SECURITY VOORBIJ DE TOEGANG

Fryqua plaatst identiteit, toegang en gebruikersgedrag in context voor betere securitybeslissingen.



Fryqua Executive Positioning Paper | 2026

FRYQUA.COM | 2026

1. Managementsamenvatting

Het risico dat u niet ziet, heeft al toegang.
Stel: een medewerker logt correct in met MFA. Binnen twintig minuten opent het account bestanden op locaties waar het nog nooit eerder was, kort nadat de rechten zijn gewijzigd. Voor uw securitysystemen is er niets aan de hand. De inlog was geldig. De rechten ook.

> “Wat gebeurt er daadwerkelijk nadat toegang is verleend?"

De blinde vlek
U heeft geïnvesteerd in beveiligingsoplossingen voor de voordeur: IAM en MFA, EDR/XDR en SIEM. Maar een gestolen account, een menselijke fout of verouderde rechten zien er voor die systemen uit als normaal werk. De signalen bestaan wel, maar liggen verspreid over verschillende systemen. Wie wil weten wat er is gebeurd, begint met puzzelen, terwijl de tijd doortikt.

Wat Fryqua doet
Fryqua is de security-intelligentielaag tussen identiteit, toegang en gebruikersgedrag. Het platform brengt drie vragen samen in één beeld:

- Identiteit: wie is deze gebruiker en wat is er recent veranderd?
- Toegang: welke rechten heeft hij, en heeft hij die nog nodig?
- Gedrag: past wat hij doet bij zijn rol, zijn achtergrond en de situatie?

Geen extra stroom aan alerts, maar onderbouwde casussen waarop uw team direct kan beslissen.

Wat het u oplevert
- Sneller onderzoek: de context staat klaar in plaats van verspreid over systemen.
- Scherpere access reviews: rechten worden beoordeeld op daadwerkelijk gebruik, niet alleen op wat is toegekend.
- Aantoonbare verantwoording: u kunt laten zien waarom een risico is onderzocht, gemitigeerd of geaccepteerd.

Zonder de regie uit handen te geven
Fryqua vult uw bestaande securitystack aan en vervangt niets. Het platform draait on-premises of hybride, vereist geen internetverbinding en uw data verlaat uw omgeving niet.

Geen belofte op papier
Wij tonen het aan in uw eigen omgeving. Vooraf bepalen we samen de onderzoeksvragen en de succescriteria. Een proof of value laat daarna zien welke context Fryqua oplevert die u vandaag mist.

Inhoudsopgave

Onderwerp	Pag.
1. Managementsamenvatting	1
2. De blinde vlek na toegang	3
3. Wat doet Fryqua?	4
4. Drie samenhangende intelligence-capabilities	5
5. Fryqua vult bestaande security aan	6
6. Concrete securityvraagstukken	7
7. Voor welke organisaties is Fryqua relevant?	8
8. Van inzicht naar bedrijfswaarde	9
9. Architectuur en security onder eigen regie	10
10. Van signalen naar intelligente security	11
11. Aantoonbare waarde	13

2. De blinde vlek na toegang

De meeste securitycontroles zijn ontworpen om de toegang te beveiligen. Zodra toegang succesvol is verleend, blijven andere vragen over:

- Zijn toegekende rechten nog noodzakelijk?
- Wordt toegang gebruikt zoals verwacht?
- Verandert gebruikersgedrag plotseling?
- Hangen identity-, access- en activiteitssignalen met elkaar samen?
- Welke activiteit verdient als eerste onderzoek?

Dit is niet uitsluitend een insider-threatvraagstuk. Risico kan ook ontstaan door menselijke fouten, overmatige privileges, verouderde rechten, misbruik van geldige credentials, gecompromitteerde accounts of veranderend gebruik.

