
IGEL now
&next

The IGEL Platform

UMS, Zero Trust and Multi Regulatory Framework Compliance

John Walsh, Office of CTO, Field CTO for Gov & Critical Industries

IGEL Adaptive Secure Endpoint Platform™

paloalto NETWORKS · zscaler · CISCO ISE · FORESCOUT · CLOUDFLARE · netskope

imprivata · Microsoft Entra ID · okta

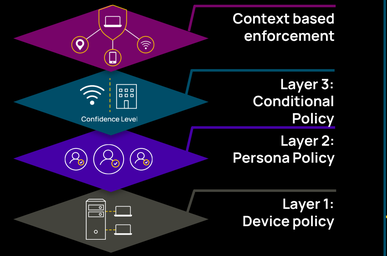
splunk> · control up · cisco ThousandEyes · Panorama · sumo logic · liquidware · Lakeside · 1E

Microsoft Intune

IT Endpoints - IGEL Adaptive Secure Desktop™

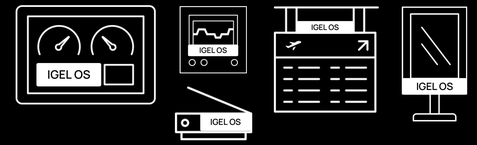
IT Endpoint Chipsets – IGEL Enclave TMSE™

Universal Management Suite™



IGEL unified management for X86+Arm Chip architectures

OT Endpoints - IGEL Adaptive Secure OT™

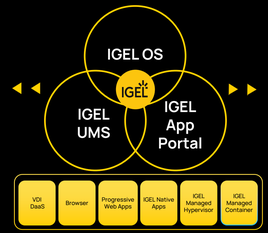


OT Endpoint Chipsets – IGEL Enclave TMSE™

Manageability - IGEL IT & OT Adaptive Secure Endpoint Orchestration

IASD™ integrates

- VDI/DaaS
- Browser
- PWAs
- Native Apps
- IMH-Hypervisor
- IMC-Containers



IASOT™ "IGEL IT for OT"

OT Managed like IT for Gov't & Critical Industries

- Central Mgmt., Control, and Compliance
- Edge Modernization & Automation
- Critical Industries – SCADA
- Manufacturing
  - Human Machine Interface (HMI) Display
  - Management Execution System (MES)
- Digital Signage

IGEL's Platform Spans Multiple Verticals

Highly Regulated Markets

	Healthcare	Government	Finance	Manufacturing	Retail/Transport
Industry Regulations IGEL Supports	HIPAA CISA	FISMA/NIST SP 800-34 VsnfD ZTA + CMMC FIPS	PCI DSS FINRA GLBA / SOX FIPS	FDA IEC 62443 ISO27001	FAA – DOT PCI DSS
IGEL Advantage	PSM - ZTA Fast User Switching Kiosk MFA / FIDO2	PSM - ZTA Enforce Policy - TMSE™ IT+OT Security CAC/PIV MFA	PSM – ZTA IHM/IHC Desktop modernization MFA / FIDO2	PSM – ZTA Enforce Policy - TMSE™ IT+OT Security Edge virtualization IMH/IMC	PSM –ZTA IT+OT Security
IGEL Ready Partners	Imprivata Phillips Nuance EHR -EPIC	NAC – SSE/SASE 90meter Cisco ISE Fortinet	Bloomberg Payment CC ATM -POS	OEM – Honeywell, … Nymi ARM devices	ARM devices POS

IGEL Adaptive Secure Endpoint Platform

UMS Control Plane: Policy Information, Decision, Administration and Enforcement

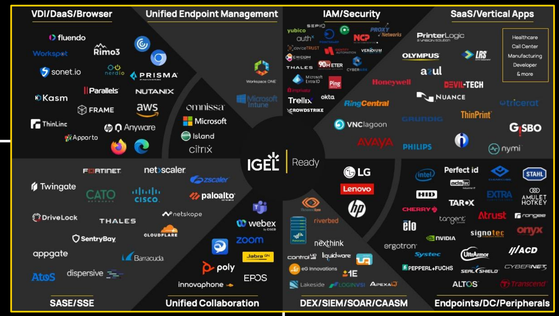
App Portal Data Plane: Policy Enforcement

