SOLUTION BRIEF

Trygg drift och säkra styrsystem – en guide till OT-cybersäkerhet för VA-sektorn

Innehållsförteckning

Inledning

Den snabba digitaliseringen inom kommunala vatten- och avloppsbolag (VA) skapar stora möjligheter – men också nya hot. Allt fler anläggningar kopplas upp och blir en del av en modern, datadriven drift. Smarta sensorer, fjärrövervakning och automatiserade styrsystem (SCADA) effektiviserar verksamheten, men de öppnar också nya vägar in för cyberangrepp.

Samtidigt suddas gränsen ut mellan IT och OT. När administrativa system kopplas samman med driftsteknik – som pumpar, ventiler och reningsprocesser – krävs en djupare förståelse för båda miljöerna och deras respektive risker. En attack mot IT-system kan leda till dataintrång. En attack mot OT-system kan påverka vattenkvaliteten, stoppa försörjningen eller orsaka utsläpp av orenat avloppsvatten.

Historiskt har IT och OT varit separerade världar. I dag är de i många fall sammankopplade – en utveckling som ger stora fördelar, men också nya risker. Denna konvergens skapar förutsättningar för:

- Bättre tillförlitlighet - genom realtidsdata om vattenkvalitet, tryck och flöden.
- Effektivare drift och underhåll - med hjälp av prediktiv analys.
- Lägre kostnader - tack vare optimerad energianvändning.

Parallellt växer den digitala attackytan. Cyberangrepp mot vattenreningsverk och VA-infrastruktur blir allt vanligare – och flera incidenter har redan visat hur allvarliga konsekvenserna kan bli.

Därför krävs en modern cybersäkerhetsstrategi. Dagens skydd måste:

- Omfatta både IT, SCADA och fältutrustning.
- Samverka mellan olika säkerhetslösningar och snabbt identifiera hot.
- Automatisera skydd och åtgärder – för att begränsa skador och snabbt återställa driften.

Denna guide förklarar hur Fortinet på ett effektivt sätt skyddar hela den sammankopplade IT- och OT-infrastrukturen, möjliggör full integration mellan Fortinets egna och partners säkerhetslösningar samt stödjer säkerhetsautomatisering i hela ekosystemet. Den belyser även skillnaderna mellan IT och OT – och hur dessa miljöer blir alltmer integrerade, med ökade säkerhetsrisker som följd.

Dessutom beskrivs hur Fortinet OT Security Platform stödjer säkerhetskontroller i ledande cybersäkerhetsregleringar, standarder och ramverk. Den beskriver en säkerhetsarkitektur för OT baserad på Purdue Enterprise Reference Architecture (PERA) och föreslår konkreta nästa steg för organisationer som vill stärka sin cybersäkerhet. Guiden innehåller även en bilaga som matchar vanliga OT-säkerhetsbehov med relevanta lösningar inom Fortinets portfölj.

Digital transformation inom VA: möjligheter, utmaningar och IT/OT-konvergens

OT-nätverk inom VA-sektorn består av industriella styrsystem (ICS) som styr och övervakar pumpar, ventiler, UV-ljusrening, kemikaliedosering och andra processer i vattenverk och avloppsreningsverk. Dessa system har ofta funnits i årtionden och var från början analoga och isolerade från externa nätverk. Detta gjorde att man länge litade på den så kallade ”air gap”-säkerheten, där OT-nätverken ansågs säkra just eftersom de inte var uppkopplade.

Men som en del av den digitala utvecklingen har kommunala VA-bolag börjat koppla samman IT och OT för att dra nytta av moderna teknologier som:

- Internet of Things (IoT) och Industriellt IoT (IIoT) för fjärrövervakning och smart styrning av VA-nätet. Detta inkluderar användning av sensorer, drönare och satellitdata för övervakning av vattensystemen.
- Molntjänster för förbättrad datainsamling och analys av driftparametrar.
- Artificiell intelligens (AI) och maskininlärning (ML) för prediktivt underhåll, läcksökning, automatisk feldetektion, optimering av kemikaliedosering och andra processer, samt som beslutsstöd.
- Digitala tvillingar för att övervaka och simulera anläggningar och processer, vilket möjliggör virtuell testning av nya styrstrategier och optimering av drift.

Genom att integrera dessa teknologier kan VA-bolag optimera driften, förbättra säkerheten och öka tillförlitligheten i vattenförsörjningen.

Den ökade effektiviteten och smidigheten som kommer med IT/OT-konvergens innebär dock också större risker. När den traditionella air gap-säkerheten minskar blir VA-infrastrukturen exponerad för samma cyberhot som traditionella IT-system – och i värsta fall kan en attack leda till att driften av vattenförsörjning eller reningsverk påverkas, vilket kan äventyra både hälsa och miljö.

För VA-organisationer som anpassar sin IT- och OT-infrastruktur till digitaliseringens krav måste säkerheten utvecklas i samma takt för att skydda mot de alltmer avancerade cyberhoten.

De senaste cybersäkerhetstrenderna

Utvecklingen från isolerade styrsystem till fullt uppkopplade IT–OT–moln-miljöer har skett stegvis över flera decennier. I takt med ökad uppkoppling har även den systemiska cybersäkerhetsrisken ökat. Det som tidigare var lokala och avgränsade system är i dag en del av en sammanhängande digital infrastruktur där beroenden och attackytor har vuxit.

Trendperiod	1980–1990-tal	2000-tal	2010-tal	2020-tal – Nu
Teknik	Proprietära ICS-system	Ethernet, Modbus TCP	IoT, IIoT	Moln, AI/ML, SaaS
Uppkoppling	Helt airgapped nätverk	Fjärråtkomst (VPN)	IT–OT-bryggor, DMZ-zoner	Fullt uppkopplat (IT–OT–moln)
Driftsfördel	Manuell, lokal drift	Automation	Fjärrdrift, analys	Optimering i realtid
Säkerhetsexponering	**Ökad** säkerhetsrisk med ökad uppkoppling → **Låg**	**Växande**	**Bred angreppsyta**	**Hög/systemisk cybersäkerhetsrisk**

Figur 1: Minskad isolering mellan system har drivit på digital transformation – men till priset av ökade cybersäkerhetsrisker i OT-miljöer

Trots att många organisationer har gjort framsteg i sin säkerhetsmognad under de senaste åren, är många OT-system fortfarande sårbara av flera orsaker. Ett exempel är att majoriteten av OT-säkerhetspersonalen (52,6 %) har arbetat i fältet i fem år eller mindre, och färre än hälften har relevanta certifieringar inom OT-säkerhet.

Fem framträdande trender belyser de specifika utmaningar som präglar säkerhetsarbetet i dagens OT-miljöer:

52,6%

av OT-säkerhetspersonalen har fem års erfarenhet eller mindre, och färre än hälften har relevanta OT-säkerhetscertifieringar.

Ökade OT-relaterade säkerhetsrisker

Geopolitiska händelser fortsätter att driva på riktade cyberattacker mot cyberfysiska system (CPS) och samhällskritisk infrastruktur. Exempelvis har satellitnätverk och tillverkningsindustrier i både USA och Europa attackerats. I vissa fall har attackerna varit kopplade till oroligheter i Mellanöstern, där angripare riktat in sig på programmerbara logikstyrningar (PLC:er) – bland annat sådana tillverkade i Israel – vilket ledde till driftstörningar hos mindre vattenbolag.