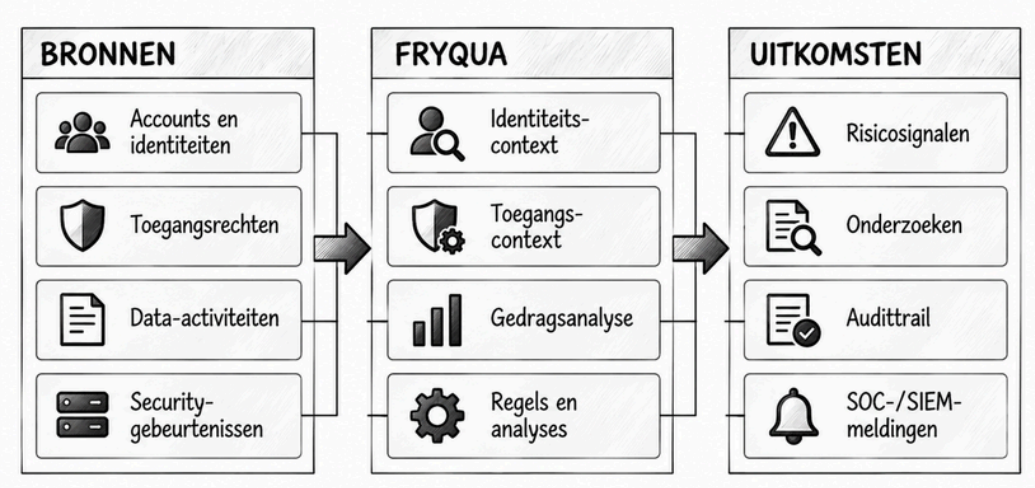
Toegang bepaalt wat iemand kan doen. Authenticatie en MFA bevestigen de identiteit. IAM en IGA beheren wie toegang mag krijgen. EDR/XDR detecteert technische dreigingen, SIEM correleert events en SOC/MDR onderzoekt incidenten.

De focus van Fryqua ligt op de verborgen risico's binnen geldige toegang. Door gebruikersgedrag continu te analyseren en te koppelen aan identiteit en rechten, worden afwijkingen zichtbaar die anders tussen systemen verloren gaan. Zo verkleint Fryqua een blinde vlek in de beveiliging en kan de organisatie sturen op feiten in plaats van aannames.



3. Wat doet Fryqua?

Fryqua is een gespecialiseerd security analytics-platform dat identiteit, toegangsrechten en gebruikersgedrag samenbrengt tot gekwalificeerde anomalieën en bruikbare inzichten voor onderzoek, risicobeoordeling en besluitvorming.

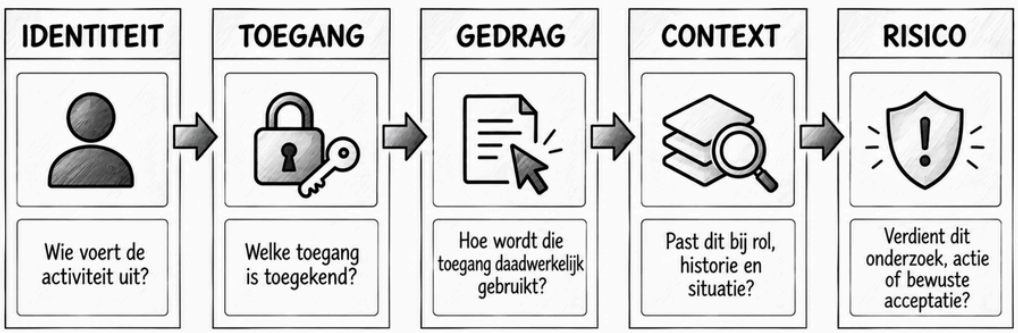


Afbeelding 1. Van verspreide data naar samenhangende context en bruikbare uitkomsten

Fryqua verzamelt, registreert en analyseert relevante data-, account- en toegangsactiviteiten en brengt deze samen in dashboards, audittrails en kant-en-klare casussen. Geavanceerde regels en analytics vertalen gebeurtenissen naar bruikbare inzichten. Dit stelt securityteams in staat om risico's tijdig te identificeren en effectief te mitigeren.

Relevante signalen kunnen worden aangesloten op bestaande SOC- en SIEM-oplossingen, zodat Fryqua aanvullend werkt op de bestaande securitycontroles in plaats van deze te vervangen.
De productarchitectuur ondersteunt agent-based monitoring, een centrale Fryqua-server en integratie met Active Directory en Entra ID. De verzamelde informatie kan worden gebruikt voor dashboards, rapportages, audittrails en bestaande monitoringprocessen. Fryqua kan worden ingezet in on-premises, hybride omgevingen en heeft geen internetverbinding nodig.

De kern van Fryqua is het verbinden van identiteit, toegangsrechten en gebruikersgedrag zodat bestaande data betekenisvoller wordt voor onderzoek en risicobeoordeling.