OS Execution Plane: Policy Information and Enforcement

External Partners: Policy Information, Decision, Administration

UMS12
IGEL Management
PSM

POLICY
PIP, PDP, PE*



Secure
Agile
Scalable

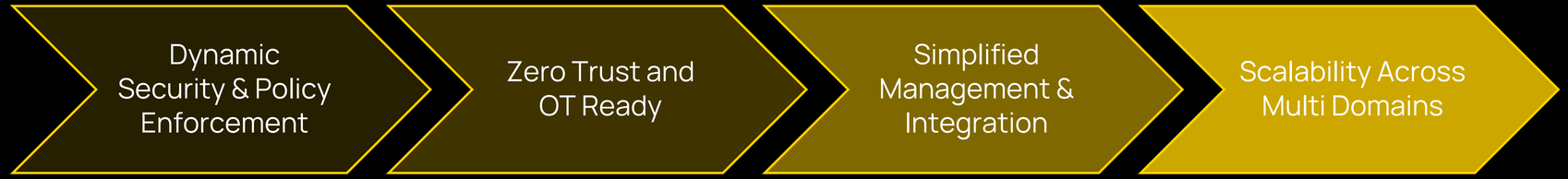
PSM

Optimized Experience
Centralized Control

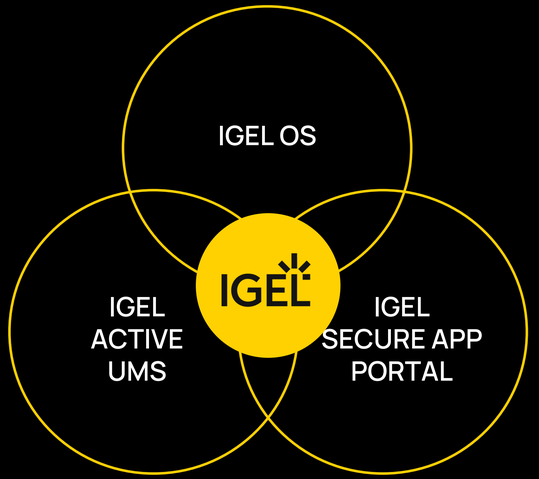
CLOUD SERVICES
IGEL App Repository
PSM

IGEL Centralized Management Capabilities With IGEL UMS

A Key Component to Integration and Solution Architectures



Benefits of IGEL Policy Integration/Orchestration



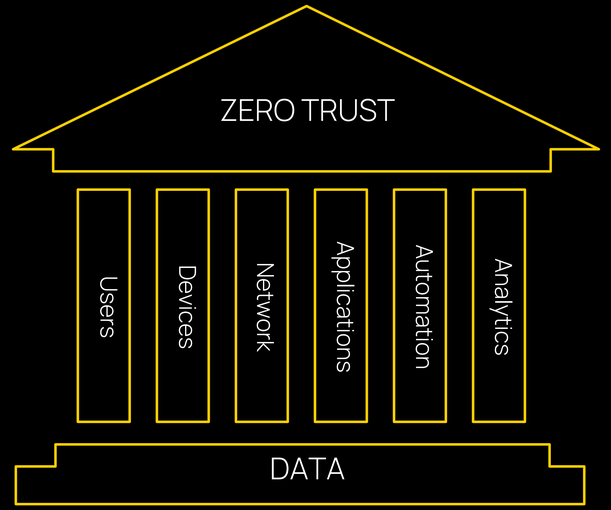
Extending Trust with Active UMS, IMH, and IMC

Key Features:

- UMS for Centralized management of client-side virtual machines (VMs) and Containers
- Full control and policy enforcement of VMs and Containers deployed at the edge (start/stop/reset/refresh)
- Provides separation of duties from Sec/Dev for Container Ops Deployments
- Traditional OS's made immutable – reboot resets to known good state

Zero Trust in a Heterogeneous Environment

Integration and Orchestration



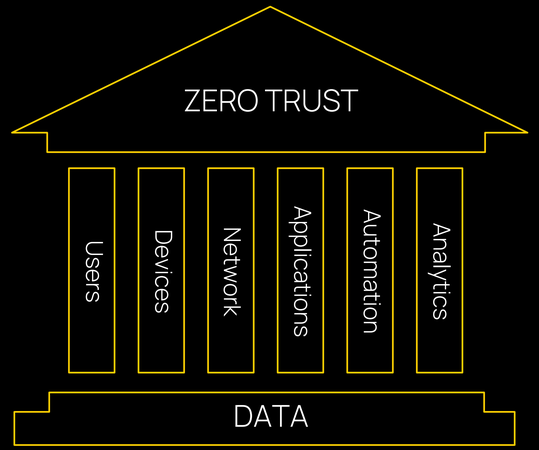
NOTE:

Since US Zero Trust Journey started @ DreamPort, Columbia MD in January 2019 – biggest challenge – integration and orchestration!

- Sort through the “Zero Trust” buzz – no one product!
- Determine your critical assets/ priorities
- **Establish boundaries:** ZT Enclave
- Leverage your existing investment
- Map to Zero Trust Outcomes
- Requires platform integration vs point products/layers
- **Develop a roadmap:** crawl, walk, run

For Customers Who Want Zero Trust

More than “designed in”



