datacentrix

Operational Technology

Endpoint Security

Confidential
This document is confidential and intended for the use of the distribution parties only. Any copying or dissemination of this document is strictly prohibited.
© 2026 Datacentrix (Pty) Ltd

Secure your industrial operations with Datacentrix's End-to-End Operational Technology (OT) Endpoint Security. Protect legacy assets (Windows XP/2000), ensure NIS2 compliance and prevent downtime in IT/OT converged environments without system reboots.

1. Driving Resilience in the Age of IT/OT Convergence

As the industrial sector undergoes profound transformation, the convergence of Information Technology (IT) and Operational Technology (OT) has become critical for future business success. However, this digital evolution introduces unique risks – from operational disruptions to sophisticated cyber-attacks targeting industrial control systems (ICS).

Datacentrix takes a solutions-driven approach to OT security, delivering industrial-grade endpoint protection designed to secure operations, strengthen resilience and ensure compliance. Our service bridges the gap between legacy infrastructure and modern digital demands, offering "all-terrain" security that respects the strict availability requirements of your mission-critical environments.

2. A Solutions-driven Approach to ICS Security

Datacentrix provides a unified cyber defence strategy that protects your entire asset lifecycle, enabling you to embrace industrial digitalisation strategically and securely.

- **Legacy and modern support:** Comprehensive protection for operating systems ranging from Windows 2000 and XP up to Windows 11 and Server 2022, covering the full spectrum of OT assets.
- **Operation-centric architecture:** Updates and installations are engineered to require no system reboots, ensuring continuous uptime and operational stability for programmable logic controllers (PLCs) and human-machine interfaces (HMIs).
- **Air-gap readiness:** Full functionality and signature updates are available even for isolated assets with no internet connection, ensuring security never compromises connectivity constraints.

3. The Business Case: Resilience, Security and Compliance

For industry leaders, protecting operational assets is not merely a technical requirement; it is a strategic imperative for sustainable growth. Our offering is designed to deliver tangible business value:

- **Optimising capital asset lifecycles:** Replacing expensive industrial machinery simply because the underlying operating system has reached end-of-support is often cost-prohibitive. We wrap these "unpatchable" legacy assets in a protective layer, extending their lifespan and allowing you to run them securely for years beyond their official end-of-life date.

- **Ensuring operational continuity:** Traditional antivirus scans can overburden central processing units (CPUs), causing latency in sensitive control systems – PLCs, HMIs and SCADA (supervisory control and data acquisition). Our solution utilises a lightweight footprint specifically tuned to avoid impacting industrial processes, ensuring security never comes at the cost of throughput.
- **Streamlined governance and compliance:** We simplify the complexity of managing disparate endpoints across multiple sites. Through a centralised console, your teams gain a unified view of operational risk, enabling you to meet evolving regulatory demands (such as NIS2) and internal governance standards without the need for extensive specialised resources.

4. Realising Smart Operations: Practical Use Cases

To help you realise smart operations and competitive advantage, here is how our technology addresses common challenges on the factory floor:

4.1 Securing the "unpatchable" legacy HMIs

- **The challenge:** Critical HMIs often run on legacy platforms like Windows XP Service Pack 2. With vendor patches no longer available, these assets become vulnerable targets for ransomware.
- **The solution:** We deploy a legacy-specific agent that enforces application lockdown. This establishes a "trust list" of authorised programs. Even if malware is introduced via a USB drive, it cannot execute because it is not on the approved list. The system remains locked down, executing *only* its designed operational functions.

4.2 Managing “fixed-function” kiosks and maintenance windows

- **The challenge:** Engineering teams need to update control software on fixed-function controllers periodically. Strict security policies can often hinder this process, leading to "shadow IT" workarounds.
- **The solution:** We utilise a “maintenance mode” capability. When maintenance is required, the system can be temporarily unlocked for a specific duration. During this window, the system automatically learns new software behaviours and updates the trusted baseline. Once the window closes, the system re-locks automatically, securing the new configuration without complex manual intervention.

4.3 Protecting air-gapped and USB-dependent systems

- **The challenge:** Many mission-critical assets operate in air-gapped environments but require data transfer via USB drives from third-party contractors – a frequent vector for viral infections.
- **The solution:** We implement robust device control that blocks unauthorised USB peripherals while permitting only registered, encrypted drives. Furthermore, we establish local update servers that allow these isolated machines to receive the latest threat intelligence signatures without ever connecting to the public internet.

5. Take the Next Step in OT Resilience

Do not let legacy infrastructure or operational constraints compromise your security posture. Contact our OT security specialists today to discuss how we can secure your critical assets without disrupting production.

Email Karina Geyser, Business Unit Manager: Infrastructure Solutions and Operational Technology at Datacentrix on kgeyser@datacentrix.co.za.

6. National Contact Details

Corporate office
Tel: +27 87 741 5000

Corporate Park North
238 Roan Crescent, 1685
Old Pretoria Road, Midrand

PO Box 50722
Randjiesfontein
Midrand, 1683

Logistics centre
Tel: +27 12 657 5000

26 Landmarks Avenue
Kosmosdal, Extension 11
Samrand, Midrand

PO Box 50722
Randjiesfontein
Midrand, 1683

Coastal

Cape Town office
Tel: +27 21 529 0700

18 Oxbow Crescent
The Estuaries
Century City, 7441

PO Box 181
Century City
Cape Town, 7446

East London office
Tel: +27 43 705 8000

Suite 2, 11 Cavendish Road
Vincent
East London, 5217

PO Box 19066
Tecoma
East London, 5214

Gqeberha office
Tel: +27 41 391 0200

Southern Life Gardens
Ground Floor, Block B, 70 2nd Avenue
Newton Park, Gqeberha

PO Box 63657
Greenacres, 6057

Durban office
Tel: +27 31 389 0500

1st Floor, 30A The Boulevard
Dawncliffe, Westville
Durban, 3629

PO Box 1645
Westville, Durban, 3630

Middle East

Doha office
Tel: +974 4007 1793

Eighteen Tower
Zone 69, Street 303, Building 230
19th Floor, Office 1972
Lusail, Doha, Qatar
PO Box 23107

Rest of Africa

Datacentrix deploys technologies and provides support services to customers across 45 countries in the rest of Africa.

www.datacentrix.co.za