Afbeelding 2. Van identiteit naar risico: toegang beoordelen in context

4. Drie samenhangende intelligence-capabilities

Identity & Access Intelligence
Maakt accounts, rollen, toegangsrechten, wijzigingen en daadwerkelijk gebruik inzichtelijk. De vraag verschuift van ‘wie heeft toegang?’ naar ‘waarom bestaat die toegang en hoe wordt die gebruikt?’

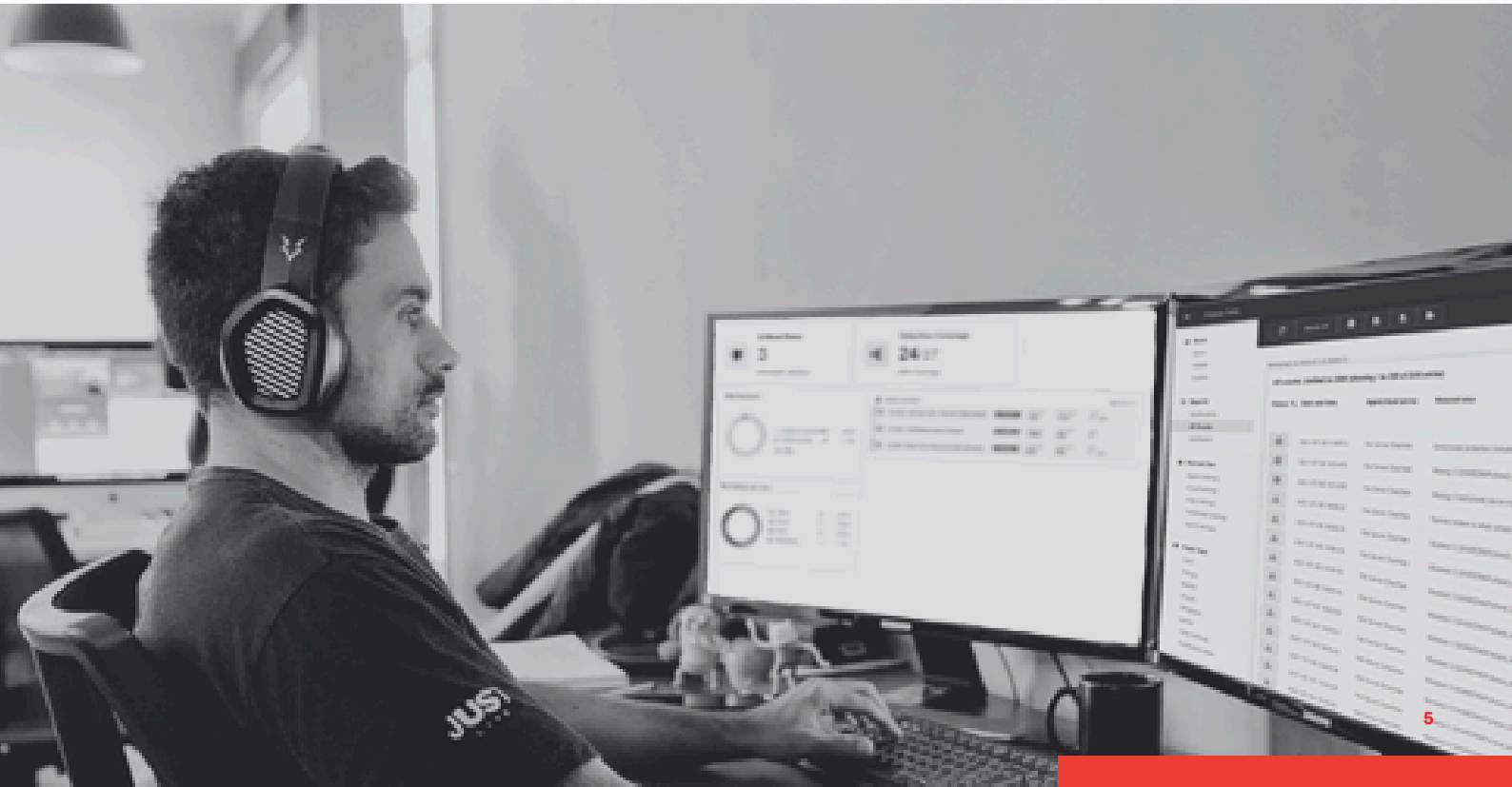
User Anomaly Detection
Maakt gedrag zichtbaar dat afwijkt van gebruikelijke patronen of van ingestelde risicoregels. Een afwijking is geen incident, maar een signaal dat mogelijk onderzoek en extra context verdient.

