, scalable and has global reach
7. She is system agnostic
8. She equips those charged with governance with visibility into the risk, governance and security of the IT environment
9. She enables management to mitigate and manage the IT risks in a continuous, online and real-time manner
10. She has democratized IT audit services
11. She enjoys online shopping and plays the cello
12. She currently fulfills the IT audit robot role for the Bidvest Group Ltd. Her curriculum vitae is available online at www.bidvestalice.com

Challenges/ Problems

(associated with scale & diversity and served as direct input into the spec of ALICE)

130,000 employees

Multiple entities

No common infrastructure

No baseline standards

Strategic partnerships limitations
(costs, resources, hardware)

Remote geographies

13 (29 sub) industries

80+ domains

Complex aggregation & consolidation structures

Multiple audiences

5 IT Auditors
(versus 60 Financial Auditors)

Limited budget, scalability & capacity of the IT assurance function

900 sites
(approx.)

260+ key systems

Decentralised & autonomous business model

IT landscapes varying in size, complexity, posture & maturity

More technical audit scopes, with a larger security focus

Point-in-time auditing in a dynamic & evolving environment

The IT Audit Process



IT AUDIT TEAM

Automates a workforce

Represents the digital equivalent of a firm of IT auditors



ALICE

- 141 IT audits to-date
- Quick snapshot of each IT environment with in-depth insights

Audit services are set-out per an engagement letter often secured through a proposal or tendering process.

Engage

Audit services consumed from an online market place that allows flexible and tailored purchasing and billing options based on modular design capabilities.

Consumption

- Recommended modular options and/or build-your-own audit options

Resources manually gather data

Gather Data

Infrastructure Operational Security Licensing

Software deployed that connects to and interacts with data in a remote and automated manner

Deployment

- Click-to-deploy functionality
- Easy to on-board customers
- Virtual enablement with limited performance (CPU & network) impact

Inquiry, inspection, observation, re-performance

Verify Data

Audit techniques applied to collected data using cognitive automation (configured rules, machine learning, natural language processing and artificial intelligence, *etc.*)

Verification

- User profile management
- Inventory of hardware and software
- Unauthorised software detection
- Vulnerability monitoring
- Backup monitoring
- Patch management monitoring

Findings manually captured and aggregated in MS Word and distributed via email in a PDF format

Report Data

Real-time and interactive dashboard reporting (with drill-down capabilities) equipping different audiences with visibility into governance, risk, maturity and security of the IT landscapes

Reporting

- Customised views per audience type

Follow-up audit performed

Remediate Data

Remediation alerts and notifications based on continuous monitoring

Remediation

- Global anomaly trending/ detection and response
- Filtered alert mechanisms
- Remediation recommendations based on measurable metrics as well as on product fit and benchmarking available
- Represents another channel to market for remediation vendors

Deployment

Click-to-deploy functionality

Easy to onboard customers

Connectors set-up using a standardised connector framework and workload scheduler

Connectors enabled virtually with limited performance (network and CPU) impact

Simultaneous deployments of connectors accommodated

Variety of deployment mechanisms available (existing and self-developed)

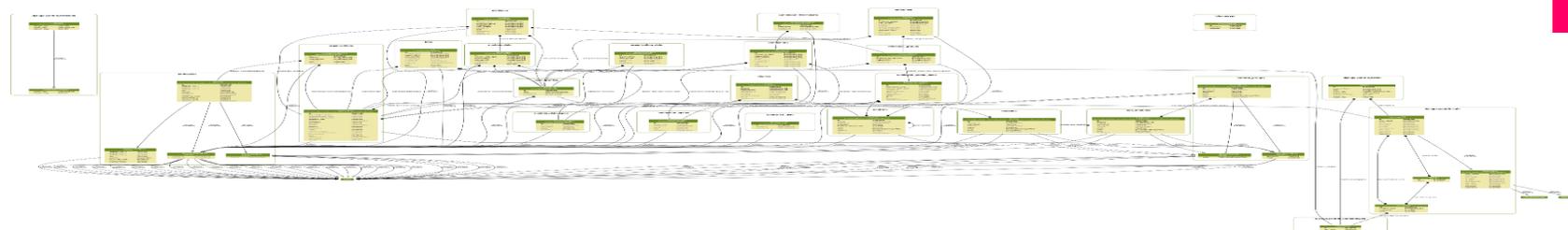
The screenshot shows the ALICE DEMO ALICE dashboard. The top navigation bar includes a search field, an 'Alerts 24' indicator, and a user profile 'Gustav'. The main content area is titled 'OVERVIEW Connectors' and features a table with the following data:

