5 redenen om jouw OT netwerk te beveiligen

Een whitepaper van Fortinet in samenwerking met Exclusive Networks

Inhoudstabel

Uitdagingen 3

Hoe OT-beveiliging OT-uitdagingen aanpakt 4

Vijf overwegingen voor het beveiligen van uw netwerk 6

Kies voor een eenvoudige aanpak van OT-beveiliging 9

Uitdagingen

Uit recent onderzoek van Fortinet blijkt dat het aantal CISO's dat verantwoordelijk is voor OT-infrastructuur in twee jaar tijd is verdrievoudigd. Toch blijft het in de praktijk lastig om deze omgevingen effectief te beveiligen. Veel OT-netwerken missen basisvoorzieningen zoals zichtbaarheid, segmentatie en patchbeheer. Bovendien worden ze steeds aantrekkelijker voor goed georganiseerde cybercriminelen, juist omdat de impact van een geslaagde aanval vaak groot is. De OT-omgeving is in hoog tempo aan het veranderen. Voorheen geïsoleerde systemen zoals fabrieken, installaties of voertuigen worden steeds vaker verbonden met IT-netwerken en de cloud. Die nieuwe verbindingen vergroten het aanvalsoppervlak en stellen kwetsbare, vaak verouderde OT-systemen bloot aan externe dreigingen.

Daarbij komt dat OT verschilt van IT: andere protocollen, andere hardware, andere prioriteiten. Beveiliging vraagt dus om een aanpak die specifiek is afgestemd op OT.

Wat Is OT?

Operational Technology (OT) verwijst naar de hardware en software die fysieke apparaten, processen en infrastructuur aanstuurt. Denk aan PLC's, SCADA-systemen of industriële controlesystemen die zorgen voor continue productie, energiedistributie of transport. In tegenstelling tot IT, dat draait om data en netwerken, richt OT zich op de fysieke wereld. OT-systemen zijn onmisbaar voor sectoren zoals industrie, energie, transport en nutsvoorzieningen, en vragen daarom om een veilige en betrouwbare aanpak.

OT is essentieel voor bedrijven en overheden wereldwijd, waaronder infrastructuur, gezondheidszorgsystemen en productieprocessen. Juist omdat ICS en OT onmisbaar zijn, lopen ze een verhoogd risico.

Bron: Fortinet, 2024 State of Operational Technology and Cybersecurity Report.

Hoe OT-beveiliging deze uitdagingen aanpakt

OT-beveiliging biedt inzicht in assets, kwetsbaarheden en dreigingen binnen industriële omgevingen. Denk hierbij aan het beveiligen van specifieke OT-protocollen zoals Modbus, Profinet en DNP3, maar ook aan industriële toepassingen, machines en automatiseringssystemen.

Een effectieve OT-securityoplossing omvat onder andere:

