



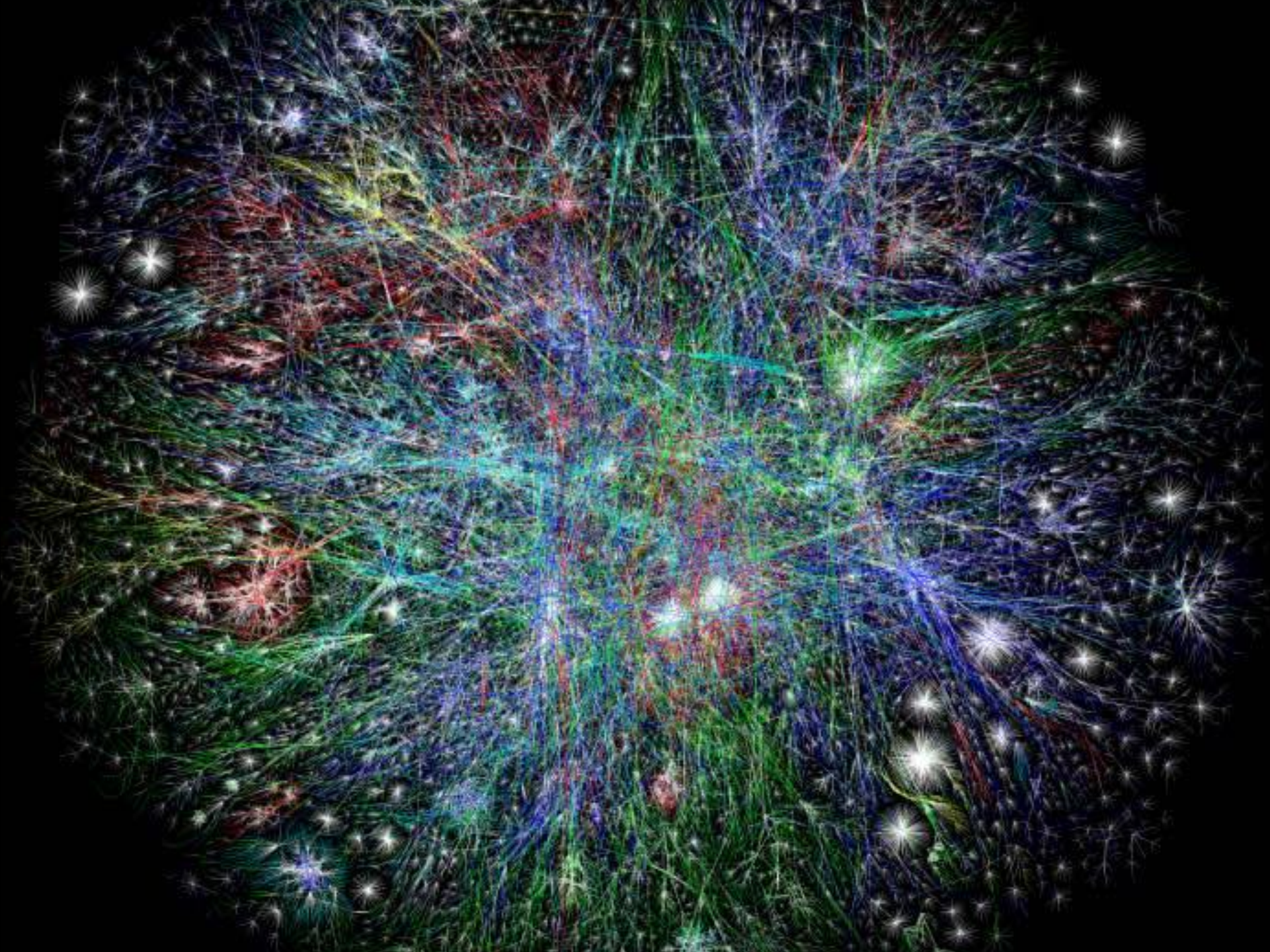
Molnet, skolan och säkerheten

Anne-Marie Eklund Löwinder, säkerhetschef,