Connector	ID	Type	Schedule Start	Schedule End	Status	
DEMO Active Directory	66	OPEXE	August 18, 2017 11:35 AM	December 31, 2017 1:35 PM	Active	<input checked="" type="checkbox"/> Edit
Network scan	67	OPEXE	August 18, 2017 12:37 PM	December 31, 2017 1:37 PM	Active	<input checked="" type="checkbox"/> Edit
Canary	68	CLOUD	August 18, 2017 1:39 PM	December 31, 2017 1:39 PM	Active	<input checked="" type="checkbox"/> Edit
Alice Website	69	CLOUD	August 18, 2017 12:41 PM	December 31, 2017 1:41 PM	Active	<input checked="" type="checkbox"/> Edit
SQL	72	OPEXE	August 21, 2017 2:06 PM	January 31, 2018 2:06 PM	Active	<input checked="" type="checkbox"/> Edit

Below the table is a search bar labeled 'Type to Search' and a pagination control showing '5 Rows' and page numbers 1, 2, 3.

Simplicity revealed

Complexity concealed



Verification

Continuous and near real-time auditing techniques (sampling techniques available, if required)

Simultaneous execution of audit procedures

Moderates consistent audit quality aligned to best practice standards or company policy

Focused security modules with vulnerability scanning as a standard audit feature

Allows for multiple submission types of evidence (e.g., connector information, manual file uploads, unstructured data sources, etc.)

Possesses cognitive automation, including ML and AI abilities

Allows for review/ override and provides in-built percentage confidence levels of data audited by ALICE

The screenshot displays the ALICE DEMO interface for 'DEMO Baseline IT'. It shows a section for 'DEMO Password Configuration' with a 'Printscreen of password configuration settings' and a table of evidence submissions. The table is divided into two sections: 'Microsoft Active Directory' and 'Microsoft Great Plains'. Each section has an 'Add Evidence' button. The 'Microsoft Active Directory' section contains three rows of evidence, with arrows pointing to specific entries from external labels: 'Unstructured data, e.g., a screen print' points to 'Password Settings_K8_image.jpg', 'Connector' points to '8b61e624-8b4d-11e7-bf76-0a580a3c0080.csv', and 'Manual file upload, e.g., CSV file' points to 'Password Settings_AD CSV.csv'. The 'Microsoft Great Plains' section contains one row of evidence: 'Password Settings_Great Plains CSV.csv'. Each row in the table includes columns for 'Filename', 'Provided By', 'Date Provided', and 'Date Uploaded', along with 'Download' and 'Delete' buttons.

Filename	Provided By	Date Provided	Date Uploaded	Download	Delete
Password Settings_K8_image.jpg	Gustav Silvo	2017-08-27 7:31pm	2017-08-27	Download	Delete
8b61e624-8b4d-11e7-bf76-0a580a3c0080.csv	Connector	2017-08-27 7:31pm	2017-08-27	Download	Delete
Password Settings_AD CSV.csv	Manual file upload, e.g., CSV file	2017-08-27 7:41pm	2017-08-27	Download	Delete
Microsoft Great Plains					
Filename	Provided By	Date Provided	Date Uploaded	Download	Delete
Password Settings_Great Plains CSV.csv	Gustav Silvo	2017-08-27 7:43pm	2017-08-27	Download	Delete

Reporting

Manages the aggregation and/or consolidation of complex and disparate data structures