Advanced Security Analytics
Transformeert losse gebeurtenissen van gebruikers-, account-, toegangs- en activiteitsinformatie tot één samenhangend beeld, zodat afwijkingen en risico’s zichtbaar worden en gericht kunnen worden opgevolgd.

Hoe werkt dat?
Fryqua bouwt per gebruiker (en per rol of groep) een beeld op van normaal gedrag met behulp van onze neurale netwerken, gebaseerd op historische activiteit in de eigen omgeving gedurende een bepaalde periode. De modellen draaien volledig lokaal op de Fryqua-server en er verlaat geen data de omgeving.

Een afwijking leidt niet automatisch tot een alert. Ze wordt eerst gewogen tegen de toegangsrechten, recente accountwijzigingen en de ingestelde regels. Securityteams kunnen drempelwaarden aanpassen en afwijkingen als legitiem identificeren, zodat het aantal onterechte meldingen afneemt.

De kracht zit in de combinatie. Pas wanneer toegangsrechten, gedragsafwijkingen en analyse samenkomen, wordt duidelijk of een activiteit past bij de gebruiker en de situatie.



5. Fryqua vult bestaande security aan

Fryqua specialiseert zich op het gebied van identiteit, toegang en gebruikersgedrag en vult de bestaande securitystack aan.

Categorie	Kernvraag	Waar sterk in	Waar Fryqua toevoegt
FRYQUA.com	Hoe wordt geldige toegang daadwerkelijk gebruikt en past dit bij de context?	Context rond gebruiker, rechten en activiteit	Gespecialiseerde inzichten voor onderzoek en risicobeoordeling
SIEM (Security Information and Event Monitoring)	Welke securityevents zien we?	Brede logging, search en detectie	Gericht contextmodel voor identiteit, toegang en gedrag
IAM (Identity & Access Management) / **IGA** (Identity Governance & Administration)	Wie mag toegang hebben?	Provisioning, rollen en reviews	Daadwerkelijk gebruik van toegekende toegang
UEBA (User and Entity Behavior Analytics)	Welk gedrag wijkt af?	Statistische en gedragsmatige afwijkingen	Verbindt afwijkend gedrag met toegangsrechten en activiteitencontext
EDR (Endpoint Detection & Response) / **XDR** (Extended Detection & Response)	Welke technische signalen wijzen op een dreiging?	Endpoint-, workload- en threatdetectie en response	Gebruikers- en toegangscontext rond de waargenomen activiteit
DLP (Data Loss Prevention) / Data Security	Wat gebeurt er met gevoelige data?	Bescherming, classificatie en monitoring van datagebruik/-beweging	Plaats gegevensactiviteit in de context van gebruiker, account en toegangsrechten

Afbeelding 3. Primaire focus per oplossing

Fryqua voegt een gedetailleerd onderzoeksperspectief toe: hoe wordt toegang daadwerkelijk gebruikt en zorgt ervoor dat bestaande data betekenisvoller wordt voor onderzoek en het beoordelen van dat gedrag.

Onze toegevoegde waarde ligt in gerichte intelligentie binnen dit specifieke risicodomein. Fryqua verbindt data rondom identiteit, toegang en daadwerkelijk gebruikersgedrag tot één samenhangend beeld, dat helpt om risico's binnen geldige toegang te onderzoeken en te beoordelen.

6. Concrete securityvraagstukken

Wij maken direct zichtbaar wat nu onzichtbaar blijft en transformeren complexe securityvraagstukken in één samenhangend beeld. Waar anderen stoppen, ziet Fryqua wat er écht gebeurt.

1. Plotseling afwijkend datagebruik
Een gebruiker benadert in korte tijd veel meer bestanden of andere locaties dan gebruikelijk is. Fryqua relateert deze activiteit aan identiteit, account en toegekende toegang.

2. Overmatige toegangsrechten
Een account heeft toegangsrechten die technisch geldig zijn, maar nauwelijks worden gebruikt of niet meer aansluiten bij de huidige rol. Dit ondersteunt access reviews en de toepassing van het principe van least privilege.

3. Nieuwe rechten, direct actief gebruikt
Een account krijgt gewijzigde of aanvullende rechten en gebruikt deze kort daarna voor relevante data-activiteiten. Fryqua verbindt accountwijziging, toegang en activiteit in één samenhangend beeld.

