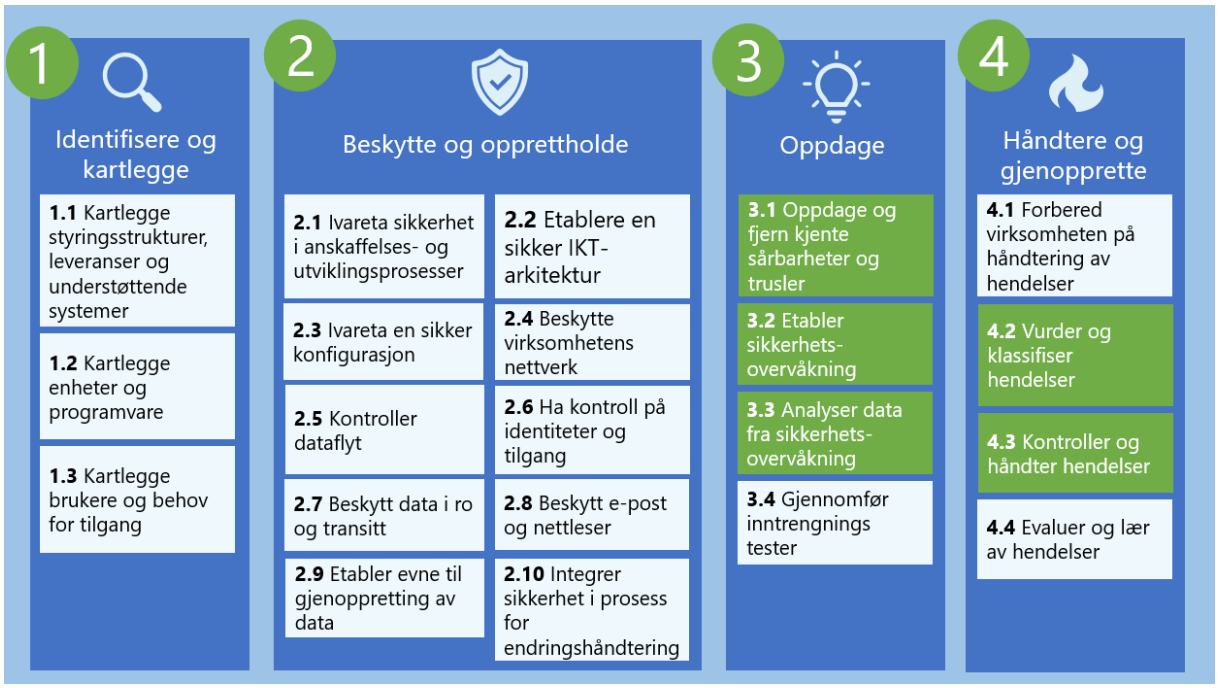
Passer på at du er sikker, døgnet rundt, hele året

Sikkerhetssenteret (SOC) passer på deg 24/7 og kan oppdage og stoppe Cyberangrep mot ditt Microsoft 365 miljø eller dine maskiner slik at du kan jobbe trygt og sikkert.

Sikkerhetssenter	
Umulig reise: Bruker logger seg fra ukjent lokasjon eller uvanlig sted på Microsoft 365	●
Monitorering og loggføring av all aktivitet i Microsoft 365	●
Automatisk sak ved deteksjon av datainnbrudd eller Cyberangrep mot Microsoft 365 miljø	●
Agent på enhet som analyserer og overvåker PC eller Mac	●
Overvåker Windows, MacOS for mistenkelige prosesser, hendelser, sikkerhetsrelaterte aktiviteter som mislykkede påloggінger, sletting av sikkerhetslogger og uautorisert aktivitet.	●
Oppdage sårbarheter, programmer, kryptominere, hackerverktøy og passordknekkere mm.	●
Kontinuerlig overvåking av prosesser som kan indikere et tidlig hackerangrep	●
Oppdager nettverksforbindelser til forskjellige nasjonalstater som er kjent for å engasjere seg i cyberterror-aktiviteter.	●
Automatisk isolering av klienten dersom den er utsatt for angrep eller er hacket	●
Pris pr. mnd. pr. bruker pr. PC eller Mac	**149,-**

