



**AI Generated with Adobe Firefly**  
Cinematic night view of a European industrial facility protected by glowing red (segmentation) and blue (encryption) digital layers. Data streams flow securely. Dark futuristic atmosphere with metallic textures and subtle cyber threat cues. No text.

// WHITEPAPER

# DE STILTE VOOR DE QUANTUMSTORM



**Fi** AI Generated with Adobe Firefly

## // INHOUDSOPGAVE

|                                                                  |    |
|------------------------------------------------------------------|----|
| Nieuwe dreigingen vereisen een nieuwe aanpak .....               | 3  |
| Quantum computing en OT: het onzichtbare risico .....            | 4  |
| AI-resistente encryptie en privacy-preserving data-analyse ..... | 4  |
| Waarom encryptie niet voldoende is .....                         | 5  |
| Gelaagde beveiliging: segmentatie én encryptie .....             | 6  |
| Integratie en beheer in industriële netwerken .....              | 9  |
| Praktijktoeepassingen in vitale sectoren .....                   | 10 |
| De route naar futureproof OT-beveiliging .....                   | 11 |



## // NIEUWE DREINGEN VEREISEN EEN NIEUWE AANPAK

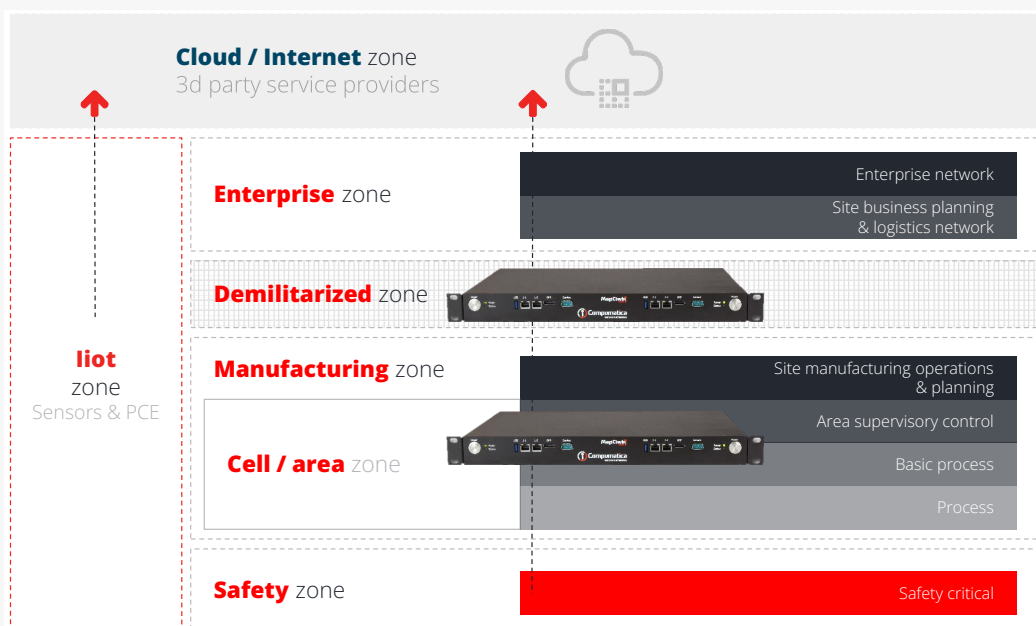
We bevinden ons in de aanloop naar een digitale storm die onze beveiliging fundamenteel verandert. Quantum computing raakt niet alleen industriële controlesystemen, maar ook IT-infrastructuur, van cloud tot thuiswerkverbindingen. Juist waar deze werelden elkaar raken, ligt de kwetsbaarheid. Quantum computers en AI ontwikkelen zich razendsnel en zullen binnen enkele jaren de huidige standaarden aantasten. Wat vandaag nog onkraakbaar lijkt, kan morgen eenvoudig worden ontcijferd. Deze opkomende “quantumstorm” vraagt om actie vóórdat de impact voelbaar wordt.

Tegelijkertijd verplicht wetgeving zoals NIS2 en de BIO organisaties om hun beveiliging aantoonbaar te versterken – niet alleen in IT, maar vooral in OT-omgevingen. Juist daar, waar continuïteit cruciaal is, groeit de druk om toekomstbestendige bescherming te realiseren.