4. Accountmisbruik of gecompromitteerde identiteit
Een geldig account vertoont gedrag dat niet past bij eerder of verwachte gebruikspatronen. Authenticatie blijft geldig, maar het gedrag verdient nader onderzoek.

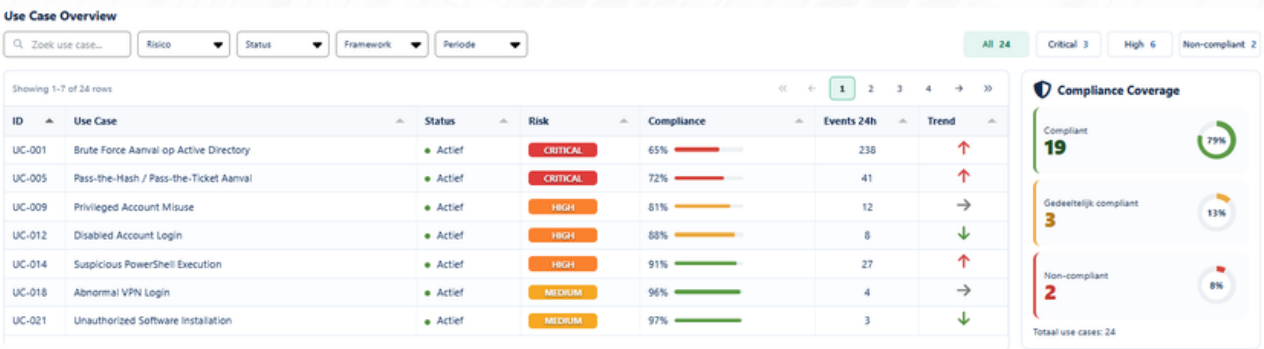
5. Ongebruikelijke wijzigingen of encryptie
Grote aantallen bestanden worden in korte tijd gewijzigd of versleuteld. Rules en monitoring kunnen een alert genereren en de actie stoppen.

6. Audit en reconstructie
Na een incident moet worden vastgesteld wie wat heeft gedaan en wanneer. Doordat Fryqua de audit trail en de bijbehorende account- en activiteitsgegevens continu monitort, ondersteunt dit de reconstructie en verantwoording.

7.Bedrijfsafhankelijke en klantspecifieke vraagstukken
Naast standaard risicopatronen beantwoordt Fryqua specifieke, door de klant gedefinieerde security- en compliancevragen. Hoe complex of uniek uw interne bedrijfsprocessen of governance-regels ook zijn: zodra de benodigde brondata aanwezig is, brengen wij de gewenste logica en risico's betrouwbaar in beeld.

Fryqua behandelt niet elke afwijking als incident. Het doel is relevante signalen zichtbaar en onderzoekbaar te maken, zodat mensen een onderbouwde beslissing kunnen nemen.

Afbeelding 4. Fryqua Use Case Dashboard



7. Voor welke organisaties is Fryqua relevant?

Fryqua is met name relevant voor organisaties die werken met gevoelige of bedrijfskritische data, complexe toegangsstructuren en verschillende gebruikersrollen.

Dit geldt voor organisaties die de samenhang tussen identiteit, toegang en daadwerkelijk gebruikersgedrag willen reconstrueren. Dit kan in on-premises, Windows-/Linux- en hybride omgevingen.

Fryqua helpt organisaties met gespecialiseerde analysecapaciteit om sneller inzicht te krijgen in het daadwerkelijke gebruik van toegangsrechten, afwijkend gedrag te onderzoeken en access reviews beter te onderbouwen.

Waar al IAM-, endpoint- of SIEM-oplossingen aanwezig zijn, sluit Fryqua daarop aan en brengt het de beschikbare signalen samen tot één beeld van wat er daadwerkelijk gebeurt, zodat organisaties onderbouwde beslissingen kunnen nemen.



Toepassingsmarkten

MKB
Praktisch inzicht in toegangsrechten, gebruikersgedrag en afwijkingen binnen de IT-omgeving, zonder groot gespecialiseerd securityteam.

Zorg
Inzicht in hoe gevoelige patiënteninformatie wordt benaderd en of dat gebruik past bij de identiteit, rechten en context.

Overheid
Ondersteunt controle en aantoonbaarheid in het kader van compliance en onderzoek naar de toegang tot gevoelige of kritieke informatie.

Onderwijs
Van studenten en medewerkers tot onderzoekers en tijdelijke accounts: Fryqua laat zien wat er daadwerkelijk met toegangsrechten gebeurt.