Utmaningar med patchning i OT-miljöer

Förutom PLC:er kräver även nätverkslösningar, fysiska säkerhetssystem (som kameror och övervakningsutrustning), sensorer och olika typer av styrsystem i VA-driften regelbunden uppdatering. Men många OT-miljöer bygger fortfarande på äldre, omoderna enheter som inte uppdateras regelbundet – samtidigt som verksamheten måste vara igång dygnet runt. I många fall är det helt enkelt inte möjligt att ta ner systemen i veckor eller månader för att genomföra patchning eller underhåll. Dessutom kan patchning av äldre OT-system leda till kompatibilitetsproblem som är svåra eller omöjliga att lösa. Samtidigt ställs det i allt högre grad regulatoriska krav på att vissa brister åtgärdas eller att en specifik patchstrategi införs.

Ökad användning av molntjänster

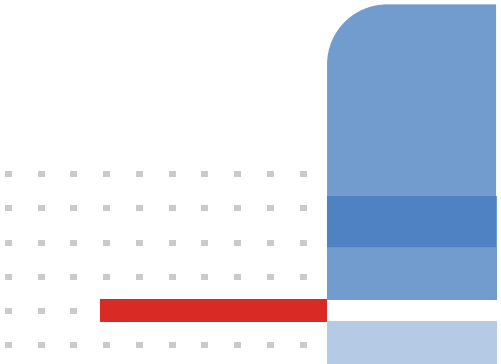
Molnbaserade lösningar inom OT blir allt vanligare, och integrationen mellan IT-molntjänster och OT-system växer. I takt med att VA-organisationer överger isolerade OT-system till förmån för mer sammankopplade miljöer, skapas nya beroenden. Drivkrafter som processeffektivisering och bättre insyn i driftdata har lett till en ökad användning av industriell IT, molntjänster och trådlösa system. Enligt en färsk undersökning från SANS använder redan 26 % av organisationer molnteknik för ICS och OT – en ökning med 15 % på bara ett år.

Ökad användning av 5G för driftsäker uppkoppling

Många VA-system är beroende av stabil uppkoppling med låg fördröjning, inte minst som reservväg vid driftstörningar. 5G-nät ger bättre prestanda och tillförlitlighet än traditionella alternativ som ADSL eller satellit. Inom industrin används 5G i allt högre grad som kommunikationsnät för exempelvis autonoma fordon och andra IIoT-enheter. Även inom VA används 5G ofta för fjärrövervakning på platser där kabelanslutning saknas – exempelvis pumpstationer eller vattenreservoarer – vilket gör 5G till en nyckelkomponent i det digitala VA-nätet.

AI:s växande roll i OT-säkerhet

AI används redan i VA-driften för prediktivt underhåll, läcksökning och optimering av kemikaliedosering. Men dess roll inom cybersäkerhet växer snabbt. AI används nu för att upptäcka avvikelser, analysera nätverksbeteenden, hantera sårbarheter och automatisera säkerhetsåtgärder. Även fysiska säkerhetssystem integrerar AI – exempelvis för intelligent videoanalys, miljöövervakning, hotdetektering, samt övervakning med hjälp av kameror, sensorer och drönare.



Cybersäkerhetshot mot OT

Enligt Fortinets Threat Landscape Report 2025 fortsätter statsstödda aktörer att använda utpressningsprogram (ransomware) som ett aktivt vapen – framför allt mot tillverkningsindustrin, som är den mest utsatta sektorn.

Även om VA-sektorn ännu inte är det primära målet i lika hög grad, ser vi en ökande trend där samhällskritiska infrastrukturer – inklusive vattenförsörjning och avloppshantering – blir allt mer intressanta för cyberangripare. Dessa system har ofta lägre säkerhetsmognad och hög påverkan vid störning, vilket gör dem särskilt attraktiva vid både ekonomiskt och geopoltiskt motiverade attacker.

Figur 2: Typiska vektorer för cyberattacker

Dagens cyberhot är globala till sin natur. Nya skadliga program som är specifikt utvecklade för industriella styrsystem (ICS) inkluderar till exempel FrostyGoop – som riktar sig mot teknik som används av över 46 000 uppkopplade ICS-enheter världen över – och PIPEDREAM, som är den första ICS-malware som kan skalas upp för angrepp mot flera system och sektorer samtidigt.

Cyberattacker mot programmerbara styrsystem (PLC:er) i vattenverk, kemiska anläggningar och tillverkningsindustri har blivit allt vanligare. Samtidigt utgör cyberspionage ett växande hot mot samhällskritiska infrastrukturer inom energi, vattenförsörjning, transporter och kommunikation.

Som beskrivs i MITRE ATT&CK for ICS-ramverket varierar angriparens taktik (anledning till åtgärd) och teknik (hur målet uppnås), men resultatet av ett framgångsrikt OT-intrång är nästan alltid allvarligt och förödande för den drabbade verksamheten.

Lärdomar från de senaste attacktrenderna

Analys av aktuella attacktrender ger flera viktiga insikter:

- Eftersom OT-miljöer traditionellt varit isolerade har säkerhet inte varit ett prioriterat område. Det innebär att grundläggande säkerhetshygien ofta saknas. För att säkerhetsbeteenden ska kunna få genomslag måste säkerhet – liksom säker drift – bli en systemisk del av organisationens kultur. Det krävs ett systematiskt arbetssätt för att införa och följa bästa praxis i uppkopplade OT-miljöer.
- Till skillnad från cybersäkerhet inom IT – som i första hand fokuserar på skydd av data – handlar OT-säkerhet om att säkerställa den fysiska driften och säkerheten i kritiska system.

44%

av organisationerna saknar fortfarande fastställda rutiner för incidenthantering i ICS/OT vid upptäckt av en attack.

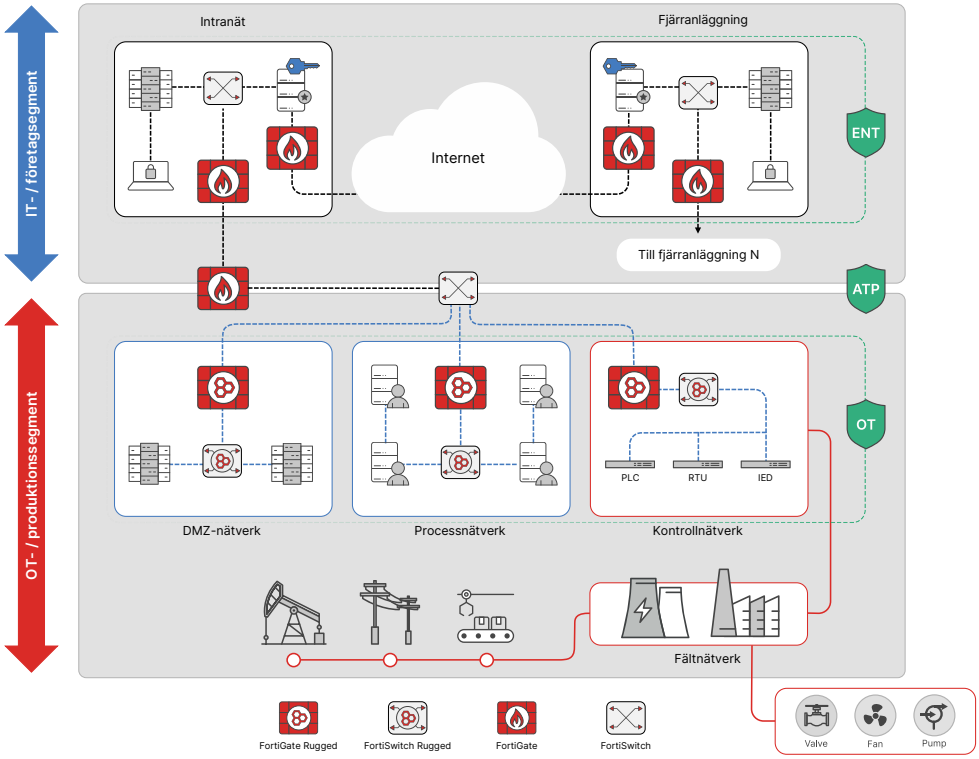
- Spear phishing, komprometterade enheter och stulna inloggningsuppgifter är vanliga angreppsvägar. Det understryker behovet av tvåfaktorsautentisering, kontinuerlig övervakning samt utbildning av personal kring cybersäkerhet och hotindikatorer (IOC).
- Angripare blir allt mer specialiserade på att sabotera OT-miljöer. De utvecklar, köper och säljer verktyg och exploits som är anpassade för att ta sig in i OT-nätverk och störa driften.
- Bristande segmentering mellan IT och OT är fortfarande en kritisk sårbarhet. Det gör att exempelvis ransomware och maskar kan spridas från IT-miljön till OT-systemen, där de sedan kan röra sig fritt och orsaka stor skada.
- Även om upptäckten av cyberincidenter i OT-miljöer har förbättrats – från i genomsnitt dagar (2019) till timmar (2024) – saknar fortfarande nästan hälften (44 %) av organisationerna specifika rutiner för incidenthantering i ICS/OT efter en upptäckt attack.
- Mindre än en tredjedel av organisationerna har en säkerhetsorganisation (SOC) med stöd för OT-specifik incidentrapportering. Trots ökade satsningar på ökad nätverksinsyn, är det endast 12 % som uppger att de har omfattande övervakning – den faktor som starkast korrelerar med snabb upptäckt av cyberincidenter.

