E-book

Ontdek de kracht van Elastic search, observability en security

Wat zijn de voordelen en waar kun je het voor gebruiken?

PUUR DATA

De databerg waar haast elke organisatie tegenwoordig op zit, is een potentiële goudmijn. Wil je deze ontginnen? Dan is het essentieel dat je grip krijgt op je data. Want alles draait om inzicht en snelheid. Hoe eerder je in jouw data verborgen trends kunt blootleggen, hoe beter je kun inspelen op veranderende omstandigheden. In dit e-book lees je hoe de slimme technologie van Elastic je hierbij helpt.

Wat is Elastic?

Elastic is in de kern een zoekoplossing, ontworpen om grote hoeveelheden data uit diverse bronnen te doorzoeken. De belangrijkste eigenschappen zijn schaalbaarheid en snelheid. Dat is de reden waarom de toepassing veel wordt gebruikt, door organisaties over de hele wereld. In feite zijn er drie pijlers:

1. Search

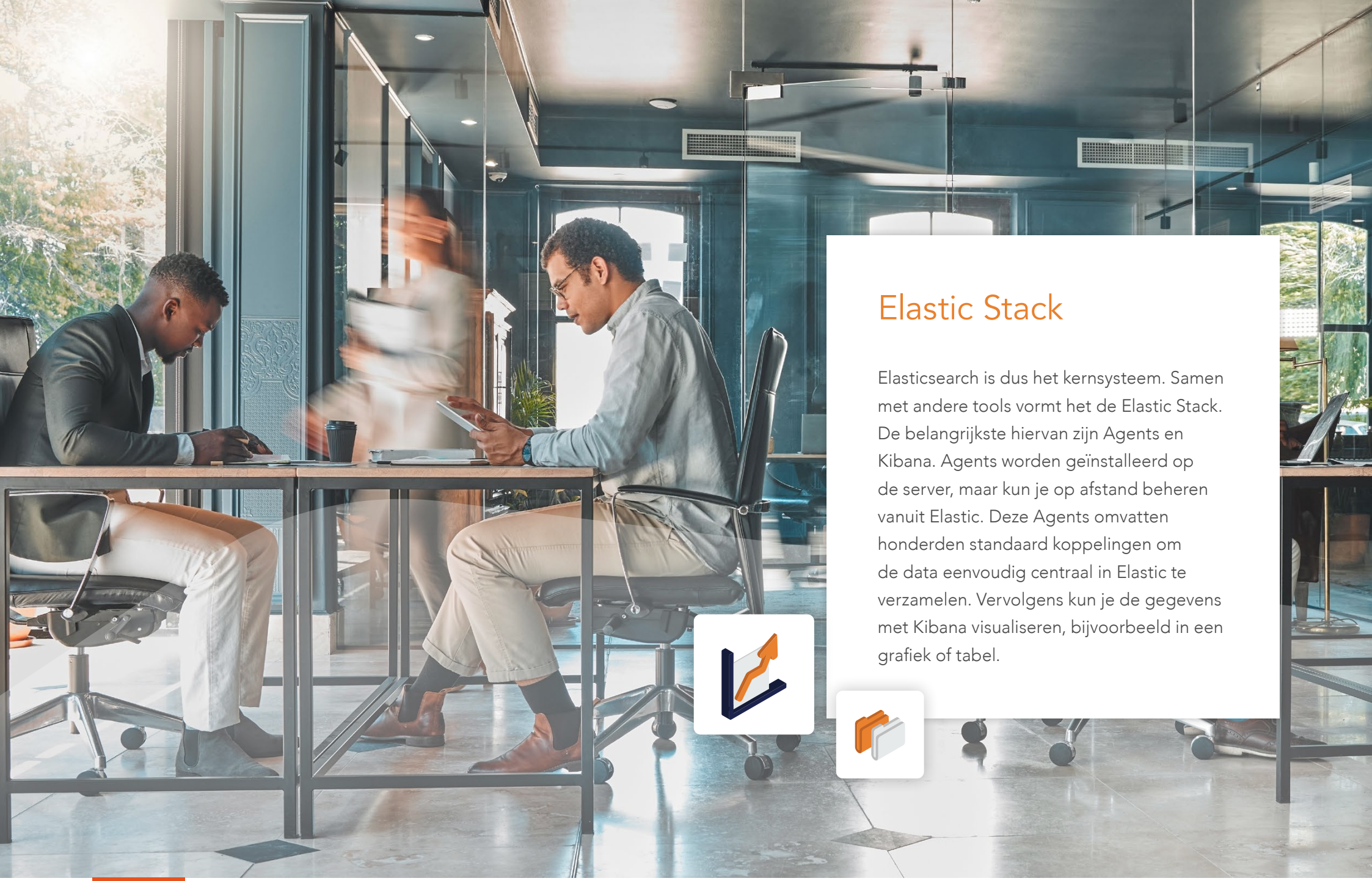
Hoewel wel eens wordt getypeerd als een soort Google, biedt Elasticsearch veel uitgebreidere mogelijkheden. Dankzij filters en sorteeropties bijvoorbeeld, vind je eerder antwoorden waar je ook echt iets aan hebt. Je krijgt dieper inzicht in data, dankzij verrijking van data door koppeling met andere bronnen, en door visualisatie van patronen.