De digitalisering van vitale infrastructures heeft geleid tot een nauwere verweving van IT en OT. Dat biedt voordelen, maar vergroot ook het aanvalsoppervlak. Wat vroeger fysiek gescheiden was, is nu digitaal verbonden en daardoor kwetsbaarder.

Een belangrijk hulpmiddel om industriële risico's te duiden is het Purdue-model (PERA). Dit deelt industriële omgevingen op in zes lagen – van fysieke processen en sensoren tot cloudgebaseerde applicaties – en biedt inzicht in waar beveiligingsmaatregelen effectief kunnen worden toegepast. Hoewel het geen cybersecurityraamwerk is, vormt het wel een gemeenschappelijke taal om te begrijpen hoe aanvallen zich kunnen verspreiden, van een geïnfecteerde e-mail tot manipulatie van PLC's in de proceslaag. Een toekomstbestendige OT-strategie vraagt om het herstel en de versterking van digitale grenzen. Segmentatie met MagiCtwin voorkomt ongewenste communicatie tussen IT- en OT-zones, terwijl CryptoGuard met post-quantum encryptie de toegestane datastromen beschermt.

Volgens het Fortinet State of Operational Technology and Cybersecurity Report 2025 had 75% van de organisaties het afgelopen jaar minstens één OT-incident. Slechts 19% beschikt over een volwassen strategie. Compumatica, als volledig Europese ontwikkelaar, biedt oplossingen die bijdragen aan digitale soevereiniteit en de bescherming van kritieke netwerken en processen.





Quantum computing zal binnen enkele jaren de basis van traditionele encryptie ondermijnen. Algoritmen als RSA en ECC, die vandaag nog het fundament vormen van dataveiligheid, zijn straks in minuten te kraken.

De dreiging van store now, decrypt later – waarbij aanvallers vandaag versleutelde data onderscheppen om die later met quantum machines te ontcijferen – is geen hypothetisch scenario meer. Vooral in omgevingen waar data jarenlang wordt bewaard, zoals in operationele technologie (OT) en industriële processen, vormt dit een groot risico. Log- en meetdata, productieparameters en communicatie tussen systemen worden vaak voor lange perioden opgeslagen, soms tien tot twintig jaar, voor kwaliteitsborging, compliance of veiligheidsonderzoek.

Zodra quantum computers krachtig genoeg zijn, kunnen deze historische datasets – die vandaag als veilig worden beschouwd – alsnog worden ontcijferd. Dat maakt het essentieel om nu al te migreren naar quantum-safe encryptie en sleutelbeheer, zodat ook toekomstige toegang tot oude data wordt afgeschermd.

In juli 2024 publiceerde NIST de eerste post-quantum cryptografiestandaarden (CRYSTALS-Kyber en Dilithium). Europese initiatieven, zoals het EuroQCI-netwerk, bouwen ondertussen aan quantum veilige communicatiekanalen voor overheden en vitale infrastructuur. Voor vitale sectoren betekent dit dat bescherming tegen toekomstige ontcijfering vandaag al moet worden geïmplementeerd.

## // AI-RESISTENTE ENCRYPTIE EN PRIVACY-PRESERVING DATA-ANALYSE

Naast de dreiging van quantum computers speelt ook kunstmatige intelligentie (AI) een steeds grotere rol in de evolutie van cyberaanvallen. AI maakt het mogelijk om patronen in netwerkverkeer sneller te herkennen, versleuteld verkeer te modelleren en zelfs gedragsanalyse toe te passen op sleutelgebruik en systeeminteractie.

Om deze dreigingen het hoofd te bieden, is een nieuwe generatie AI-resistente encryptie nodig, met kenmerken als contextuele sleutelrotatie, tijdsgebonden policies en gedragsafhankelijke toegangscontrole. Dergelijke context-aware encryption voorkomt dat encryptie voorspelbaar wordt of blootstaat aan machine learning-aanvallen op metadata en verkeer.