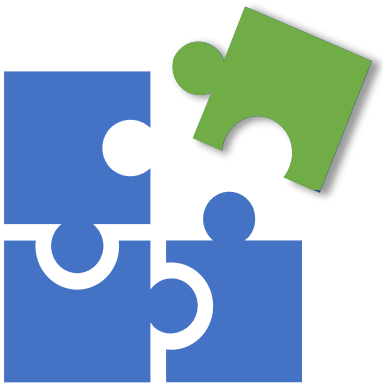


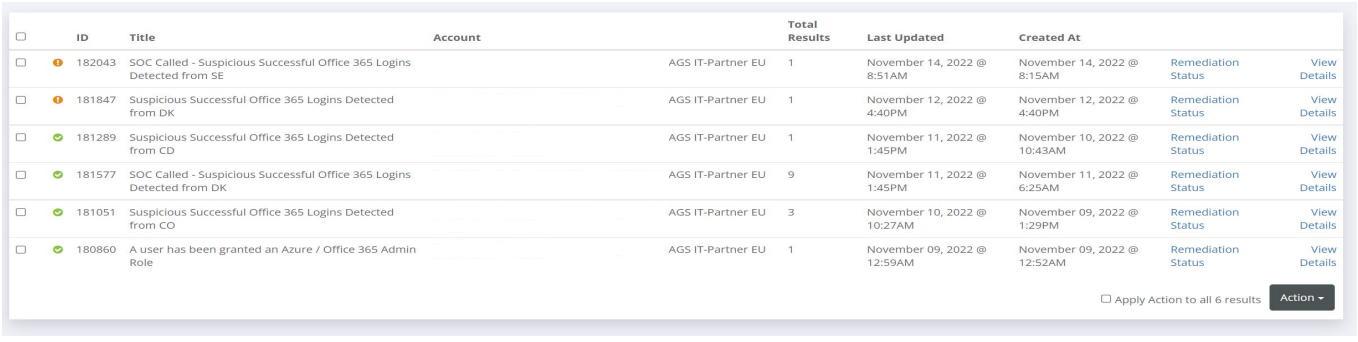
NSM (Nasjonal sikkerhetsmyndighet) - 4 grunnprinsipper for sikkerhet

Sikkerhetssenteret jobber med utgangspunkt i NSM (Nasjonal Sikkerhetsmyndighet) 4 grunnprinsipper om sikkerhet.

Målet er å hjelpe deg å oppfylle kravene som stilles til IT-sikkerhet i grunnprinsippene. Her vil Sikkerhetssenteret bidra til å dekke følgende punkter.

- **3.1** Oppdage og fjern kjente sårbarheter og trusler
- **3.2** Etabler sikkerhets-overvåkning
- **3.3** Analyser data fra sikkerhets- overvåkning
- **4.2** Vurder og klassifiser hendelser
- **4.3** Kontroller og håndter hendelser





	ID	Title	Account		Total Results	Last Updated	Created At		
☐	182043	SOC Called - Suspicious Successful Office 365 Logins Detected from SE		AGS IT-Partner EU	1	November 14, 2022 @ 8:51AM	November 14, 2022 @ 8:15AM	Remediation Status	View Details
☐	181847	Suspicious Successful Office 365 Logins Detected from DK		AGS IT-Partner EU	1	November 12, 2022 @ 4:40PM	November 12, 2022 @ 4:40PM	Remediation Status	View Details
☐	181289	Suspicious Successful Office 365 Logins Detected from CD		AGS IT-Partner EU	1	November 11, 2022 @ 1:45PM	November 10, 2022 @ 10:43AM	Remediation Status	View Details
☐	181577	SOC Called - Suspicious Successful Office 365 Logins Detected from DK		AGS IT-Partner EU	9	November 11, 2022 @ 1:45PM	November 11, 2022 @ 6:25AM	Remediation Status	View Details
☐	181051	Suspicious Successful Office 365 Logins Detected from CO		AGS IT-Partner EU	3	November 10, 2022 @ 10:27AM	November 09, 2022 @ 1:29PM	Remediation Status	View Details
☐	180860	A user has been granted an Azure / Office 365 Admin Role		AGS IT-Partner EU	1	November 09, 2022 @ 12:59AM	November 09, 2022 @ 12:52AM	Remediation Status	View Details

☐ Apply Action to all 6 results Action

Her ser du et eksempel fra Sikkerhetssenterets saks-logg over mistenkelig påloggingen og trafikk.

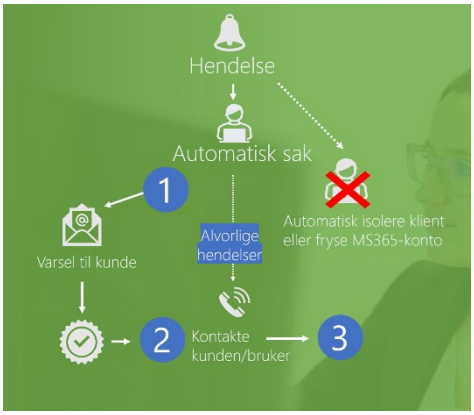
Slik fungerer det

Ved deteksjon av alvorlige hendelser og angrep vil Sikkerhetssenteret (SOC) kontakte deg og informere deg om hendelsen.

- Er en av Microsoft 365 brukerne dine under angrep eller utsatt for datainnbrudd vil Sikkerhetssenteret hjelpe deg med å bytte passord eller midlertidig deaktivere kontoen.

- Dersom det oppdages angrep eller mistenkelig aktiviteten av dine PC eller Mac brukere vil vi automatisk isolere klienten fra nettverket og andre brukere.

