KiNS TECH 2026

Vet kommunene hvor alle dataene bor?

Fra antakelser til faktabasert kontroll på sensitive innbyggerdata

Niels Fredrik Berthelsen
Country Sales Manager - Thales Cybersecurity

THALES
CYBERSECURITY

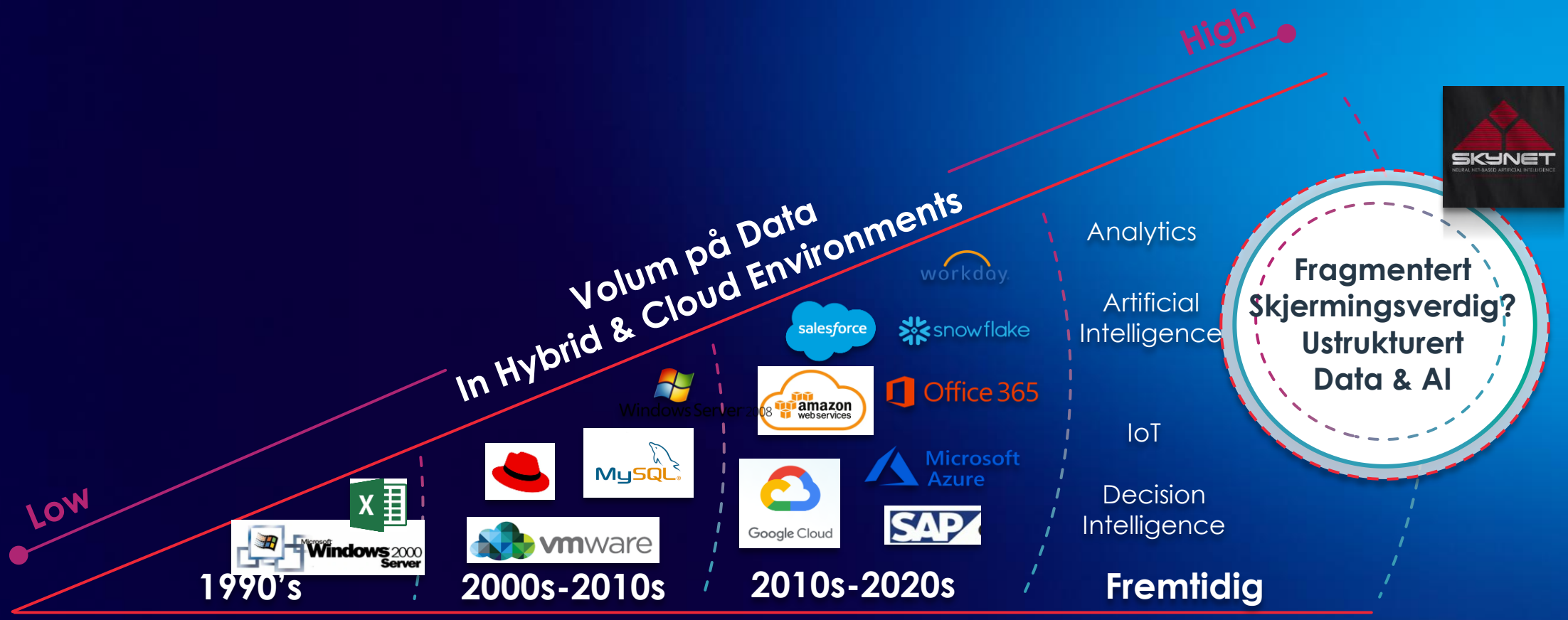
Thales i Norge

- Thales er en betydelig del av norsk samfunnssikkerhet og beredskap
- Tilstede i Norge siden 1998
- Thales sikrer norske bank & finans-, helse- energiplattformer og kritiske data
- Vi er partnere med Kongsberg Group
- Vi lager nasjonal ID: norske pass, førerkort og ID-kort
- Norsk flytrafikk og Avinor stoler på Thales
- Vipps, NATO, SWIFT m.m
- Partnersalg: Atea, Sopra, Mnemonic, Orange, Vivicta, Netnordic, Accenture, Exclusive Networks (Disti), DXC, Dell, HPE, Google, AWS

THALES

Mengden data øker betydelig og eksponsensielt

(...men det finnes metoder for å analysere, klassifisere og kryptere alt)



Hvordan beskytter du dine data i fremtiden?