Tegelijkertijd groeit de vraag naar het analyseren van gevoelige data zonder deze te ontcijferen. In sectoren als gezondheidszorg, overheid en finance worden daarom privacy-preserving analytics steeds belangrijker. Denk aan technieken zoals:

- **Fully Homomorphic Encryption (FHE)** – data blijven versleuteld tijdens verwerking
- **Zero Knowledge Proofs (ZKP)** – valideren zonder te onthullen
- **Secure Multi-Party Computation (MPC)** – collectieve analyse zonder centrale toegang

Deze ontwikkelingen tonen aan dat encryptie niet alleen gericht moet zijn op transportbeveiliging, maar ook op de levenscyclus van data, van opslag tot verwerking.

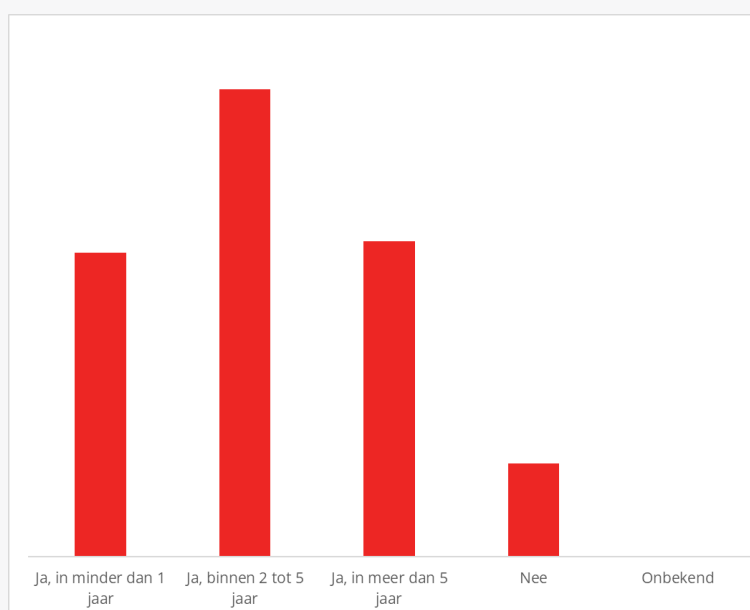


Encryptie beveiligt de inhoud van gegevens, maar niet het pad waarover die gegevens reizen. De meeste OT-incidenten beginnen niet met het breken van cryptografie, maar met het binnendringen van het netwerk via kwetsbaarheden of configuratiefouten.

In het rapport *The Challenges of IT/OT Convergence* wordt dit expliciet benoemd: bij 75% van de organisaties kwam de aanval op OT via een IT-systeem binnen. De oorzaak ligt vaak in het ontbreken van netwerksegmentatie, gedeelde credentials of onvoldoende isolatie tussen domeinen.

Encryptie alleen beschermt niet tegen laterale beweging, malwareverspreiding of insider threats. Fysieke segmentatie – het scheiden van OT- en IT-domeinen – vormt daarom de noodzakelijke eerste barrière.

Stel: een aanvaller dringt via een kwetsbare Windows-server in laag 5 het netwerk binnen. Zonder segmentatie kan hij via remote desktopservices laag 3 bereiken, waar SCADA-historian servers draaien met toegang tot realtime procesdata. Encryptie beschermt de data-inhoud, maar niet de route waarlangs die data stroomt. Segmentatie blokkeert die route volledig.



Verwachte toename van regelgeving en naleving



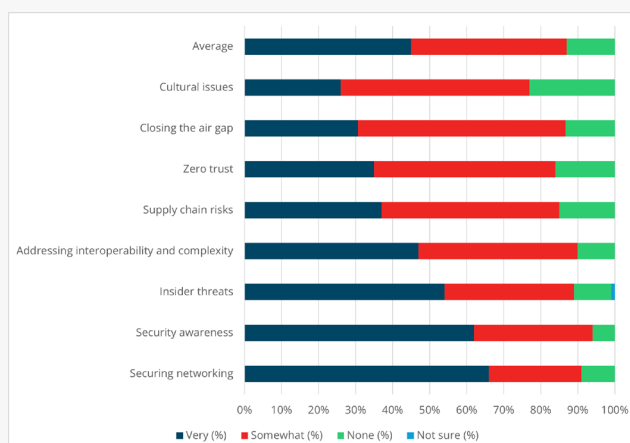
Segmentatie en encryptie worden steeds vaker gezien als belangrijke bouwstenen voor OT-beveiliging, al is volledige encryptie in veel industriële omgevingen nog niet haalbaar. Veel protocollen en apparaten in de OT-wereld ondersteunen het eenvoudigweg niet, of vertragen kritieke processen wanneer encryptie wordt toegepast. Segmentatie vormt daarom de eerste en meest haalbare stap: het scheiden van zones en netwerken om de impact van een aanval te beperken en controle te behouden over kritieke processen. In een tijd waarin aanvallen slimmer, sneller en grensoverschrijdender worden, biedt een gelaagde aanpak de beste basis voor weerbaarheid en continuïteit.