Internetstiftelsen i Sverige

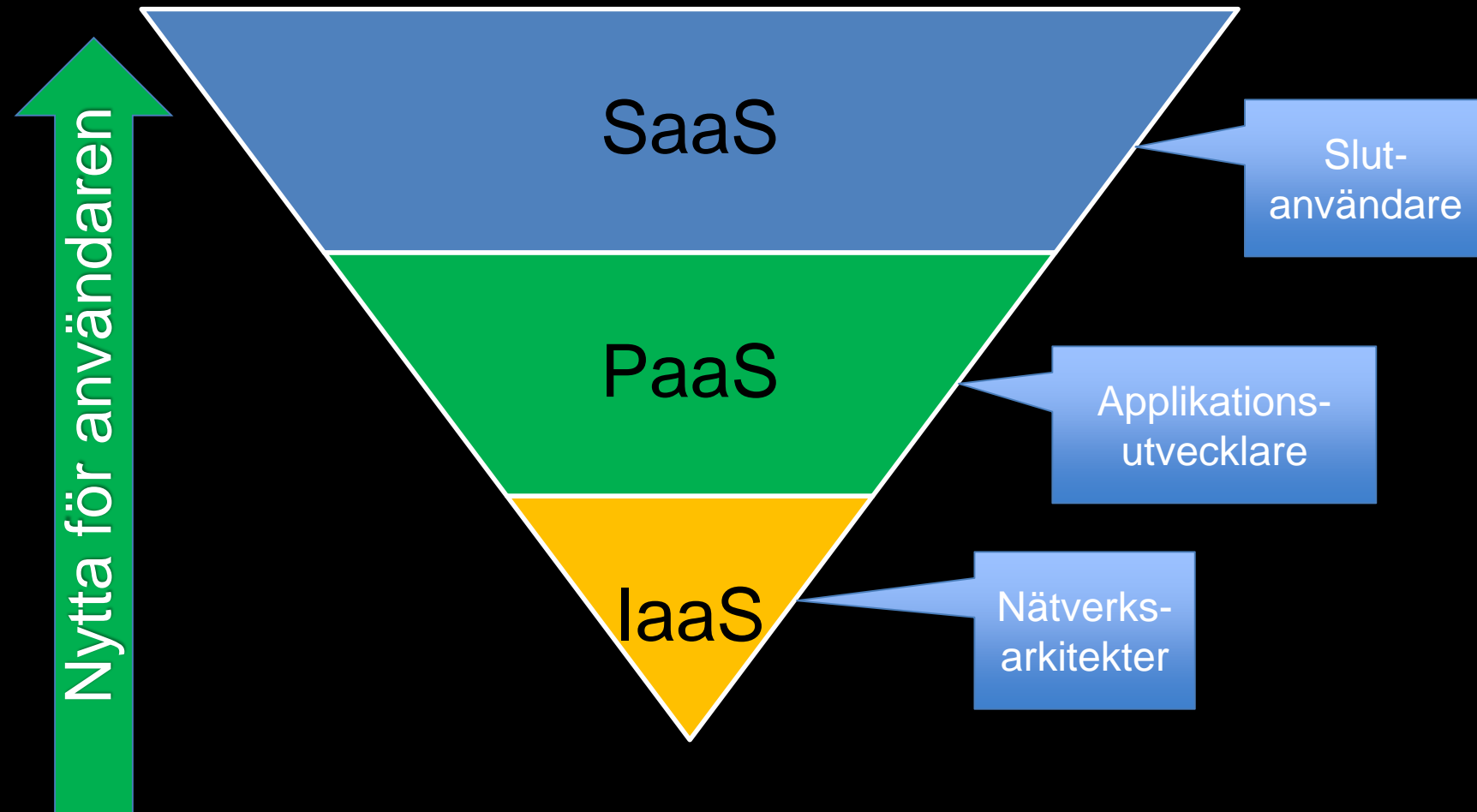
@amelsec

amel@iis.se





Vad finns under ytan?



