Braathe AS
Nærumveien 24, 1580 Rygge / Org.nr. 981 933 311 MVA
69 01 30 00 / post@braathe.no / www.braathe.no

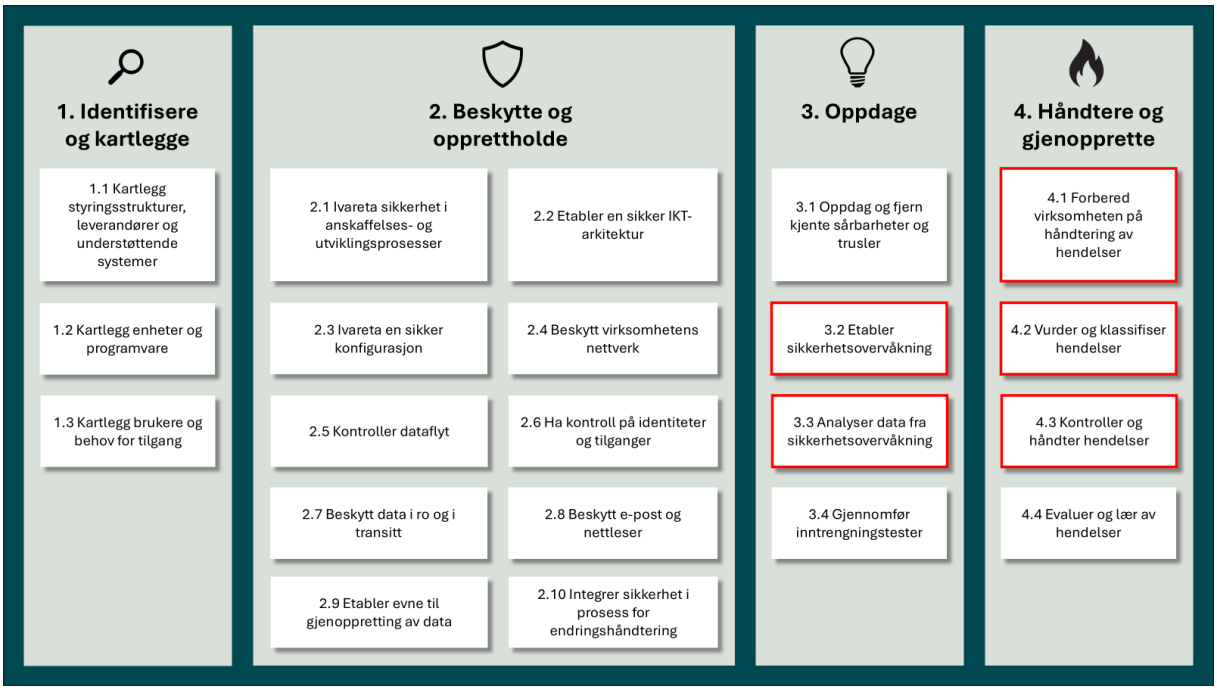
Tjenestebeskrivelse for MDR 24/7

Tjenestebeskrivelse gjeldende fra 01.10.2025. Underlagt Generelle Betingelser og Sikkerhets SLA, samt Nettskyavtale eller SSA avtale.

1 Om MDR 24/7 for klientendepunkt og identitet

Managed Detection and Response (MDR) er en sikkerhetstjeneste som kombinerer avansert teknologi, kontinuerlig overvåking og ekspertkompetanse for å oppdage, analysere og håndtere sikkerhetstrusler, som er i stadig endring, så tidlig som mulig.
MDR 24/7 øker sannsynligheten for at man oppdager trusler og angrep på et tidlig tidspunkt, for dermed å bedre beskytte virksomhetens data, systemer, enheter og brukere. Dette gir økt trygghet, bedre samsvar og redusert risiko for økonomisk tap og omdømmeskade.

- Aktiv overvåkning med akutt håndtering
- Identifisere og stoppe hendelser på et tidlig tidspunkt
- Identitet og endepunkt er ofte en start og et utgangspunkt for større angrep
- Mer automasjon hos angriper, gjør at rask respons er blitt viktigere
- Bidrar til å dekke NSMs grunnprinsipper 3.2, 3.3, 4.1, 4.2 og 4.3



Figur: NSMs grunnprinsipper for IKT-sikkerhet

2 Etablering

MDR 24/7 settes opp etter Leverandørens standard i hht gjeldende rammeverk. Dersom kunde ønsker tilpasninger, testing eller teknisk rådgivning leveres dette som timebasert Konsulentoppdrag.

