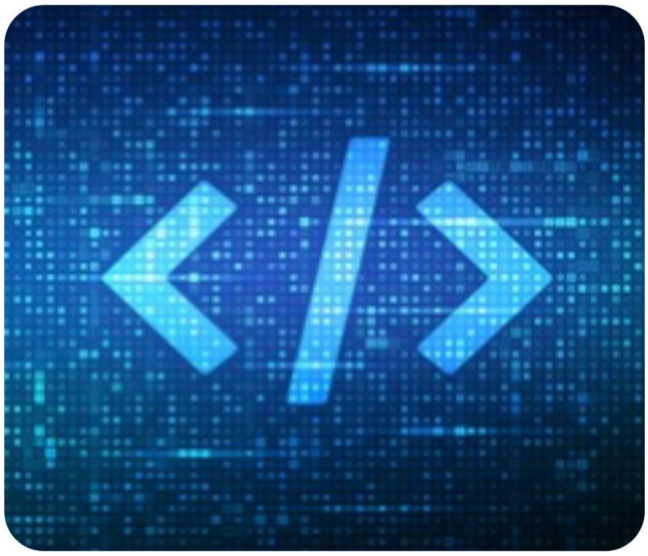
IT sikkerhet og personvern



tradesolution

Revidert 10. oktober 2024

Vårt sikkerhetsarbeid

Tradesolution jobber kontinuerlig med informasjonssikkerhet for å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Sikkerhetsarbeidet er forankret i ledelsen som årlig gjennomgår våre sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene.

Dette gir retningslinjer som setter krav til våre tekniske og organisatoriske tiltak. Dette følges opp gjennom vår internkontroll. Vår internkontroll og informasjonssikkerhetspolicy sikrer behandling av informasjonsverdier og personopplysninger på en lovlig, sikker og forsvarlig måte.

Våre viktigste sikkerhetstiltak

- Alle som jobber i Tradesolution må signere taushetserklæring og sikkerhetsinstruks
- Alle systemer etterlever OWASP Top-10
- Alle våre systemer testes ukentlig for kjente sårbarheter gjennom Detectify
- Alle produkter i Microsoft Azure settes opp med bestemte sikkerhetstiltak tiltenkt produkttypen. Disse tiltakene etterlever de tekniske krav fra ISO27001

