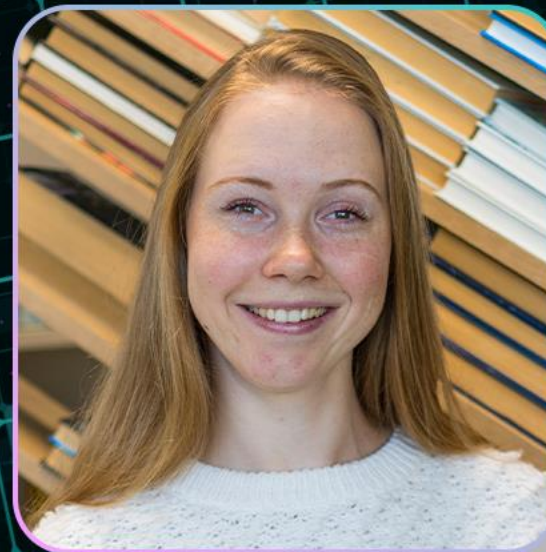




**SECURITY
DAYS**

5 INSIDER RISK BLIND SPOTS YOUR LEGACY DLP CAN'T SEE



DARIYA MINX
Safetica Sales Engineer



DARIO TAVERI
Safetica Sales Director
EMEA/APAC

safetica

It's Not Always a Hacker — Most of the Time It's Just a Normal Tuesday

September 2026

ESET Security Days

5 Insider Risk Blind Spots that your Policy-based DLP Can't See



Data shared with AI tools

Source code and PII pasted into ChatGPT and more



Departing employees taking data

Records and IP leaving during a notice period



Abnormal after-hour access

Late-night activity that looks like real work



Privileged user misuse

Access into finance, HR or personnel files

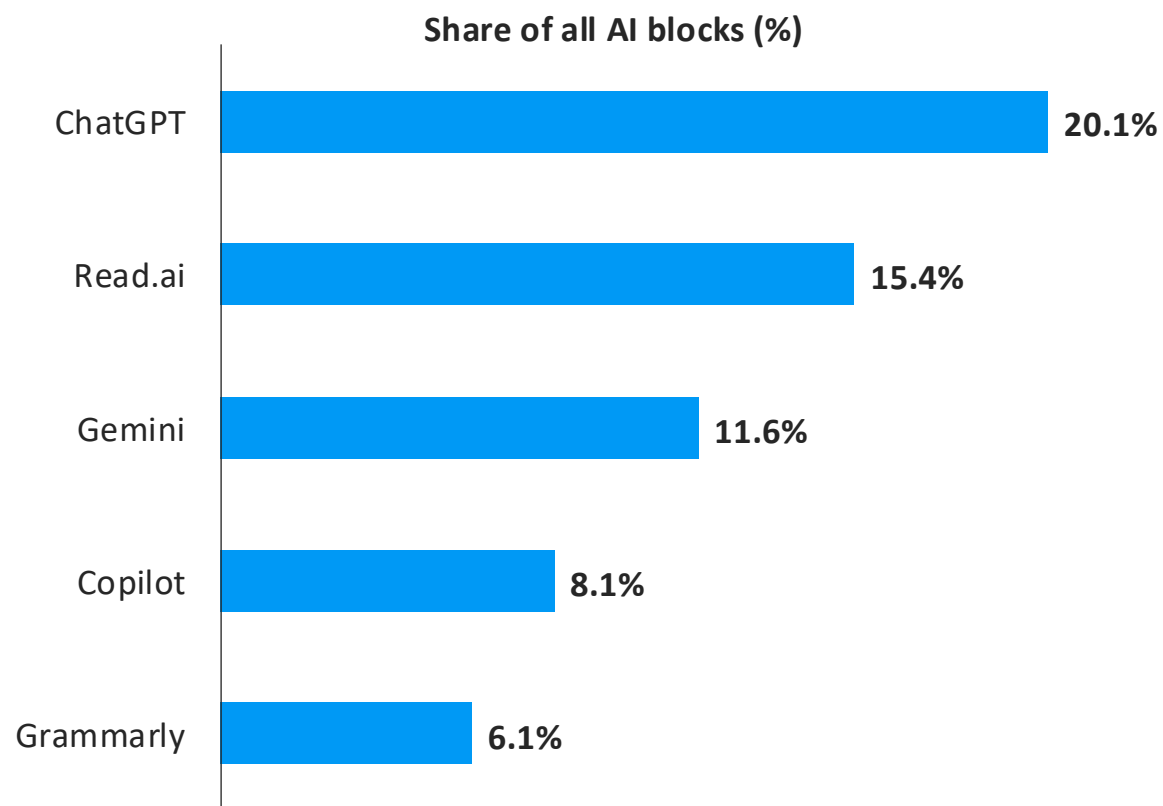


Gradual data exfiltration

Small, repeated transfers under set thresholds

AI use is exploding, and so is data exposure

Top AI tools blocked: H2 2025*



20.1%

of all blocked AI activity was ChatGPT, ahead of Gemini, Copilot and a dozen more tools

CUSTOMER USE CASE

Regional healthcare provider

Found staff pasting patient PII into public AI tools. With Safetica, they had full visibility in days and applied controls, without blocking the tools clinicians rely on.

*Source: Safetica H2 2025 Data Protection Trends Report

Stopping data theft by a departing employee

Manufacturer | employee resigned, then began moving sensitive sales data

Resigned, gave two-week notice

Began exfiltrating sales data

Caught and removed early

WHAT WAS AT STAKE

- Lost business and competitive theft
- Eroded customer trust
- Exposed PII and payment data

HOW SAFETICA HELPED

Behavioral analytics flagged the abnormal data movement, giving the team the context to act before the employee's final day.

Insider risk is normal, common and expensive*

NORMAL

91%

of insider breaches are non-malicious

COMMON

57%

of organizations hit by insider incidents

EXPENSIVE

\$17.4M

average annual cost of insider events

**Sources: IBM Cost of a Data Breach 2025; Gartner, Treat Insider Risk as Human Risk, 2026*

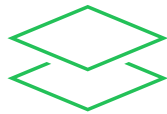
Four things DLP alone can't do

Other tools stop at DLP. Safetica adds the behavior layer they miss with IRM & DLP.