Identity/Subject

- Personal
- Device
- Applications
- Geo-location
- Network
- Data

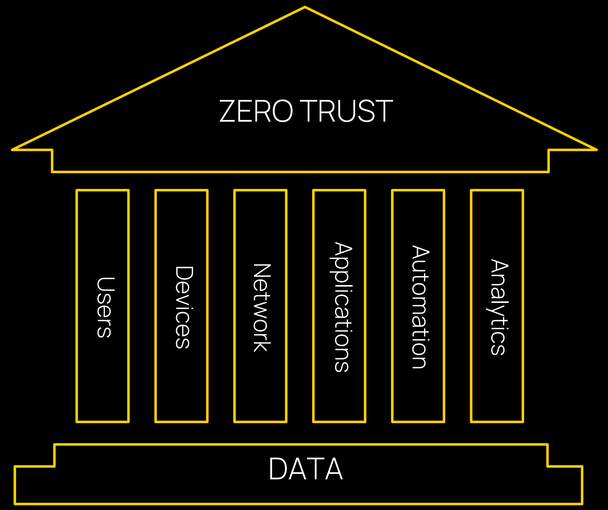
Confidence Level

Policy Enforcement Least Privilege Access

Continuous Monitoring & Enforcement

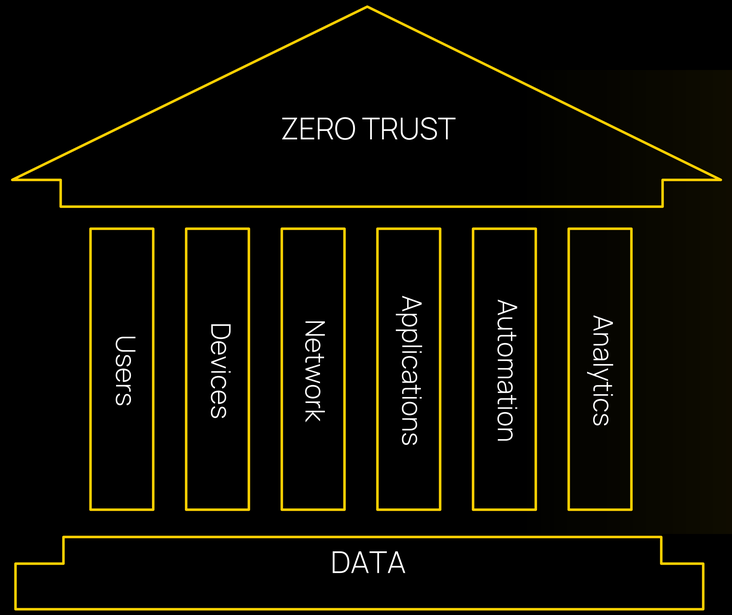
Zero Trust Requires Systemic Approach Using Integration Mapping

Meeting ZT 91 Target and 61 Advanced Activities with IGEL & Partners



IGEL Integration with Active UMS ▶ 42 ZT Functions & IGEL Partners ▶ IGEL Integration = ZT Flow ▶ ZT Functions & Policy Enforce

Partnering for Zero Trust Next-Gen Defense



zscaler™ netskope Island

CROWDSTRIKE paloalto® NETWORKS FORESCOUT®

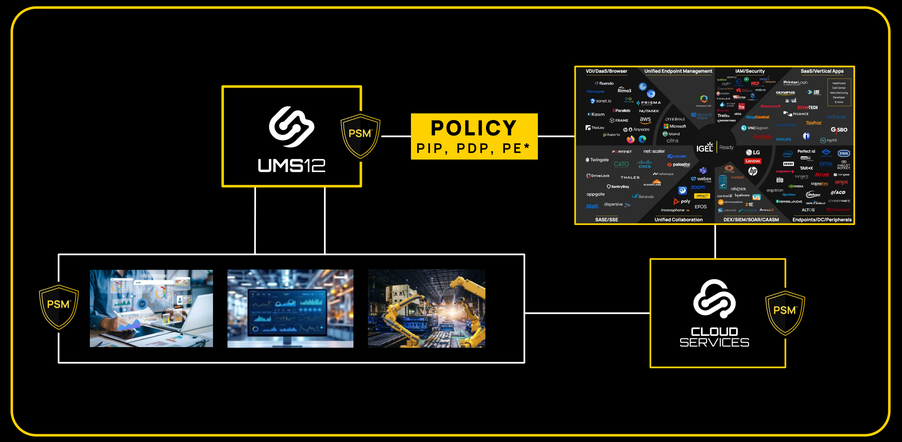
omnissa™ Trellix cisco appgate

Introducing Trusted Macro Secure Enclave™

Extending Zero Trust Principles with Interactive Policy Management and Enforcement

Preventative Security Model

- Immutable OS (Execution Plane) (PE)
- Hardware Root of Trust With TPM (Identity)
- UMS: Network Access and Policy Enforcement (Control Plane) - PA, PE
- Attestation and Verification
- Certified App Portal (Data Plane) (PA, PE)



