



Säker lagring i molnet

Daniel Akenine

KORT OM MIG

- Teknik och säkerhetschef Microsoft
- Ordförande IASA – Sveriges IT arkitekter
- Ledamot i regeringens samordningsråd för säkerhet och integritet i smarta elnät.
- Ledamot i ISO's internationella expertgrupp för standarder inom cloud computing
- Ledamot i ledningsgruppen för Cloud Sweden samt EuroCloud.
- Undervisar på KTH

FÖRTROENDE FÖR MOLNET

FRÅGAN FINNS ÖVERALLT – “KAN JAG LITA PÅ MOLNET?”

“Concerns”

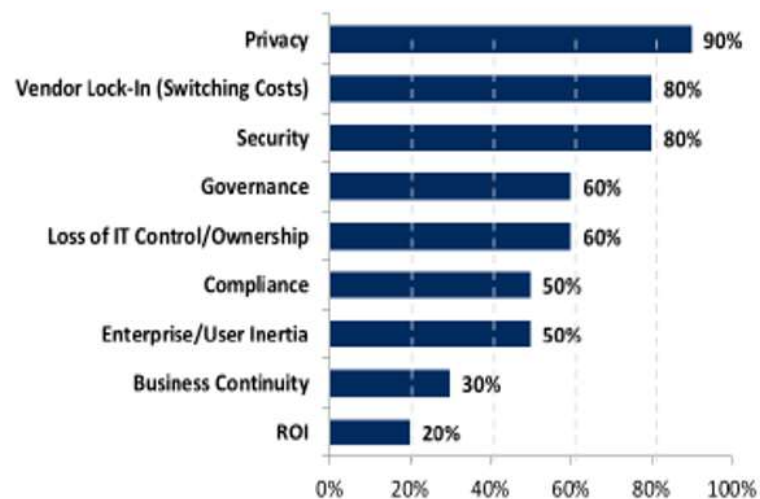
✓ Privacy

✓ Loss of Control

✓ Regulatory Compliance

✓ Security

FIG. 19: PUBLIC CLOUD CONCERNS IN THE EUROPEAN PUBLIC SECTOR



VANLIGA FRÅGOR

SÄKERHET

- Är molnet säkert?
- Är era molntjänster säkra?

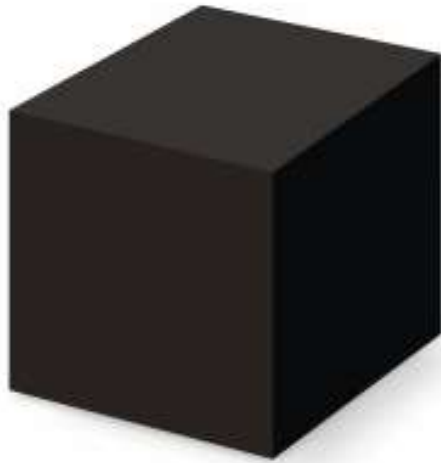
PRIVACY

- Vad betyder integritet för Microsoft?
- Var finns mitt data ?

COMPLIANCE

- Vilka certifieringar och förmågor kan ni garantera?
- Hur stödjer Microsoft mitt behov kring regulatoriska krav ?
- Har jag rätt att utföra en audit av Microsofts datacenter?