Catch it early

Spot risky behavior before data leaves



Full context

Context on every case: error, compromise, malice



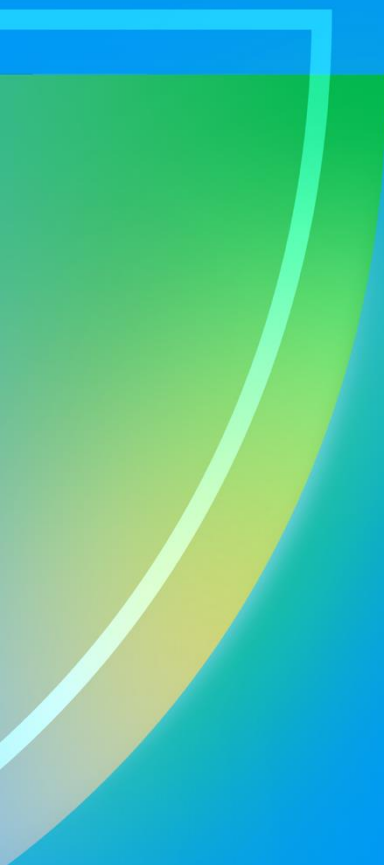
Fewer false alarms

Fewer false positives and less alert fatigue



Faster response

Faster, more accurate incident response



The Safetica approach

Safetica's 4 Pillars of Intelligent Data Security

Content and Contextual Awareness

Data Protection



Visibility of sensitive data

Insider Risk & User Behavior



Stay ahead of insider risks

Compliance & Data Discovery



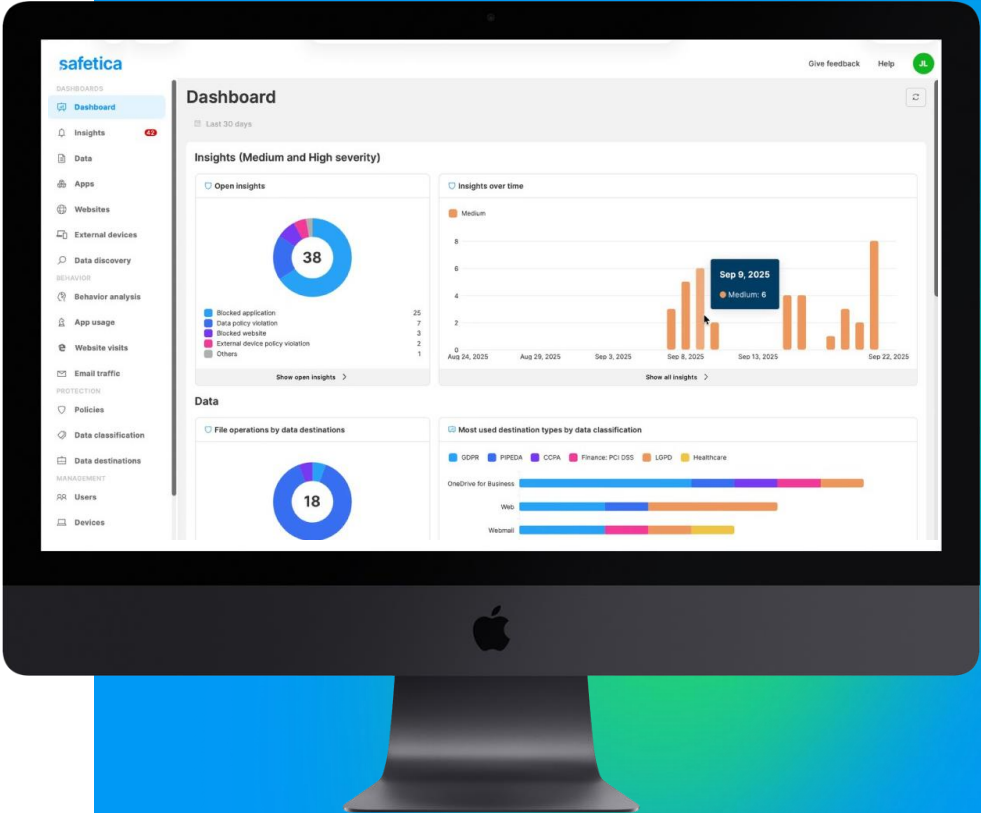
Discover, control, and ensure compliance