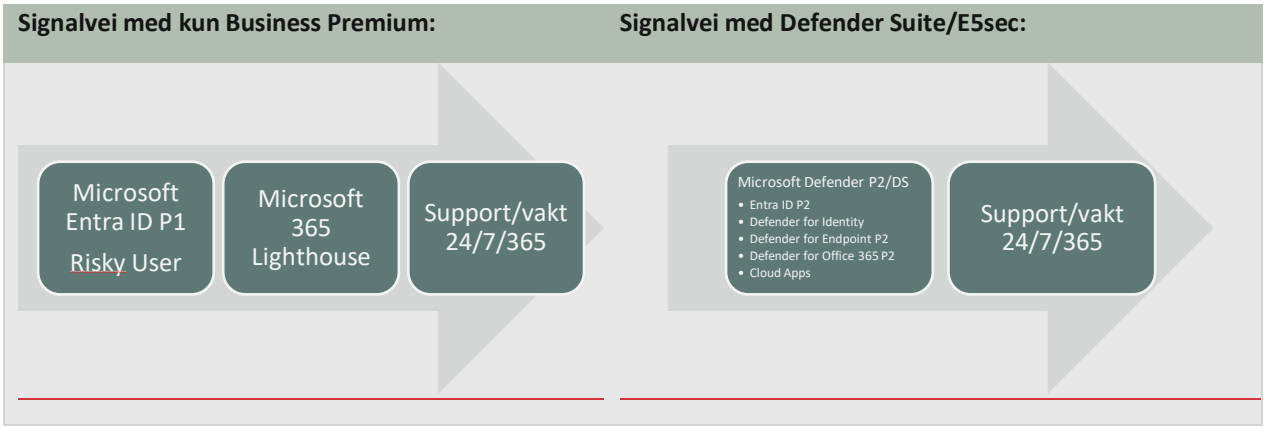
3 Tjenesteinnhold

3.1 Ved Business Premium

Tjenesten baseres på Microsoft Defender produktene inkludert i lisenspakke Microsoft 365 Business Premium.
- For funksjons-tjenester som Exchange, F3 ol legges Microsoft Entra ID P1 til.
Enkelte signaler går via Microsoft 365 Lighthouse.

3.2 Ved Defender Suite/E5 (XDR-drevet)

Defender Suite for Business eller E5 gir flere og samordnede signaler (XDR), raskere signalvei og dermed bedre beskyttelse (se illustrasjon under).
- For Microsoft 365 Business Premium legges Defender Suite til.
- For Microsoft 365 E3 legges E5 Security til.
- For funksjons-tjenester som Exchange, F3 ol legges Microsoft Entra ID P2 til.
- For Microsoft 365 E5 trengs ingen ekstra lisens.



Tjenesten baseres på sensorfangst fra Microsofts til enhver tid gjeldende utvalg.

- Varsling settes opp per tenant som benytter tjenesten
- I arbeidstid behandles hendelsene av support med eskalering til Sikkerhetsavdeling
- Utenfor arbeidstid benyttes varsling til Vakt

4 Identitet- og Endepunktsbeskyttelse

- Microsoft Defender for Endpoint
- Microsoft Entra ID Identity Protection
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Office

Braathe

5 Akutthåndtering 24/7/365

- Døgnkontinuerlig vakt utfører akutt-tiltak for å stoppe videre spredning, isolere enhet og minimere skadeomfanget.
    - Klient
        - Isoleres
        - Bruker / kundekontakt varsles
    - Bruker/identitet
        - Kontoens integritet gjenopprettes ved å tilbakestille passord og MFA samt avslutte aktive sesjoner
        - Bruker / kundekontakt varsles
- Dersom det er spredning utover dette, kan saken eskaleres til CIR (Customer Incident Response) eller MIR (Major Incident Response) levert av Braathe, eller IR (Incident Reponse) levert av tredjeparts sikkerhetsleverandør.
- Videre bistand som gjelder analyse av hendelse, feilretting, gjenoppretting og gjenåpning av konto utføres i vanlig arbeidstid som Timebasert Konsulentoppdrag.
- Rapport utarbeides på kundens forespørsel som Timebasert Konsulentoppdrag.

6 SLA

SLA Punkt	SLA Verdi
Tilgang til supporttelefon	Hverdager 07:30-16:30
Akutthåndtering pr. hendelse	Akutthåndteringsgebyr
Tilgang til Vakttelefon vedr. sikkerhetshendelser	Vakthenvendelsesgebyr
Responstid fra alarmmottak i Leverandørens systemer	<1 time
Vaktrespons med akutthåndtering ved hendelser	24/7/365
Prioritert konsulentbistand	Påfølgende virkedag

7 Forutsetninger

- Tjeneste og respons er begrenset til hvilke signaler valgt lisens til enhver tid gir
- MDR-varsler kan være falske positiver som krever verifisering. Ikke alle varsler representerer reelle sikkerhetstrusler
- Klientutstyr må onboardes med Microsoft Defender for Endpoint
- Brukere må ha en av følgende lisenser (Defender Suite/E5 Security anbefales):
    - Microsoft 365 Business Premium
    - Microsoft 365 Business Premium med Defender Suite for Business
    - Microsoft 365 E3 med E5 Security add-on
    - Microsoft 365 E5

- Funksjonskontoer (som Exchange, F3 eller tilsvarende) må ha en av følgende lisenser (Entra ID P2 anbefales):
    - Entra ID P1
    - Entra ID P2
- Gjelder alle lisensierte brukere i kundens tenant (ulisensierte brukere dekkes ikke)
- Microsoft lisenser og tjenester leveres alltid i henhold til de til enhver tid gjeldende betingelser fra Microsoft. Gjeldende dokumenter kan lastes ned fra følgende kilde: Commercial Licensing Terms (microsoft.com) (Språk kan velges i blå meny øverst til høyre)

8 Tjenestegaranti

Ved forsinket respons ut over SLA, som skyldes Leverandøren selv, bortfaller Akutthåndteringsgebyr for den forsinkede hendelseshåndteringen.

9 Begrensninger

Tjenesten er basert på tredjeparts online tjenester. Feil eller bortfall av disse tjenestene gir ikke rett til refusjon.

10 Underleverandører

Tjenesten baseres på online tjenester fra Microsoft og Atlassian.
Våre Underdatabehandlere er angitt her: https://braathe.no/pve/underdatabehandlere/