SECURITY BEYOND ACCESS

Fryqua puts identity, access and user behaviour into context to enable better security decisions.



Fryqua Executive Positioning Paper | 2026

FRYQUA.COM | 2026

1. Executive summary

The risk you can't see has already gained access.
Imagine this scenario: an employee logs in correctly using MFA. Within twenty minutes, the account opens files in locations it has never accessed before, shortly after permissions were modified. Your security systems see nothing amiss. The login was valid. The permissions were, too.

> "What actually happens once access has been granted?"

The blind spot
You have invested in front-line security solutions: IAM and MFA, EDR/XDR, and SIEM. Yet these systems treat a compromised account, human error, or outdated permissions as normal activity. The warning signs are there, but they are scattered across different systems. Anyone trying to figure out what happened has to start piecing the puzzle together while the clock is ticking.

What Fryqua does
Fryqua is the security intelligence layer linking identity, access and user behaviour. The platform brings together three questions in a single view:

- Identity: who is this user and what has changed recently?
- Access: what permissions do they have, and do they still need them?
- Behaviour: Is what they are doing consistent with their role, background and the situation?

Not an extra stream of alerts, but substantiated cases on which your team can make immediate decisions.

The benefits for you
- Faster investigations: the context is readily available rather than scattered across different systems.
- More precise access reviews: access rights are evaluated based on actual usage, not just on what was originally granted.
- Demonstrable accountability: you can show why a risk was investigated, mitigated, or accepted.

Without relinquishing control
Fryqua complements your existing security stack rather than replacing anything. The platform runs on-premises or in a hybrid environment, requires no internet connection, and keeps your data within your environment.

Not just a promise on paper
We demonstrate it in your own environment. We jointly define the research questions and success criteria beforehand. A proof of value then reveals the context Fryqua provides, context that is currently missing from your operations.

Table of contents

Subject	Page
1. Executive summary	1
2. The blind spot after access	3
3. What does Fryqua do?	4
4. Three interconnected intelligence capabilities	5
5. Fryqua complements existing security	6
6. Specific security issues	7
7. For which organisations is Fryqua relevant?	8
8. From insight to business value	9
9. Architecture and security under your control	10
10. From signals to intelligent security	11
11. Demonstrable value	13

2. The blind spot after access

Most security controls are designed to secure access. Once access has been successfully granted, other questions remain:

- Are the granted rights still necessary?
- Is access being used as expected?
- Has user behaviour changed suddenly?
- Do identity, access, and activity signals correlate?
- Which activity warrants investigation first?

This is not exclusively an insider threat issue. Risk can also arise from human error, excessive privileges, outdated access rights, misuse of valid credentials, compromised accounts, or changing behaviour patterns.

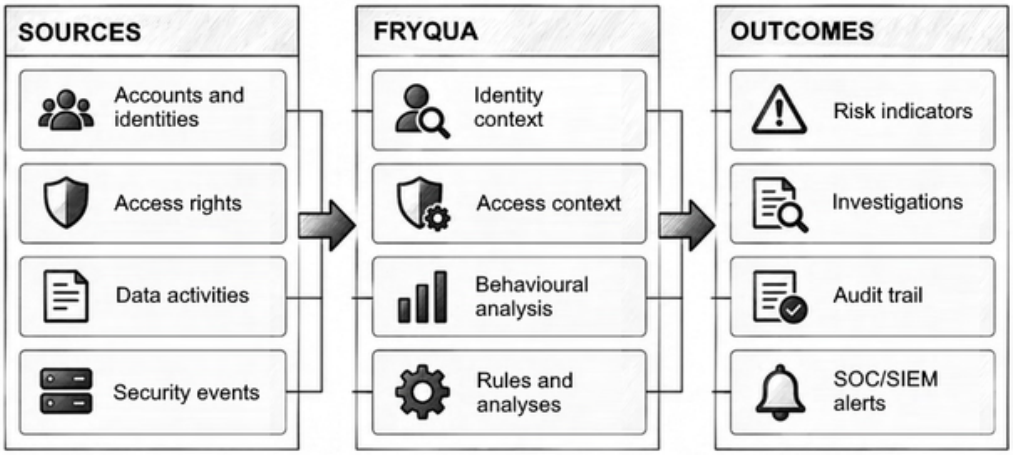
Access determines what someone can do. Authentication and MFA confirm identity. IAM and IGA manage access grants. EDR/XDR detects technical threats, SIEM correlates events, and SOC/MDR investigates incidents.