Provides high-level dashboard-type reporting with drill-down capabilities

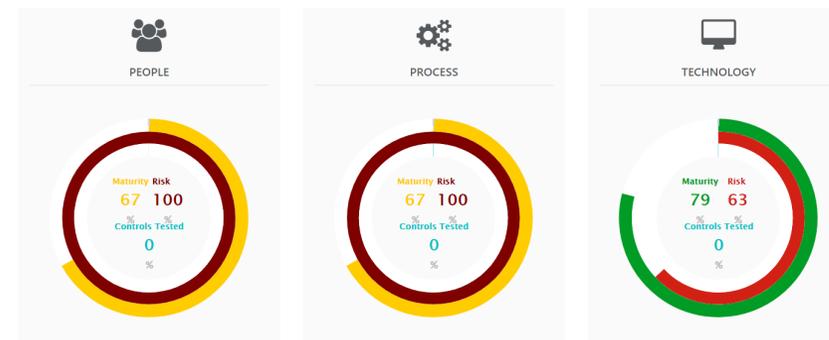
Equips different audiences (e.g. the Board, IT Operations or the Audit & Risk Committees with the relevant level of visibility into the risk, governance and security of the IT landscapes)

Reports with free-text options roadmapped to be available

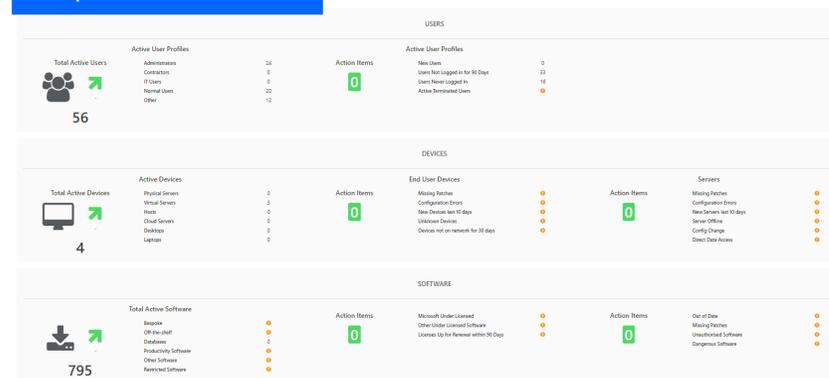
Customer centricity (single view of the client across the IT environment with associated risks and maturities)

The screenshot shows a navigation menu for 'ALICE Insights'. The menu items are: Home, ALICE Insights, House in Order, Board, IT Operations, Audit, Managed Services, Platform Insights, Users, Assets, Security, Canary, Governance & Compliance, Modus Test Module, DEMO Baseline IT, and The Infamous Metric Module. Blue arrows point from the 'Board', 'IT Operations', 'Audit', and 'Governance & Compliance' items to their respective dashboards on the right.