- Du vil også bli kontaktet dersom vi ser mistenkelige vellykkede påloggінger fra land, eller nettverk som er kjent for Cyberangrep på ditt Microsoft 365 miljø



Scenario vi passer på

Sikkerhetssenteret gjenkjenner mange metoder for angrep på Microsoft 365 eller på maskinen din. Det kan oppdage sårbarheter, programmer, kryptominere, hackerverktøy og passordknekkere på enheten din, og overvåker kontinuerlig prosesser som kan indikere et tidlig hackerangrep.

Umulig reise:
Bruker logger seg på vellykket fra en ukjent lokasjon eller uvanlig sted på Microsoft 365

Lekket passord
Brukers Microsoft 365 passord er lekket via andre tjenester på DarkWeb

Mistenkelig trafikk
Oppdager nettverksforbindelser til forskjellige nasjonalstater som er kjent for å engasjere seg i cyberterror-aktiviteter.

Her får du Sikkerhetssenteret

Du kan få Sikkerhetssenteret levert på flere måter fra oss. Vi har integrert løsningen i våre beste supportavtaler og pakkeløsninger slik at du skal få mest mulig for it-pengene.

Ønsker du kun tilgang til Sikkerhetssenteret kan du få levert løsningen som et Stand-Alone produkt.

Funksjonalitet	Stand Alone	Premium Support	All-Inclusive	Smart Bedrift	Smart Bedrift+
Lekket Microsoft 365 passord på DarkWeb	●	●	●	●	●
Pålogging fra ukjent lokasjon på Microsoft 365	●	●	●	●	●
Monitorering av aktivitet i Microsoft 365	●	●	●	●	●
Deteksjon av Cyberangrep mot Microsoft 365-miljø	●	●	●	●	●
Automatisk sikkerhets-oppdatering av PC	✕[3]	●	●	●	●
Premium support pakke	✕	●	●[4]	●	●
Antivirus mot malware og løspengevirus	✕[5]	✕[5]	✕[1]	●	●
2-trinns pålogging og kryptering av PC mot tyveri	✕[2]	✕[2]	✕[2]	●	●
Analyserer og overvåker PC eller Mac for angrep	●	✕	●	✕	●
Overvåker mistenkelige prosesser og hendelser	●	✕	●	✕	●
Oppdage kryptominere og hackerverktøy	●	✕	●	✕	●
Nettverksforbindelser til land kjent for angrep	●	✕	●	✕	●
Automatisk isolering av klienten ved angrep	●	✕	●	✕	●
Pris pr. mnd. pr. bruker	149,-	265,-	365,-	699,-	799,-

Inkludert i Microsoft Business Premium abbonement[1]
Må settes opp i Microsoft Business Premium (Sikkerhetspakke I)[2]
Egen driftstjeneste og sikkerhetsoppdateringer for PC og Mac[3]
Inneholder All-Inclusive supportpakke[4] Egen tjeneste[5]

Microsoft lisenser som du bør ha

Vi anbefaler deg minimum Microsoft Business Premium som grunnleggende Microsoft lisens for dine desktop brukere. For å effektivt overvåke ditt Microsoft 365 miljø er dette den beste lisensen for bedrifter opptil 300 brukere.

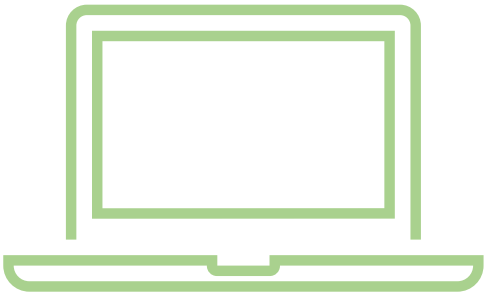
Det anbefales også at du har en eller flere Azure AD P2 abonnement for at Microsoft skal gi mer informasjon raskere til Sikkerhetssenteret for å stoppe mulige angrep eller innbrudd.

Har du ikke denne lisensen vil informasjonen som Sikkerhetssenteret får fra Microsoft ikke være helt optimal, og bli noe begrenset og forsinket i forhold til å detektere, analysere og reagere på angrep.

Slik får du tilgang til Sikkerhetssenteret

Oppstart og tilgang til Sikkerhetssenteret gjøres enkelt og raskt dersom du ønsker å komme i gang.

- Vi trenger tilgang til ditt Microsoft 365 miljø slik at vi kan integrere Sikkerhetssenteret.
- Du vil få en link som automatisk laster ned og installerer klienten på Mac eller PC.
- Sikkerhetssenteret har ingen bindingstid, men vil automatisk fornyes for en ny måneds-periode dersom du ikke sier opp abonnementet før ny periode starter.
- Maskinen din vil bruke litt ekstra kapasitet noen dager etter installasjonen da Sikkerhetssenteret må kartlegge maskinen din første gangen.



- Har du en Supportavtale Premium, All-Inclusive eller Smart Bedrift pakken vil Sikkerhetssenteret allerede være inkludert i onboarding av bedriften din.

Ta gjerne kontakt med oss dersom du ønsker mer informasjon eller et møte.

TA KONTAKT
start@ags.no