Fryqua focuses on the hidden risks associated with valid access. By continuously analysing user behaviour and linking it to identity and permissions, it surfaces anomalies that would otherwise remain hidden across systems. This way, Fryqua reduces a security blind spot and enables the organisation to make decisions based on facts rather than assumptions.



3. What does Fryqua do?

Fryqua is a specialised security analytics platform that combines identity, access rights and user behaviour to identify meaningful anomalies and provide actionable insights for investigation, risk assessment and decision-making.



Firgure 1. From scattered data to coherent context and actionable outcomes

Fryqua collects, records and analyses relevant data, account and access activities, and consolidates them into dashboards, audit trails and ready-to-use cases. Advanced rules and analytics translate events into actionable insights. This enables security teams to identify risks in a timely manner and mitigate them effectively.

Relevant alerts can be integrated with existing SOC and SIEM solutions, enabling Fryqua to complement rather than replace existing security controls.
The product architecture supports agent-based monitoring, a central Fryqua server and integration with Active Directory and Entra ID. The collected information can support dashboards, reports, audit trails, and existing monitoring processes. Fryqua can be deployed on-premises or in hybrid environments and does not require an internet connection.

At the heart of Fryqua is the linking of identity, access rights and user behaviour, making existing data more meaningful for investigation and risk assessment.

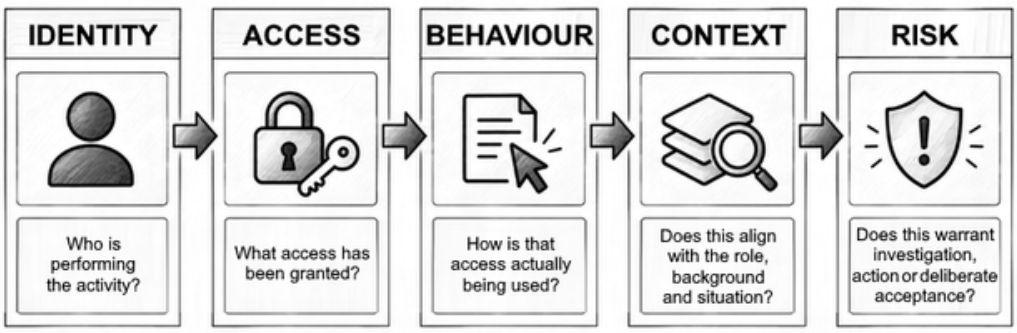


Figure 2. From identity to risk: assessing access in context

4. Three interconnected intelligence capabilities

Identity & Access Intelligence
Provides visibility into accounts, roles, access rights, changes and actual usage. The focus shifts from ‘who has access?’ to ‘why does that access exist and how is it being used?’