MSP / MSSP
De verantwoordelijkheid ligt bij je klant. De verwachting ligt bij jou. Klanten moeten steeds beter kunnen aantonen wie toegang heeft, welke rechten zijn toegekend en wat er gebeurt. Met Fryqua kan niet alleen beheerd worden, maar ook aantoonbaar worden gemaakt.

Hybride omgevingen
Fryqua is ontworpen voor omgevingen waarin verschillende netwerken, locaties en technologieën samenkomen: on-premises, cloud, managed services én netwerken zonder directe internetverbinding.

De beste fit wordt bepaald door de aard van de omgeving en de securityvraag die je wilt beantwoorden, niet door de sector of omvang.



8. Van inzicht naar bedrijfswaarde

Door signalen, identiteit, toegang en gedrag samen te brengen, wordt zichtbaar wat er werkelijk gebeurt en welke actie nodig is. Fryqua ziet wat anderen missen.

1. Geautomatiseerde reconstructie
Relevante identiteit, toegangsrechten en activiteiten komen automatisch samen en worden met behulp van neurale netwerken vergeleken en beoordeeld.

2. Sterkere access reviews
Niet alleen beoordelen welke rechten bestaan, maar ook hoe ze daadwerkelijk worden gebruikt.

3. Trendanalyse
Veranderingen, afwijkingen en trends worden continu zichtbaar gemaakt, die anders moeilijk te herkennen zijn.

4. Betere bestuurbaarheid
Aantonen waarom een risico is onderzocht, gemitigeerd of geaccepteerd.

5. Bescherming van continuïteit
Eerder begrijpen welke situaties daadwerkelijk aandacht vereisen, helpt organisaties bewuster te prioriteren en te handelen.

6. Compliance is geen productfeature.
Fryqua ondersteunt compliance en levert inzicht en onderbouwing, terwijl de verantwoordelijkheid voor beleid, processen en maatregelen bij de organisatie blijft.

9. Architectuur en security onder eigen regie

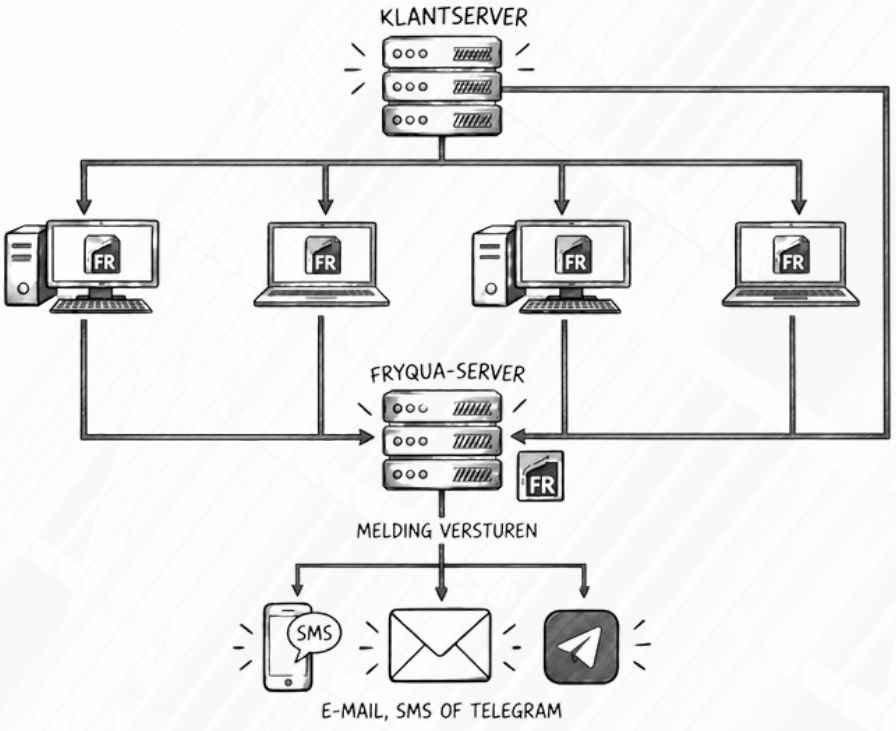
Voor organisaties is niet alleen van belang welke inzichten een oplossing oplevert, maar ook hoe data wordt verzameld, verwerkt en beheerd. Zeker wanneer het gaat om gevoelige gebruikers-, toegangs- en activiteitsgegevens, is controle over de technische architectuur een belangrijk onderdeel van het besluitvormingsproces.