1. Lova

2. Bevisa

OM ATT LOVA OCH BEVISA I MOLNET

1. Följ säkerhetsstandarder (ISO 27001)
2. Revision och audit (SSAE 16)
3. Visa

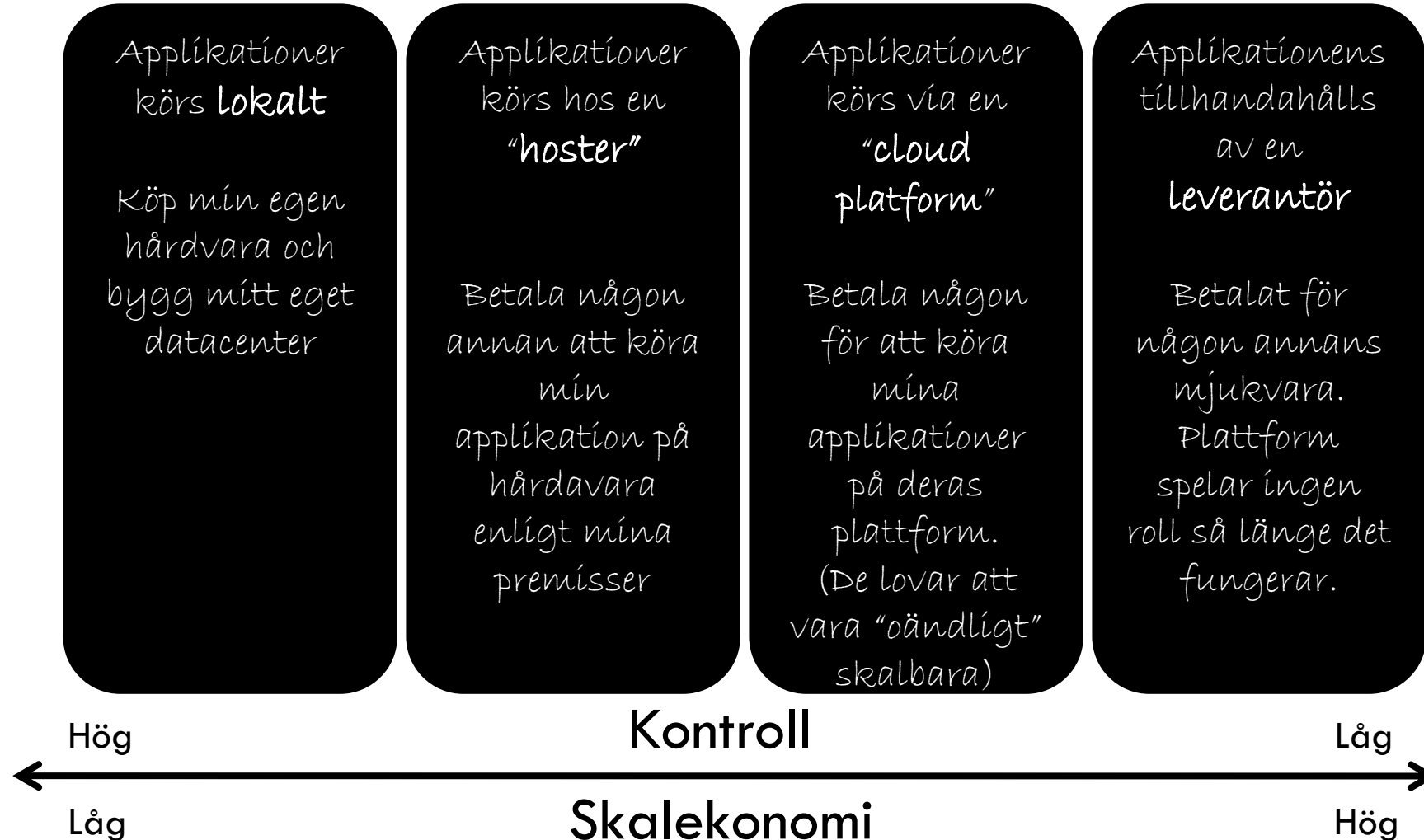
DET FINNS OLIKA TYPER AV MOLN

”Take your pick”

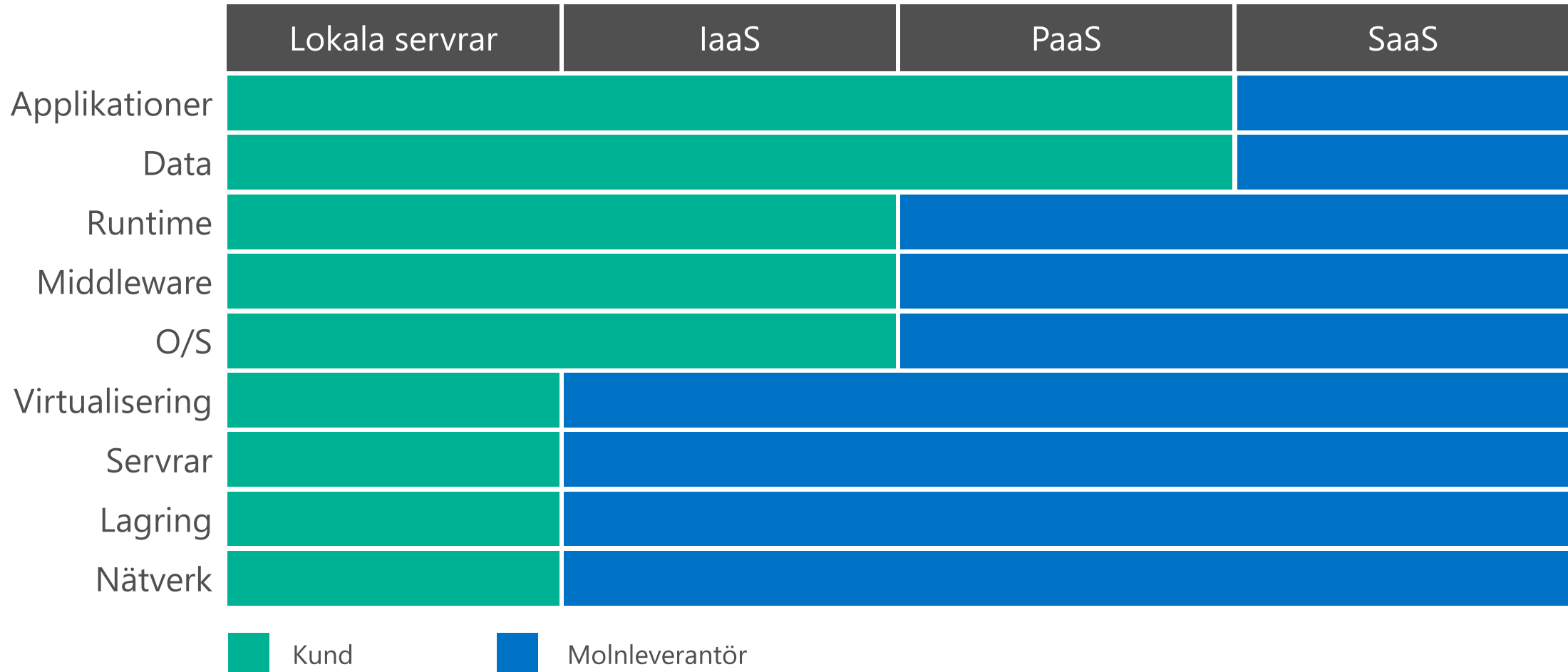
Idag finns det ett val mellan
kontroll och “skalekonomi”