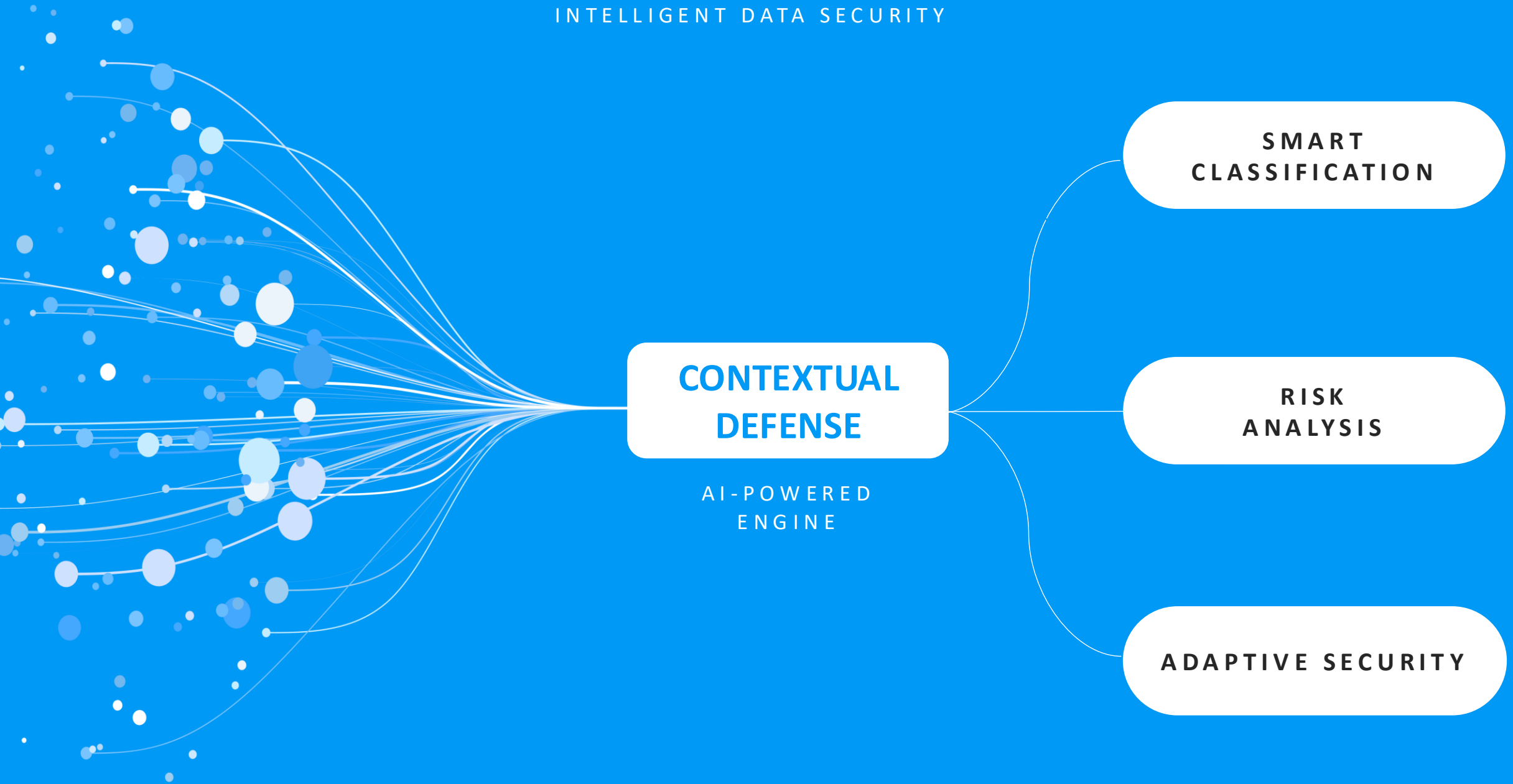
Cloud Security



Secure sensitive cloud-based data

Intelligent Data Security in a Single, Unified Platform





CONTEXTUAL DEFENSE

AI-POWERED ENGINE

SMART
CLASSIFICATION

RISK ANALYSIS

ADAPTIVE
SECURITY

Reduce False Positives Through Contextual Insights



Adaptive learning continuously learns what “normal” looks like to **accurately detect** sensitive data.

Context-aware analysis examines file origin, metadata, and third-party labels—**reducing false alerts**.