Een toekomstbestendige OT-architectuur berust op twee samenwerkende lagen:

- Fysieke segmentatie: via data diodes en firewalls wordt verkeer éénrichtingsverkeer of gecontroleerd tweerichtingsverkeer, zodat kritieke OT-netwerken nooit direct benaderd worden.
- Post-quantum encryptie: beschermt de datastromen die wel mogen passeren, tegen onderschepping en toekomstige ontcijfering.

Volgens het OT-cybersecurityrapport staat netwerksegmentatie bovenaan de prioriteitenlijst van OT-leiders, gevolgd door encryptie en zero trust. Omdat dit toevoegt dat 80% van bedrijven erkent dat convergentie de risico's vergroot, maar minder dan 20% die risico's structureel adresseert.

### Hoe goed is uw organisatie voorbereid op de volgende gebieden van geconvergeerde IT/OT-beveiliging binnen bedrijven?



Bron: Omdia



MagiCtwin dual firewall appliance

## // MAGICTWIN: FYSIEKE NETWERKSEGMENTATIE OP MAAT

MagiCtwin scheidt IT- en OT-netwerken fysiek via een dubbele firewallarchitectuur in één behuizing. De Diode-variant garandeert eenrichtingsverkeer, ideaal voor SCADA-uitwisseling zonder dat verkeer terug kan. Firewall<sup>2</sup> maakt gecontroleerde tweerichtingscommunicatie mogelijk via protocollaire proxies. De robuuste hardware is fanless, industrieel inzetbaar en via gescheiden interfaces te beheren zonder single point of failure. MagiCtwin is opgenomen in het BSPA-register van de AIVD en vormt een essentiële bouwsteen binnen een zero-trust OT-architectuur. Zo wordt laterale beweging geblokkeerd, terwijl datadoorstroming veilig en gecontroleerd blijft, ook in vitale infrastructuur.



CryptoGuard VPN 6500-serie

## // CRYPTOGUARD: QUANTUM-READY ENCRYPTIE ZONDER CONCESSIONS

CryptoGuard versleutelt dataverkeer op laag 2, 3 en 4 zonder tunnels of sessies, met minimale latency tot boven de 100 Gbps. De unieke CryptoGuard-modus ondersteunt post-quantum algoritmen (Kyber, Dilithium) en voorkomt overhead of pakketvergroting. Door certificering van NAVO, EU en de Nederlandse overheid (DV-niveau, herbevestigd door AIVD in 2025), is CryptoGuard geschikt voor vertrouwelijke communicatie binnen overheid en vitale sectoren. Beheer verloopt centraal via SMS. Het resultaat: een cryptografisch ondoordringbare, maar operationeel onzichtbare encryptielaag, futureproof tegen afluisteren, manipulatie en quantum dreiging.



## // FEATURES & COMPLIANCE-OVERZICHT

| Kenmerk                     | CryptoGuard                                       | MagiCtwin (Diode / Firewall <sup>2</sup> )                         |
|-----------------------------|---------------------------------------------------|--------------------------------------------------------------------|
| Encryptielagen              | OSI Laag 2, 3, 4                                  | —                                                                  |
| Encryptiemodus              | Unieke modus + IPsec (CryptoGuard modus)          | —                                                                  |
| Quantum-safe (PQC)          | ✓<br>Kyber & Dilithium                            | ✓                                                                  |
| Latency                     | < 1 milliseconde (sub-millisecond)                | Deterministisch, geen latency toegevoegd                           |
| Throughput                  | > 100 Gbps                                        | Tot 1+ Gbps                                                        |
| Gecertificeerd voor DV (NL) | ✓                                                 | ✓                                                                  |
| NATO / EU certificering     | ✓                                                 | ✓                                                                  |
| Segmentatievorm             | —                                                 | Fysiek (Diode), Software (Firewall <sup>2</sup> ), Cloud (Virtual) |
| Tweerichtingsverkeer        | —                                                 | Alleen Firewall <sup>2</sup> en Virtual                            |
| Beheer & integratie         | Centraal via SMS / firmware updates mogelijk      | Gescheiden beheer TX/RX + webinterface                             |
| Ondersteunde protocollen    | Agnostisch                                        | SCADA: IEC104, DNP3, MODBUS, (proxies)                             |
| Fail-safe ontwerp           | ✓<br>hardware bypass-modus beschikbaar            | ✓<br>geen single point of failure, dubbele firewall                |
| Cloud-compatibel            | ✓                                                 | ✓<br>MagiCtwin Virtual voor multi-RX scenario's                    |
| Toepassingen                | End-to-end encryptie tussen datacenters, OT-sites | Segmentatie tussen IT en OT-netwerken, SCADA                       |