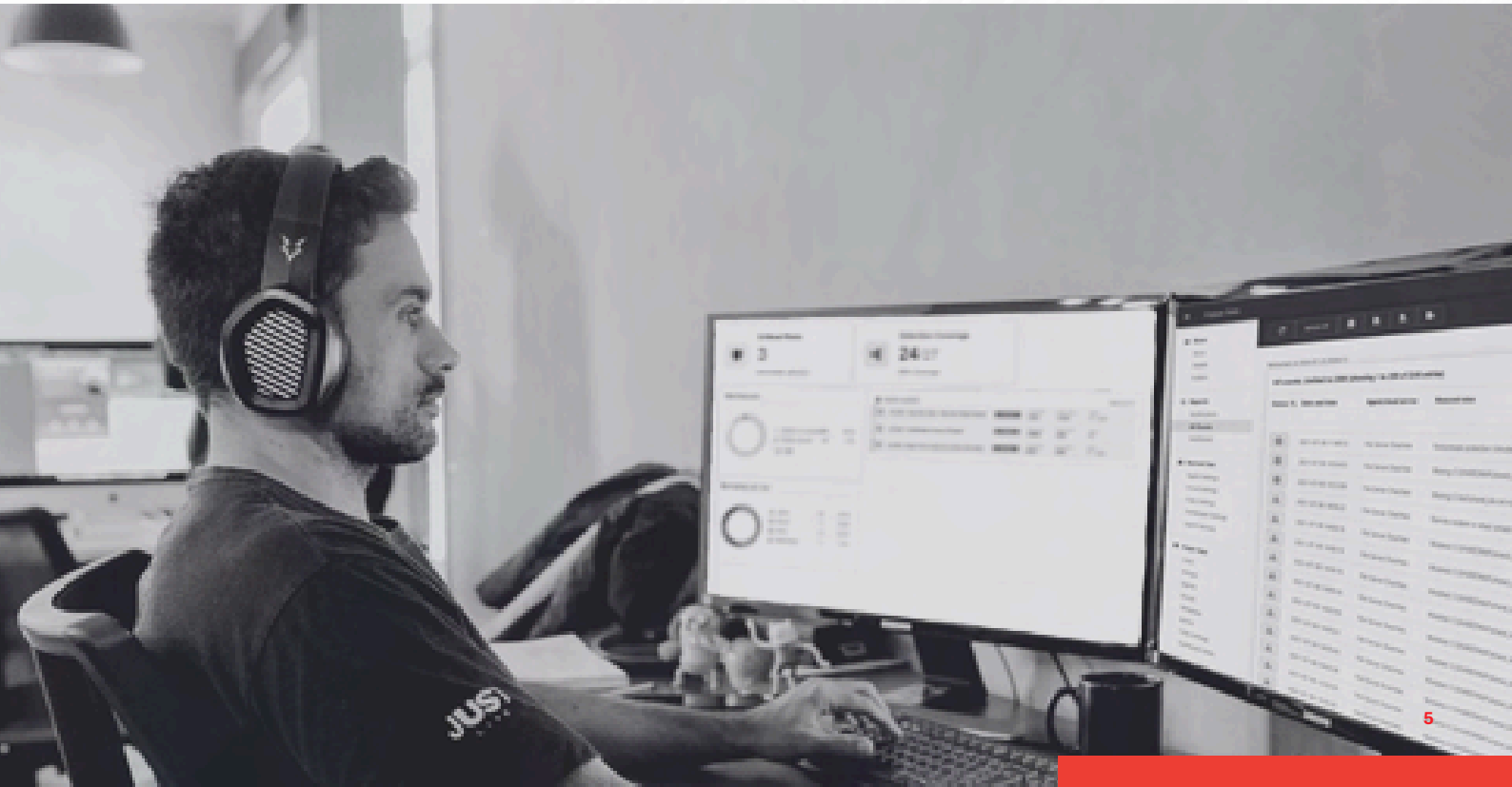
User Anomaly Detection
Identifies behaviour that deviates from usual patterns or from predefined risk rules. An anomaly is not an incident, but a signal that may warrant further investigation and additional context.

Advanced Security Analytics
Transforms disparate events relating to user, account, access and activity information into a single, coherent picture, making anomalies and risks visible so they can be addressed in a targeted manner.

How does it work?
Fryqua uses our neural networks to build up a picture of normal behaviour for each user (and for each role or group), based on historical activity within their own environment over a specific period. The models run entirely locally on the Fryqua server, and no data leaves the environment.

An anomaly does not automatically trigger an alert. It is first evaluated against access rights, recent account changes and the configured rules. Security teams can adjust thresholds and mark anomalies as legitimate, reducing false positives.

The strength lies in the combination. Only when access rights, behavioural anomalies and analysis come together does it become clear whether an activity aligns with the user and the situation.



5. Fryqua complements existing security

Fryqua specialises in the areas of identity, access and user behaviour, and complements the existing security stack.

