

WatchGuard CloudDR MSP

En komplett guide för MSP:er – från onboarding till daglig drift

Innehåll

1. Varför CloudDR är relevant för MSP:er
2. Den tekniska driftsmodellen
3. Onboarding: de första 60 minuterna
4. Dagligt MSP-arbetsflöde: från upptäckt till ärende
5. Vad bör MSP:n standardisera?
6. Anslutningar och synkronisering
   Så kopplas CloudDR till kundens miljö
7. Från inventering till risk och hot
8. Vanliga fallgropar
9. Checklista för MSP-drift

WatchGuard CloudDR
- En komplett guide för MSP:er

Tel: +46 18 65 55 85 | Mail: sakerhet@infinigate.se

Molnsäkerhet som en skalbar tjänst för MSP:er

CloudDR ger MSP:er en samlad överblick över kundernas molnapplikationer, identiteter och felkonfigurationer. Värdet ligger i att kunna arbeta på samma sätt över flera kundmiljöer genom att identifiera risker, prioritera vad som behöver åtgärdas och dokumentera arbetet.

För vem?

Tekniker, Service Desk, Security Operations och Presales hos MSP:er

1. Varför CloudDR är relevant för MSP:er

Dagens kundmiljöer består inte längre bara av brandväggar och endpointskydd. Microsoft 365, Google Workspace, SaaS-tjänster, tredjepartsapplikationer och identiteter skapar en dynamisk attackyta. CloudDR fokuserar på just dessa områden: okända molnapplikationer, riskfyllda anslutningar, osäkra konfigurationer och avvikande identitetsaktivitet.

För MSP:er är möjligheten att skala viktig. CloudDR är integrerat i WatchGuard Cloud och gör det möjligt att hantera flera kundmiljöer på ett enhetligt sätt. Det ger en gemensam process för överblick, triage, åtgärder och rapportering, samtidigt som teknikern kan gå ner på detaljnivå för varje kund.

2. Den tekniska driftsmodellen

Komponent	Teknisk uppgift	I praktiken för MSP
Discovery	Inventera molnappar, anslutna integrationer och identiteter.	Kartlägg vilka appar och integrationer kunden använder och upptäcker nya eller okända appar.
Posture	Identifierar felkonfigurationer, sårbarheter och avvikelser som påverkar regelefterlevnad.	Granska upptäcka felkonfigurationer och sårbarheter.Prioritera de viktigaste och följ upp att de åtgärdas.
Identity	Utvärdera avvikande identitetsaktivitet och riskfyllda åtkomster.	Granska riskfyllda konton och behörigheter och bedöm om åtkomsten är relevant och korrekt.
Response	Använd regler och automatisk korrigering som stöd för att åtgärda problem.	Åtgärda identifierade problem, dokumentera ändringen och följ upp att problemet är löst.

Tel: +46 18 65 55 85 | Mail: sakerhet@infinigate.se

3. Onboarding: de första 60 minuterna

En bra onboarding lägger grunden för den fortsatta driften. För varje kund bör teknikern följa en tydlig och återanvändbar process:

1. **Aktivera CloudDR**
   Aktivera licens eller trial och koppla CloudDR-licensen till tänkt slutkund i WatchGuard Cloud.
2. **Kontrollera roller och behörigheter i WatchGuard Cloud**
   Säkerställ att kundmiljö, Operator-roll och skrivrättigheter är korrekt konfigurerade. Owner/Helpdesk samt Subscriber Administrator eller Analyst behöver skrivrättigheter. Sales, Auditor och Observer har endast läsrättigheter.
3. **Anslut kundens molnapplikationer**
   Koppla relevanta SaaS tjänster och dokumentera integrationerna. CloudDR stöder över 40 tredjepartsmolnapplikationer, men funktionerna kan variera mellan integrationer.
4. **Kontrollera inventering och identiteter**
   Låt CloudDR genomföra den första inventeringen och kontrollera att konton och e-postadresser är kopplade till rätt identitet.
5. **Prioritera de första riskerna**
   Sortera identifierade risker utifrån vad som ska åtgärdas direkt, stämmas av med kunden eller bevakas/accepteras.

4. Dagligt MSP-arbetsflöde: från upptäckt till ärende

Gör CloudDR till en del av den befintliga serviceprocessen. Ett enkelt arbetssätt är:

1. **Inventera: Samla information från alla kundmiljöer på ett ställe.**
2. **Bedöm: Förstå sammanhanget innan du agerar.**
3. **Prioritera: Avgör vad som ska hanteras först utifrån risk och kundavtal.**
4. **Åtgärda: Genomför förändringar på ett kontrollerat sätt.**
5. **Dokumentera: Dokumentera och synliggör arbetet och värdet för kunden.**

Teknik-Tips:
Innan du använder en automatiserad åtgärd, kontrollera vad som kommer att ändras, vem som ansvarar för den berörda identiteten och att ändringen kan återställas. CloudDR kan automatisera åtgärden, men kundens process för godkännande av förändringar gäller fortfarande.

5. Vad bör MSP:n standardisera?

Skapa ett gemensamt arbetssätt för alla kunder. Följande delar bör vara tydligt definierade:

Standard	Rekommendationer
Kundens grundnivå	Definiera vilka molntjänster, identiteter och kritiska integrationer som är godkända.
Risknivåer	Bedöm vilka risker som klassas som P1/P2/P3/accepterad risk.
Ändringsprocess	Vem får utföra autokorrigeringar, vad och vilka ändringar bör dokumenteras. Ansvarsfördelning.
Uppföljning	Sätt en rutin för prioritering, bedömnig och sortering av inkommnade förändringar veckorvis, schemaladga månadsrapporter till kund och kvartalsvis översyn.
Kundåtkomst	Säkerställ att arbete sker i rätt kundkonto och kontrollera roller och delegeringar regelbundet.