## // BENIEUWD HOE SEGMENTATIE EN ENCRYPTIE SAMENWERKEN IN UW OMGEVING

Lees verder of plan direct een intake





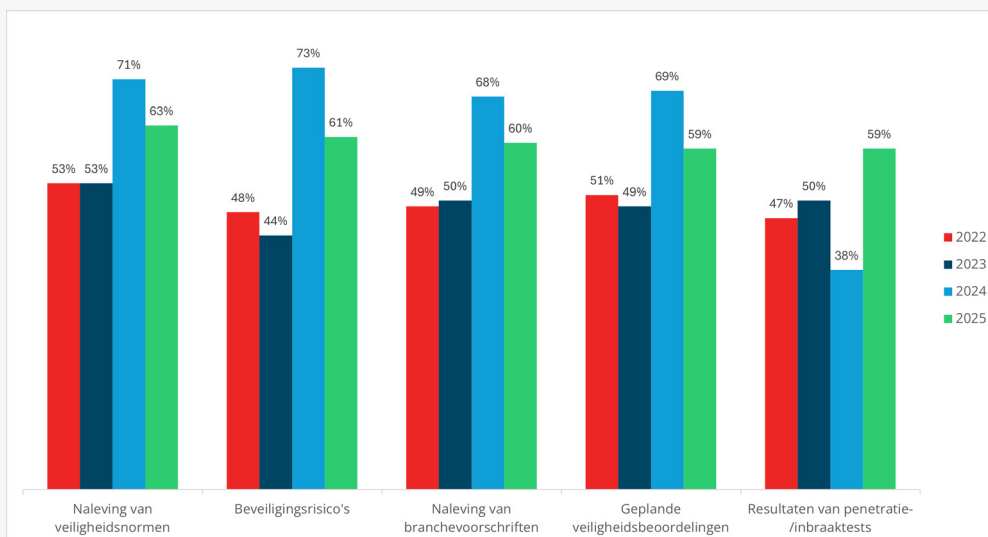
In veel organisaties vormt complexiteit de grootste barrière voor effectieve OT-beveiliging. De integratie met bestaande systemen blijft een uitdaging, en slechts een derde van de industriële organisaties beheert IT- en OT-beveiliging centraal. Die versnippering verzwakt de weerbaarheid. Juist in omgevingen waar veiligheid en beschikbaarheid cruciaal zijn, wordt eenvoud een strategisch voordeel.

Compumatica kiest daarom voor vereenvoudiging in plaats van meer lagen. De oplossingen vereisen geen software op endpoints, respecteren bestaande netwerken en bieden gescheiden beheer per zijde van het systeem.

Deze architectuur ondersteunt naleving van NIS2, BIO en VIR-BI, en sluit binnen de overheid aan op het Programma Quantum-veilige Cryptografie van het Rijk, waarin de migratie naar BBN3-conforme encryptie en

post-quantum cryptografische (PQC) algoritmen centraal staat. Daarmee sluit Compumatica aan op de nationale routekaart voor quantum-veilige communicatie in de strategische cybersecurityagenda van het Rijk.

Door segmentatie en encryptie te combineren ontstaat aantoonbare netwerkafscherming, traceerbaar sleutelbeheer en gecontroleerde data-toegang, de pijlers waarop compliance-audits worden beoordeeld. Compumatica's DV-gecertificeerde en AIVD-erkende oplossingen maken organisaties niet alleen veilig, maar ook aantoonbaar compliant. Het centrale Security Management Station (SMS) beheert alle encryptie-apparaten vanuit één punt, verlaagt beheerlast en versnelt updates. Zo ontstaat robuuste OT-beveiliging die productie ondersteunt en balans houdt tussen controle, continuïteit en compliance.