Category	Key question	Areas of strength	Where Fryqua adds value
FRYQUA.com	How is valid access actually used, and does this fit the context?	Context relating to the user, permissions and activity	Specialised in sights for investigation and risk assessment
SIEM (Security Information and Event Monitoring)	What security events do we see?	Comprehensive logging, search and detection	Targeted context model for identity, access and behaviour
IAM (Identity & Access Management) / **IGA** (Identity Governance & Administration)	Who should have access?	Provisioning, roles and reviews	Actual use of granted access
UEBA (User and Entity Behaviour Analytics)	What behaviour is out of the ordinary?	Static and behavioural anomalies	Links anomalous behaviour to access rights and activity context.
EDR (Endpoint Detection & Response) / **XDR** (Extended Detection & Response)	Which technical signals indicate a threat?	Endpoint, workload and threat detection and response	User and access context relating to the observed activity
DLP (Data Loss Prevention) / Data Security	What happens to sensitive data?	Protection, classification and monitoring of data usage and movement	Put data activity into the context of the user, account and access rights

Figure 3. Primary focus per solution

Fryqua adds a detailed research perspective: examining how access is actually used, and ensuring that existing data becomes more meaningful for research and for assessing that behaviour.

Our added value lies in targeted intelligence within this specific risk domain. Fryqua combines data relating to identity, access and actual user behaviour into a single, coherent picture, which helps to investigate and assess risks associated with valid access.

6. Specific security issues

We instantly reveal what's currently invisible and turn complex security issues into a single, coherent picture. Where others stop, Fryqua sees what is really happening.

1. Sudden anomalies in data usage
A user accesses significantly more files or other locations than usual within a short period of time. Fryqua links this activity to the user's identity, account and assigned access rights.

2. Excessive access rights
An account has access rights that are technically valid but are rarely used or no longer align with the current role. This supports access reviews and the principle of least privilege.

3. New permissions, immediately put to use
An account receives modified or additional permissions and uses them shortly thereafter for relevant data activities. Fryqua links account changes, access and activity into a single, coherent overview.

4. Account misuse or compromised identity
A valid account exhibits behaviour inconsistent with previous or expected usage patterns. Authentication remains valid, but the behaviour warrants further investigation.

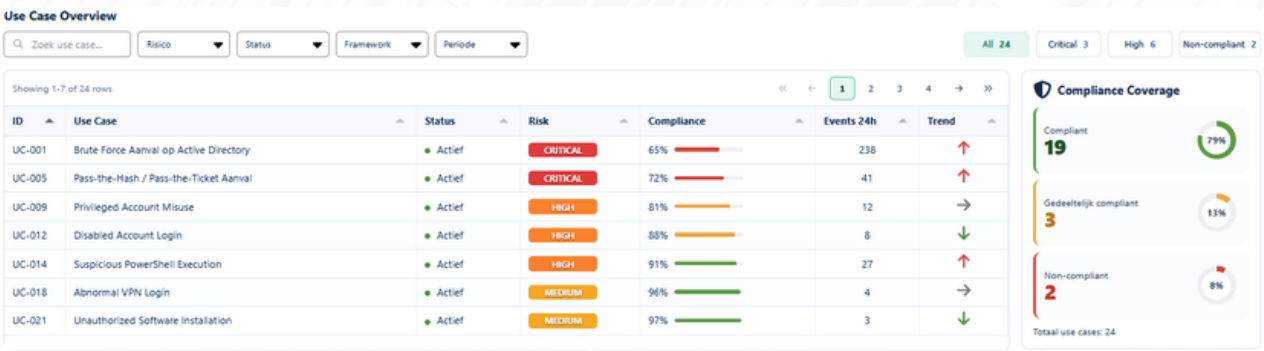
5. Unusual changes or encryption
Large numbers of files are modified or encrypted within a short period of time. Rules and monitoring can trigger an alert and halt the action.

6. Audit and reconstruction
After an incident, you need to establish who did what and when. By continuously monitoring the audit trail and associated account and activity data, Fryqua supports reconstruction and accountability.