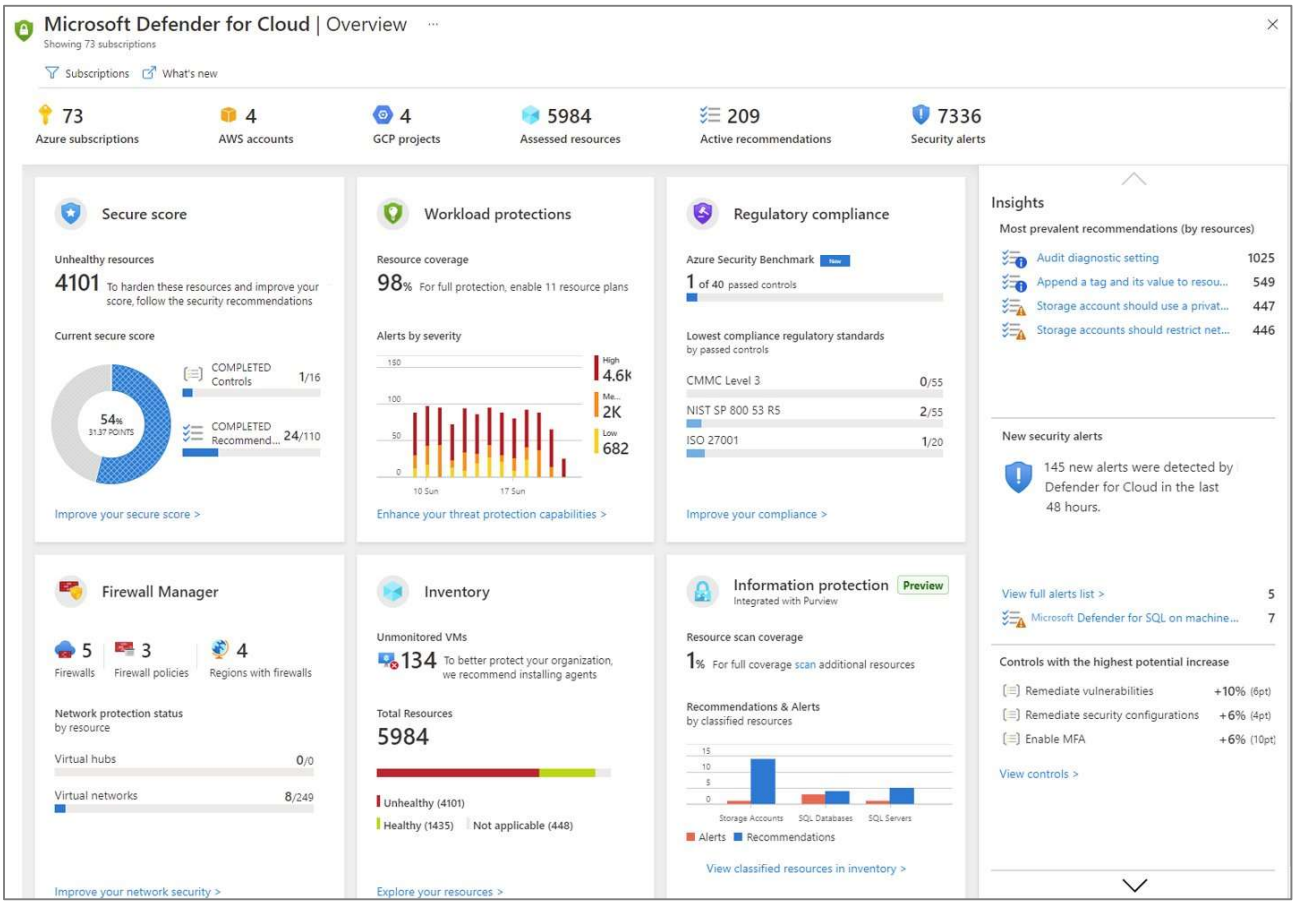
Hovedfokus i vårt sikkerhetsarbeid

- **Konfidensialitet:** Sikre at informasjonen ikke blir kjent for uvedkommende
- **Integritet:** Sikre at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- **Tilgjengelighet:** Sikre at informasjonen er tilgjengelig for autoriserte brukere etter behov
- **Robusthet:** Sikre at organisasjonen og systemene er motstandsdyktig, og evner å gjenopprette normaltilstand ved hendelser

Konfidensialitet

For å sikre at informasjon ikke blir kjent for uvedkommende har vi satt opp flere tekniske tiltak gjennom Microsoft Defender for Cloud.

Eksempelvisning hentet fra internett:



ISO27001

For å sikre tjenester og informasjon har Tradesolution valgt å etterleve tekniske krav fra ISO27001. Microsoft Defender rapporterer oppdatert status daglig.
Les mer: Defender-for-cloud: ISO27001

Kryptering

Tradesolution krypterer all kommunikasjon og lagret data. Kommunikasjon mellom klient og server blir kryptert med TLS/SSL sertifikat. Lagret data i Azure-SQL eller skylagring er satt opp med «encryption at rest».

Les mer her:
Azure SQL – Transparent Data Encryption
Storage Account – encryption for data at rest

Penetrasjonsstesting

Tradesolution benytter Detectify for overflateskanning på alle eksponerte endepunkter, og applikasjonsskanning etter sårbarheter definert i OWASP Top 10. Detectify oppdaterer sin sårbarhetsskanner jevnlig med nye sårbarheter som blir rapportert eller funnet på internett.