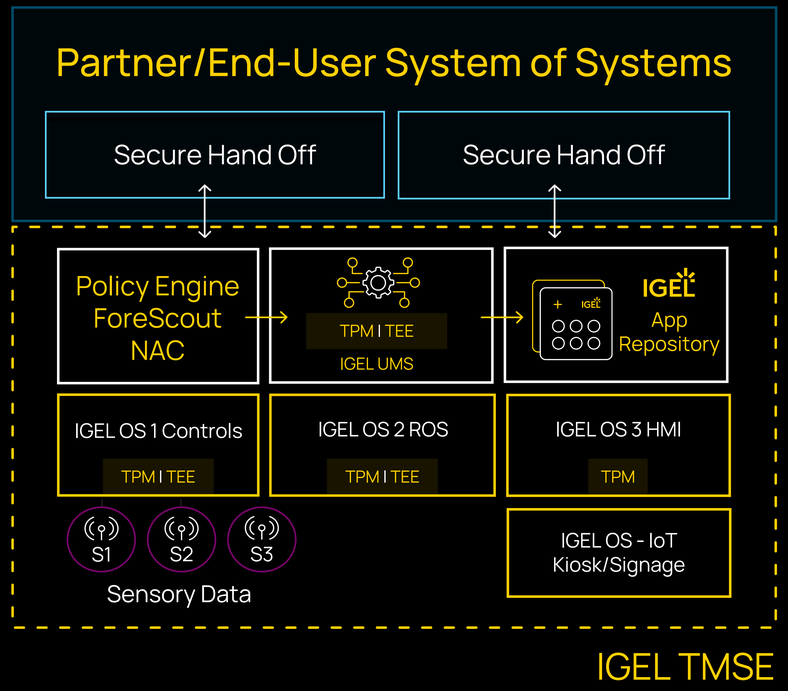
TMSE Benefits for OEM/GSI/End User

- Confidence in IGEL Endpoints
- Active Participation with System Wide Policy Engines
- Protected Data Integrity for Enterprise, Controls, ML, AI Training Data
- Establish and Enforce of Zero Trust Boundaries
- Unified Layer for Centralized End Point Management, Network Access Control, Segmentation and Policy Enforcement

TMSE™ for Complex Environments

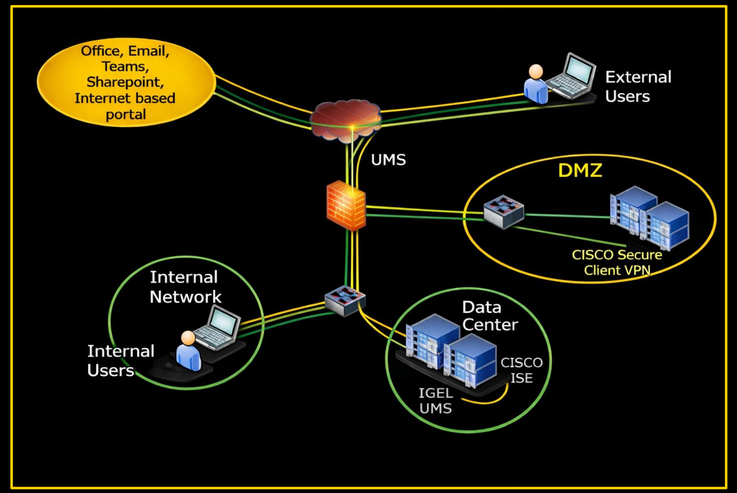
Extending PSM with Identity Aware Access Control and Policy Enforcement

- PSM locks down execution, control, and data planes
- TMSE extends trust boundaries: endpoint – network – cloud – IGEL Ready Partners
- Centralized management and segmentation for IT & OT Convergence
- Seamless secure policy-based handoffs to analytics, AI, & other critical workloads
- Enables Compliance with Zero Trust, IEC62443, NIS2, CMMC, Data Sovereignty, and other regulatory frameworks
- Secures remote access control



TMSE Demonstration

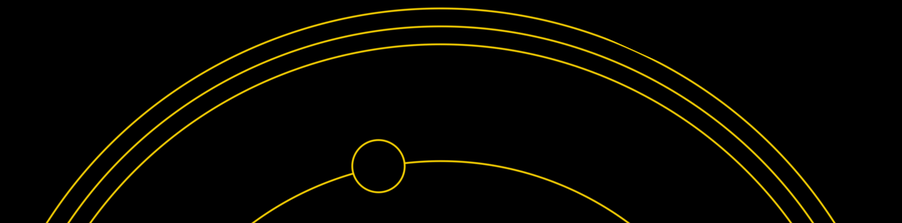
Policy Engine + UMS for Network Access, Policy Admin and Enforcement at the Endpoint



- IGEL OS reduces attack surface, complexity, cost and timeline
- UMS Integrated with CISCO ISE Policy Engine:
  - Devices individually enrolled in UMS provides segmentation
  - Policy Engine Aggregates data for C2C* for Network Access – interrogates UMS
  - UMS Enforces Network Access Control (NAC)
  - Confidence based policy administration / configuration control
  - IGEL App Repository enforces app certification
- On Prem and Remote Access

*Comply to Connect

Evidence our Model works



IGEL Compliance Mapping

- CMMC
- Zero Trust 2.0
- U 2022/2555 - NIS2
- EU 2022/2557 (CER)DE – KRITIS*
- Infrastructure
- IEC 62443
- Data Sovereignty
- NIST CSF2.0