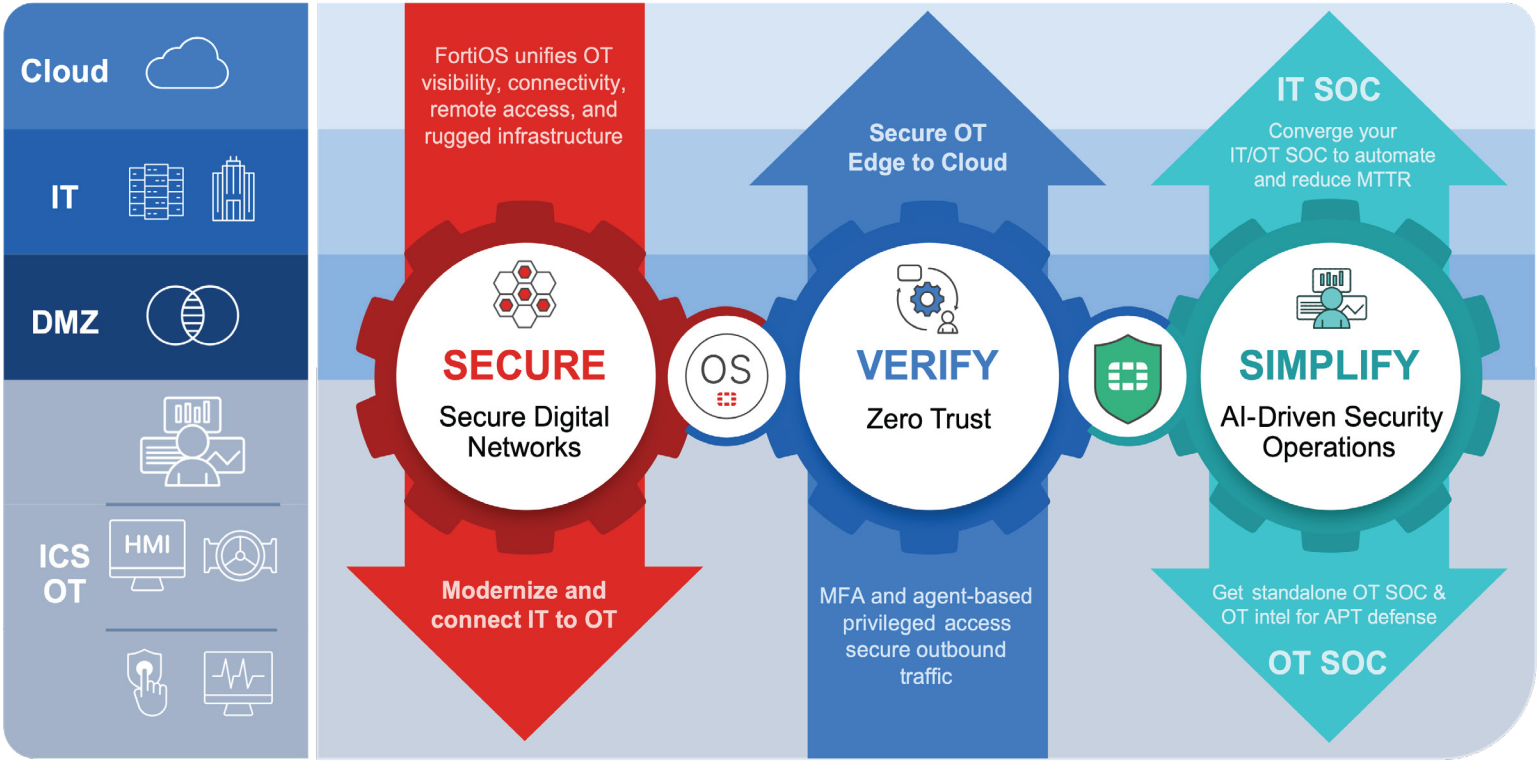
- OT-specifieke firewalls en segmentatie
- SIEM-oplossingen voor monitoring
- Integratie met centrale SOC-processen
- Incident response playbooks

Deze aanpak beperkt risico's, verbetert de zichtbaarheid en versnelt detectie en herstel bij incidenten. Cruciaal, want een succesvolle aanval kan leiden tot productiestilstand, fysieke schade of maatschappelijke gevolgen. Een veilige OT-omgeving is daarom geen luxe, het is een noodzaak.

Veiligheid van medewerkers

Operationele effectiviteit

Realtime inzicht in beslissingen



Wanneer OT-beveiliging correct wordt geïmplementeerd, biedt dit organisaties voordelen door gebruikers, applicaties en protocollen te beveiligen en te beschermen tegen geavanceerde bedreigingen. Extra mogelijkheden zijn onder meer het automatiseren van beveiligingsactiviteiten, het implementeren van veilige externe toegang en het uitbreiden van veilige connectiviteit naar externe locaties, waaronder voertuigen en wagenparken.