Fortinets cybersäkerhetslösning för IT/OT

Att säkra en OT-miljö kan initialt upplevas som överväldigande – men riskreducering kan ske stegvis. Säkerhetsarbete är en resa, och det är viktigt att ha ett tydligt mål: en robust, sammanhängande miljö som är optimerad för att hantera hot som sträcker sig över både IT och OT.

Många organisationer använder så kallade punktlösningar – specifika säkerhetsprodukter som adresserar enskilda behov. Men dessa lösningar är ofta svåra att integrera med varandra och fungerar i silos, vilket leder till ökad komplexitet, bristande överblick och potentiella säkerhetsluckor. Dessutom riskerar verksamheten att fastna i teknisk skuld, där uppdateringar och förändringar hos en leverantör påverkar hela ekosystemet.

En plattformsbaserad strategi – som Fortinet Security Fabric – förenklar säkerhetsarbetet genom att samla funktionalitet i ett integrerat ramverk. Det minskar både driftbördan och komplexiteten, samtidigt som det stärker det övergripande skyddet för hela VA-organisationens digitala infrastruktur.



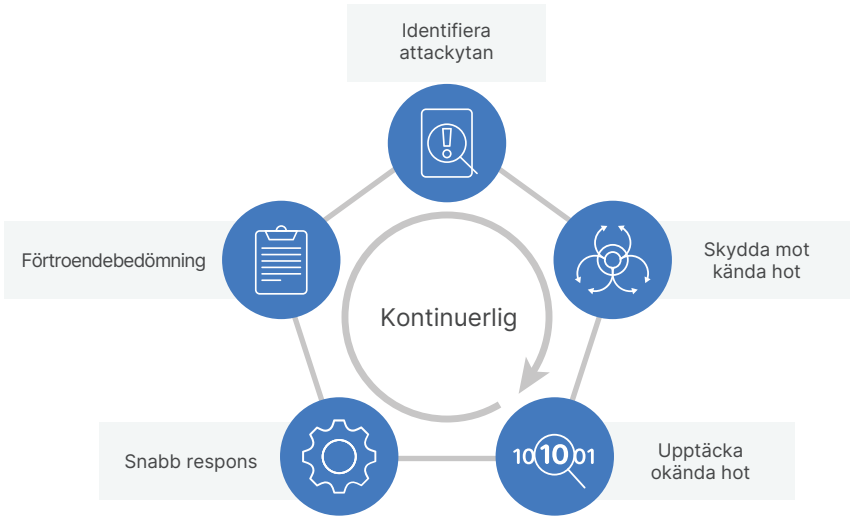
Figur 3: Sammankopplade IT- och OT-nätverk säkrade med FortiGate NGFW-brandväggar

Fortinets OT-säkerhetsplattform omfattar FortiGate-brandväggar (NGFW), FortiSwitch samt andra lösningar för säker nätverksinfrastruktur och säkerhetsoperationer (se figur 3). Plattformen möjliggör konvergens, konsolidering, enkel hantering, integration och automatisering – för ett heltäckande cyberskydd av användare, enheter och applikationer över hela nätverksytan.

Plattformen erbjuder:

- **Bred synlighet och skydd** över hela den digitala attackytan för bättre riskhantering
- **Integrerade lösningar** som minskar komplexiteten i administrationen och delar hotinformation i realtid
- **Automatiserad nätverkssäkerhet** med AI-drivna säkerhetstjänster från FortiGuard för snabb och effektiv hantering
- **Förenklad administration** genom en enhetlig vy i ett och samma gränssnitt (“single pane of glass”)

Den resulterande säkerhetsarkitekturen erbjuder löpande kontroll av tillit för enheter och arbetslaster, och anpassar sig dynamiskt när nätverkskonfigurationer förändras (se figur 3).



Figur 4: Kontinuerlig förtroendebedömning från flera punkter i nätverket möjliggör snabbare identifiering och automatiserade åtgärder, vilket minimerar tiden för riskreducering

Cybersäkerhet genom en enhetlig plattform

I en OT-miljö ger Fortinets OT-säkerhetsplattform insyn i både applikationer och nätverk genom att identifiera och klassificera IT-, OT- och IIoT-enheter. Till skillnad från många andra säkerhetslösningar är denna funktion direkt integrerad i FortiGate NGFW via nätverksoperativsystemet FortiOS.

Applikations- och nätverksinsynen kan förstärkas ytterligare genom att integrera andra Fortinet-lösningar såsom FortiSwitch, FortiAP och FortiExtender.

FortiOS upptäcker och klassificerar tillgångar – inklusive användare, applikationer och protokoll – och tilldelar dem sedan dynamiskt en riskscore baserat på deras säkerhetsstatus. Genom att göra miljön synlig kan OT-organisationer tillämpa intentionsbaserad segmentering och gruppera tillgångar i säkra zoner. Dessa zoner skyddas med anpassade policies som uppdateras kontinuerligt baserat på förtroendebedömningar.

Detta zonbaserade tillvägagångssätt gör det möjligt att automatiskt tilldela och upprätthålla grundläggande behörigheter för varje OT-tillgång – så att kritisk data kan distribueras och samlas in utan att kompromissa med systemens integritet.

FortiOS möjliggör också integration med Fortinet Security Fabric för centraliserad korrelation av hotinformation mellan säkerhetsverktyg. Tack vare denna plattformsintegration kan organisationer snabbt upptäcka avvikande beteenden och larma driftcentraler (NOC) eller säkerhetscenter (SOC).

Denna typ av snabb respons är endast möjlig när enheterna både kan se och dela information. Fortinets OT-säkerhetsplattform kan automatiskt isolera misstänkt komprometterade tillgångar för att begränsa incidenter och säkerställa ett koordinerat svar. I en OT-miljö kan plattformen konfigureras så att den övervakar, upptäcker och larmar – utan att störa produktionen.

Er säkerhetsplan för OT

När organisationer planerar sin OT-säkerhetsstrategi bör de utgå från att ett intrång förr eller senare är oundvikligt – eller att angripare redan finns i miljön. De mest förutseende verksamheterna tar höjd för att skadlig kod kan nå OT-system som historiskt sett varit dåligt skyddade, med möjlighet till lateral förflyttning och eskalering av behörigheter.

