AUTONOMOUS DATA SECURITY

CONCENTRIC

Semantic Intelligence™ Solution with Risk Distance™ Analysis for Email, Slack and Teams

Data Security Posture Management Without Rules or Policy Management

Concentric MIND

Centralized deep learning as-a-service for fast, accurate identification of business-critical data without complex rules or upfront configuration

Risk Distance

Autonomous risk analysis based on peer file comparisons to spot security concerns without rules or end-user involvement

Messaging and E-mail

Spot sensitive content in messaging text and attachments in Slack, Microsoft Teams, and e- mail

Introduction

The Semantic Intelligence™ deep learning solution prevents data loss by autonomously discovering data, categorizing content, and optimizing data security posture. It protects sensitive data shared as text and attachments on messaging services. Semantic Intelligence easily identifies business and privacy–sensitive content without rules or policies. Our Risk Distance™ analysis compares each file to baseline security practices used by similar files to identify risk without rules and policies. Concentric's User 360 and File 360 capabilities identify inappropriate user activities and provide support for access control planning so you can confidently manage your data security posture.

Highlights

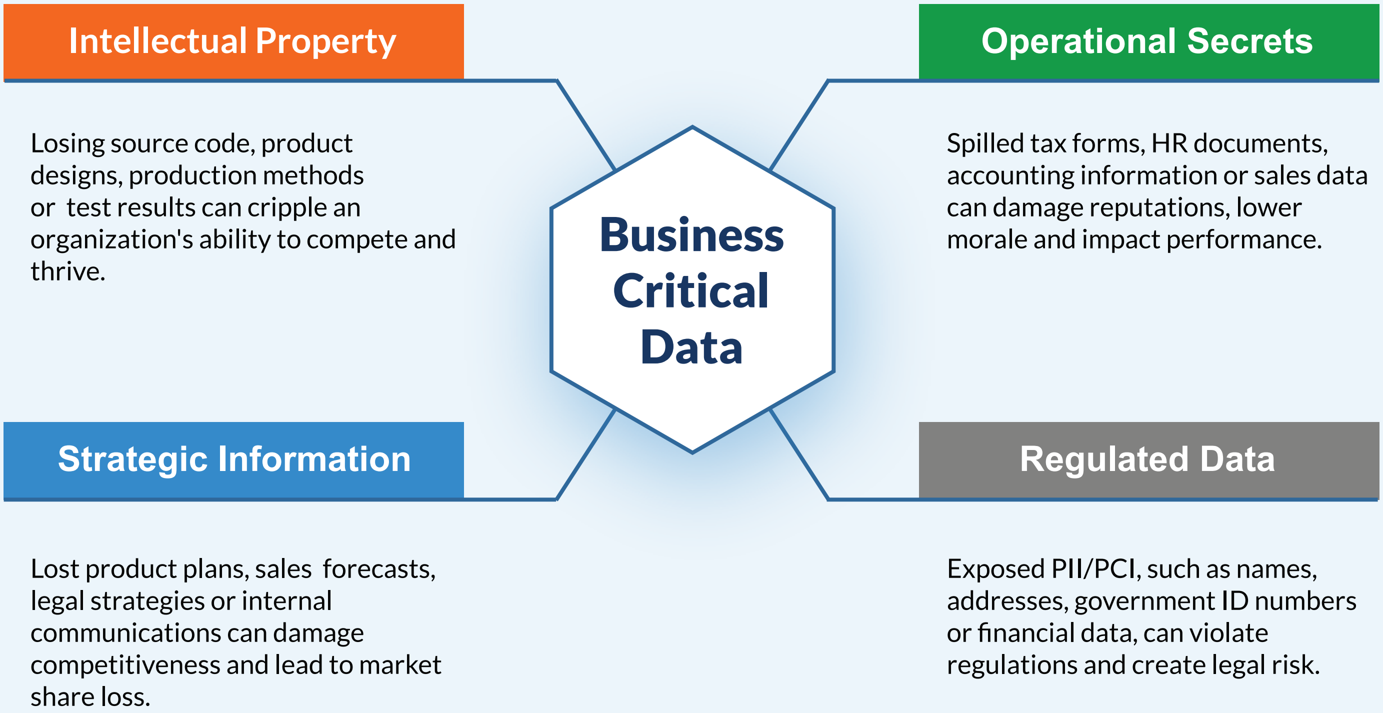
- Find mission critical data across e-mails, Slack and Teams
- Gain a risk-based view of data and users
- Automated remediation with risky data sharing to instantly fix access issues
- Find risk without rules or formal policies
- Secure SaaS solution, API based, no agents
- Easy to maintain with minimal overhead

How It Works

Semantic Intelligence automates data security governance. We use deep learning to capture the collective wisdom of content owners to understand security policies without hard-to-maintain rules or burdening end users.