CONTEXTUAL DEFENSE

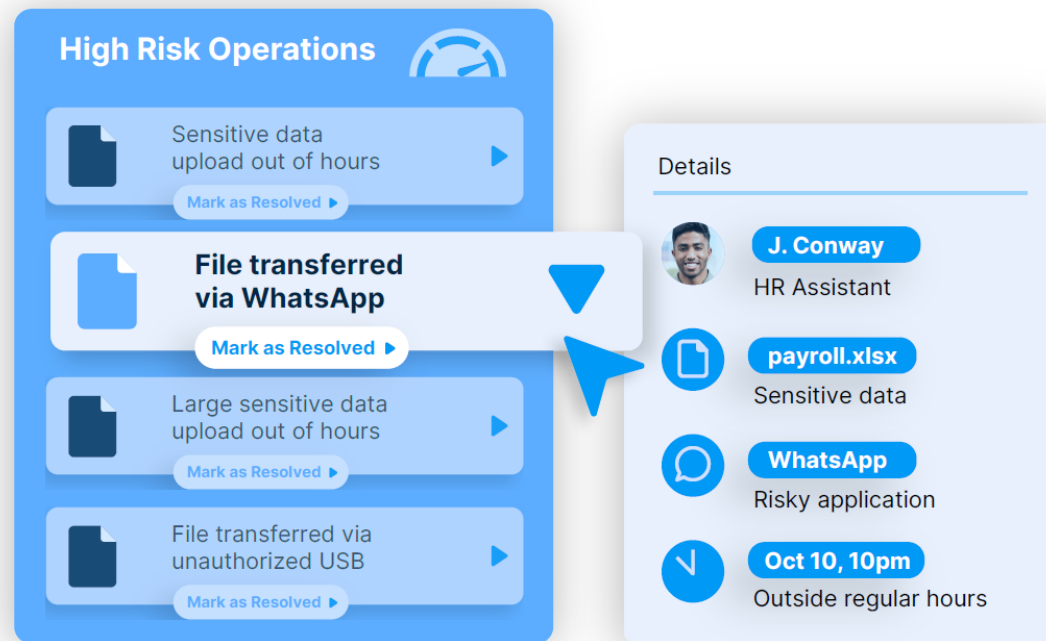
AI-POWERED ENGINE

SMART
CLASSIFICATION

RISK ANALYSIS

ADAPTIVE
SECURITY

Banish Alert Fatigue with Risk Scoring



Contextual risk scoring analyzes data in real-time, evaluating factors like time of day, destination, and transfer method to **detect high-risk behavior early**.

Proactive alerts **prioritize real threats** and cut noise **reducing alert fatigue by 83%**—keeping security teams focused on real threats.