Fryqua is daarom ontworpen op basis van het principe dat organisaties zelf regie behouden over hun eigen data en infrastructuur:

- Een centrale Fryqua-server verwerkt, analyseert en presenteert de verzamelde informatie.
- Fryqua kan worden ingezet in on-premises en hybride omgevingen.
- De Fryqua-server kan volledig binnen de eigen IT-omgeving functioneren, zonder internetverbinding.
- De organisatie heeft de regie over de opslag en het gebruik van data en logbestanden.
- Fryqua heeft geen permanente of verborgen toegang tot de omgeving en vereist expliciete autorisatie van de klant.
- Relevante alerts kunnen eenvoudig worden gekoppeld aan externe applicaties, waaronder bestaande SOC- en SIEM-oplossingen.
- Agent-based monitoring verzamelt relevante activiteiten dicht bij de bron.

> “Security intelligentie moet meer inzicht creëren zonder de controle over data uit handen te geven.“

De exacte technische inrichting wordt afgestemd op de omgeving en de gebruikte release.



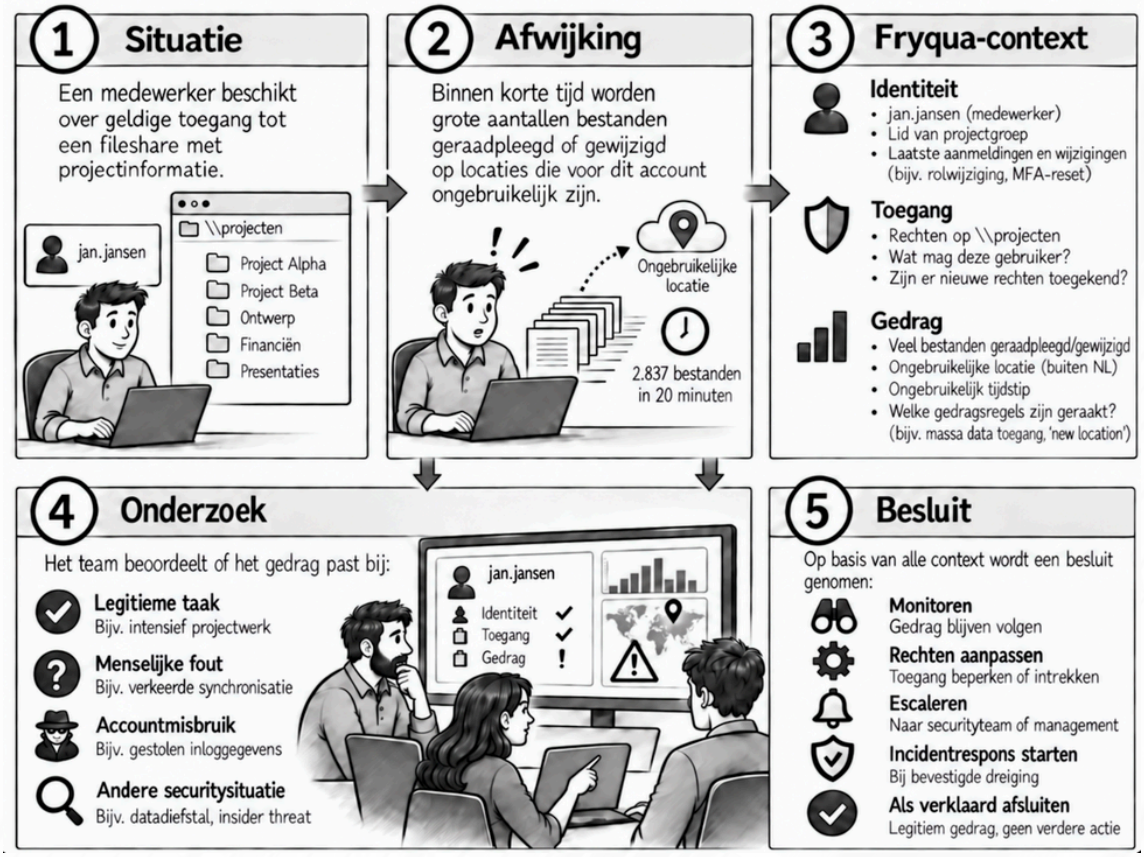
Afbeelding 5. Vereenvoudigd architectuurbeeld van Fryqua

10. Van signalen naar intelligente security

Een afzonderlijk signaal zegt vaak weinig. De waarde ontstaat wanneer identiteit, toegang, veranderingen en daadwerkelijk gedrag gezamenlijk worden beoordeeld.