7.Business-specific and customer-specific challenges
In addition to standard risk patterns, Fryqua addresses specific, client-defined security and compliance issues. No matter how complex or unique your internal business processes or governance rules may be: as soon as the necessary source data is available, we reliably map out the required logic and risks.

Fryqua does not treat every deviation as an incident. The goal is to make relevant signals visible and open to investigation, enabling informed decisions.

Figure 4. Fryqua Use Case Dashboard



7. For which organisations is Fryqua relevant?

Fryqua is particularly relevant for organisations that handle sensitive or business-critical data, have complex access structures and manage various user roles.

This applies to organisations that want to rebuild the link between identity, access, and actual user behaviour. This is possible in on-premises, Windows/Linux and hybrid environments.

Fryqua provides specialist analytical capabilities that help organisations gain faster insight into how access rights are actually being used, investigate unusual behaviour and provide a more robust basis for access reviews.

Where IAM, endpoint or SIEM solutions are already in place, Fryqua integrates with them and consolidates the available signals into a single view of what is actually happening, enabling organisations to make informed decisions.



Target markets

SMEs
Practical insight into access rights, user behaviour, and anomalies in the IT environment, without needing a large, specialised security team.

Healthcare
Insight into how sensitive patient information is accessed and whether that approach is consistent with the patient's identity, rights and context.

Government
Supports monitoring and auditability for compliance and investigations into access to sensitive or critical information.

Education
From students and staff to researchers and temporary accounts: Fryqua shows what actually happens with access rights.

MSP / MSSP
The responsibility lies with your customer. The expectations rest with you. Customers must be increasingly able to demonstrate who has access, what permissions have been granted and what is happening. With Fryqua, you can not only manage these aspects, but also provide demonstrable proof.

Hybrid environments
Fryqua is designed for environments where various networks, locations and technologies converge: on-premises, cloud, managed services, and even networks without a direct internet connection.

The best fit depends on the nature of the environment and the security question you want to address, not the sector or size.



8. From insight to business value

By bringing together signals, identity, access and behaviour, it becomes clear what is actually happening and what action is required. Fryqua sees what others miss.

1. Automated reconstruction
Relevant identity details, access rights and activities are automatically collated and then compared and assessed using neural networks.

2. More robust access reviews
Assessing not only which rights exist, but also how they are actually being used.

3. Trend analysis
Continuously highlights changes, anomalies, and trends that would otherwise be difficult to detect.

4. Improved manageability
Demonstrating why a risk has been investigated, mitigated or accepted.

5. Ensuring business continuity
Gaining an earlier understanding of which situations actually require attention helps organisations to prioritise and act more consciously.

6. Compliance is not a product feature.
Fryqua supports compliance and provides insight and evidence, whilst responsibility for policy, processes and measures remains with the organisation.

9. Architecture and security under your control

For organisations, it matters not only what insights a solution provides, but also how it collects, processes, and manages data. Especially when dealing with sensitive user, access and activity data, control over the technical architecture is a key part of the decision-making process.

Fryqua is therefore designed based on the principle that organisations retain control over their own data and infrastructure:

- A central Fryqua server processes, analyses and presents the collected information.
- Fryqua can be deployed on-premises and or in hybrid environments.
- The Fryqua server can operate entirely within the organisation's own IT environment, without an internet connection.
- The organisation retains control of the storage and use of data and log files.
- Fryqua has no permanent or hidden access to the environment and requires explicit
- customer authorisation.
- Relevant alerts can be easily integrated with external applications, including existing SOC and SIEM solutions.
- Agent-based monitoring collects relevant activity data close to the source.

> "Security intelligence must generate greater insight without relinquishing control over data."

The exact technical configuration is tailored to the environment and the release being used.