CONTEXTUAL DEFENSE

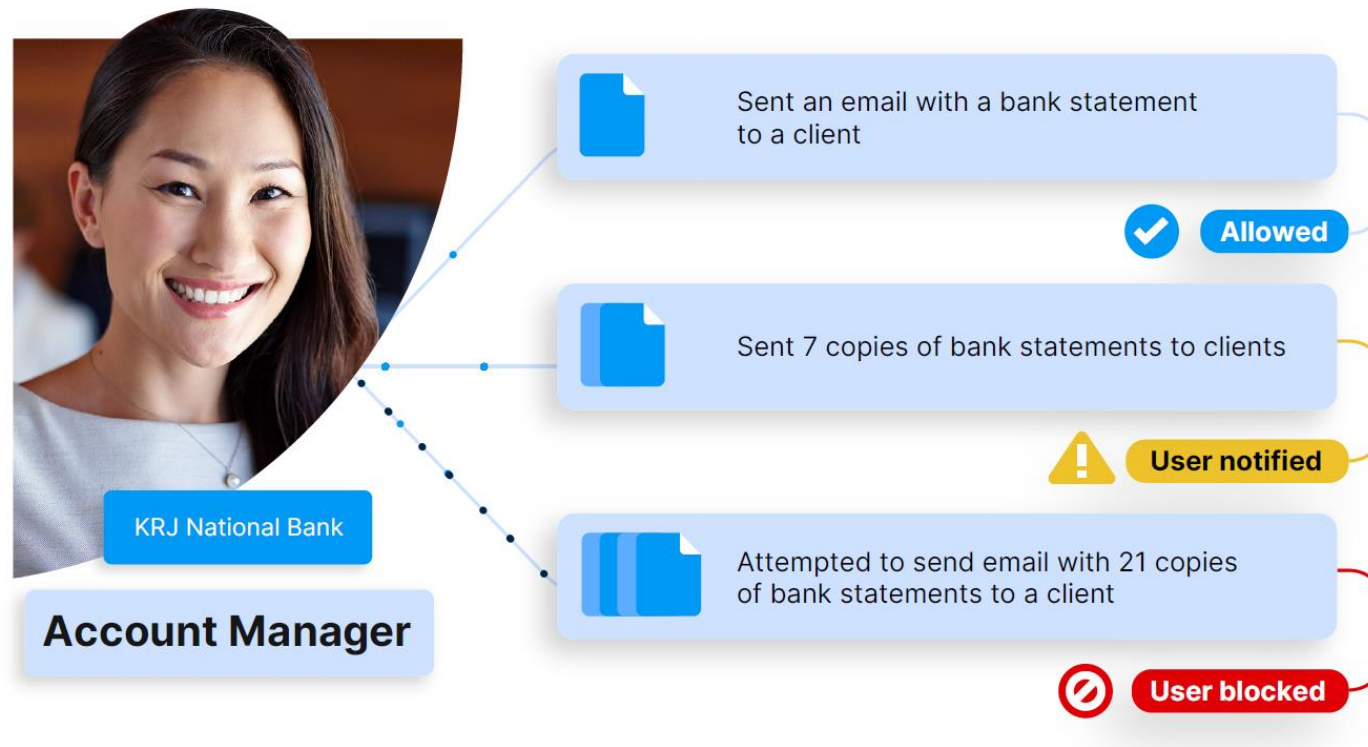
AI-POWERED ENGINE

SMART
CLASSIFICATION

RISK ANALYSIS

ADAPTIVE
SECURITY

Block Dangerous Activity Through Adaptive Defense



Dynamic policies continuously adapt to new threats and unusual behavior, applying risk-scored protection **without disrupting work**.

High-risk actions are blocked, while routine tasks continue uninterrupted—ensuring security **without slowdowns**.

Which Safetica Solution is Right For You?



Safetica Intelligent Data Security Platform

Best for organizations that:

- Operate in highly distributed, cloud-first environments
- Want lower upfront cost: no hardware or server management
- Need fast deployment and time to value
- Require scalable security that grows with the business
- Prefer built-in AI automation to reduce manual effort
- Benefit from automatic updates and maintenance



Safetica On-Prem

Best for organizations that:

- Operate in highly regulated industries with strict compliance requirements