Gemelde OT-cyberbeveiligingsproblemen



## // PRAKTIJKTOEPASSINGEN IN VITALE INFRASTRUCTUREN



### Energie

Elektriciteitscentrales en netbeheerders zijn steeds vaker doelwit van cyberaanvallen; in 2024 nam de activiteit van dreigingsactoren in de energiesector met 93% toe. Een succesvolle inbraak op SCADA- of monitoringnetwerken kan leiden tot operationele verstoringen of zelfs grootschalige uitval. Met de inzet van de MagiCtwin Data Diode kunnen realtime data vanuit het OT-netwerk veilig ontsloten worden naar monitoring- of analyseplatforms, zonder dat er een weg terug bestaat. Zo blijft het OT-netwerk afgeschermd van IT-aanvallen, terwijl bedrijfscontinuïteit en zichtbaarheid behouden blijven.



### Drinkwater

Digitale aansturing van zuiveringsinstallaties vergroot het aanvalsoppervlak: in 2024 kreeg 62% van de water- en energiebedrijven te maken met cyberaanvallen. Manipulatie van pH- of chloorwaarden kan directe gevolgen hebben voor de volksgezondheid. MagiCtwin zorgt voor een fysieke scheiding tussen procesnetwerk en externe partijen zoals toezichthouders of cloudplatforms. Data kan veilig worden doorgestuurd, maar externe toegang tot OT blijft uitgesloten.



### Olie & Gas

Offshore platforms, raffinaderijen en distributiestations vertrouwen op OT-systemen voor productie en veiligheid. Een cyberaanval op deze infrastructuur veroorzaakt niet alleen economische schade maar levert ook fysieke risico's op; zo legde de Colonial Pipeline-aanval 45% van de brandstoftoevoer aan de Amerikaanse Oostkust lam. Met MagiCtwin wordt het productie- en procesnetwerk gescheiden van het IT-landschap. Gegevensuitwisseling met het hoofdkantoor of externe applicaties verloopt strikt eenrichtingsverkeer, waardoor laterale beweging van dreigingen structureel wordt uitgesloten.



### Nucleair

Kerninstallaties hanteren van oudsher stringente veiligheidsprotocollen, maar ook hier geldt dat digitalisering nieuwe kwetsbaarheden introduceert. Historische voorbeelden zoals Stuxnet tonen aan dat zelfs goed beveiligde installaties doelwit kunnen zijn; deze aanval vernietigde bijna een vijfde van Iran's uraniumcentrifuges. Door gebruik te maken van de MagiCtwin Data Diode kunnen operationele gegevens, statusrapportages en auditlogs veilig gedeeld worden met toezichthouders, zonder dat deze systemen op enigerlei wijze bereikbaar zijn vanaf de buitenwereld.



### Overheid

Rijksdiensten, defensie-instellingen en andere overheidsorganisaties verwerken vertrouwelijke data die vaak afkomstig zijn uit gescheiden netwerken of kritieke installaties. Om deze gevoelige gegevens veilig door te sturen naar centrale analyse- of rapportageomgevingen, wordt MagiCtwin ingezet als digitale sluis. Zo wordt fysieke netwerksegmentatie afgedwongen binnen BIO-conforme architecturen, met gegarandeerde eenrichtingscommunicatie. Dit voorkomt dat bedreigingen zich vanuit kantoornetwerken verplaatsen naar strategische OT-domeinen, cruciaal aangezien 70% van de OT-aanvallen begint in de IT-omgeving.



## // DE ROUTE NAAR FUTUREPROOF OT-BEVEILIGING

In een tijdperk waarin IT en OT steeds verder in elkaar overlopen, AI-aanvallen realtime leren en quantum computers klassieke cryptografie ondermijnen, is futureproof beveiliging geen optie, maar een plicht.

Segmentatie zonder encryptie is als een kluis zonder sleutel. Encryptie zonder segmentatie is als een sleutel zonder deur. Samen vormen MagiCtwin en CryptoGuard een gelaagde beveiligingsarchitectuur die aansluit op de praktijk van vandaag en bestand is tegen de dreigingen van morgen.