2. Observability

Daarnaast wordt Elastic-technologie veel gebruikt voor observability. Dat is het continu verzamelen en analyseren van met name logdata, afkomstig van netwerkcomponenten. Deze gegevens zorgen voor inzicht hoe je IT-omgeving functioneert. Je krijgt beter begrip van oorzaken en verbanden in een systeem. Daardoor spoor je problemen eerder op en pak je ze aan voor ze schade veroorzaken.

3. Security

Elastic is ook sterk in het detecteren van afwijkende patronen of gedragingen in loggegevens, die kunnen wijzen op een cyberaanval. Denk hierbij aan een plotse toename van het aantal inlogpogingen vanaf een bepaalde locatie. De SIEM-oplossing van Elastic kan beveiligingsteams hierop attenderen, zodat ze tijdig kunnen reageren. SIEM staat voor Security Information and Event Management. Dit systeem kan je voorzien van gedetailleerde rapportages, waarmee je aan toezichthouders kunt laten zien dat je voldoet aan wet- en regelgeving.



Elastic Stack

Elasticsearch is dus het kernsysteem. Samen met andere tools vormt het de Elastic Stack. De belangrijkste hiervan zijn Agents en Kibana. Agents worden geïnstalleerd op de server, maar kun je op afstand beheren vanuit Elastic. Deze Agents omvatten honderden standaard koppelingen om de data eenvoudig centraal in Elastic te verzamelen. Vervolgens kun je de gegevens met Kibana visualiseren, bijvoorbeeld in een grafiek of tabel.

Bekende gebruikers

Zoals gezegd vertrouwen organisaties over de hele wereld op Elastic. Een van de bekendste is Netflix. Deze streamingdienst gebruikt de Elastic Stack onder meer om grote hoeveelheden door gebruikers gegenereerde data te doorzoeken. Inzicht in de kijkhistorie helpt Netflix om abonnees gepersonaliseerde aanbevelingen te doen. Het resultaat: een betere gebruikservaring en een bijdrage aan klantbehoud.

Netflix gebruikt Elastic ook om een vlekkeloos signaal aan te bieden. Door voortdurend data uit logfiles te analyseren, komen patronen die wijzen op een (dreigende) storing eerder aan het licht.

Ook Uber en T-Mobile gebruiken Elastic. Uber doorzoekt en analyseert in real-time onder meer locatiegegevens. Inzicht in het verschil is tussen de verwachte aankomsttijd en de werkelijke aankomsttijd van een voertuig, helpt om de dienstverlening te verbeteren. De technologie wordt ook gebruikt voor dynamische prijzen. Als blijkt dat er meer vraag is naar vervoer dan aanbod, dan stijgt de prijs (en andersom).

Voor T-Mobile geldt dat het dankzij Elastic inzicht krijgt in dataverkeer op het mobiele netwerk. In combinatie met Machine Learning, kan de provider voorspellen of en wanneer bepaalde afwijkingen in datastromen tot een storing leiden.