- Cannot host security solutions in the cloud
- Have established, dedicated IT and security teams
- Prefer to maintain local infrastructure or their own data center
- Require full control over data location and storage

AI data protection — new in the autumn 2026 release

See every AI in use

- Approved and shadow AI tools in one dashboard
- Who uses them, how often, and what data is shared
- Where protection is already in place

Protect data before it reaches AI

- DLP for ChatGPT Classic, Claude, and Microsoft Copilot (including their web interfaces)
- Covers files, pasted content, and prompts
- Different policy for personal vs. business accounts
- Desktop apps and Chromium browsers, Windows and macOS

Investigate with AI on your side

- AI chatbot in the console to answer questions and guide investigations
- Model Context Protocol (MCP) access, so your tools can talk to Safetica



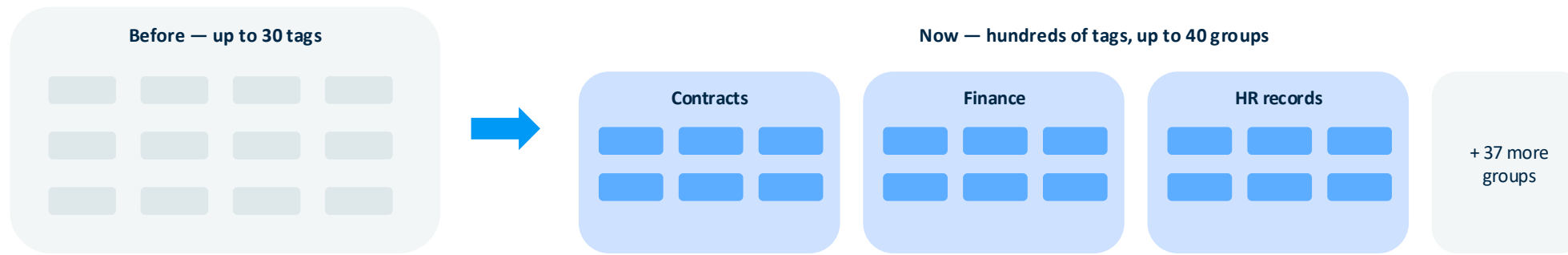
AI classification: hundreds of tags, kept manageable