Deep learning organizes data into thematic categories that offer content insights into meaning and business criticality. Risk Distance analysis uncovers each category's baseline security practices to spot at-risk individual files. Our User 360 capabilities assess risk through a user-centric lens to insider threats and data loss. The solution reveals inappropriate sharing, unusual locations, or incorrect classification – all without rules or policies.

> *"Semantic Intelligence is the foundation for our PHI and PII protection strategy. We get the visibility and control we need, including insights into sensitive content in text and attachments shared via Microsoft Teams and Exchange. It's how we empower our staff without compromising security."*
>
> **CISO, Healthcare Firm**



Business Critical Data

Intellectual Property

Losing source code, product designs, production methods or test results can cripple an organization's ability to compete and thrive.

Operational Secrets

Spilled tax forms, HR documents, accounting information or sales data can damage reputations, lower morale and impact performance.

Strategic Information

Lost product plans, sales forecasts, legal strategies or internal communications can damage competitiveness and lead to market share loss.

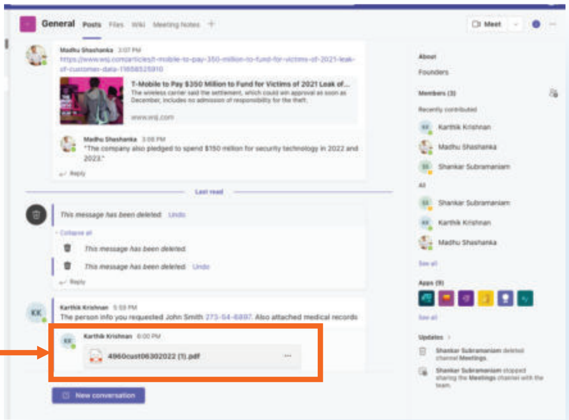
Regulated Data

Exposed PII/PCI, such as names, addresses, government ID numbers or financial data, can violate regulations and create legal risk.

AUTONOMOUS DATA DISCOVERY

Effective data access governance starts with accurate and continuous data discovery and categorization. Our sophisticated natural language processing capabilities (a type of deep learning) autonomously groups data into over 250 categories, revealing privacy-sensitive data, intellectual property, financial information, legal agreements, human resources files, sales strategies, partnership plans and other business-critical information being exchanged across workspace channels or through email. We discover this data without rules, regular expressions, user input, or IT staff overhead.

Deep learning-based semantic understanding of privacy data, intellectual property, and other sensitive data exchanged across workspace channels



Madhu Shashanka 3:07 PM
https://www.wsj.com/articles/t-mobile-to-pay-350-million-to-fund-for-victims-of-2021-leak-of-customer-data-11658525910

T-Mobile to Pay $350 Million to Fund for Victims of 2021 Leak of...
The wireless carrier said the settlement, which could win approval as soon as December, includes no admission of responsibility for the theft.
www.wsj.com

Madhu Shashanka 3:08 PM
"The company also pledged to spend $150 million for security technology in 2022 and 2023."

Last read

This message has been deleted. Undo

This message has been deleted.

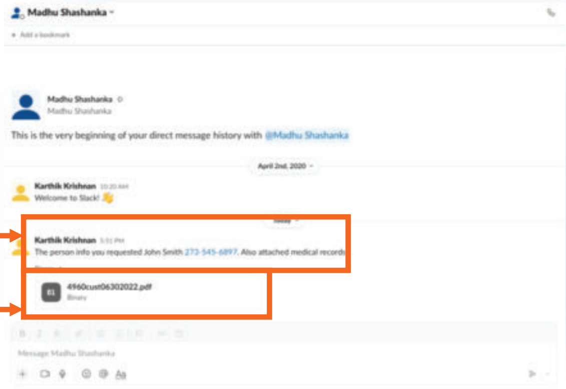
This message has been deleted. Undo

Karthik Krishnan 5:59 PM
The person info you requested John Smith 273-54-6897. Also attached medical records

Karthik Krishnan 6:00 PM
4960cust06302022 (1).pdf

Shankar Subramaniam deleted channel Meetings

Shankar Subramaniam stopped sharing the Meetings channel with the team.