Tel: +46 18 65 55 85 | Mail: sakerhet@infinigate.se

6. Anslutningar och synkronisering

Så kopplas CloudDR till kundens miljö

CloudDR kan bara analysera information som är tillgänglig via de anslutna SaaS tjänsterna. Kontrollera därför integrationerna regelbundet, särskilt efter ändringar i OAuth, administratörskonton eller API-behörigheter.

1. **Är anslutningen korrekt?**
   Kontrollera att anslutningen är autentiserad och kopplad till rätt kundmiljö.
2. **Är synkroniseringen aktuell?**
   Kontrollera när den senaste synkroniseringen gjordes och att den lyckades. Inaktuell data kan ge en felaktig bild av kundens risker.
3. **Har CloudDR rätt behörigheter?**
   Kontrollera att OAuth- och API-behörigheterna stödjer de funktioner som ska användas. För begränsade behörigheter kan påverka inventering, regler och automatiska åtgärder
4. **Är ändringarna dokumenterade?**
   Dokumentera återautentisering, ändrade behörigheter och undantag i ert ärendehanteringssystem.
5. **Prioritera de första riskerna**
   Dela in identifierade risker i tre nivåer: åtgärda direkt, stäm av med kunden eller bevaka/acceptera.

Praktisk tumregel: En grön dashboard betyder inte att allt är kontrollerat. Kontrollera alltid att integrationerna fungerar, att datan är aktuell och att CloudDR har tillgång till rätt information innan du bedömer riskerna.

7. Från inventering till risk och hot

För Service Desk är det viktigt att förstå vad CloudDR visar. Inventeringen visar vad som finns i kundens miljö, till exempel användare, enheter, molnappar och integrationer. Resultatet påvisar det som CloudDR har identifierat som en möjlig risk eller avvikelse. Därefter behöver bedömning göras om hur allvarlig den påvisade risken är och om den behöver åtgärdas.

Översiktsvy	Frågeställning	Vad gör du?
Inventering	Vad finns i kundens miljö och vem är det kopplat till?	Kontrollera och dokumentera nuläge och avvikelser.
Resultat	Vilken konfiguration eller behörighet innebär en risk?	Kontrollera orsak, påverkan, vilken identitet, applikation och inställning som berörs.
Hot	Finns det tecken på missbruk eller obehörig åtkomst?	Bedöm och analysera risken, eskalera och starta responsprocess.

Varför är detta viktigt?

Det minskar risken för två vanliga misstag: att något i inventeringen felaktigt hanteras som en incident eller att en faktisk påträffad risk avfärdas som en vanlig konfigurationsavvikelse.

8. Vanliga fallgropar

1. **CloudDR kompletterar andra säkerhetslösningar**
   CloudDR ersätter inte endpoint-, nätverks- eller identitetsskydd, utan kompletterar dem med skydd och insyn i molnmiljöer.
2. **En påträffad risk är inte automatiskt en incident**
   Bedöm alltid sammanhang, påverkan och behörigheter innan du prioriterar och eskalerar.
3. **Kontrollera identiteter vid uppstart**
   Licensiering sker per unik övervakad identitet. Säkerställ att konton och rätt identiteter påvisas i lösningen.
4. **Alla integrationer har inte samma funktioner**
   Kontrollera vilka regler, automatiska åtgärder och inventeringsfunktioner som stöds för den aktuella integrationen. Lösningen erbjuder även templates för att underlätta massåtgärder och konfigurationer.
5. **Säkerställ rätt roller och behörigheter**
   Se över roller i WatchGuard Cloud så endast behöriga har tillgång till kunddata enligt överrenskommelse.

9. Checklista för MSP-drift

- Kontrollera kundkonto, licens och användare
- Dokumentera kundens appar och integrationer
- Kontrollera identiteter och privilegierade konton
- Definiera risknivåer och eskaleringsprocess i ärendehanteringssystemet
- Konfiguera automatiska åtgärder och notifikationer
- Sätt en löpande rutin runt prioritering, bedömnig och sortering av inkommnade förändringar.
- Aktivera schemlagd månadsrapportering
- Dokumentera ändringar och undantag regelbundet
- Aktivera “compliance framwork” för bättre regelefterlevnadkontoll

Kort sammanfattning: CloudDR skapar störst värde för MSP:er när det blir en del av den löpande driften, med tydliga rutiner för att prioritera, åtgärda och följa upp risker. På så sätt får kunden inte bara en ögonblicksbild, utan en kontinuerlig och mätbar förbättring av sin molnsäkerhet och compliance.

Källor och senaste uppdatering.

Produktinformation och begrepp baseras på WatchGuards dokumentation och produktsida, hämtad den 31 augusti 2026. Funktioner, integrationer, roller och licensmodeller kan ändras beroende på produktversion och integration.

watchguard.com/help/docs/help-center/en-us/content/en-us/CloudDR/CloudDR_about.html | CloudDR_get_started.html | CloudDR/integrations/about_cdr_integrations.html

Infinigate Sverige AB
Axel Johanssonsgata 4-6
754 50 Uppsala

+46 18 65 55 85
sakerhet@infinigate.se
www.infinigate.com/se

© Infinigate 09/24