

Securing IT and OT Convergence: A Modern Approach to Cybersecurity and Operational Efficiency in Critical Environments

The convergence of Information Technology (IT) and Operational Technology (OT) is reshaping critical environments.

By integrating traditionally siloed IT systems with OT infrastructure, enterprises can unlock new levels of efficiency through automation and data-driven decision-making.

The downside of this is significant cybersecurity, compliance, and operational challenges.

According to a recent study by Dragos, ransomware attacks against industrial organizations are up 87% year over year. In addition to an 87% increase in attacks last year, Dragos saw a 60% jump in ransomware groups targeting OT and ICS, from 50 groups in 2023 to 80 in 2024.

As IT and OT networks merge, and new Cyber Physical Systems (CPS) come online, Chief Information Security Officers require new strategies and resources to safeguard these critical systems. Previously “air-gapped” or isolated OT systems connect to enterprise networks and the cloud, increasing their exposure to cyber threats such as ransomware and impact from IT outages. Additionally, the complexity of managing security policies, ensuring regulatory compliance, and bridging the skills gap between IT and OT teams presents further obstacles.

IGEL Managed Hypervisor; Achieve balance with technology upgrades and system integrity in OT environments.

The IGEL Managed Hypervisor enables seamless integration between outdated operating systems and modern hardware, including strong malware and ransomware protection, system health monitoring, remote troubleshooting, and easy-to-deploy security updates—all without compromising the operational efficiency or uptime, critical in OT environments.

IGEL Managed Hypervisor (IMH) is built on IGEL's secure endpoint operating system and the [Preventative Security Model™](#). Unlike traditional endpoint virtualization solutions, IGEL Managed Hypervisor includes **centralized management** capabilities to offer a robust and secure endpoint virtualization platform.

Preventative Security Model™ establishes trust, isolates, and enables smart login through integration with leading solutions across security and secure access service edge (SASE), identity access management (IAM), and unified endpoint management (UEM). The IGEL Universal Management Suite centrally deploys and manages the hypervisor.

The IGEL Ready program ensures solutions are tested and supported.



IGEL Managed Hypervisor enables enterprises to:

Protect OT Systems, Achieve Compliance

- Isolate legacy operating systems in a secure, virtualized environment, preventing unauthorized exploitation of OS vulnerabilities.
- Integrate seamlessly with network segmentation, firewalls, and Zero Trust architectures to reduce attack surfaces and enforce strict access controls, offering advanced protection against ransomware, malware, and data breaches.
- Streamline compliance and risk management by ensuring security policies align with industry regulations and best practices like HIPAA, NERC CIP, and NIS2.
- Supports sustainable IT strategy to achieve environment, social, and governance (ESG) and efficiency goals.

Operational Continuity, Prevent Disruption


- Enhance operational resilience, centrally manage multiple virtual machines with a secure endpoint virtualization platform designed for preventative security.
- Separate the dependency between operating systems and hardware, enable legacy Windows, Linux, and outdated operating systems in OT networks to run on more reliable, modern hardware, ensuring uninterrupted operations.
- Reduce downtime with rapid recovery options; any Windows endpoint outage can be remotely recovered, re-imaged, or restarted within minutes.
- Extend hardware refresh cycles while ensuring business-critical systems remain operational.
- Support continuity for critical OT systems, even under challenging conditions through remote troubleshooting, secure updates, and high availability.

Reduce Costs through Security and Uptime

- Repurpose existing equipment such as non-Windows 11 compatible hardware to extend the lifespan of legacy systems and delay or phase the purchase of new endpoints and hardware, reducing capital expenditures (CAPEX).
- Reduce hardware costs and e-waste disposal by using older hardware for a longer time.
- Utilize energy-efficient modern processors that decrease energy consumption and improve application performance.
- Centralized management and a Preventative Security Model™ reduce operational expenditures (OPEX) related to IT overhead, security patching, and endpoint support.