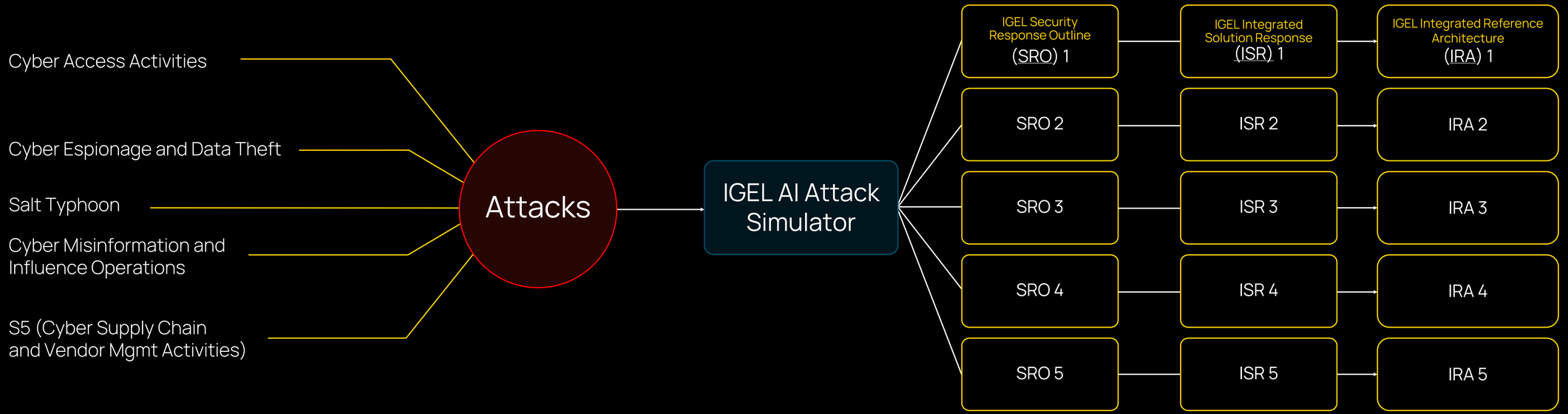
** Critical Entities Resilience Directive*

IT/OT Requirements and Compliance Mapping

Key Requirements		Compliance Directive			
		NIST CSF	ISF/IEC 62443	NIS2	PCI DSS
	Access Controls	✓	✓	✓	✓
	Identity Management	✓	✓	✓	✓
	Network Segmentation	✓	✓	✓	✓
	Data Protection	✓	✓	✓	✓

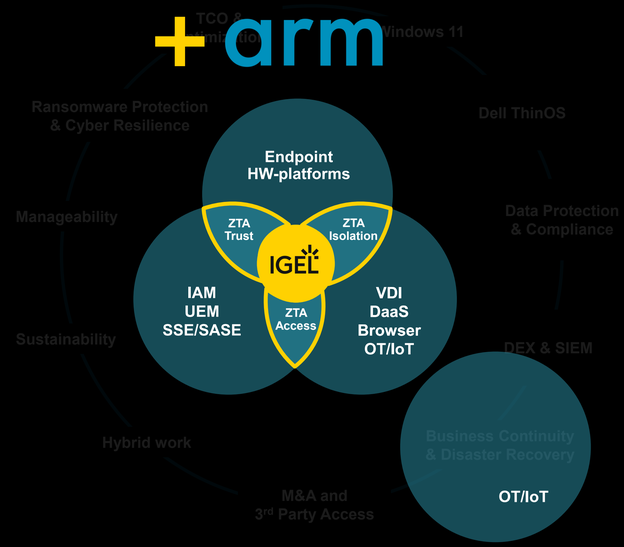
AI (IT/OT/ZT) MITRE ATT&CK Simulator

IGEL Zero Trust methodology stop attacks



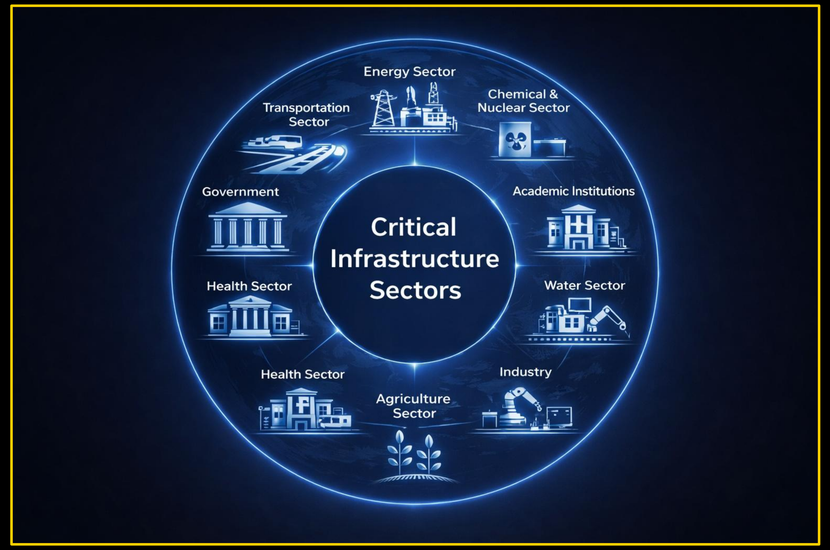
“IGEL IT for OT” with Zero Trust Architecture (ZTA)