THALES
CYBERSECURITY

Hva advarer NSM og PST kommunene mot?

NSM: Risiko 2026

1. Kjenn verdiene, avhengighetene og sårbarhetene
2. Sikkerhetsstyring må være en del av virksomhetsstyringen
3. Roller må ha ansvar, kapasitet og kompetanse
4. Tiltak må testes, kontrolleres og øves
5. Sky og leverandører påvirker kontrollen over data

PST: Nasjonal trusselvurdering 2026

1. Flere cyberoperasjoner forventes å lykkes
2. Statlige aktører bruker cyber til innhenting og kartlegging
3. Tekniske sårbarheter og sosial manipulering kombineres
4. KI kan brukes i alle faser av et datainnbrudd
5. Personer med tilgang til sensitiv informasjon er attraktive mål

For kommunene: Forebygg inntrenging, men planlegg for å begrense konsekvensene når noen kommer inn.

ERFARING

Lørenskog: Hva skjedde og hvorfor ble konsekvensene så store?

7. april
1
Skadevare lastes ned

22. april
2
Tilgang til servermiljø

8. mai
3
Angrepet gjennomføres

9. mai
4
Hendelsen oppdages

26 dager

fra første relevante varsel til første tiltak

Varsler uten rask nok respons

Signalene ble ikke raskt nok koblet sammen, prioritert og eskalert.

Eldre data ble liggende

Migrering, opprydding og dokumentert sletting var ikke fullført.

Flere forhold virket sammen

Teknologi, styring, kapasitet, eierskap og respons påvirket skadeomfanget.

Dette var ikke én enkelt feil. Det var et kontrollmiljø som ikke ga tilstrekkelig praktisk effekt.

DATAFLYT

Hvordan oppstår og spres kommunale data?

Datadelingsprinsipper: Data flyttes, kopieres, eksporteres, arkiveres og gjenbrukes gjennom hele tjenesteløpet

Fagsystemer	Skole, helse, barnevern, sosialtjenester
Databaser og integrasjoner	API-er, rapportering og datautveksling
Filområder og samhandling	Dokumenter, e-post, Teams og lokale kopier
Arkiv og backup	Historikk, sikkerhetskopier og eksportfiler
Sky og leverandører	SaaS, driftspartnere og underleverandører

DATAENES BAKGÅRD

Hvorfor blir gamle og sensitive data liggende?

1	**Uklart eierskap**	Prosjektet avsluttes, men ingen eier oppryddingen.
2	**Migrering først**	Data flyttes, mens sletting og kvalitetskontroll utsettes.
3	**Arkiv og sletting**	Krav oppfattes som vanskelige å forene i praksis.
4	**Gamle områder virker**	Ansatte fortsetter å bruke det som fortsatt er tilgjengelig.
5	**Risiko blir stående**	Tiltak, finansiering eller aksept blir ikke tydelig besluttet.

Når ingen eier avslutningen, blir midlertidig lagring permanent.

Hvem har tilgang, og hvordan brukes dataene?