Någonstans finns en fysisk maskin



Tillgång till en lösning

- Så snabbt som möjligt
- Så billigt som möjligt
- Så bra som möjligt



Molntjänster är attraktiva

- Låg inkörningströskel
- Betala i kassan
- Anpassa efter behov (skala upp/ner)
- Hög tillgänglighet (kanske)

Digitala lärplattformar och läromedel

- Vilka system används?
- Vilka uppgifter hanteras?
- Till vad används uppgifterna?
- Hur länge sparas de?
- Vem har tillgång till uppgifterna?

Potentiella sårbarheter i molntjänster

- Tillförlitlighet och tillgänglighet
- Konfidentialitet (kryptering)
- Dataskydd och portabilitet
- Inlåsnings hos leverantör
- Internetberoende

Var behövs säkerhet?

- Internetkommunikation/nätverk
- Serveråtkomst
- Programåtkomst
- Dataåtkomst
- Dataintegritet

Lösningar: säker identifiering, kryptering, et cetera

Kan du lita på din leverantör?

- Vem äger eller har nyttjanderätten till den information som skickas upp till molnet?
- Vem äger metadata eller information som skapas i molnet som en del i nyttjandet av tjänsten (statistik, loggar)?
- Vad händer när molnleverantören säljs, går i konkurs, har allvarliga driftsproblem, blir ertappad med något fuffens eller bara inte sköter sig?

Efteråt?

- Försvinner känslig information från lagringsenheter efter avslutat avtal?
- Vad händer med data som lagras i molnet när det har passerat ägarens bäst före-datum?
- Vad har molnleverantören för policy för datasanering när de ska pensionera gamla lagringsenheter och maskiner?

Säkerhetskravställning ISO 27017:2015

- Tillgänglighet
- Autentisering och behörighetshantering
- Kryptering
- Nätverkssäkerhet
- Spårbarhet
- Gallring
- Avveckling och förstöring

Utvärdering

- Gruppera och ställ krav till rätt målgrupp:
 - driftkrav (alla nivåer)
 - krav på tjänsten (SaaS)
 - integrationskrav (SaaS)

Utvärdering - drift

- Behörighetsprocess
- Härdning/patchning
- Lagring och backup
- Spårbarhet - åtkomst till loggarna
- Incidenthantering (inkl. säkerhet)

Utvärdering - tjänst

- Säker utveckling (SDL, OWASP)
- Säkerhetstester (pen-test)
- Web Application Firewall (WAF)
- Autentiseringsmekanismer
- Kryptering av information
- Spårbarhet

Utvärdering - integration

- Autentisering (SAML/ADFS)
- Vilka nätintegrationer krävs?
- Vilken infrastruktur krävs internt?
 - API gateway
 - integration gateway
 - proxy lösningar
- Tredjepartsintegratörer

Uppföljning

s?

- Går det att genomföra audit (enligt avtalet)?
- Extern revision eller kunden själv?
- Regelbundna pentester
 - Kräv rapport från test och hantering av upptäckta sårbarheter

Avslut

- Strategi för avslut?
- Finns det stöd i avtalet att informationen kan exporteras till en annan tjänst eller kunden själv?
- Tas informationen bort efter exit?
- All information? Även behörigheter? Loggar?

Inget nytt under solen...

- Behovsanalys
- Kravspecifikation
- Ansvarsfördelning
- Avtal
- Uppföljning
- Granskning

Sammanfattning 1 (2)

- Molntjänster är här för att stanna
- Många är bra, men det finns spelare med bristande rutiner
- Utvärdera kvalitet och säkerhet på alla nivåer
- Avtal bör innehålla alla relevanta delar
- Beräkna en totalkostnad inklusive integration

Sammanfattning 2 (2)

- Genomför risk- och sårbarhetsanalys
 - vad blir konsekvensen för dig och din information
 - agera efter det

Tack!
Frågor?

Anne-Marie Eklund Löwinder
Säkerhetschef, IIS

amel@iis.se

@amelsec

<https://www.iis.se>