Genom att ha detta som utgångspunkt kan OT-säkerhetsteam implementera en mer heltäckande strategi för att identifiera och hantera åtkomst till affärskritiska OT-tillgångar. Det innebär också att man stärker kontrollmekanismer för att snabbt kunna upptäcka och reagera på avvikande beteenden i känsliga miljöer.

Modern och proaktiv OT-säkerhet behöver byggas in direkt i systemen – inte läggas till i efterhand. I de följande exemplen visar vi hur VA-organisationer kan höja säkerheten i sina IT-/OT-miljöer genom konkreta användningsfall.

Use case

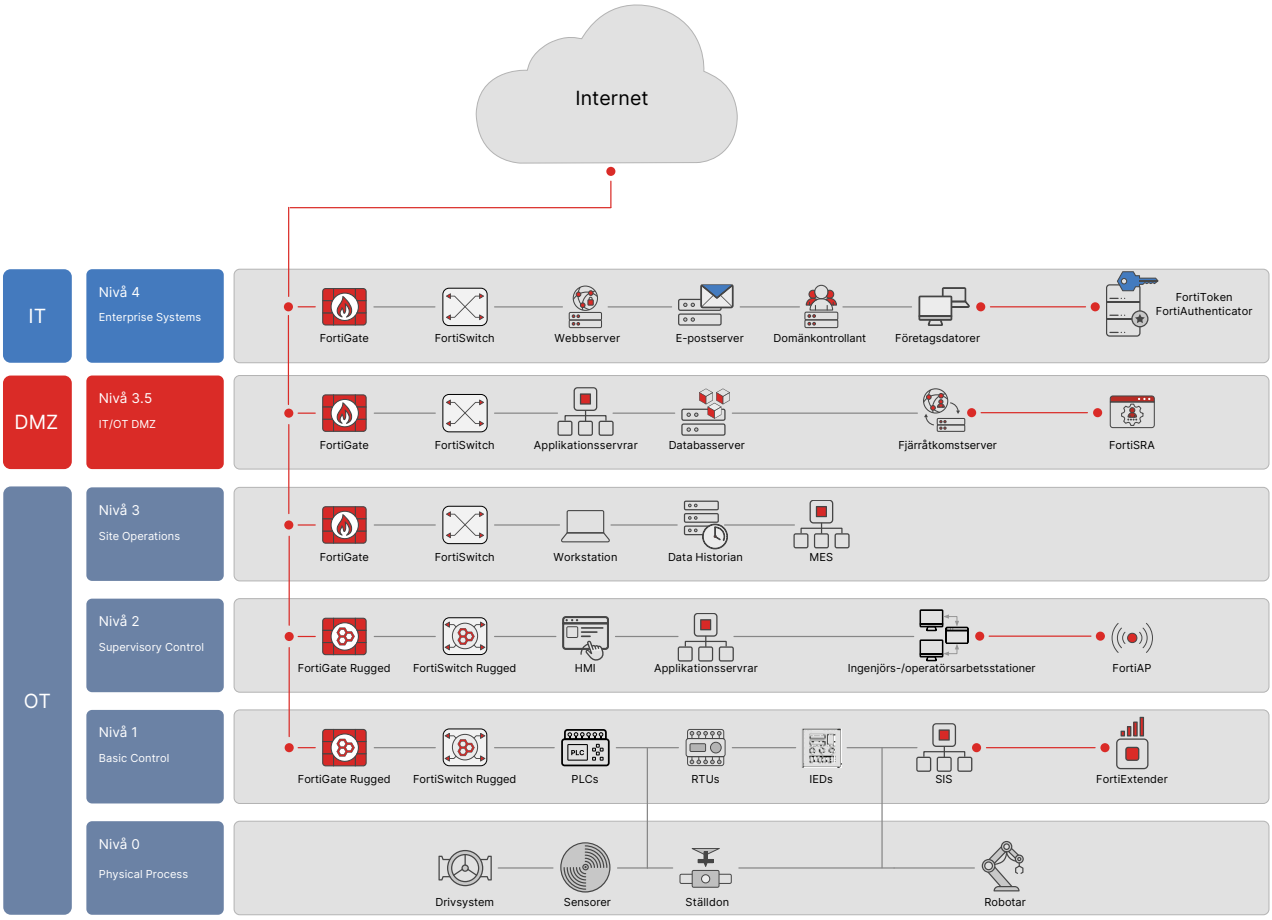
Dessa säkerhetsscenarier bygger på branschstandarder och beprövade metoder för att stärka skyddet av OT-miljöer och annan kritisk infrastruktur.

Use case 1: WAN-säkerhet

WAN-säkerhet omfattar både fasta och trådlösa WAN-anslutningar. Den yttre perimetern för ett OT-nätverk måste säkras – både som ett skydd mot cyberattacker och som en kontrollerad ingång för auktoriserade användare och anslutningar.

Exempelvis behöver fjärranställda eller externa leverantörer tillgång till systemen för att kunna utföra uppgifter som logghantering, underhåll eller felsökning av industriella styrsystem (ICS). Personal som ansvarar för driften måste kunna övervaka tillgängligheten i realtid och vid behov snabbt identifiera och åtgärda eventuella problem på distans.

En säker lösning för fjärråtkomst bör inkludera funktioner som flerfaktorsautentisering (MFA) och kryptering av nätverkslänkar. Om kontrollcentralen och anläggningarna är sammankopplade via flera kommunikationsvägar kan även säker SD-WAN vara en viktig komponent för att bibehålla tillgängligheten på ett kostnadseffektivt sätt.



Figur 5: Fortinets WAN-säkerhet representeras av de röda linjerna i diagrammet

Specifika säkerhetsfunktioner som krävs i detta use case inkluderar:

- Skydd för trådlösa WAN-anslutningar (Wi-Fi, 3G, 4G LTE, 5G)
- IPsec och VPN
- SSL- och TLS-kryptering
- Säker fjärråtkomst
- Säker SD-WAN
- Secure Access Service Edge (SASE)

FortiGate NGFW
Ger säkerhetskontroll och policyhantering, samt stöd för IPsec, VPN, SSL- och TLS-kryptering. FortiGate möjliggör även säker SD-WAN och IPS-funktionalitet för att skydda OT-nätverkets yttre gräns mot intrångsförsök.

FortiAP
Tillhandahåller säker Wi-Fi-åtkomst för både LAN- och WAN-segment. Säkerställer krypterad trådlös kommunikation inom och utanför anläggningen.

FortiExtender
Bygger en säker bro mellan lokala nätverk (LAN) och trådlösa WAN-anslutningar via LTE och 5G. En idealisk lösning för fältinstallationer där kabelanslutning inte är möjlig.

FortiPAM (Privileged Access Management)
Erbjuder säker fjärråtkomst med stöd för hantering av autentiseringsuppgifter, övervakning och inspelning av sessioner i realtid, säker filöverföring samt rollbaserad åtkomstkontroll.

FortiToken
Möjliggör tvåfaktorsautentisering via engångslösenord (OTP), antingen via pushnotiser i FortiToken Mobile (FTM) eller via fysiska OTP-enheter. Full integration med FortiClient, FortiGate och FortiAuthenticator garanterar en säker autentiseringskedja.

Use case 2: LAN-säkerhet

I takt med att allt fler tillgångar och applikationer kopplas upp i OT-nätverk utgör det lokala nätverket (LAN) en växande attackyta. För att skydda dessa miljöer krävs ökad säkerhet utan att öka komplexiteten. Samtidigt är det avgörande att nätverksprestandan är tillräckligt hög för att stödja driftskritiska enheter och system.

