Dutch IT Channel Awards | 08. Endpoint Security Innovator of the Year

IGEL is een wereldwijd leider in endpoint-beveiliging en aanbieder van IGEL OS, een veilig en toekomstbestendig besturingssysteem voor endpoints.

IGEL OS staat bekend om zijn Preventative Security Model. Dit model is ontwikkeld ter ondersteuning van zero trust- en Secure Access Service Edge (SASE)-initiatieven. Met het model maakt IGEL een einde aan kwetsbaarheden in de beveiliging van endpoints die door cybercriminelen misbruikt kunnen worden.

Cijfers laten namelijk zien dat een traditionele aanpak van endpointbeveiliging tekortschiet:

- $4,88 miljoen: gemiddelde kosten van een datalek in 2024 (https://www.ibm.com/reports/data-breach)
- 47% van de organisaties heeft een beleid om losgeld te betalen (IBM)
- 59% van de organisaties kreeg in 2024 te maken met een ransomware-aanval
- Slechts 8% van de organisaties die betaalden, kreeg alle data volledig terug (https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/)

IGEL's antwoord hierop is een holistische oplossing voor een veilige digitale werkplek, in samenwerking met toonaangevende technologiepartners. Het Preventative Security Model (PSM) biedt op vijf manieren ondersteuning voor zero trust- en SASE-initiatieven:

- Een read-only besturingssysteem. Het op Linux gebaseerde IGEL OS beschermt gebruikers tegen het per ongeluk of met opzet installeren van malware op endpoints. Dit verkleint de kans op succesvolle phishingpogingen, besmettingen met ransomware en andere cyberaanvallen.
- Geen lokale gegevensopslag. Er kunnen geen klantgegevens, patiëntgegevens, financiële gegevens of andere data naar het endpoint worden gedownload of worden opgeslagen op aangesloten USB-apparatuur. Dat betekent dat diefstal en verlies van endpoints niet leiden tot datalekken en dat ook medewerkers met kwade bedoelingen gegevens niet extern kunnen verspreiden.
- Een vertrouwd applicatieplatform. De veilige opstartprocedure van het IGEL OS zorgt ervoor dat niemand met programmatuur kan knoeien. Het endpoint wordt altijd opgestart naar de laatst bekende goede toestand. Zo kunnen organisaties na een cyberaanval in enkele minuten alle diensten herstellen.
- Authenticatie, SSO-integratie en SASE. IGEL werkt samen met leveranciers van authenticatieoplossingen, waaronder Microsoft, Imprivata, Okta, Ping Identity, VMware en Citrix, zodat het ondersteuning kan bieden voor een breed scala aan standaarden. IGEL werkt daarnaast met SASE-partners samen aan de optimalisatie van zero trust-implementaties.
- Een modulair ontwerp. Met een grootte van slechts 2 GB biedt het IGEL OS een kleiner aanvalsoppervlak dan traditionele besturingssystemen voor endpoints. Organisaties kunnen aanvullende functionaliteit, zoals integraties met oplossingen van partners als Citrix en VMware en security-leveranciers downloaden via het IGEL App Portal.

Direct herstel bij ransomware
Met de introductie van IGEL Business Continuity & Disaster Recovery (BC/DR) en IGEL Dual Boot eerder dit jaar tilt IGEL endpointbeveiliging naar een nieuw niveau. Bij een ransomware-aanval kunnen gebruikers hun besmette Windows-apparaat simpelweg opnieuw opstarten in het veilige IGEL OS, zonder nieuwe hardware of re-imaging.

Voordelen:

- Herstel van veilige toegang binnen minuten in plaats van dagen.
- Bedrijfscontinuïteit zelfs tijdens een aanval
- Behoud van forensisch bewijs voor compliance en verzekeringsclaims
- Geen dataverlies, geen downtime

Hoe het werkt

- Geen gegevensherstel of decryptie nodig: IGEL herstelt geen verloren data, en herstelt al evenmin Windows. Gebruikers kunnen in plaats daarvan besmette endpoints opnieuw opstarten in een schone omgeving met het IGEL OS. Daarmee krijgen ze opnieuw toegang tot alle bedrijfsapplicaties, communicatieplatforms en workflows, zelfs tijdens een aanval.
- Bewaren van bewijsmateriaal in het kader van compliance: De besmette Windows-partitie blijft onaangeraakt, zodat het forensisch bewijs in stand blijft voor nader onderzoek en verzekeringsclaims.
- Centraal, schaalbaar en simpel: Alle herstelbewerkingen worden beheerd via de IGEL Universal Management Suite™ (IGEL UMS™), met expertdiensten voor de installatie, het testproces en de validatie.