Ansatte og ledere

Rollebasert tilgang

Applikasjoner og API-er

Maskinell tilgang

Leverandører

Drift og support

KI og automatisering

Nye tilgangsaktører

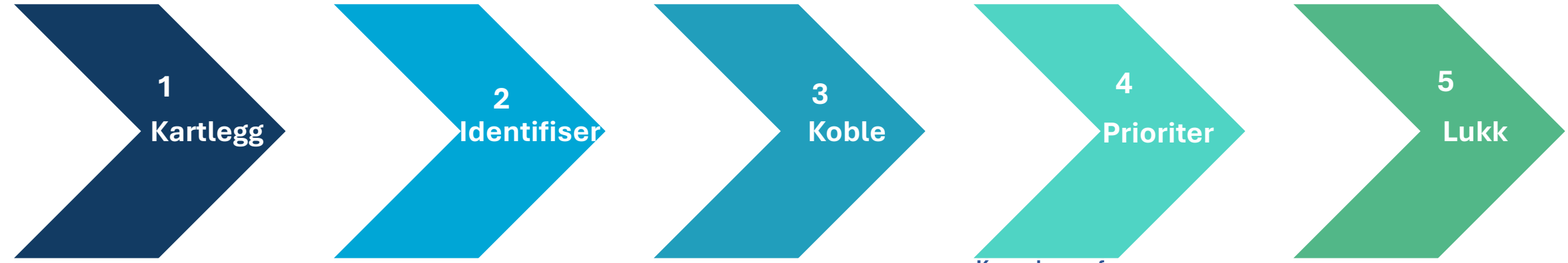
Administratorer og tjenestekontoer

Privilegert tilgang

Tilgang må vurderes mot tjenestelig behov, faktisk bruk og endringer over tid.

ANBEFALT ARBEIDSMÅTE

Fra antakelser til et faktabasert risikobilde



Et risikobilde er først nyttig når det kan besvare:

- Hva finnes faktisk?
- Hva kan gå galt?
- Hva betyr det?
- Hvem eier det?
- Hva gjør vi nå?

Målet er ikke flere funn. Målet er beslutninger som reduserer risiko.

KONTROLL GJENNOM HELE LIVSLØPET

Klassifisering, eierskap og livssyklusstyring i praksis

Formål og kilde

Riktig tilgang

Kontrollert flyt

Arkiv og beskyttelse

Dokumentert avslutning

KLASSIFISERING

Gjør risiko og krav forståelige

EIERSKAP

Gjør beslutninger og ansvar tydelige

DOKUMENTASJON

Viser at kontrollene faktisk virker

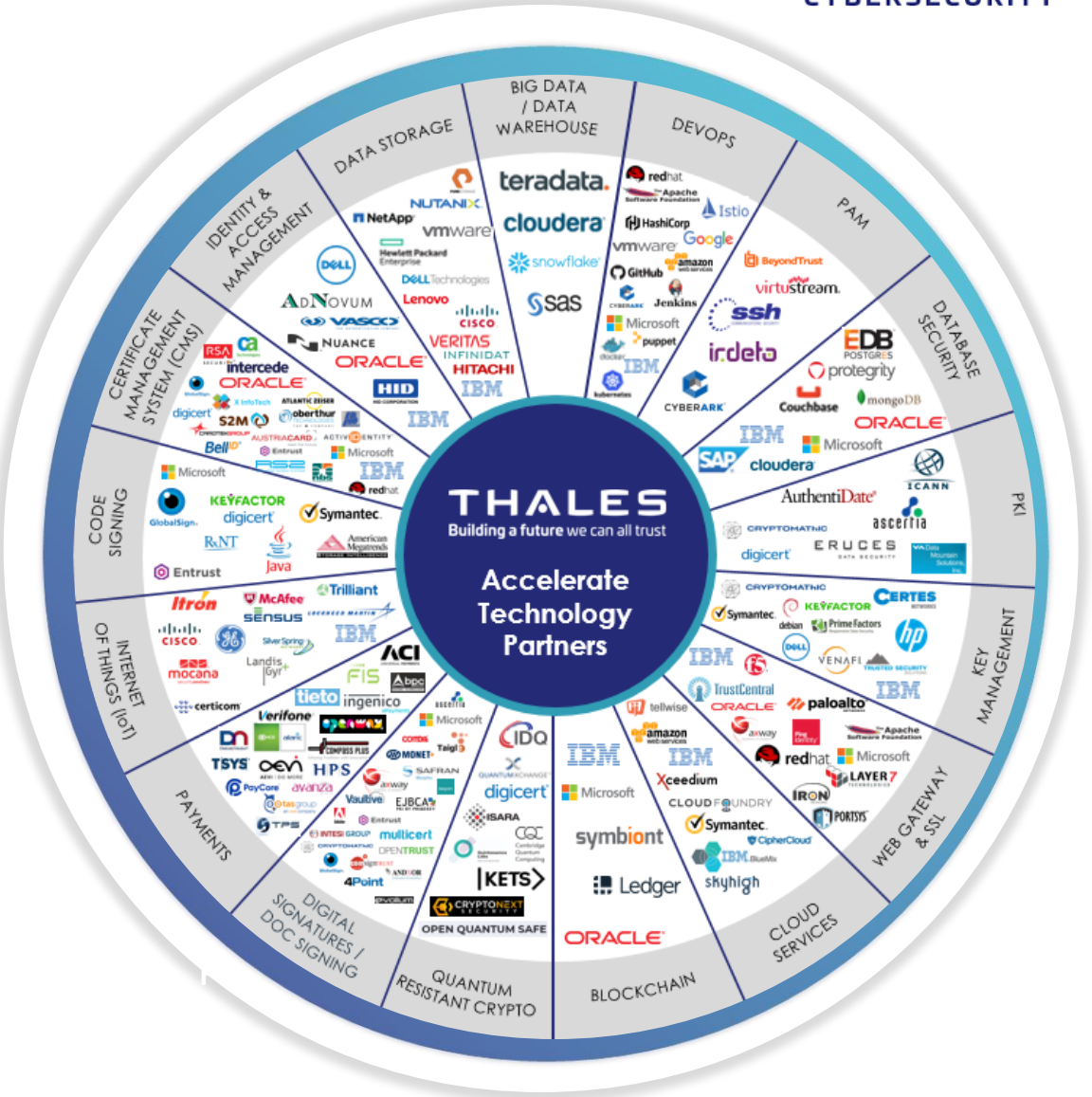
Datastyring er en løpende virksomhetsprosess, ikke et engangsprosjekt.