Les mer her: Detectify

Fysisk sikring – Microsoft datasenter

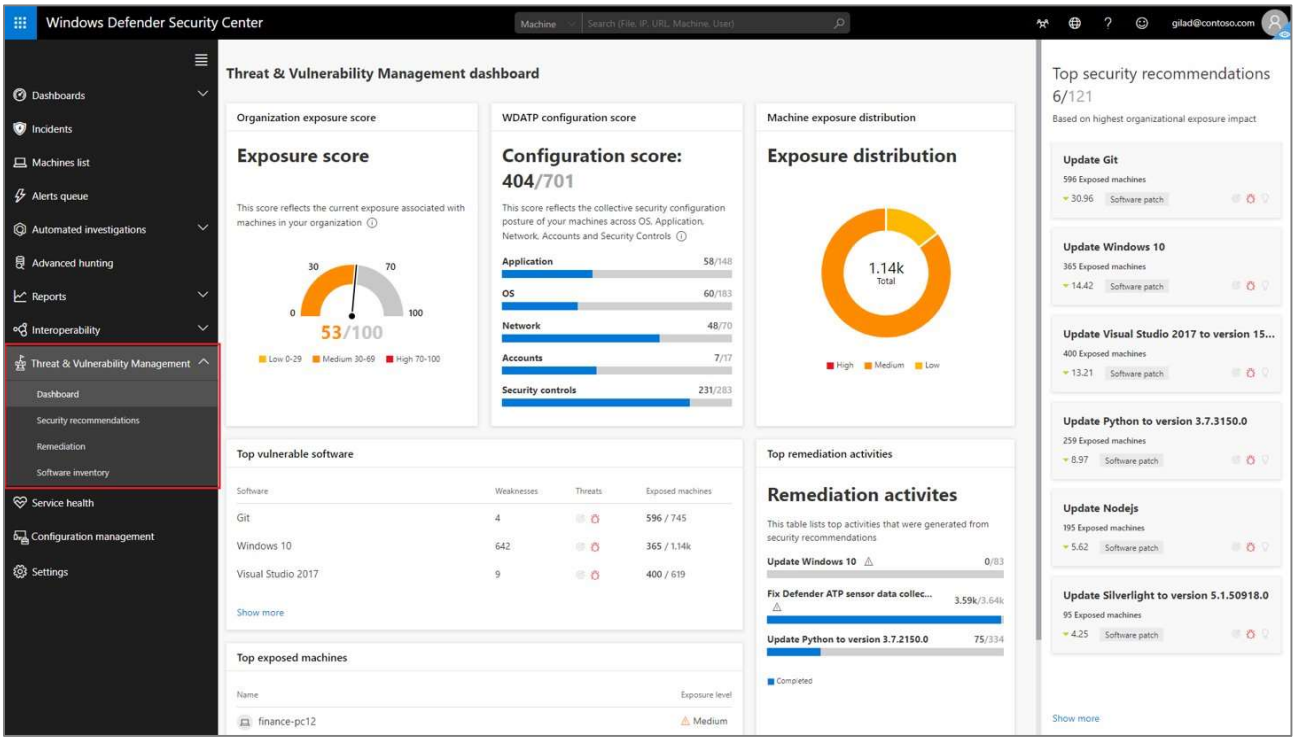
Tradesolution har satt opp all infrastruktur i Microsoft Azure (Europa). Microsoft Azure datasenter infrastruktur er ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2 compliant. For å sikre tilgjengeligheten av informasjon er all fysisk infrastruktur (f.eks. kontorer, datasentre) beskyttet mot skade ved uventede hendelser. Dette inkluderer å sikre infrastruktur mot brann, naturkatastrofer, ondsinnede angrep osv.

Les mer her: Azure datasenter

Integritet

For å sikre at informasjonen ikke blir endret av utilsiktet eller av uvedkommende har vi satt opp flere tiltak gjennom Microsoft Defender.

Eksempel visning hentet fra internett:



Tilgangskontroll

Tradesolution bruker rollebasert tilgangsstyring på alle ressurser i Azure. Tilgangen settes på abonnement, ressursgruppe eller enkelt ressurser i Azure. Vi delegerer rettigheter basert på behovet til brukeren og etterstreber at brukere våre ansatte opererer med minst mulig rettigheter, "Least Privileges" prinsippet.

Les mer: Rollebasert tilgangskontroll

Privileged Identity Mangement

Privileged Identity Management (PIM) gir oss tidsbasert tilgangsstyring gjennom bruker aktivering for å minimere risiko av misbruk eller feilhåndtering. Godkjente brukere kan elevere sin rolle for en kort periode til å utføre nødvendige endringer. Alle tilgangsroller som er administrerende er satt opp med PIM.