Far broader coverage

- Until now AI classification generated up to 30 tags — now it surfaces hundreds
- Tags are grouped into up to 40 meaningful categories, with drill-down to the tags underneath
- Improved tag-creation algorithm raises coverage and accuracy

Refresh on demand

- Refresh AI tags at any time, so classification keeps up as data changes
- Used tags are kept and improved; unused tags are removed
- Tags get better with every cycle



Illustrative — group names come from the customer's own data

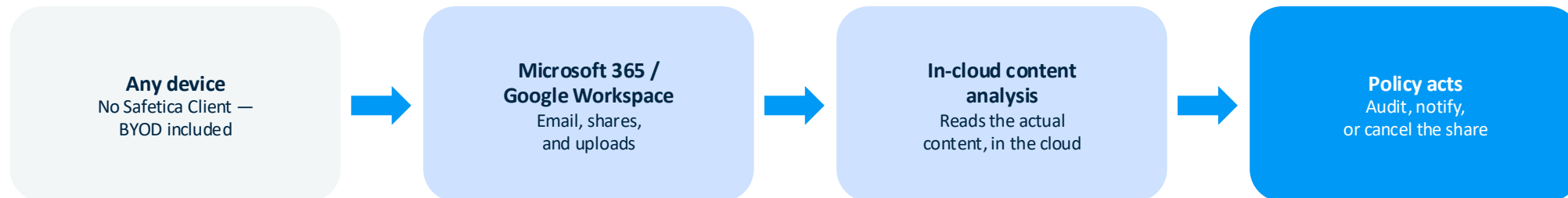
Cloud protection: content analysis, Google Drive GA

In-cloud content analysis

- Reads email bodies, subjects, attachments, and shared files directly in the cloud
- Content-based policies work with no client on the device — including BYOD

Google Drive protection

- Now in general availability, with enhanced coverage
- Audits every sharing and upload operation, and classifies by content with in-cloud analysis
- Recognizes safe and untrusted destinations
- Safetica's Google Workspace app is officially verified by Google



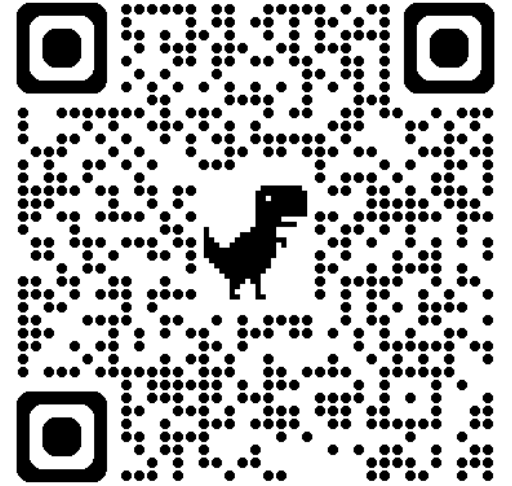
Don't miss out – lock Your Safetica trial for 30 days today!

Thank you!

Contact person for our local Distributor, “NOD Baltic”, UAB:
Andrius Mickevičius (CSO)
andrius@nodbaltic.com

+370 699 10 788

[NOD Baltic - IT sprendimai](#)



Check out reviews on [G2.com](https://www.g2.com)