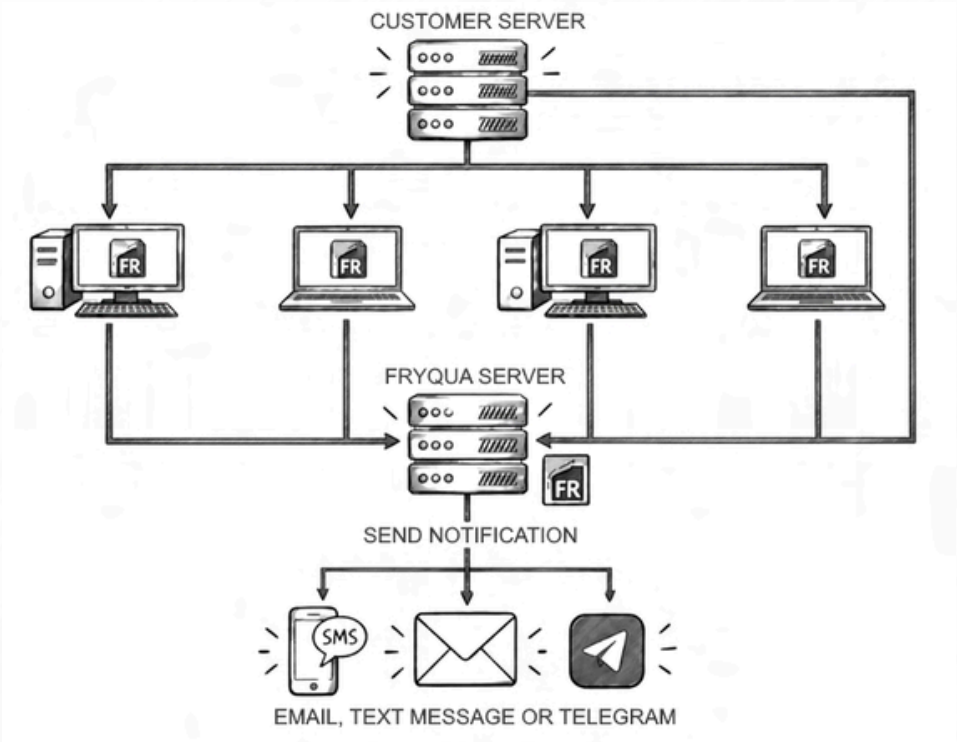


Figure 5. Simplified architectural overview of Fryqua

10. From signals to intelligent security

An isolated signal often conveys little information. Value emerges when identity, access, changes and actual behaviour are assessed together.

Fryqua connects various disparate signals and evaluates them from multiple perspectives. In this way, it examines who the user is, what access they have, what has recently changed, and their actual behaviour, all in context. This provides insight into whether a user's behaviour is consistent with their role and the situation in question.

This shifts the focus from isolated signals and rights to a perspective that enables better security decisions.

