# Advanced Reporting Tool

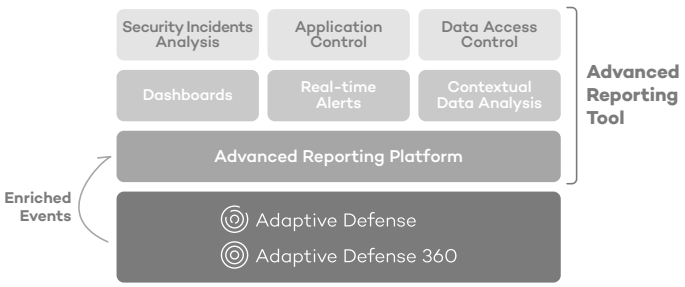
## Doelgericht detecteren en bestrijden van interne en externe kwetsbaarheden

Bedrijven genereren en verwerken dagelijks steeds vaker grote hoeveelheden gegevens, waaronder soms zeer gevoelige informatie. Zonder een uitgebreid overzicht van de IT-infrastructuur en de lopende processen, lopen IT-afdelingen snel het risico dat belangrijke details over het hoofd gezien worden. Hierdoor loopt de veiligheid van het gehele IT-systeem gevaar.

Informatie over lopende processen kan selectief worden verwerkt en geanalyseerd om beveiligingsincidenten in bedrijfsnetwerken op te sporen, of ze nu van buiten komen of worden veroorzaakt worden door insiders.

### De oplossing: Adaptive Defense met geïntegreerde Advanced Reporting Tool

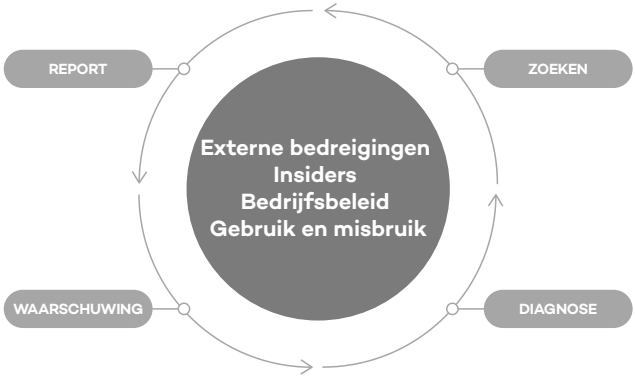
Het Advanced Reporting Platform automatiseert de opslag en overeenstemming van Adaptive Defense procesgegevens. Met behulp van deze gegevens kunnen IT-beheerders met slechts één klik gedetailleerde beveiligingsinformatie genereren. Hierdoor kunnen aanvallen en ongebruikelijke gedragspatronen worden gedetecteerd, evenals intern misbruik van bedrijfsnetwerken en -systemen.




Met slechts één klik kunt u met de Advanced Reporting Tool gedetailleerde resultaten van het IT- en beveiligingsmanagement van de onderneming genereren. Op basis hiervan kan vervolgens een actieplan worden opgesteld aan de hand van de volgende punten:

- Bepaal de oorsprong van vbedreigingen om toekomstige aanvallen te voorkomen.
- Beleid implementeren ter restrictie van toegang tot kritieke bedrijfsgegevens.
- Toezicht op, en controle van, het misbruik van bedrijfsmiddelen.
- Correctie van het gedrag van medewerkers als het niet voldoet aan de vastgestelde gebruiksrichtlijnen.

## Belangrijkste voordelen




### 1. Relevante informatie vinden

- Maximaal uw inzicht in alle processen die draaien op uw endpoints en servers en verhoog de productiviteit en efficiëntie van uw IT.
- Toegang tot logboekgegevens om de beveiliging en gebruiksindicatoren van uw bedrijfsmiddelen te analyseren.
- Gedetailleerde informatie over beveiligingsrisico's en eventueel misbruik van de IT-infrastructuur door insiders.

### 2. Diagnose van netwerkproblemen

- Verminder het aantal tools en gegevensbronnen dat nodig is om te analyseren wat er op endpoints gebeurt en hoe dit de veiligheid en het gebruik van de bedrijfsmiddelen van uw organisatie beïnvloedt.
- Verkrijg informatie over het resourcegebruik en gedragspatronen van gebruikers om hun potentiële invloed op het bedrijf aan te tonen.