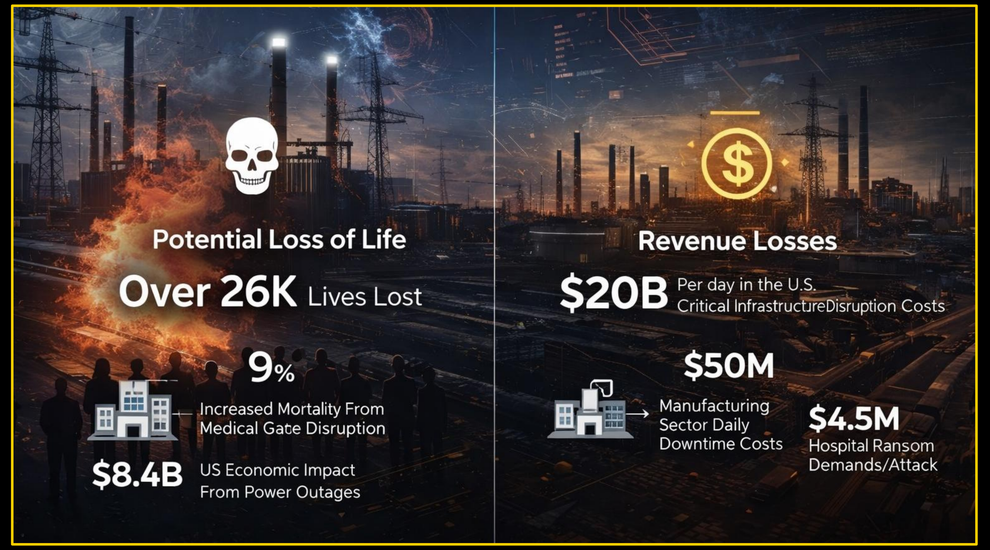
IGEL Preventative Security Model™ for OT/IoT



Threat Shifting to Critical Industries OT

Industrial Risks and Economic Impact





OT Cyber Attacks to Escalate

Geopolitical Environment – Nation State Attacks Now In the Wild & Living Off the Land

- Iran's digital strike offers an early glimpse of how Iran could retaliate against the U.S. as war escalates....
- Nearly one week after attack, Stryker says online ordering remains offline
- Iran targeting water supplies, utilities, and critical Industries
- Salt Typhoon, Volt Typhoon, CyberAve3ngers, Poland Grid, Colonial Pipeline, Shamoon, ...Ransomware
- 89 percent of Orgs Prioritizing Security and 42 Percent reporting incidents impacting operational systems

Source: 2026 – 3-17 Sam Sabin Axios

AI Reducing the Time form Vulnerability Discovery to Exploit

OT Needs to Modernize

Modernize the Edge
Virtualization, Containers, Standard Interfaces

Sustainability &
Green Operations

Compliance,
Control &
Compatibility

Reduce Complexity & Cost
IT / OT Convergence

Security & Resilience
Availability

Organizations Status: 70-90% Strategic Intent; 30-50% Making Real Progress; and Only 10-20% Modernized and Future Ready

Priorities – Availability, Industrial Safety, and Compliance

Secure

- Prevents ransomware reaching critical OT Systems
- Isolates vulnerable ICS/SCADA/HMI endpoints
- Turns legacy OS/computers into hardened, managed devices

Compliance

- Aligns with NIST CSF, IEC 62443, NIS2, TSA SD02
- Minimizes audit risk and potential fines
- Protects operational data and intellectual property (IP)

Safety

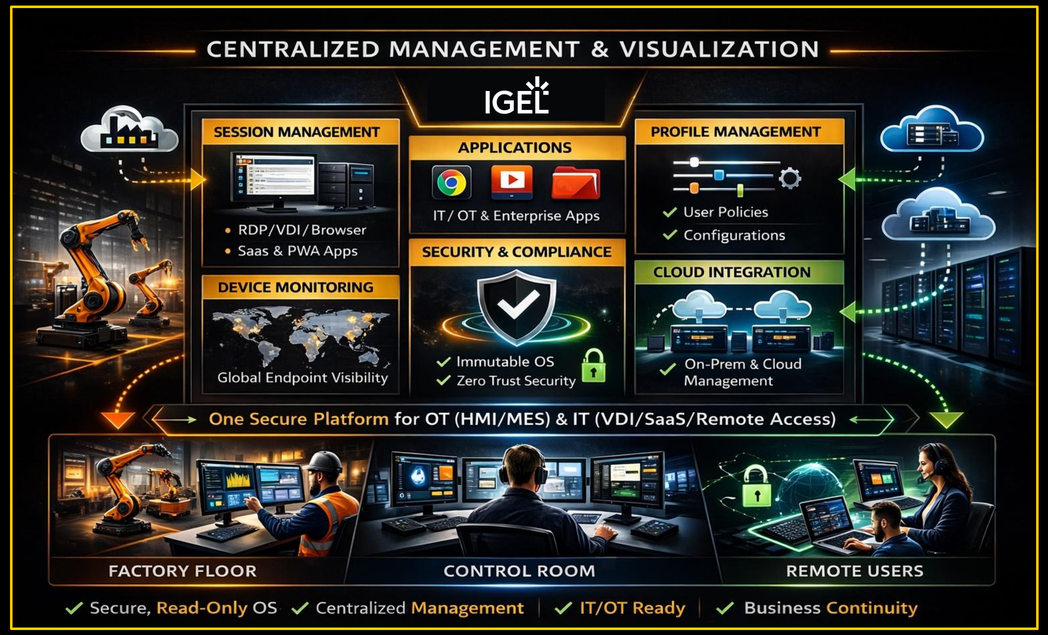
- Protects human operators from harm/disruption
- Prevents unplanned outages endangering staff
- Secures SCADA / HMI no matter their OS