Vijf aandachtspunten voor een veilige OT-omgeving

Een effectieve OT-beveiligingsstrategie vermindert risico's, versterkt operationele continuïteit en verhoogt de veiligheid op de werkvloer. Dit zijn de belangrijkste pijlers:

1. Segmentatie van het netwerk

   Veel OT-netwerken zijn 'plat' ingericht, waardoor aanvallers zich eenvoudig kunnen verplaatsen. Segmentatie voorkomt ongeautoriseerde communicatie tussen systemen en beperkt de impact van indringers.

   Een goede oplossing biedt:

   - Network Access Control (NAC)
   - Beleidshandhaving tot op switchpoortniveau
   - Segmentatie binnen en tussen VLAN's

   Vragen die je jouw organisatie moet stellen:

   - Hoe ondersteunt jullie oplossing netwerksegmentatie?
   - Is segmentatie toepasbaar per VLAN en switch poort?
   - Zit er NAC-functionaliteit in het platform?
   - Wordt handhaving geautomatiseerd?

2. Zichtbaarheid en compenserende maatregelen

   Wat je niet ziet, kun je niet beveiligen. OT-netwerken bestaan vaak uit oude, bedrijfskritische systemen die niet zomaar gepatcht kunnen worden. Deze systemen communiceren bovendien vaak via onversleutelde protocollen.

   Essentiële functionaliteiten:

   - Volledig inzicht in assets, kwetsbaarheden en OT-protocollen
   - Virtuele patching of shielding van verouderde systemen
   - Inzet van IPS-regels gebaseerd op OT-threat intelligence

   Vragen die je jouw organisatie moet stellen:

   - Welke OT-protocollen en virtuele patches ondersteunt jullie oplossing?
   - Welke maatregelen zijn er voor legacy-technologie?

3. Integratie met SOC en incident response

Zichtbaarheid en segmentatie zijn cruciaal, maar niet voldoende. OT moet geïntegreerd worden in de centrale beveiligingsprocessen, zoals het SOC en incident response.

Denk hierbij aan:

- Network Detection and Response (NDR)
- Endpoint Detection and Response (EDR)
- Deceptietechnologie
- OT-specifieke rapportage en beheer

Vragen die je jouw organisatie moet stellen:

- Hoe ondersteunt jullie oplossing netwerksegmentatie?
- Welke geavanceerde detectie- en responsmogelijkheden biedt het platform?
- Hoe ondersteunt het systeem bij risicobeoordeling en compliance?

4. Platformbenadering

Losse tools leiden vaak tot complexiteit en verminderde zichtbaarheid. Een geïntegreerd beveiligingsplatform biedt uitkomst.

Voordelen van één platform:

- Minder leveranciers, meer overzicht
- Centraal beheer en automatisering
- Eenduidige integratie van IT en OT

Vragen die je jouw organisatie moet stellen:

- Welke functies bevat het platform?
- Is alles vanuit één console te beheren?
- Welke integraties met derden zijn mogelijk?

5. OT Threat Intelligence

Actuele OT-specifieke dreigingsinformatie is essentieel. Veel aanvallen beginnen in IT en slaan over naar OT, maar steeds vaker zijn OT-systemen het directe doelwit.

Let op:

- Real-time OT-threat intelligence
- IPS-regels en virtuele patches afgestemd op OT
- Inzicht in nieuwe aanvalspatronen en varianten

Vragen die je jouw organisatie moet stellen:

- Hoe actueel en OT-specifiek is de threat intelligence?
- Hoeveel OT-protocollen en -applicaties worden ondersteund?

Maak OT-beveiliging overzichtelijk

De stap naar volledige OT-security hoeft niet ingewikkeld te zijn. Begin met basismaatregelen zoals zichtbaarheid en segmentatie. Voeg daar geavanceerde bescherming en threat intelligence aan toe. Integreer OT in je SOC- en incidentprocessen.

Kies voor een alles-in-één platform. Zo minimaliseer je risico's, verlicht je de werklast van je beveiligingsteam, en versterk je je weerbaarheid tegen dreigingen.

Kortom: beveiliging van OT is eenvoudiger, doeltreffender én toekomstbestendig met het juiste platform.

www.fortinet.com