Les mer her: PIM

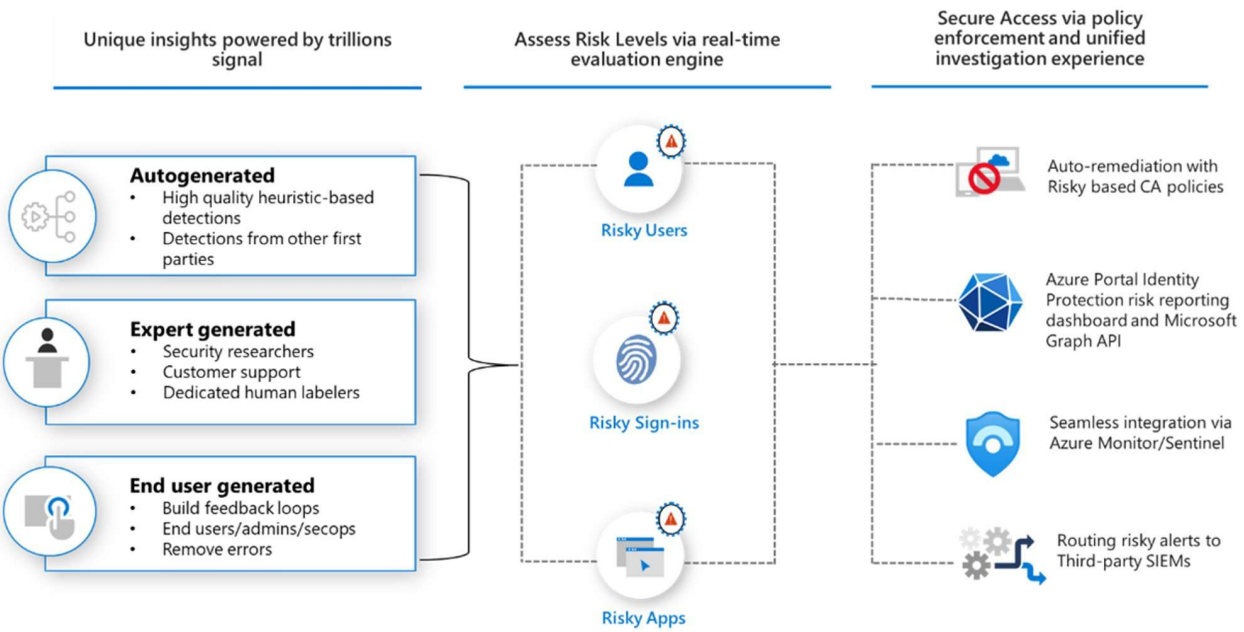
Delt infrastruktur

For å sikre de mest sensitive scenarioene har vi delt infrastrukturen i Azure slik at kritisk infrastruktur kun er tilgjengelig til et svært begrenset antall brukere i Tradesolution. Ved behov kan data også krypteres og gjøres utilgjengelig for Tradesolution ansatte.

User Entity Behavioural Analytics

Microsoft Defender for Cloud hjelper oss med å identifisere og varsle mistenksom oppførsel på brukere for å minimere risiko og skadeomfang til ransomware, annen type kryptering, kompromitterte brukere og mer. Brukere som blir rapportert med høy risiko blir automatisk satt i karantene og må bytte passord før de får tilgang.

Les mer her: UEBA



Microsoft Defender for Cloud

Microsoft Defender for Cloud gir avansert og intelligent beskyttelse av Azure ressurser. Det er designet beskyttelsesplaner for hver type ressurs som: servere, storage, databaser, kubernetes, webapps og mer. Microsoft Threat Intelligence detekterer og varsler uvanlige og potensielle farlige forsøk på å få tilgang.

Les mer her: Protect cloud workloads

Access reviews

Vi har satt opp automatisk rapportering av alle medlemmer av administrative tilgangsgrupper for å periodisk verifisere at kun tiltenkte brukere har tilgang.

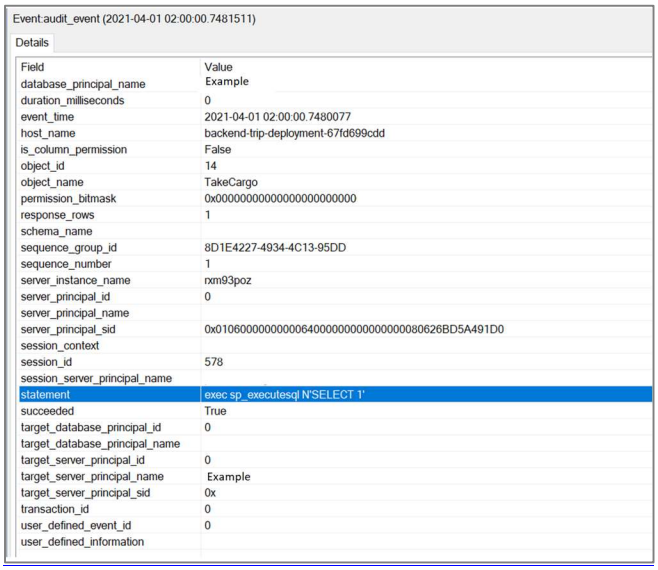
Les mer her: What are access reviews

Sporbarhet

Vår primære lagringskilde er Azure SQL og vi sporer alle endringer i databaser for de 2 siste år med Azure SQL Audit. Se bilde under for referanse.