Voorbeelden van hoe Elastic-klanten van PuurData vooruithelpt, zijn MARIN en Zuyderland. MARIN is een onafhankelijk instituut voor maritiem onderzoek dat enorm veel onderzoeksverslagen en projectdocumenten in huis heeft. Het gebruikt Elastic om medewerkers in staat te stellen om al deze gegevens te doorzoeken, en relevante antwoorden te krijgen op onderzoeksvragen.

Zuyderland is een zorgconcern met een complex IT-landschap dat meer dan honderd applicaties telt, die soms letterlijk van levensbelang zijn. Met Elastic log monitoring kan IT-beheer via een dashboard prestaties van elk netwerkonderdeel in de gaten houden en problemen tijdig verhelpen.

Klik op de links voor de volledige verhalen van Marin en Zuyderland.

Waarom kiezen organisaties voor Elastic?

In een onderzoek zeggen professionals onder meer dat het makkelijk is om aan de slag te gaan met Elastic. Ze roemen vooral Elasticsearch "een geweldige zoekmachine". De (near) real-time zoek- en analysemogelijkheid gelden als grote pluspunten. Ook noemen ze de krachtige Application Programming Interface (API), die het makkelijk maakt om oplossingen aan te passen aan verschillende gebruikersscenario's.

Open source

Een andere veelgenoemde reden om te kiezen voor Elastic, is dat het open source software is. Het voordeel daarvan is dat niet alleen werknemers van Elastic zich bezighouden met verbetering van de software, maar ook een hele gebruikersgemeenschap. Ook op het gebied van security is Elastic ervan overtuigd dat open security het beste is. Omdat er voortdurend nieuwe dreigingen de kop op steken, kiest Elastic ervoor om met zoveel mogelijk mensen te betrekken bij het vinden van de meest adequate manier om ze te detecteren.

Elastic kan de brug zijn tussen enerzijds jouw bedrijfsdata, en anderzijds large language models die chatbots als ChatGPT ook gebruiken.

Conclusie en vooruitblik

De Elastic Stack helpt je dus om snel de juiste inzichten uit grote hoeveelheden data te halen. Je krijgt meer grip op data, neemt beter onderbouwde beslissingen en kunt sneller reageren. Zoeken gaat razendsnel en inzichten krijg je op een overzichtelijke, visueel aantrekkelijke manier gepresenteerd.

Elastic past bij een proactieve werkwijze. Door observability krijg je inzicht in hoe je netwerk presteert en pik je eerder signalen op die wijzen op een (dreigende) storing. SIEM geeft je inzicht in de cyberrisico's die je loopt, wat helpt om je weerbaarheid te vergroten.

Het open karakter van de software draagt bij aan continue verbetering en toevoeging van nieuwe functionaliteiten. Steeds vaker worden die ondersteund door AI. Op dit moment heeft generative AI de wind in de zeilen, een vorm van kunstmatige intelligentie die nieuwe toepassingen kan creëren. Elastic kan de brug zijn tussen enerzijds jouw bedrijfsdata, en anderzijds large language models die chatbots als ChatGPT ook gebruiken. Je krijgt dan bijvoorbeeld rijkere zoekresultaten, betere en uitgebreidere antwoorden op zoekvragen en nauwkeurigere voorspellingen. Dit plaveit de weg naar steeds weer nieuwe, out-of-the-box toepassingen, die je intern kunt gebruiken of waarmee je klanten en partners beter kunt bedienen.

PuurData

Als Elite-partner van Elastic kunnen we je als geen ander helpen met advies, implementatie en beheer. PuurData is zelfs erkend als Elastic Benelux Partner van het jaar 2023. Daardoor kunnen we je als geen ander adviseren over de oplossing die het beste past bij jouw uitdagingen. We kunnen je ook helpen bij het opzetten en het beheer van je Elastic-omgeving.

Wil je meer weten over hoe Elastic jouw organisatie vooruit helpt en generative AI? Neem dan contact met ons op. Of kijk op puurdata.nl.

PuurData
Argonstraat 28
6718 WT Ede
T +31 (0)88 7887328
E info@puurdata.nl