Fortinets lösning för säker nätverksinfrastruktur konsoliderar nätverkshantering i FortiGate NGFW – en branschledande brandvägg som erbjuder komplett säkerhet för LAN-miljön, samtidigt som den förenklar den dagliga hanteringen. Fortinet möjliggör snabb och effektiv etablering av storskaliga nätverk med inbyggda rekommenderade konfigurationer. Zero-touch provisioning gör det enkelt att rulla ut mallar till flera sajter med minimal teknisk insats.

Funktioner som krävs i detta use case:

- Synlighet över tillgångar och nätverk
- Nätverkssegmentering och mikrosegmentering
- Network Access Control (NAC)
- Användaråtkomstkontroll (t.ex. MFA och SSO)
- Redundansprotokoll för LAN (MRP, PRP, HSR)
- Säkerhet för trådlösa nätverk (Wi-Fi)

Utöver lösningarna för WAN-säkerhet bidrar följande Fortinet-komponenter till att stärka LAN-säkerheten:

FortiGuard OT Security Service

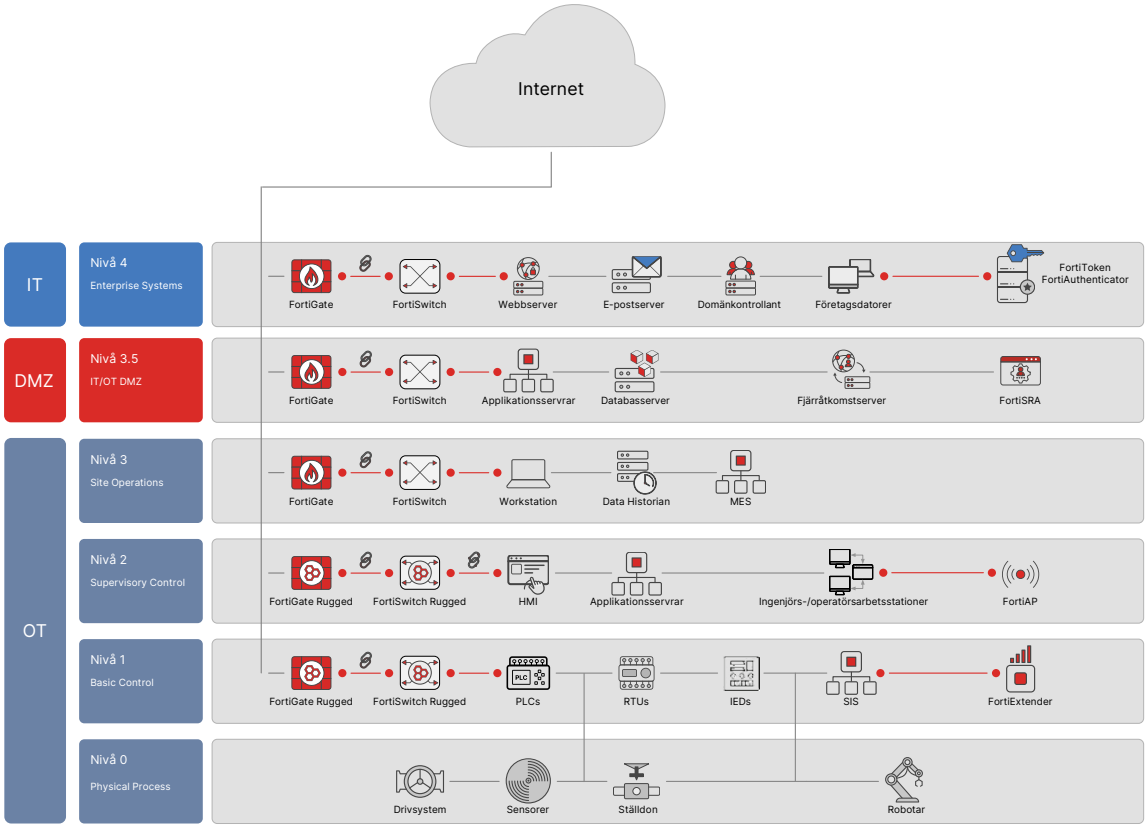
Möjliggör för FortiGate NGFW att upptäcka, analysera och skydda mot nätverksbaserade OT-hot. Tjänsten stöder virtuell patchning och ger djup insyn i OT-protokoll och applikationer, både i LAN- och WAN-miljöer.

FortiSwitch

Ger fullständig kontroll och insyn över användare och tillgångar i nätverket. Bidrar till ökad säkerhet och bättre segmentering av nätverkstrafik.

FortiLink

Underlättar segmentering och mikrosegmentering genom att automatiskt upptäcka nätverkstillgångar och tilldela rätt åtkomst enligt principen om minsta privilegium. FortiLink möjliggör även centraliserad hantering av en eller flera FortiSwitch-enheter direkt från FortiGate.



Figur 6: Fortinets LAN-säkerhet representeras av de röda linjerna i diagrammet

Use case 3: Avancerat hotskydd

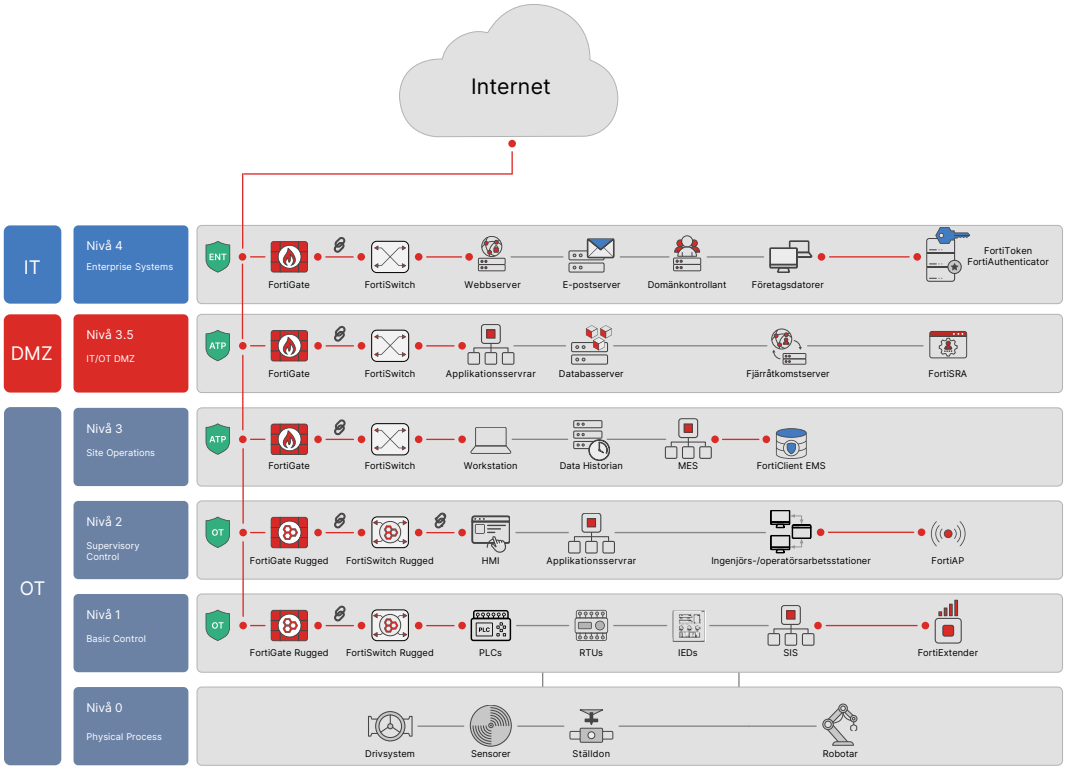
För att effektivt skydda OT-miljöer krävs både insyn i och kontroll över hur applikationer och protokoll kommunicerar i nätverket. FortiGate NGFW har inbyggt Intrusion Prevention System (IPS) och möjliggör applikationskontroll baserat på signaturer, vilket gör det möjligt att tillämpa skräddarsydda brandväggspolicys för OT-trafik. FortiGate stöder dessutom virtuell patchning – särskilt värdefullt i nätverk med äldre och sårbara enheter där säkerhetsuppdateringar inte är möjliga eller önskvärda.