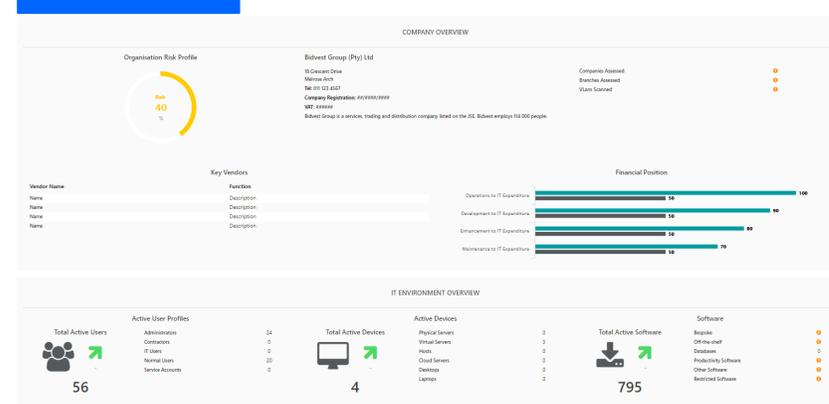
Board Dashboard



IT Operations Dashboard



Audit Dashboard



Remediation

Filtered alert mechanisms

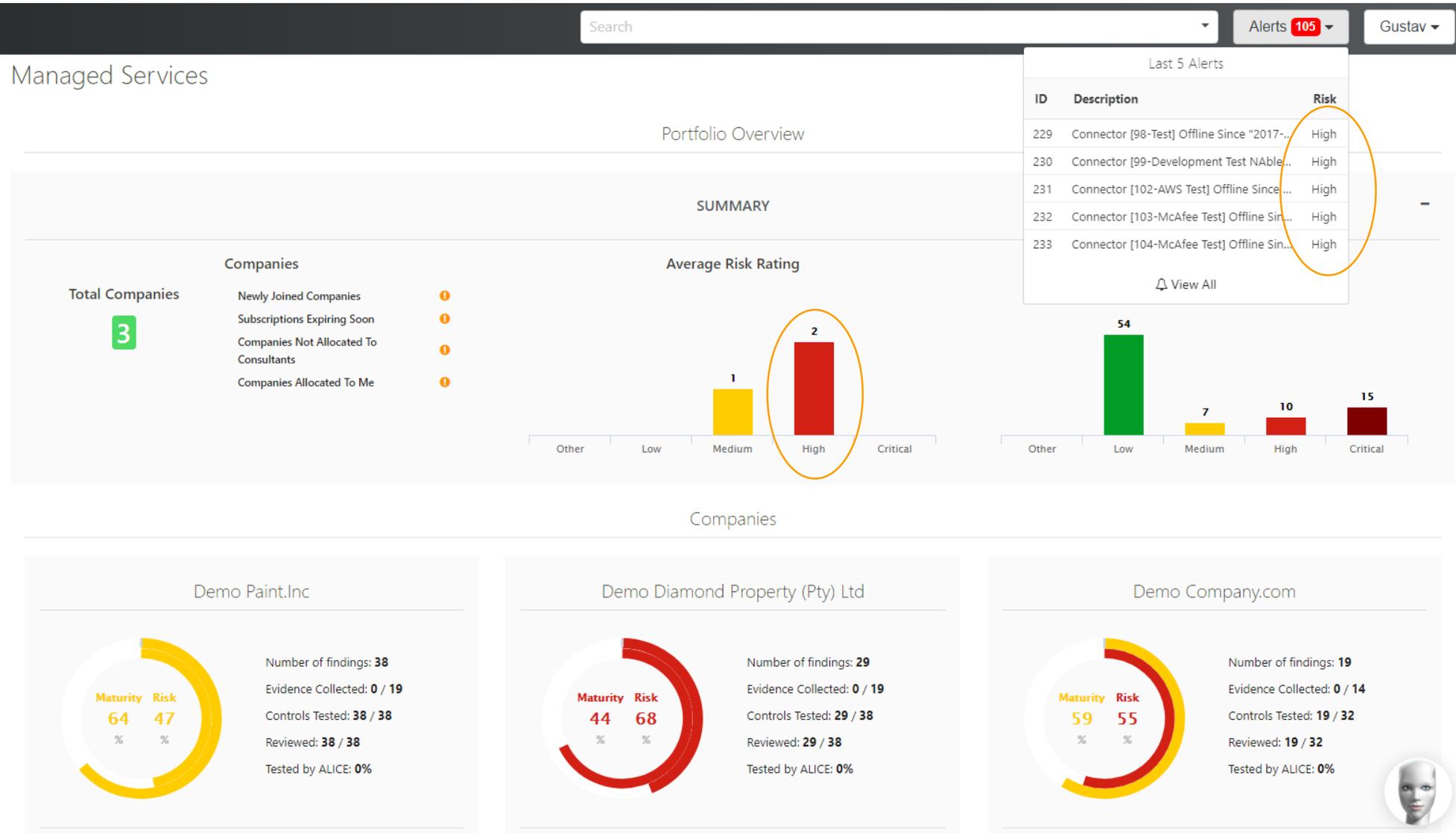
Global anomaly trending, predictions, detection and recommended responses