Madhu Shashanka
Madhu Shashanka

This is the very beginning of your direct message history with @Madhu Shashanka

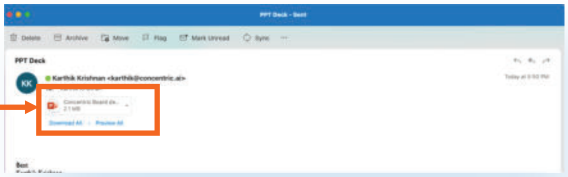
April 2nd, 2020

Karthik Krishnan 10:20 AM
Welcome to Slack! 👋

Today

Karthik Krishnan 5:51 PM
The person info you requested John Smith 273-545-6897. Also attached medical records

4960cust06302022.pdf
Binary



PPT Deck

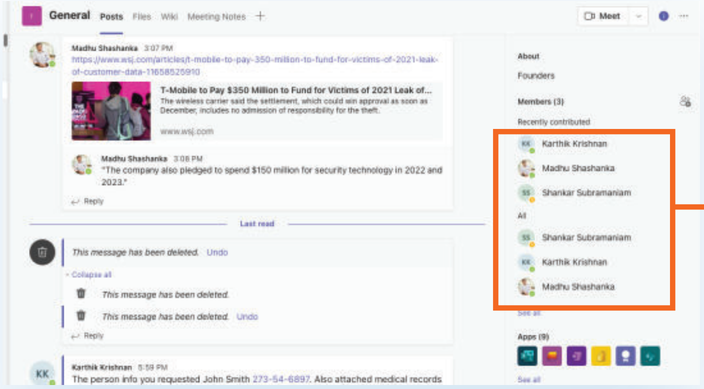
KK Karthik Krishnan <karthik@concentric.ai>

Concentric Board de...
2.1 MB
Download All | Preview All

Best
Karthik Krishnan

RISK DISTANCE ANALYSIS

Semantic Intelligence uses Risk Distance to determine who has access to this data. Autonomously find inappropriate sharing or unauthorized access by internal user or third parties.



Madhu Shashanka 3:07 PM
https://www.wsj.com/articles/t-mobile-to-pay-350-million-to-fund-for-victims-of-2021-leak-of-customer-data-11658525910

T-Mobile to Pay $350 Million to Fund for Victims of 2021 Leak of...
The wireless carrier said the settlement, which could win approval as soon as December, includes no admission of responsibility for the theft.
www.wsj.com

Madhu Shashanka 3:08 PM
"The company also pledged to spend $150 million for security technology in 2022 and 2023."

Last read

This message has been deleted. Undo

Collapse all

This message has been deleted.

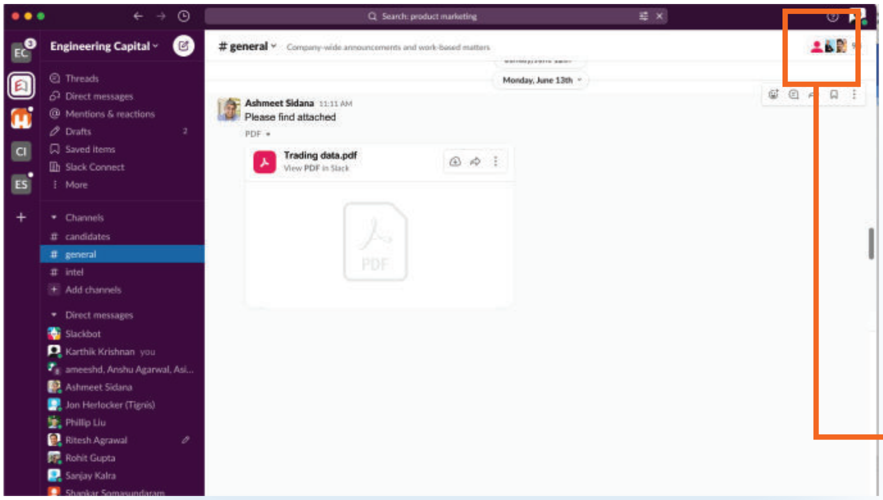
This message has been deleted. Undo

Karthik Krishnan 5:59 PM
The person info you requested John Smith 273-54-6897. Also attached medical records

Autonomous Risk Distance assesses access and spots oversharing

CENTRALIZED REMEDIATION

Concentric Semantic Intelligence centrally remediates oversharing and inappropriate permissions by disabling access, recalling messages, or via integrations with end-user and SOC workflows for redress.