Hvordan? Og hva skal kommunen oppnå?

THALES
CYBERSECURITY

Bygg eller anskaff en plattform for:

- Crunch, scanne og oppdage
- Agnostisk: på tvers av onprem, hybrid og sky
- Analysere
- **Beskytte, sikre, kryptere**
- For dermed å kontrollere
- Få innsyn I dine egne **data**, inkludert klassifisering, **risk insights**, shaping av **datalake til SIEM & SOC**
- Integrerer med **dine** løsninger for Compute, DC, Cloud og den AI`n kommunedirektøren hørte om på Arendalsuka nylig
- Repeter! Det er en kontinuelig prosess



Oppdag:
CONTINUOUSLY DISCOVER & CLASSIFY DATA AT SCALE

Analyser:
INTELLIGENCE TO ACCURATELY ASSESS DATA RISK

Beskytt:
INSTANT, CONFIGURABLE DATA DEFENSES

Kontroller:
CENTRALLY MANAGED PRIVILEGES AND DATA ACCESS

Improved Unified Workflows

Move from passive to proactive risk remediation with a simplified user interface, easier deployment, faster time to value

External Vendor Integration

Ticketing systems, SIEMs, Data classification, DSPM & CSPM external feeds (aka - Vulnerability assessments), integration with DLP

Advanced Use Cases

Keys & secrets posture management,
AI posture management,
Post-quantum posture management

THALES
CYBERSECURITY

MULIGHET OG RISIKO

KI trenger riktige, kontrollerte og pålitelige data

1 **Datakvalitet** Feil og utdaterte data gir svakere resultater

2 **Tilgang** KI kan kombinere mer informasjon enn enkeltbrukere

3 **Avledede data** Sammendrag og dokumenter blir nye sensitive datasett

4 **Styring** Formål, eierskap og lagring må være tydelig

34% Har full oversikt over hvor dataene er lagret

39% Kan klassifisere alle dataene sine

KI blir ikke bedre enn dataene, tilgangene og styringen den bygger på.

LEDELSESDIALOG

Fra teknologispråk til ledelsesspråk: Hva må kommunen vite?

1. Hvilke tjenester og innbyggere kan bli berørt?
2. Hvilke sensitive data har vi ikke tilstrekkelig kontroll på?
3. Hvem eier risikoen og beslutningen?
4. Hvilke tiltak er gjennomført, og virker de?
5. **Hvilken restrisiko aksepterer kommunen bevisst?**

Kan kommunen svare på hvor dataene er, hvem som bruker dem, og hva som skjer når noe avviker?

+ IKKE BE OM PENGER TIL DATAKLASSIFISERING!

TUSEN TAKK!

Niels Fredrik Berthelsen
Country Sales Manager
niels.berthelsen@thalesgroup.com
+47 99483521

THALES
CYBERSECURITY