“Ransomware is onvermijdelijk, maar downtime hoeft dat niet te zijn”, aldus Klaus Oestermann, CEO van IGEL.

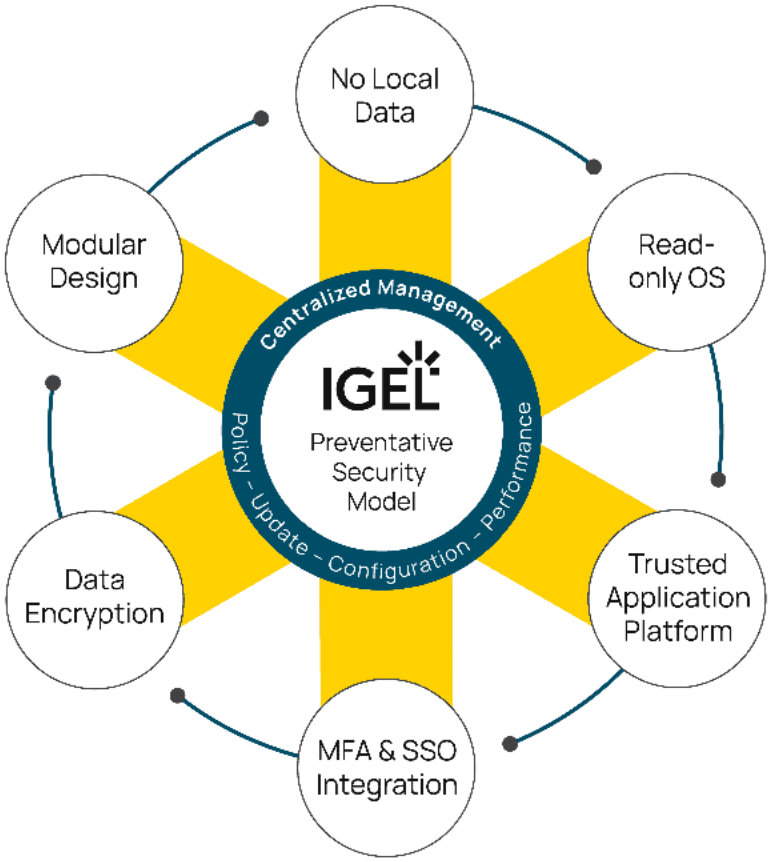
Duurzaamheid
Daarnaast zet IGEL in op duurzaamheid en kostenbesparing. Door bestaande hardware langer te benutten en de software-footprint te minimaliseren, realiseren klanten een lagere TCO en CO_2-reductie. IGEL’s rol verandert daarmee van thin client-leverancier naar toonaangevend softwareplatform voor veilige en duurzame digitale werkplekken.