Zero Trust Secures Fragile Industrial Systems

- ✓ Eliminates attack surface (No exploit persistent/DR)
- ✓ Blocks local privilege escalation, fileless malware, untrusted assets
- ✓ Centrally controls policies & versioning via Adaptive Secure Ops

IGEL IT for OT – IGEL Adaptive Secure OT™

- Unified Endpoint Mgmt. & Control
- Secure Workflow Delivery (PSM + TMSE)TM
- Segmentation for IT/OT Convergence
- Centralized Control
- Identity Aware Policy Enforcement and Access Control
- Enhanced Cyber Resilience and Operational Availability
- Reduced TCO through Lifecycle Standardization & Sustainability
- Modernization - Edge Virtualization, Containers, ….
- Regulatory - IEC 62443, Zero Trust 2.0, CSF2, NIS2, SOC2 Compliance



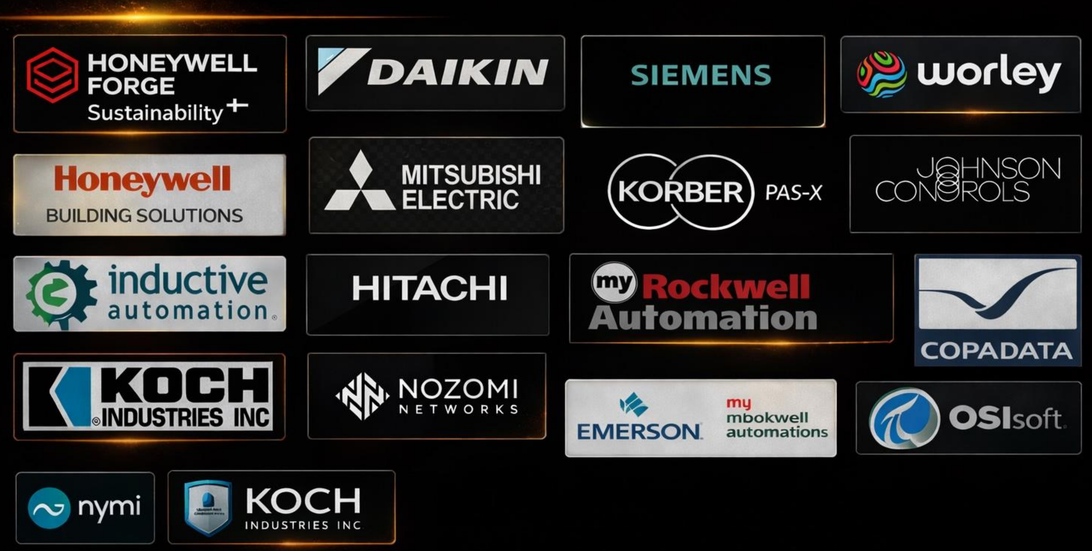
IGEL OT Deployed NOW vs. NEXT

“NOW”

- Focus on eco-system partners integration
- Collaborating customers – VDI, IMH, IMC….IT for OT
  - Business Systems
  - Signage, Inventory, ERP
  - Eng Workstations, Controls, HMI, Virtualized PLC’s control….

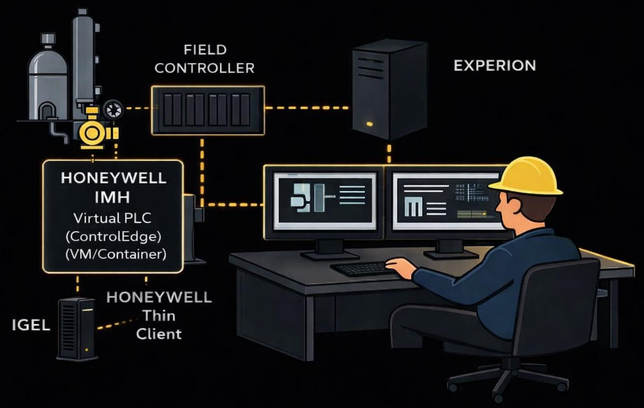
“NEXT”

- Increasing OEM integration
- Enhancing IMH/IMC/IMI - feature capabilities
- OT Eco-system Partners – IGEL Ready
- New Features for OT
- IT for OT: Supporting Open-Source Standards, Linux Margo….