Funktioner som krävs i detta användningsfall:

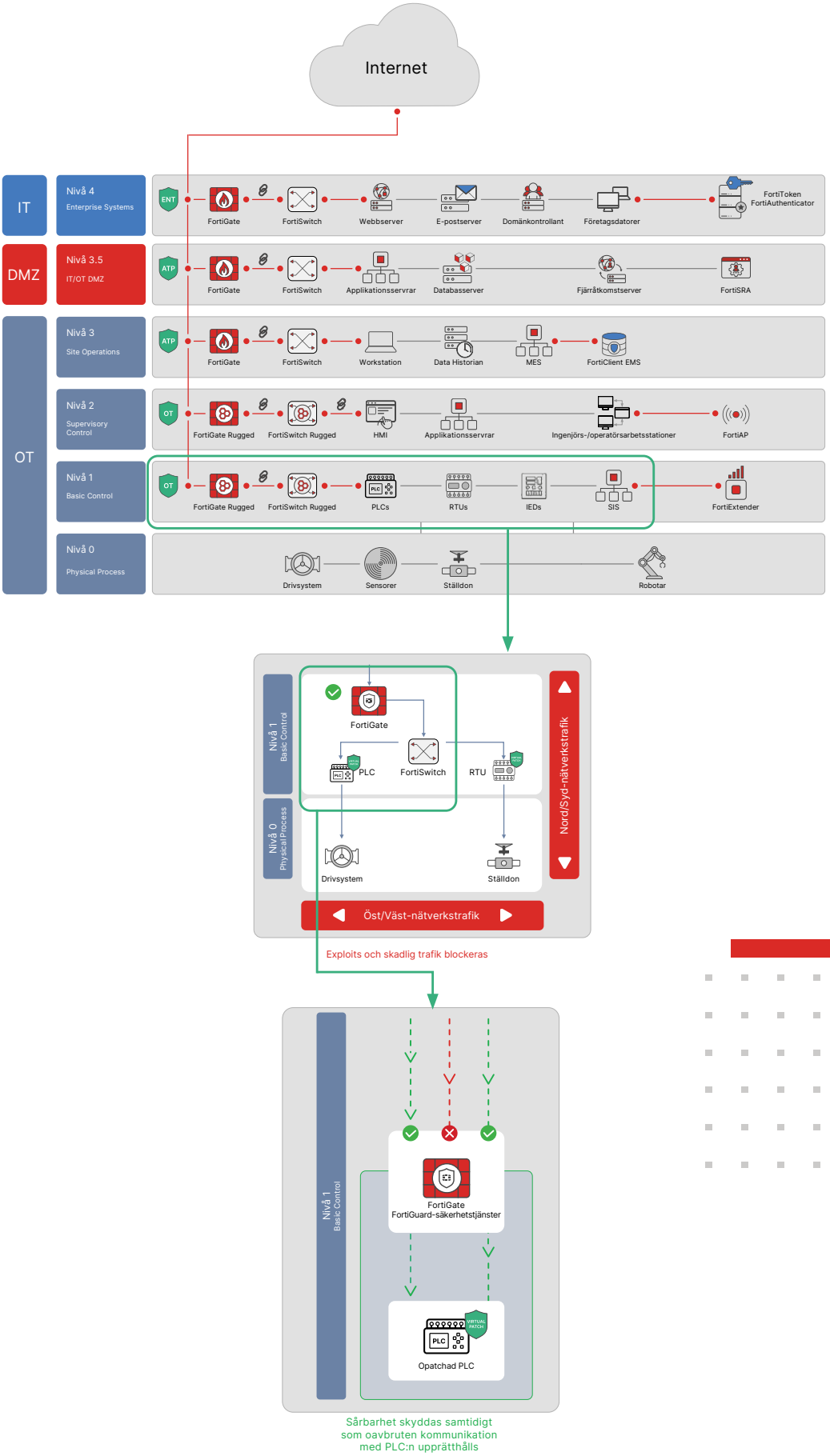
- Kontroll av OT-applikationer
- Skydd mot sårbarheter i både OT- och IT-miljöer (IPS)
- Virtuell patchning
- Anti-malware
- Webbfiltrering
- Sandboxing
- Säkerhet på endpoint-nivå

Flera Fortinet-lösningar stödjer detta användningsfall:

- **FortiGate NGFW** – Har inbyggd nästa generations IPS som integreras med FortiGuard-säkerhetstjänster. Erbjuder djup paketinspektion (DPI) och intrångsskydd mot både IT- och OT-hot.
- **FortiGuard OT Security Service** – Innehåller applikations- och sårbarhetssignaturer särskilt framtagna för OT-miljöer. Möjliggör identifiering och skydd mot nätverksbaserade hot och ger omfattande insyn och kontroll över OT-applikationer och protokoll. Kan även tillämpa virtuell patchning på enheter som saknar skydd, i väntan på en permanent uppdatering. Fortinet samarbetar med tillverkare av automations- och styrsystem för att utveckla IPS-signaturer som täcker kända sårbarheter.
- **FortiSandbox** – Tillhandahåller avancerad detektering och skydd mot ihållande hot. Lösningen kan användas som en fristående produkt eller integreras direkt i FortiGate NGFW.
- **FortiEDR** – Erbjuder realtidsbaserad, automatiserad hotdetektering, skydd, incidentrespons och forensik på endpoints. FortiEDR kan även integreras med FortiGate NGFW för att blockera hot direkt vid källan.
- **FortiClient** – Stödjer hantering av endpoints samt Zero Trust Network Access (ZTNA). Integreras med FortiGate NGFW för att säkerställa att klienter uppfyller säkerhetskrav innan åtkomst tillåts.



Figur 7: Avancerat hotskydd över IT/OT, med FortiGate NGFWs och FortiGuard Security Services, representeras av de röda linjerna i diagrammet (1/2)



Figur 8: Avancerat hotskydd över IT/OT, med FortiGate NGFWs och FortiGuard Security Services, representeras av de röda linjerna i diagrammet (2/2)

Use case 4: Säkerhetsautomatisering

Målet för ett moget säkerhetsprogram inom IT/OT är att etablera ett samordnat och integrerat NOC/SOC – där både drift- och säkerhetsteam arbetar utifrån samma plattform med stöd för delvis eller helt automatiserade åtgärder dygnet runt.

Ett sådant gemensamt operationscenter ansvarar för threat intelligence, analys, hotdetektering, incidenthantering, threat hunting samt styrning och regelefterlevnad.