Ashmeet Sidana 11:11 AM

Please find attached

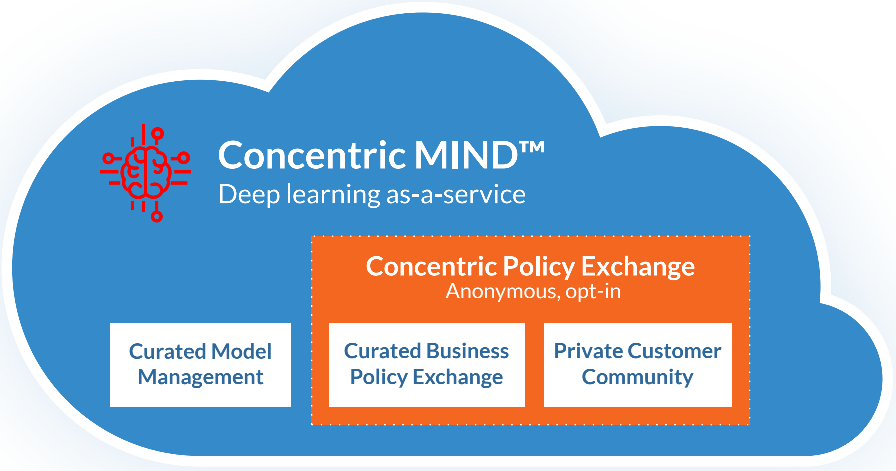
Trading data.pdf

View PDF in Slack

Centralized remediation restricts access and prevents data loss

CONCENTRIC MIND

Centralized MIND, a deep-learning-as-a-service capability, improves categorization coverage and speeds model adaptation by aggregating intelligence across Concentric customers. MIND curates all of Semantic Intelligence's deep learning models (whether developed by Concentric or our customers) to offer the best-fitting model to every customer when they need it. Shared models are entirely mathematical and do not contain source data to ensure customer privacy and security



Concentric MIND™

Deep learning as-a-service

Concentric Policy Exchange

Anonymous, opt-in

Curated Model Management

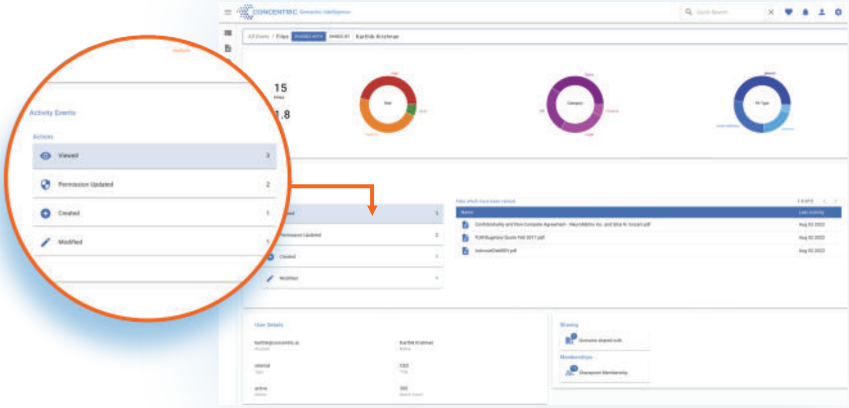
Curated Business Policy Exchange

Private Customer Community

MIND Deep Learning-as-a-Service

User 360 offers a user-centric view of each file accessible by a specific employee. Quickly establish usage patterns, spot inappropriate storage locations, and find risky sharing patterns. Compare a user's access and sharing practices with similar users, spot personal email sharing and understand what privacy-sensitive content each user can access. User 360 proactively protects against insider threats and data loss without rules or hard-to-maintain policies.