Honeywell

Honeywell Advanced Virtualization and Automation Systems



ENVIRONMENT:

IGEL OS embedded on Honeywell Endpoint; OT Use Case in Oil and Gas Honeywell deploys solutions for Experion® Process Knowledge System (PKS) users through the IGEL Ready Program.

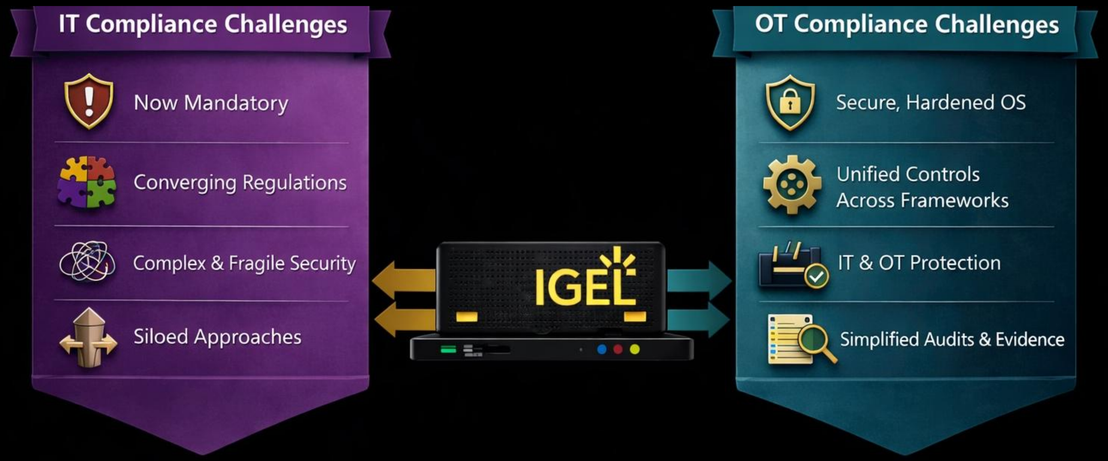
The IGEL Linux-based solution integrated with Honeywell's Universal Thin Client Operating System and Experion PKS provides users access to an ecosystem of cutting-edge hardware and software, delivering a powerful, productive and secure end-user experience.

CUSTOMER TESTIMONIAL:

"The solution provides a secure experience for end-users using virtualization while significantly reducing the challenges traditionally associated with deploying thin client technology. The Universal Thin Client Operating System also allows for much stronger administration and management capabilities, which in turn allows users to save time and labor costs associated with maintaining their control systems."

Summary - Adaptive Secure Endpoint Platform

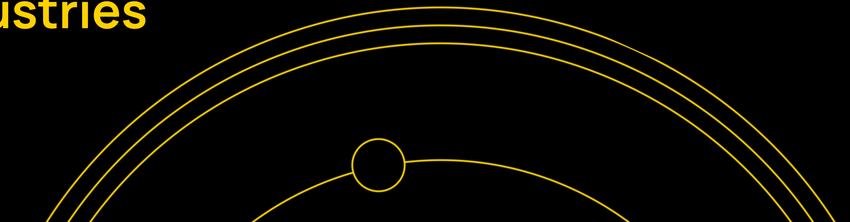
- Risk and Compliance are central criteria for organizations looking to modernize, increase resilience, and reduce TCO
- Especially in OT/edge and regulated contexts
- Customer in regulated environments (e.g., OT, industrial, finance, healthcare) prioritize heavily
- Who Cares: CEO, CISO, CIO, VP/Dir, Sol Architects, Investors.....Auditors, Insurance Companies



Meeting the Challenges to Achieving Resilience

Shift – Security to Resilience

John Walsh, Office of CTO, Field CTO for Gov & Critical Industries



Paul M. Nakasone
Former Commander, U.S. Cyber Command & Former Director of the National Security Agency, Four-Star Army General (Ret.)

Michele Iversen
Fmr. NSA, DOW CIO Office, Chertoff Group principal

Patrick Arvidson
Fmr. NSA
Cyber Resilience

Brian Hennigan
Fmr. DISA
Endpoint Security

Carlos Rivera
Senior Analyst – Zero Trust, Forrester

To Learn More

From Compliance to Confidence:
Building the Preventive Workspace

March 31st | GLIMMER 3 | 3:10pm-3:50pm

Securing the Edge: Why Supply Chain Risk Management is Critical for Endpoint Security

March 31st | GLIMMER 3 | 4:30pm-5:10pm

Successes and 3 Pitfalls in Applying Cyber & ZT to OT

March 31st | GLIMMER 3 | 5:10pm-5:50pm

The Shift to Cyber Resilience in Government and Critical Industries

April 1st | GLIMMER 3 | 12:10pm-12:50pm

IGEL OEM and Enterprise OT Architecture and its' Capabilities/Benefits

April 1st | GLIMMER 3 | 4:10pm-4:50pm

Compliance Across a Multi-Regulatory Environment

March 31st | GLIMMER 3 | 5:00pm-5:40pm

Thank You


IGEL now
&next