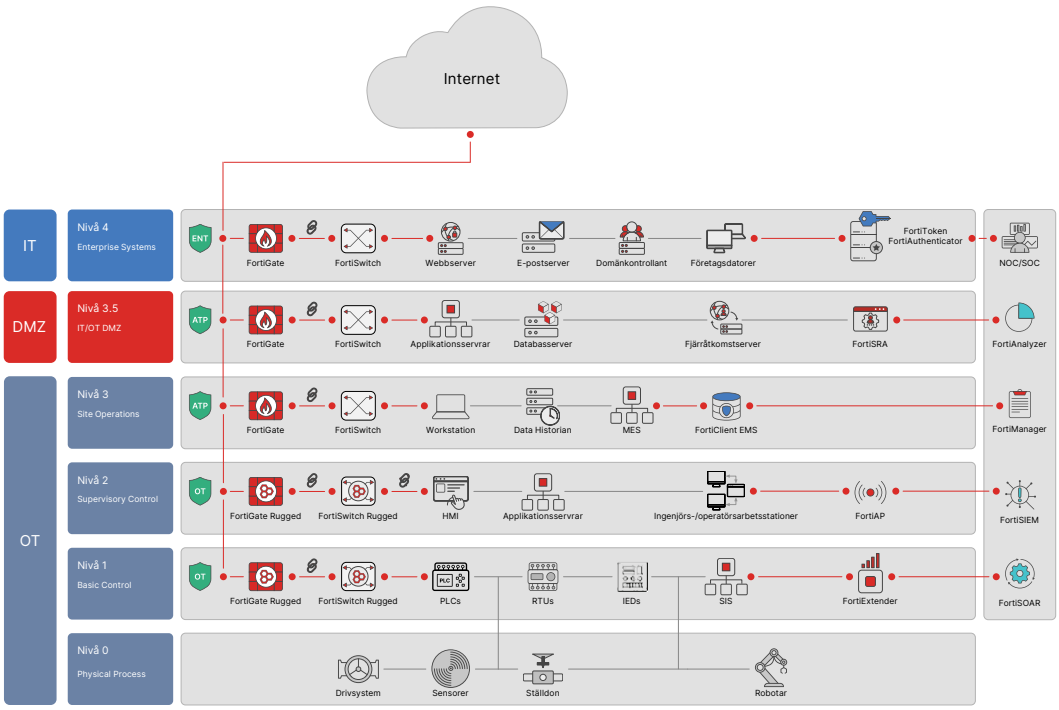
Genom att konsolidera IT och OT i en gemensam vy får organisationen full insyn i användare, system, åtkomsträttigheter, incidenter, larm och hotinformation från externa källor. Denna typ av integration möjliggör snabbare och mer koordinerade åtgärder vid säkerhetshot – utan att störa driftkritiska system.

Exempel på funktionalitet som behövs i detta use case:

- Riskhantering inom cybersäkerhet
- Efterlevnad av cybersäkerhetskrav
- Centraliserad hantering av nätverkssäkerhet
- Detektion och respons på nätverksnivå
- Incidenthantering
- SIEM/SOAR

Flera lösningar inom Fortinet Security Fabric The Internet:

- **FortiAnalyzer** – tillhandahåller centraliserad övervakning, logghantering och rapportering för FortiGate-enheter distribuerade över både IT och OT.
- **FortiManager** – möjliggör central hantering av FortiGate-enheter och implementering av säkerhetspolicys. Lösningen säkerställer enhetlig policytillämpning och uppdateringar via ett samlat och användarvänligt gränssnitt.
- **FortiNDR** – erbjuder nätverksbaserad detektion och respons (NDR) genom att kombinera AI-teknik, mänsklig analys och beteendebaserad nätverkstrafikövervakning för att identifiera skadlig aktivitet med minimerade falsklarm.
- **FortiSIEM** – samlar in och analyserar loggdata från både IT- och OT-miljöer, vilket möjliggör korrelation av hotbeteenden över hela verksamheten. FortiSIEM kan även visualisera hotaktivitet enligt MITRE ATT&CK-ramverket för både traditionell IT och ICS-/OT-miljöer.
- **FortiSOAR** – är ett heltäckande verktyg för säkerhetsorkestrering, automatisering och incidentrespons (SOAR). Det är utformat för SOC-team som behöver hantera stora mängder larm, repetitiva manuella processer och resursbrist. Plattformen erbjuder automatiserade playbooks, prioritering av incidenter och realtidsåtgärder för att snabbt identifiera, hantera och motverka cyberattacker i både IT- och OT-miljöer.



Figur 9: Fortinets säkerhetsautomation, drift och hantering representeras av de röda linjerna i diagrammet

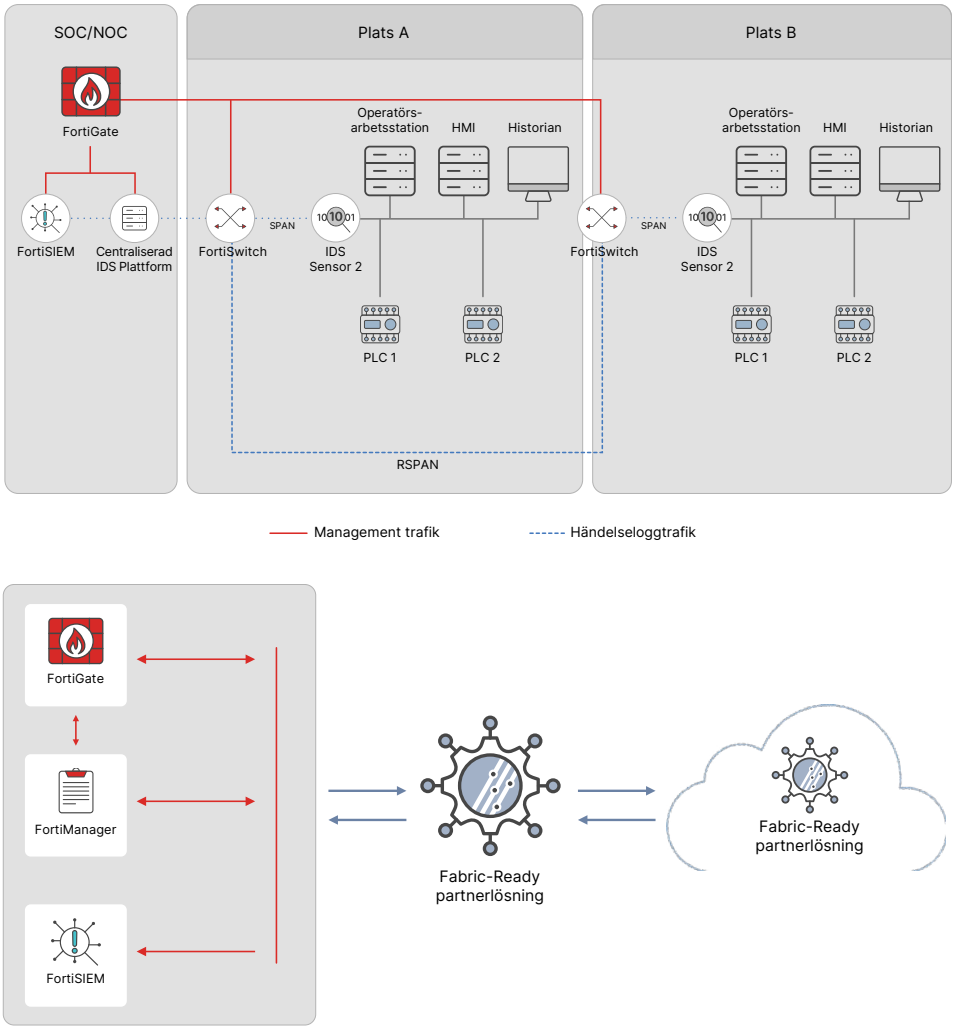
Use case 5: Integration med tredjepartsleverantörer

Att skapa pålitlig uppkoppling och säkerhet i OT-miljöer – som ofta är geografiskt spridda – kräver mer än en enskild lösning. Fortinet samarbetar med både leverantörer av industriella styrsystem (såsom Siemens, Schneider Electric och Rockwell Automation) och OT-säkerhetsaktörer (bland andra Armis, Nozomi Networks, Claroty och Dragos) för att leverera plattformsintegrerade end-to-end-lösningar.