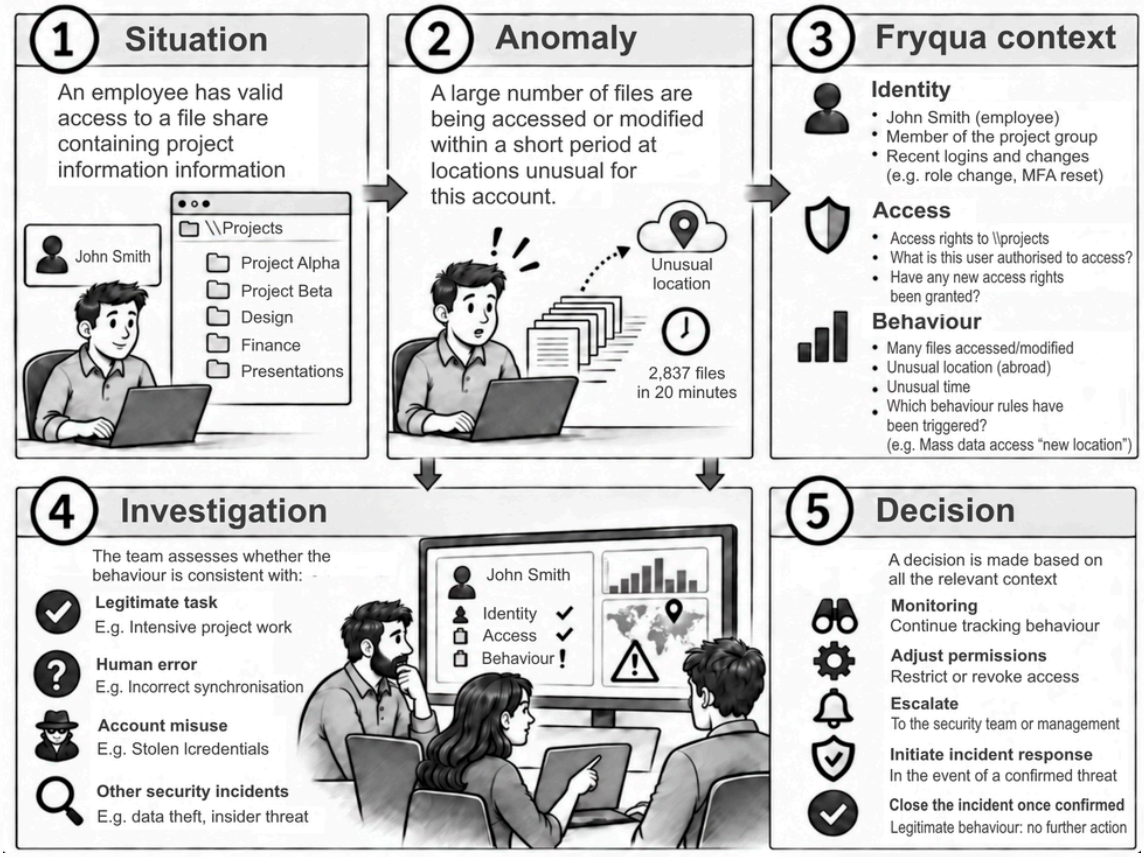


Figure 6. Example of intelligent security

Example scenario

An employee has valid access to project information. Within a short period of time, there is a sharp spike in file activity at locations that are unusual for this account. At the same time, a permission has recently been changed. None of these indicators needs, on their own, to constitute an incident. Taken together, however, they do raise a relevant question for investigation.

By bringing together signals, identity, access and behaviour, it becomes visible what is actually happening and what action is required,even when the individual signals, scattered across systems, would otherwise go unnoticed.



10.1. Why context makes all the difference

Security teams face vast amounts of signals, while time and expertise are in short supply. When identity, access and activity information is spread across multiple systems, every investigation starts with gathering and piecing that information together.

Fryqua brings all these elements together. This not only provides insight into what is happening, but, above all, into what the activity means in this specific situation.

This brings three benefits for the organisation:

Less noise: signals are assessed in conjunction rather than solely as isolated events.

Faster insights: investigations start with the user, the account, the permissions and the relevant activity.

Improved prioritisation: monitoring, adjusting access, escalation or incident response can be based on verifiable context.

Fryqua's positioning therefore goes beyond traditional access monitoring. Fryqua links identity, access and user behaviour to help determine the appropriate action based on the actual risk.



11. Demonstrable value

Why Fryqua?

- A specialised focus on risks associated with valid access.
- Insight into how granted permissions are actually being used.
- Users, accounts, access and activity, all viewed from a single investigative perspective.
- Additional context alongside existing IAM, SIEM, EDR/XDR, UEBA and DLP investments.
- Fryqua sees what others miss.

Demonstrating value in practice

We work with you in advance to identify key research questions and the success criteria Fryqua must meet.

Access Intelligence
Can unused, conspicuous or potentially excessive access rights be made visible and better justified?

Unusual user behaviour
Are there any relevant behavioural anomalies that warrant further context or investigation?

Research and analysis
Which identity, access and activity contexts no longer need to be consolidated from multiple systems?

Integration with the existing environment
How does Fryqua integrate with existing SOC, SIEM and identity processes, and what management effort does this require from the organisation?

The aim is not to generate as many alerts as possible, but to demonstrate the additional security context that Fryqua provides in your environment.



Fryqua
Dorsvloer 15
9205 BN Drachten
The Netherlands

T: +31 (0)512 54 84 84
E: info@fryqua.com
www.fryqua.com

This document is provided for information purposes only. No rights may be derived from its contents.
Copyright © 2026 Fryqua.com. All rights reserved.