Fryqua verbindt verschillende losse signalen en beoordeelt deze vanuit meerdere perspectieven. Zo worden wie deze gebruiker is, welke toegang hij heeft, wat recent is gewijzigd en het feitelijke gedrag in samenhang bekeken. Daarbij ontstaat inzicht in de vraag of het gedrag van een gebruiker past bij diens rol en de betreffende situatie.

Daarmee verschuift de focus van losse signalen en rechten naar een perspectief voor betere securitybeslissingen.



Afbeelding 6. Voorbeeld van intelligente security

Voorbeeldscenario

Een medewerker heeft geldige toegang tot projectinformatie. Binnen korte tijd ontstaat er een sterke piek in bestandsactiviteit op locaties die voor dit account ongebruikelijk zijn. Tegelijkertijd is onlangs een recht gewijzigd. Geen van deze signalen hoeft op zichzelf een incident te zijn. In combinatie vormen zij wel een relevante onderzoeksvraag.

Door signalen, identiteit, toegang en gedrag samen te brengen, wordt zichtbaar wat er werkelijk gebeurt en welke actie nodig is, ook als de losse signalen verspreid over systemen onopgemerkt blijven.



10.1. Waarom context het verschil maakt

Securityteams worden geconfronteerd met grote hoeveelheden signalen, terwijl tijd en expertise schaars zijn. Wanneer identity-, access- en activiteitsinformatie over meerdere systemen is verdeeld, begint elk onderzoek met het verzamelen en reconstrueren van die informatie.

Fryqua brengt die context samen. Daardoor ontstaat niet alleen zicht op wat er gebeurt, maar vooral op wat de activiteit in deze specifieke situatie betekent.

Voor de organisatie levert dat drie voordelen op:

Minder ruis: signalen worden in samenhang beoordeeld in plaats van uitsluitend als losse gebeurtenissen.

Sneller inzicht: onderzoek start vanuit de gebruiker, het account, de rechten en de relevante activiteit.

Betere prioritering: monitoring, aanpassing van toegang, escalatie of incidentrespons kan worden gebaseerd op aantoonbare context.

De positionering van Fryqua gaat daarmee verder dan de klassieke toegangsmonitoring. Fryqua verbindt identiteit, toegang en gebruikersgedrag om te helpen bepalen welke actie past bij het daadwerkelijke risico.



11. Aantoonbare waarde

Waarom Fryqua?

- Gespecialiseerde focus op risico's binnen geldige toegang.
- Inzicht in hoe toegekende rechten daadwerkelijk worden gebruikt.
- Gebruiker, account, toegang en activiteit in één onderzoeksperspectief.
- Aanvullende context naast de bestaande IAM-, SIEM-, EDR/XDR-, UEBA- en DLP-investeringen.
- Fryqua ziet wat anderen missen.

Waarde aantonen in de praktijk

Vooraf bepalen we samen welke onderzoeksvragen centraal staan en aan welke succescriteria de inzet van Fryqua moet voldoen.

Toegangsintelligentie
Kunnen ongebruikte, opvallende of mogelijk overmatige toegangsrechten zichtbaar worden gemaakt en beter worden onderbouwd?

Afwijkend gebruikersgedrag
Worden relevante gedragsafwijkingen zichtbaar die aanvullende context of nader onderzoek verdienen?

Onderzoek en analyse
Welke identity-, access- en activiteitscontext hoeft niet langer uit meerdere systemen te worden samengebracht?

Aansluiting op de bestaande omgeving
Hoe sluit Fryqua aan op bestaande SOC-, SIEM- en identityprocessen, en welke beheerinspanning vraagt dit van de organisatie?

Het doel is niet om zoveel mogelijk alerts te genereren, maar om aantoonbaar te maken welke nieuwe en bruikbare securitycontext Fryqua in jouw omgeving beschikbaar stelt.

Fryqua
Dorsvloer 15
9205 BN Drachten
The Netherlands

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

Dit document is uitsluitend bedoeld ter informatie. Er kunnen geen rechten aan de inhoud worden ontleend.
Copyright © 2026 Fryqua.com. Alle rechten voorbehouden.