Grunden för detta samarbete är Fortinets öppna arkitektur och integrationsgränssnitt, vilket gör det snabbt och enkelt att integrera nya lösningar med Fortinet OT Security Platform och det bredare Fortinet Security Fabric-ekosystemet.

Exempel på funktionalitet som behövs i detta användningsfall:

- **Fortinet Open Ecosystem** är ett av branschens största cybersäkerhetsekosystem och består av Fabric-Ready-teknologipartners, organisationer för hotdelning samt andra integrationslösningar inom Security Fabric. Detta möjliggör sömlös integration av avancerade säkerhetslösningar från flera leverantörer.
- **Fortinet Fabric-Ready Technology Alliance Partner Program** förenar ett globalt partnernätverk med specialiserad teknisk kompetens. Programmet tillhandahåller verktyg och resurser för snabb och effektiv integration. De förintegrerade lösningarna hjälper kunder att spara tid och resurser vid implementering, drift och support.



Figur 10: Fortinets integration med tredjepartsleverantörer

Planering av OT-säkerhet: IT/OT-cybersäkerhetsarkitektur

Referensarkitekturer

När man utformar en cybersäkerhetsplan för en OT-miljö är det värdefullt att jämföra säkerhetsfunktioner mot etablerade standarder, ramverk och arkitekturer. Det ger stöd för att förstå den tekniska infrastrukturen och implementera lämpliga säkerhetskontroller. Några av de mest etablerade referensarkitekturerna är:

Purdue Enterprise Reference Architecture (PERA):
Purdue-modellen utvecklades under 1990-talet av Purdue University Consortium for Computer Integrated Manufacturing. Även om modellen inte i sig är en säkerhetsarkitektur används den ofta som referens av organisationer för att strukturera sina IT/OT-nätverk och införa säkerhetskontroller. Den har bland annat legat till grund för standarder som ISA99.

Modellens styrka ligger i dess tydliga hierarki för nätverkssegmentering, där varje nivå har olika krav på cybersäkerhet. En utmaning är dock den ökade konvergensen mellan IT och OT – inte minst med tillkomsten av IIoT-enheter – vilket innebär att modellen i många fall behöver kompletteras.

Open Process Automation Standard (O-PAS):
Open Group:s O-PAS-initiativ syftar till att etablera en öppen arkitektur som stöds av industrins användare, leverantörer och systemintegratörer. O-PAS fungerar som ett "standardernas standard" och definierar en öppen, interoperabel och säker arkitektur för industriell processtyrning. O-PAS bygger på ett proaktivt secure-by-design-tänkande, där säkerhet integreras redan i designfasen – snarare än att läggas till i efterhand. För att användas i produktion måste O-PAS-komponenter uppfylla minst säkerhetsnivå 2 (SL2) enligt ISA/IEC 62443-4-2.

Industrial Internet Reference Architecture (IIRA):
IIRA är en öppen arkitektur baserad på standarder som tagits fram för att möjliggöra utveckling av interoperabla IIoT-system inom olika sektorer – både offentlig och privat. Arkitekturen har utvecklats av Industry IoT Consortium (IIC) och bygger på återkommande mönster, egenskaper och krav i verkliga användarfall. IIRA används även för att identifiera teknikluckor och driva vidare utveckling inom IIoT-området.

Framåtblick: Vägen mot modern OT-säkerhet i VA-sektorn

Fortinets OT Security Platform skyddar den digitala angreppsytan i både IT- och OT-nätverk och kan implementeras stegvis, i takt med era säkerhetsprioriteringar. De användningsfall som tidigare beskrivits speglar etablerade bästa praxis för att skydda dagens VA-infrastruktur – men det är också viktigt att ta höjd för de trender som formar framtidens OT-säkerhet:

Containerisering i VA-miljöer:
VA-organisationer kommer på sikt att kunna dra nytta av containerteknik för att förenkla drift och uppdateringar av IoT- och IIoT-funktioner, exempelvis i styrning av pumpstationer, kemikaliedosering eller fjärrövervakning. Det kräver dock ny typ av säkerhetsstyrning, med insyn i alla containrar samt kontroll av sårbarheter och felkonfigurationer innan driftsättning.

Generativ AI i drift och säkerhet:
GenAI öppnar upp för nya möjligheter inom prediktivt underhåll, intelligent styrning och hotdetektion i VA-nät. AI kan användas för att upptäcka läckor, optimera reningsprocesser och automatisera övervakning – men det ställer också krav på säker tillämpning. Det krävs tillgång till korrekt data, kunskap om AI-modellernas begränsningar och nya skydd mot manipulerade sensordata eller AI-driven attackteknik.

Kompetensförsörjning inom OT-säkerhet:
I många kommunala VA-organisationer är OT-säkerhet fortfarande ett nytt kompetensområde. Medarbetare som arbetar nära processnära system behöver stärka sin förståelse för hur cybersäkerhet påverkar driften – och säkerhetsteam behöver mer kunskap om OT-specifika tekniker och rutiner. En modern säkerhetsstrategi måste inkludera kompetensutveckling i takt med förändrade hot och teknologier.

Vill ni diskutera nästa steg i ert säkerhetsarbete?

Läs mer på fortinet.com/ot eller kontakta oss på sweden@fortinet.com.
För tekniska guider och lösningsbeskrivningar, besök även **OT Security Solutions Hub**.

Tillsammans stärker vi skyddet för vattenförsörjningen – steg för steg.

Appendix

Fortinets OT-säkerhetsplattform kopplad till olika användningsområden

Solution	Use Cases
FortiAuthenticator	• Identitet- och åtkomsthantering • Enkel inloggning (SSO)
FortiToken	• Flerfaktorsautentisering

Solution	Use Cases
FortiGate	• Avancerat hotskydd • Enhets och nätverksinsyn • Nästa generations brandvägg • Nästa generations intrångsskydd • Nätverkssegmentering • Säker SD-WAN • Virtuellt privat nätverk (VPN)
FortiGate Rugged	
FortiLink	• Mikrosegmentering av nätverk • Nätverkshantering
FortiLink NAC	• Nätverksåtkomstkontroll

Solution	Use Cases
FortiSwitch	• Enhets och nätverksinsyn • Mikrosegmentering av nätverk • Säker nätverksanslutning
FortiSwitch Rugged	

Solution	Use Cases
FortiAP	• Säkerhet för trådlöst WAN (Wi-Fi/3G/4G LTE/5G)
FortiExtender	

Solution	Use Cases
FortiPAM	• Säker fjärråtkomst • Hantering av privilegierad åtkomst • Rollbaserad åtkomstkontroll

Solution	Use Cases
FortiAnalyzer	• Centraliserad övervakning, loggning och rapportering för FortiGate-enheter och resurser distribuerade inom IT och OT
FortiManager	• Centraliserad enhetshantering och implementering av säkerhetspolicyer för FortiGate-enheter distribuerade inom IT och OT
FortiSIEM	• Centraliserad övervakning, loggning, loggkorrelation och rapportering • Rapportering av cybersäkerhetsrisker och efterlevnad
FortiSOAR	• Orkestrering, automatisering och respons inom säkerhet • Rapportering av cybersäkerhetsrisker och efterlevnad
Fabric-Ready Partner Solution	• Tredjepartslösning integrerad med Fortinet-teknologier via Security Fabric API:er

Solution	Use Cases
FortiClient EMS	• Upptäckt och respons på enhetsnivå • Zero Trust-nätverksåtkomst
FortiClient	

Solution	Use Cases
FortiGuard Security Services	• Skydd mot hot inom IT/OT • Sårbarhetshantering inom IT/OT • Virtuell patchning inom IT/OT

June 4, 2026 4:04 PM / EMKTG-1834-0-1-SV