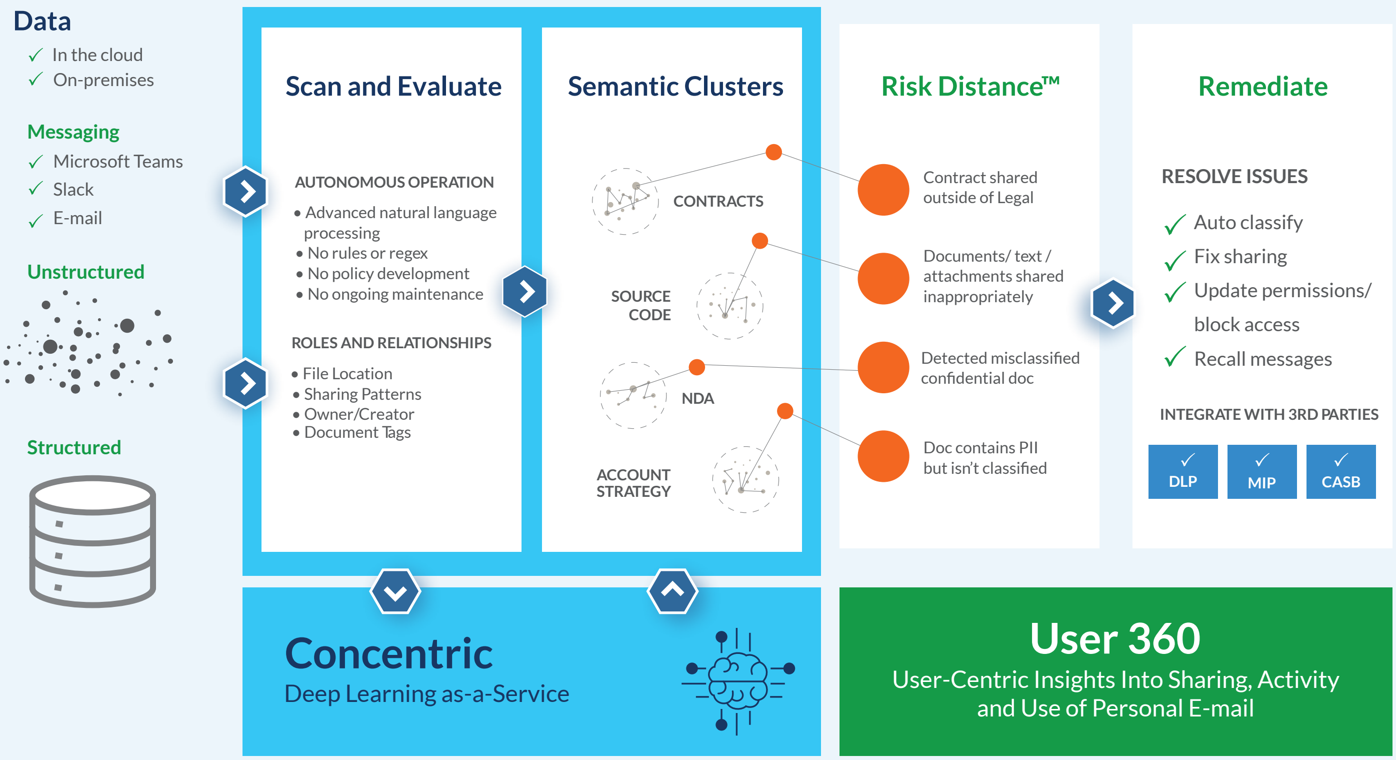
USER 360



Gain Insights Into User Behavior

Architecture

Concentric Semantic Intelligence™ Solution



Data

- ✓ In the cloud
- ✓ On-premises

Messaging

- ✓ Microsoft Teams
- ✓ Slack
- ✓ E-mail

Unstructured

Structured

Scan and Evaluate

AUTONOMOUS OPERATION

- Advanced natural language processing
- No rules or regex
- No policy development
- No ongoing maintenance

ROLES AND RELATIONSHIPS

- File Location
- Sharing Patterns
- Owner/Creator
- Document Tags

Semantic Clusters

CONTRACTS

SOURCE CODE

NDA

ACCOUNT STRATEGY

Risk Distance™

- Contract shared outside of Legal
- Documents/ text / attachments shared inappropriately
- Detected misclassified confidential doc
- Doc contains PII but isn't classified

Remediate

RESOLVE ISSUES

- ✓ Auto classify
- ✓ Fix sharing
- ✓ Update permissions/ block access
- ✓ Recall messages

INTEGRATE WITH 3RD PARTIES

✓ DLP ✓ MIP ✓ CASB

Concentric

Deep Learning as-a-Service

User 360

User-Centric Insights Into Sharing, Activity and Use of Personal E-mail

Broad Connectivity

Concentric Semantic Intelligence offers API connectivity to securely scan unstructured data wherever it's stored: on-premises, in the cloud, in email or on messaging platforms.

We support Office365, Slack, Microsoft Teams, e-mail, Amazon S3, OneDrive, Google Drive, Box, Dropbox, SharePoint Online, Windows file shares, PostgreSQL, MySQL, and more (click here for current list). Continuous autonomous monitoring ensures your data is constantly protected and compliant.

Office 365
DELL EMC
Dropbox
Microsoft SQL Server
box
MySQL
ORACLE DATABASE
PostgreSQL
Windows Server
NetApp
NUTANIX
slack
Teams
Exchange

About Concentric

Venture funded by top Silicon Valley VCs

A secure SaaS solution, API driven

SOC 2 Type 2 certified

Gartner COOL VENDOR 2021

2021 FINALIST SCawards Rookie Security Company of the Year

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2021

Try Concentric using your own data. Contact us today for a free risk assessment and we'll help you plan your next data privacy move.

Visit our web site | Read our blog | Request a demo | Send us an email