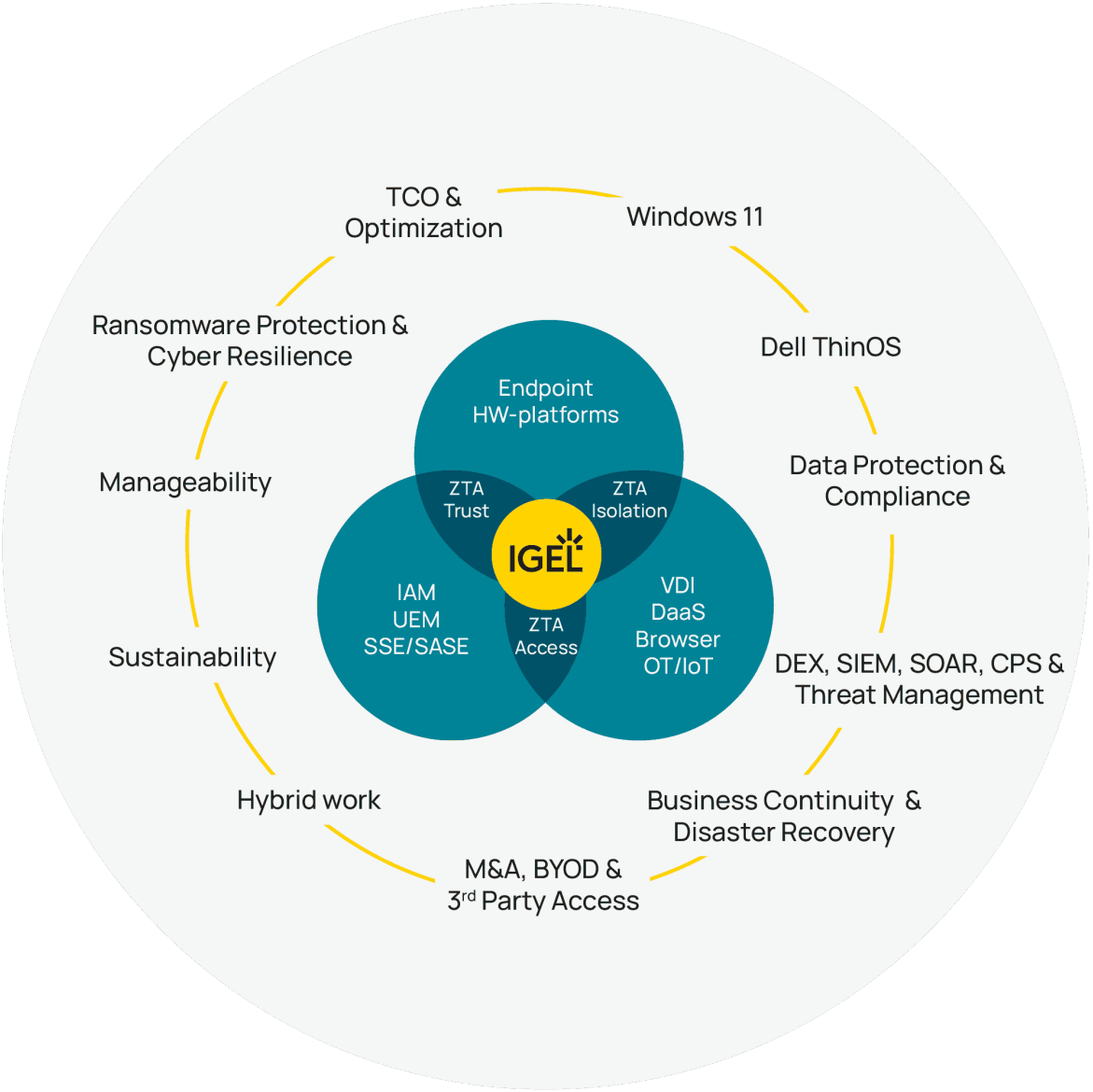
Innovaties in 2025
IGEL Dual Boot – instant herstel van besmette endpoints; veilig herstarten naar IGEL OS zonder re-imaging of nieuwe apparatuur.
IGEL BC/DR Platform – directe bedrijfscontinuïteit tijdens ransomware-aanvallen met behoud van compliance-bewijsmateriaal.

Voor meer informatie: https://www.dutchitchannel.nl/news/710363/igel-laat-organisaties-systemen-binnen-enkele-minuten-herstellen

Kortom
IGEL herdefinieert endpoint security en disaster recovery. Waar traditionele aanpakken zich richten op detectie en herstel, voorkomt IGEL uitval door cyberdreigingen en zorgt voor continuïteit. Met IGEL BC/DR en Dual Boot transformeert elke endpoint tot een zelfherstellende werkplek – veilig, betaalbaar en toekomstbestendig.

Ondersteunend beeldmateriaal [IGEL]


No Local Data
Read-only OS
Trusted Application Platform
MFA & SSO Integration
Data Encryption
Modular Design
Centralized Management
Policy – Update – Configuration – Performance
IGEL
Preventative Security Model


TCO &
Optimization
Windows 11
Dell ThinOS
Data Protection &
Compliance
DEX, SIEM, SOAR, CPS &
Threat Management
Business Continuity &
Disaster Recovery
M&A, BYOD &
3rd Party Access
Hybrid work
Sustainability
Manageability
Ransomware Protection &
Cyber Resilience
Endpoint
HW-platforms
ZTA
Trust
ZTA
Isolation
IGEL
IAM
UEM
SSE/SASE
ZTA
Access
VDI
DaaS
Browser
OT/IoT