### 3. Wees waakzaam

- Zet ontdekte afwijkingen om in real-time waarschuwingen en rapporten.
- U kunt beveiligingsproblemen en misbruik van IT-middelen door medewerkers detecteren.

### 4. Horizontale en verticale informatie

- Genereer en configureer rapportages de beveiligingsstatus van uw organisatie systematisch te analyseren om zo misbruik van bedrijfsmiddelen en gedragsafwijkingen te identificeren.
- Analyseer de status van belangrijkste veiligheidsindicatoren en volg de ontwikkeling hiervan. Zo kunt u genomen maatregelen evalueren.

# Advanced Reporting Tool

## FLEXIBELE, INDIVIDUEEL AANGEPASTE ANALYSES

De Advanced Reporting Tool bevat dashboards met sleutelindicatoren, zoekopties en standaardwaarschuwingen voor drie belangrijke gebieden:

- Veiligheidsincidenten.
- Toegang tot belangrijke informatie.
- Gebruik van toepassingen en netwerkbronnen.

Zoekprocessen en waarschuwingen kunnen worden aangepast aan de individuele omstandigheden van uw bedrijf.

## INFORMATIE OVER VEILIGHEIDSINCIDENTEN

Genereer gedetailleerde beveiligingsinformatie door gebeurtenissen die zich voordoen tijdens aanvalspogingen onmiddellijk te verwerken en met elkaar te vergelijken.

De tijdlijnen in de Advanced Reporting Tool tonen u het volgende:

- Malware en PUP's die in de afgelopen jaren zijn ontdekt.
- Computers met het grootste aantal besmettingspogingen en ontdekte malware.
- Status van malware op computers in uw netwerk.
- Computers met kwetsbare toepassingen.


## KOSTPRIJS REDUCTIE

Analyseer de gebruikspatronen van uw IT-resources om zo te ontdekken welke mogelijkheden er zijn om kosten te reduceren.

- Identificatie van bedrijfs- en niet-zakelijke toepassingen in uw netwerk.
- Overzicht van aangeschafte versus daadwerkelijk gebruikte licenties.
- Toepassingen met het hoogste bandbreedtegebruik.
- Overzicht van toepassingen die zijn geïnstalleerd op het netwerk en infecties kunnen veroorzaken die de bedrijfsprestaties en herstelkosten kunnen beïnvloeden.


## DE TOEGANG TOT BEDRIJFSGEGEVENS CONTROLEREN

De Advanced Reporting Tool toont toegang tot vertrouwelijke bestanden en gegevenslekken in het netwerk. De volgende informatie kan worden opgevraagd:

- Met welke landen uw netwerk het vaalst connecties maakt.
- Welke bestanden worden opgehaald en uitgevoerd.
- Hoe vaak specifieke netwerkcomputers worden gebruikt.
- Gedetailleerde informatie over gegevensoverdracht (in de vorm van een tijdlijn).

## REALTIME WAARSCHUWINGEN

Configureer en ontvang waarschuwingen voor mogelijke beveiligingsinbreuken of schendingen van het datamanagement beleid:

- Standaard waarschuwingen voor risicosituaties.
- Bedrijfsspecifieke waarschuwingen op basis van eigen parameters.
- Directe informatieweergave via beeldscherm of e-mail, JSON, Service Desk, Jira, Jira, Pushovery en PagerDuty.

## FLEXIBELE, CLOUD-GEBASEERDE BIG DATA SERVICE

- Aangepast aan de behoeften van netwerkbeheerders, zowel wat betreft opslagruimte als de mogelijkheid om door de loggegevens te bladeren.
- Onmiddellijk klaar voor gebruik, omdat er geen wijzigingen in het netwerk van de klant of de installatie van extra infrastructuur nodig zijn.

### TECHNISCHE VEREISTEN

Aanbevolen browsers:

- Mozilla Firefox.
- Google Chrome.

Internetverbinding en beveiligde communicatie via poort 443.

Minimale resolutie: 1280 x 1024 (aanbevolen: 1920 x 1080 x 1080).

Alleen te combineren met Adaptive Defense (360)