Les mer her: SQL-auditing

Eksempel audit event:



Event:audit_event (2021-04-01 02:00:00.7481511)

Details

Field	Value
database_principal_name	Example
duration_milliseconds	0
event_time	2021-04-01 02:00:00.7480077
host_name	backend-trip-deployment-67fd699cdd
is_column_permission	False
object_id	14
object_name	TakeCargo
permission_bitmask	0x00000000000000000000000
response_rows	1
schema_name	
sequence_group_id	8D1E4227-4934-4C13-95DD
sequence_number	1
server_instance_name	nxm93poz
server_principal_id	0
server_principal_name	
server_principal_sid	0x0106000000000064000000000000000080626BD5A491D0
session_context	
session_id	578
session_server_principal_name	
statement	exec sp_executesql N'SELECT 1'
succeeded	True
target_database_principal_id	0
target_database_principal_name	
target_server_principal_id	0
target_server_principal_name	Example
target_server_principal_sid	0x
transaction_id	0
user_defined_event_id	0
user_defined_information	

Tilgjengelighet

For å sikre at informasjon er tilgjengelig for autoriserte ved behov har vi satt opp følgende tiltak.

Redundante systemer

Alle produksjonssystemer kjører på minst 2 instanser som standard, hvilket gir redundans og automatisk «failover» ved serverproblemer. Dette kan skaleres for å gi bedre ytelse ved behov som høy belastning eller DDOS angrep. Tradesolution overvåker alle instanser for å avdekke ytelsesproblemer og bruker automatisert skalering for å sikre tilgjengeligheten.

SLA

Tradesolution etterlever en oppetidsgaranti på minst 99,5%.

Azure SQL – Business Critical service tier

Økt tilgjengelighet gjennom automatisk replisering av data over 3 soner i en region, også replisering av data til 1 sone i en annen region.

Les mer her: Business Critical - RA-GRS

Storage – Zone Redundant Storage

Redundant lagring over 3 tilgjengelighets soner. Hver sone er en individuell fysisk lokasjon med dedikerte ressurser til nettverk, strøm og kjøling.

Robusthet

For å sikre at organisasjonen og systemene er motstandsdyktig og evner å gjenopprette normaltilstand ved hendelser har vi følgende tiltak.

Disaster Recovery

Må vi gjenopprette miljøet for tjenesten på nytt grunnet katastrofe, så vil estimerer vi at dette vil ta 4 – 10 timer arbeidstimer.

Restore SQL: 2-6 timer
Konfigurering av ressurser(infrastruktur) i Azure: 2 timer
Redeploy av applikasjoner: 2 timer

SQL-Backup

Databasene er satt opp med definerte backup planer for å overholde nødvendig tilgjengelighet av data. Dette kan endres etter behov, men standard backup plan er:

PITR (Point In Time Recovery):	35 dager
Weekly LTR (Long-term retention):	5 uker
Monthly LTR:	7 måneder
Yearly LTR:	Backup av uke 26 for 5 år.
Restore test:	Månedlig
Backup storage redundancy:	RA-GRS (Read-Access Geo-Redundant)

Les mer her: SQL-Backup

DevOps

Tradesolution bruker Azure DevOps for automatisk utrulling av kode til tjenestene, og sporing av endringer av publiserte versjoner. Våre utviklere må sjekke inn kode til Git repository for versjonskontroll og backup.

Personvern

Tradesolution har som mål om å behandle personopplysninger forutsigbart og transparent slik at våre forbrukere kan føle seg trygge på at vi behandler personopplysninger på en lovlig, sikker og forsvarlig måte. Alle nye og eksisterende tjenester følges opp gjennom internkontrollen og blir årlig gjennomgått for endringer.
Vi som databehandler er pliktig til å ha en databehandleravtale med alle våre kunder. Denne avtalen regulerer hvordan vi sikrer godt personvern og beskytter personopplysninger. Avtalen regulerer forholdet til våre kunder, samt ivaretar vår plikt til å sikre at våre underleverandører følger reglene i GDPR.

Les mer på vår hjemmeside.

Schrems II

Tradesolution har kartlagt alle våre overføringer til tredjeland etter Schrems II og undersøkt at overføringsgrunnlaget gir ett tilstrekkelig beskyttelsesnivå i forhold til landet vi overfører personopplysninger til.

Vi lagrer kun generelle persondata som navn, e-post, mobilnummer, adresse i forbindelse med bruker autorisasjon og logging av hver enkelt brukers aktiviteter for funksjonelle behov i tjenestene. Vi skanner våre data jevnlig for å kontrollere hvilken type informasjon som lagres.

Les mer her: Schrems II
Våre overføringer: Våre underleverandører
Purview (klassifisering): Les mer her

Sikkerhetsbrudd – varslingsrutine

Sikkerhetsbrudd, tap av integritet eller tilgjengelighet vil bli varslet til Nkom og kunder innen 24 timer etter hendelsen er oppdaget.