"Take your pick"



Ditt ansvar beror på vilken molntjänst du väljer



Vilka komponenter bygger trovärdiga moln?

Cybersäkerhet



Integritet



Compliance



Transparens



Fysisk säkerhet



Fysisk tillgång



Brandskydd



2-factors auth

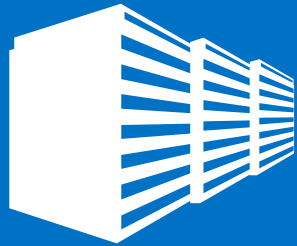


Övervakning



Vad innebär transparens?

Var är data lagrad?



Ex: Azure kunder kan själv välja var data skall lagras.

Vem har tillgång och vad har de fått tillgång till?



Kunddata endast möjlig att nå vid support case.

Varje access ses som ett undantag som loggas i minsta detalj.

Hur får jag reda på vad som händer?



Alla ändringar runt data policy meddelas.

Alla ändringar i underleverantörer meddelas.

Tillgång till tredjeparts revisioner av tjänsterna

Compliance

1. Fundament

- Plattform och tjänster är certifierade mot ett stort antal standarder som: ISO 27001, EUMC, HIPAA, FISMA
- Personuppgiftsbiträdesavtal

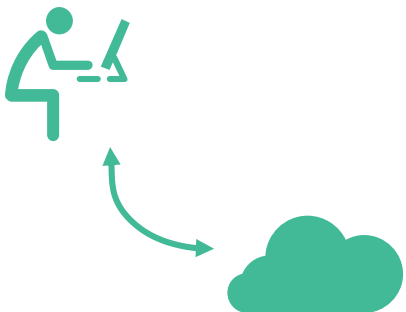
2. Anpassning

- Möjligheter för administratörer att hantera arkivering, loggning, "data loss prevention" för egen lagstifning

Lite kort om kryptering för säker lagring i molnet

TYPER AV KRYPTERING

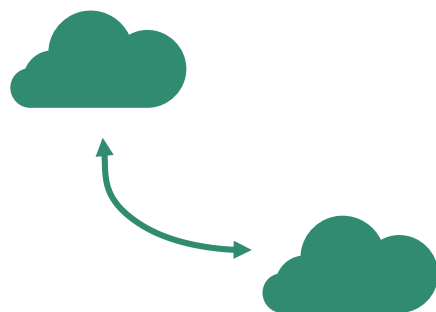
1



Data som rör sig mellan en användare och en tjänst.

Skyddar data på internet och ser till att behålla integritet i en transaktion.

2



Data som rör sig mellan datacenters.

Skyddar mot massövervakning.

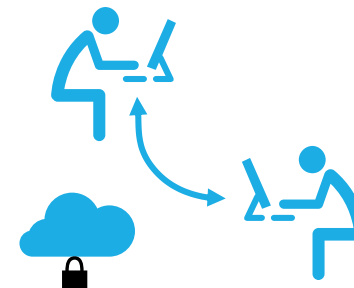
3



Data i vila

Skyddar mot stöld av fysisk media.

4



Punkt-till-punkt kryptering av kommunikation mellan användare.

Skyddar data och integritet mellan användare.

CASE STUDY: SÄKRA LOGGAR INOM BANK/FINANS



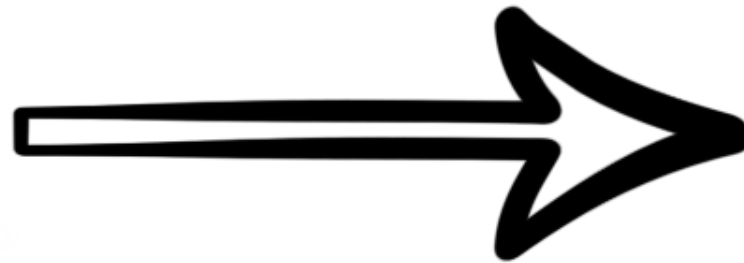
CASE:

Hur ser man till att skapa en datalogg där man inte kan ta bort data, lägga till data eller förändra data?

LÖSNING: SKYDDA DATALOGGAR ALGORITMISKT

Tjänster som SecureLog använder "molnet" för att säkerställa att databaser och loggar inte kan manipuleras i efterhand.

Exempel: Penningtvättjänster.



SAMMANFATTNING - VAD ÄR “SÄKER LAGRING”?

Tillförsikt till:

- Säkerhet
- Integritet
- “Compliance”
- Transparens