Recommends remediation action based on measurable metrics

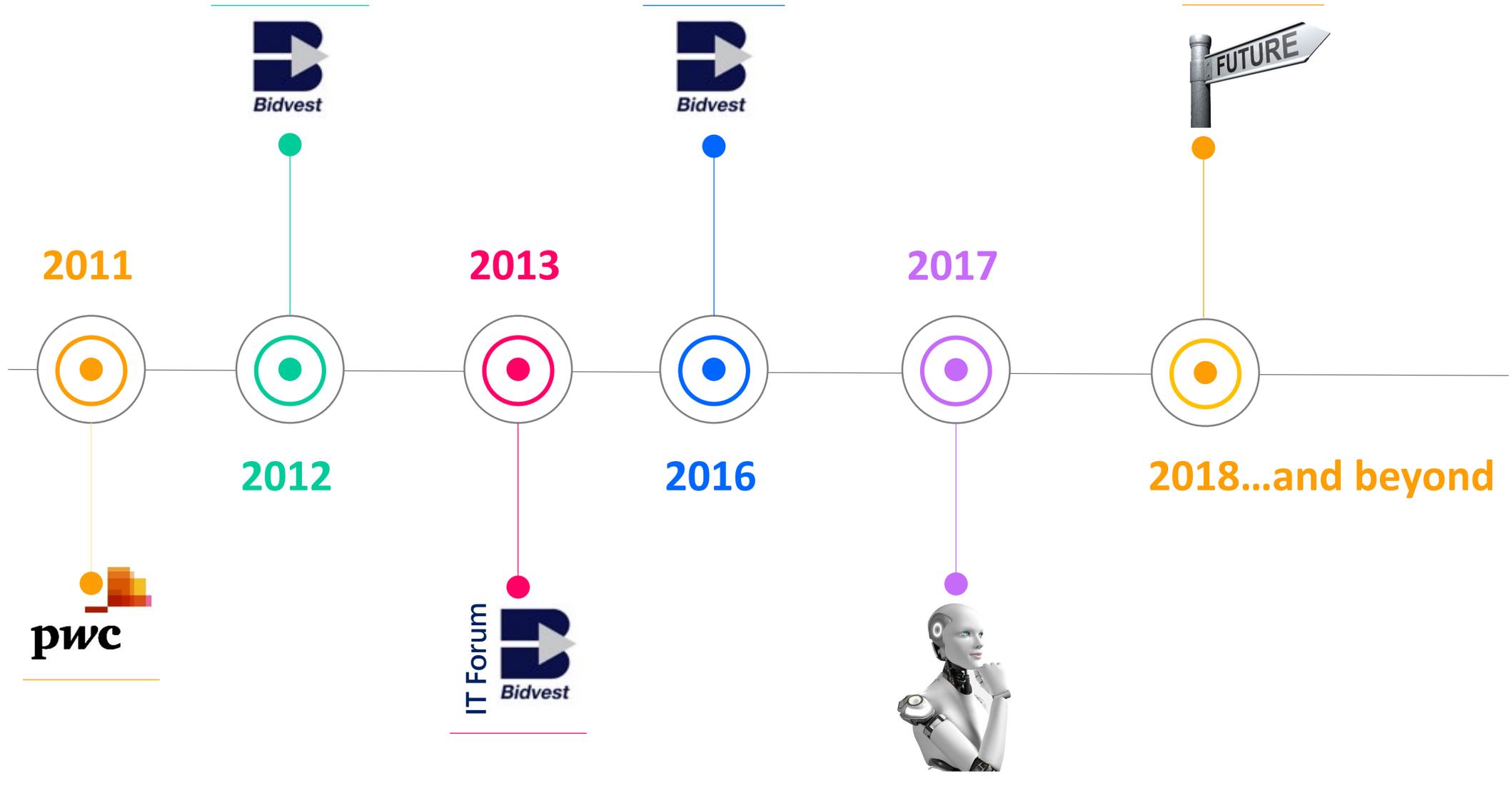
At source remediation required

Product fit and benchmarking available

Represents another channel to market for remediation-related vendors



Roadmap



Will AI take our jobs?