Wie vandaag begint met segmentatie én encryptie, bouwt aan de veerkracht van morgen. Niet omdat het moet, maar omdat de continuïteit van onze samenleving ervan afhangt.

De toekomst vraagt niet alleen om bescherming tegen quantum dreiging, maar ook om weerbaarheid tegen AI-gestuurde aanvallen en de mogelijkheid om data veilig te analyseren zonder die te ontcijferen. Wie nu kiest voor een toekomstgerichte architectuur, investeert niet alleen in veiligheid, maar in aanpasbaarheid, digitale soevereiniteit en continuïteit op lange termijn.



## // BEGIN VANDAAG

Uw OT-netwerk is nu misschien nog veilig. Maar is het ook bestand tegen wat eraan komt? Quantum Computers, AI-gedreven aanvallen en nieuwe wetgeving zoals NIS2 veranderen de spelregels permanent. De tijd om te handelen is vóórdat de dreiging realiteit wordt.

Twijfelt u of uw OT-omgeving futureproof is? Dan is het antwoord waarschijnlijk nee. Plan een vrijblijvend intakegesprek met een van onze OT-securityexperts en ontdek hoe u uw netwerk écht voorbereidt op de toekomst.

Scan de QR-code of ga naar:  
<https://info.compumatica.com/toekomstbestendig/contact>



## Compumatica secure networks B.V.

Oude Udenseweg 29, 5405 PD Uden

[www.compumatica.com](http://www.compumatica.com)

### Gebruikte openbare bronnen

Quantum Computers Are Coming, and the Netherlands Is Ready (Government of the Netherlands, 2025), European Quantum Communication Infrastructure (European Commission, 2024), NATO Quantum Technologies Strategy (North Atlantic Treaty Organization, 2024), Technology Strategy Towards 2030 (NATO Communications and Information Agency, 2024), NIST PQC Standards Announcement (National Institute of Standards and Technology, 2024), ISO/IEC 23837-1:2023 (International Organization for Standardization, 2023), Quantum: Problem and Solution for the Next Decade of Data Security? (Laser Focus World, 2024), Hybrid Quantum-Safe Encryption System Launch (The Quantum Insider, 2025), QKD: Part of a Defense-in-Depth Security Strategy (ID Quantique / QED-C, 2024), CISA's Post-Quantum OT Guidance (Post-Quantum & U.S. Cybersecurity and Infrastructure Security Agency, 2024), NATO Trials 'Anti-Quantum' Encryption in 5G Exercise (International Cutting-Edge Tech Vision, 2024), State of Operational Technology and Cybersecurity Report 2025 (Fortinet, 2025), The Challenges of IT/OT Convergence (Omdia, 2024), Stuxnet analyse (Kaspersky Lab, 2021), Dragos OT Cybersecurity Year in Review 2024 (2025), Semperis Critical Infrastructure Resilience onderzoek (2025)

### Disclaimer

Deze whitepaper is met de grootst mogelijke zorgvuldigheid samengesteld. Compumatica streeft naar het verstrekken van accurate, actuele en relevante informatie. Aan de inhoud van dit document kunnen echter geen rechten worden ontleend. De beschreven technologieën, standaarden, toepassingsvoorbeelden en inzichten zijn uitsluitend bedoeld voor algemene informatievoorziening, en vormen geen juridisch, technisch of strategisch advies. Compumatica behoudt zich het recht voor om zonder voorafgaande kennisgeving wijzigingen aan te brengen in producten, specificaties of documentatie. Gebruik van de informatie in deze whitepaper is geheel op eigen risico. Compumatica aanvaardt geen enkele aansprakelijkheid voor directe of indirecte schade die voortvloeit uit het gebruik of de interpretatie van deze publicatie. Het Compumatica-logo en de merknaam Compumatica, evenals de productnamen MagiCtwin en CryptoGuard, zijn eigendom van Compumatica secure networks B.V. Alle overige merknamen, logo's en handelsmerken die in deze whitepaper worden genoemd of weergegeven, zijn eigendom van hun respectieve houders. Vermelding hiervan impliceert geen goedkeuring, partnerschap of samenwerking tussen Compumatica en deze partijen, tenzij uitdrukkelijk anders vermeld.