Challenges faced by OT today and how IGEL Managed Hypervisor can help

Challenge	Legacy OS and Hardware	IGEL Managed Hypervisor (IMH)
Existing solutions do not provide centralized management capabilities	Existing endpoint hypervisor solutions are intended for single device support. They lack the centralized management capabilities to troubleshoot and update, integrations with security, networking, and management solutions.	IGEL enhances operational resilience with a centrally managed, secure endpoint virtualization platform designed for preventative security. With IGEL, admins can shadow, troubleshoot and restart distributed virtual machines.
Business Continuity is complex, time and resource intensive	Legacy systems running outdated Windows XP or Windows 7, are particularly vulnerable to cyber threats and often lack the redundancy and recovery mechanisms necessary to maintain continuity. When these systems are impacted, recovery is hindered by the time and hands-on effort required to restore operations.	IGEL Managed Hypervisor virtualizes legacy systems and centrally manages remote troubleshooting, remote boot of services., real-time monitoring of recovery efforts. Implement Zero Trust architectures and network segmentation to minimize the impact of security breaches and contain potential threats.
Complex Multi-OS Management	Managing multiple operating systems on a single machine traditionally requires either separate hardware or frequent reboots.	IGEL Managed Hypervisor enables you to run multiple operating systems in tandem on a single machine, streamlining operations and reducing hardware needs
Complex development and testing environments	Developers and QA engineers use up valuable time creating and maintaining diverse, isolated environments.	IGEL Managed Hypervisor provides isolated, customizable virtual environments to facilitate efficient development and testing.
Security Vulnerabilities in Legacy Windows running OT Controller Hardware	Existing endpoint hypervisor solutions are intended for single device support. They lack the centralized management capabilities to troubleshoot and update, integrations with security, networking, and management solutions.	IGEL enhances operational resilience with a centrally managed, secure endpoint virtualization platform designed for preventative security. With IGEL, admins can shadow, troubleshoot and restart distributed virtual machines.
Modern Hardware Lacks Support for Legacy Windows Versions	Older Windows operating systems, such as Windows XP or Windows 7, are no longer supported by Microsoft. This means they no longer receive critical security patches, leaving them highly vulnerable to cyberattacks, such as ransomware or malware specifically targeting outdated systems.	Isolate legacy operating systems in a secure, virtualized environment, preventing unauthorized exploitation of OS vulnerabilities.
Reduced Efficiency and Functionality	The older hardware required to run legacy Windows operating systems is significantly slower than modern endpoints, severely impacting controller software's efficiency and the overall performance of OT environments	IGEL's Managed Hypervisor supports continuity for critical OT systems, even under challenging conditions through remote troubleshooting, secure updates, and high availability.
Compatibility and Integration Difficulties	Older endpoint hardware often lack compatibility with modern protocols, security features like secure boot and encryption, and networking capabilities, causing security vulnerabilities and performance bottlenecks. This makes it difficult to integrate these systems into modern, data-driven industrial environments.	IGEL Managed Hypervisor provides a robust platform for reliable virtual appliance delivery, offering integrations across network segmentation, firewalls, and Zero Trust architectures to reduce attack surfaces and enforce strict access controls, offering advanced protection against ransomware, malware, and data breaches
Operational Downtime	Older endpoint hardware may be more prone to breakdowns or errors, leading to unplanned downtime that disrupts operations.	Reduce downtime with rapid recovery options; any Windows endpoint outage can be remotely recovered, re-imaged, or restarted within minutes.
Regulatory Compliance	Older hardware often lacks features such as Trusted Platform Modules (TPMs) or encrypted storage, which are required to meet modern compliance standards. This can result in fines, penalties, or operational restrictions.	Achieve compliance and risk management with IGEL Managed Hypervisor by ensuring security policies align with industry regulations and best practices like HIPAA, NERC CIP, and NIS2.

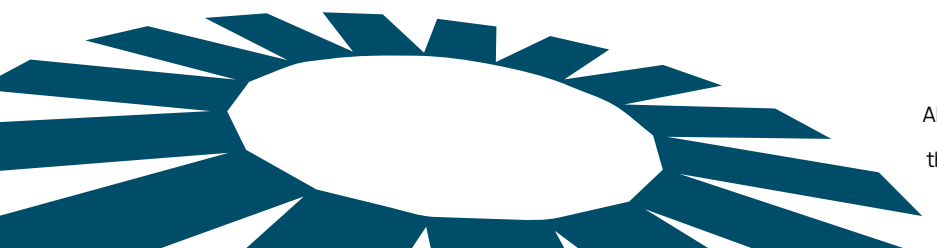


Navigating these challenges requires a secure, scalable, and efficient approach.

The IGEL Managed Hypervisor enables seamless integration between outdated operating systems and modern hardware, including strong malware and ransomware protection, system health monitoring, remote troubleshooting, and easy-to-deploy security updates—all without compromising the operational efficiency or uptime critical to OT environments.

For organizations in critical infrastructure and OT, cost efficiency cannot come at the expense of security, uptime, or regulatory compliance. IGEL enhances operational resilience with a centrally managed, secure endpoint virtualization platform designed for preventative security. By adopting a modern IT/OT security strategy with IGEL, enterprises can safeguard their critical operations while leveraging the full potential of Industry 4.0 innovations.

Request a demo on igel.com/secure-managed-hypervisor/



IGEL is a registered trademark of IGEL Technology GmbH.
All hardware and software names are registered trademarks of
the respective manufacturers. Errors and omissions excepted.
Subject to change without notice. © 07/2025