perigonone™

When you need IT

Future of IT

What Happens if Your Digital Twin Goes Rogue?



perigonone

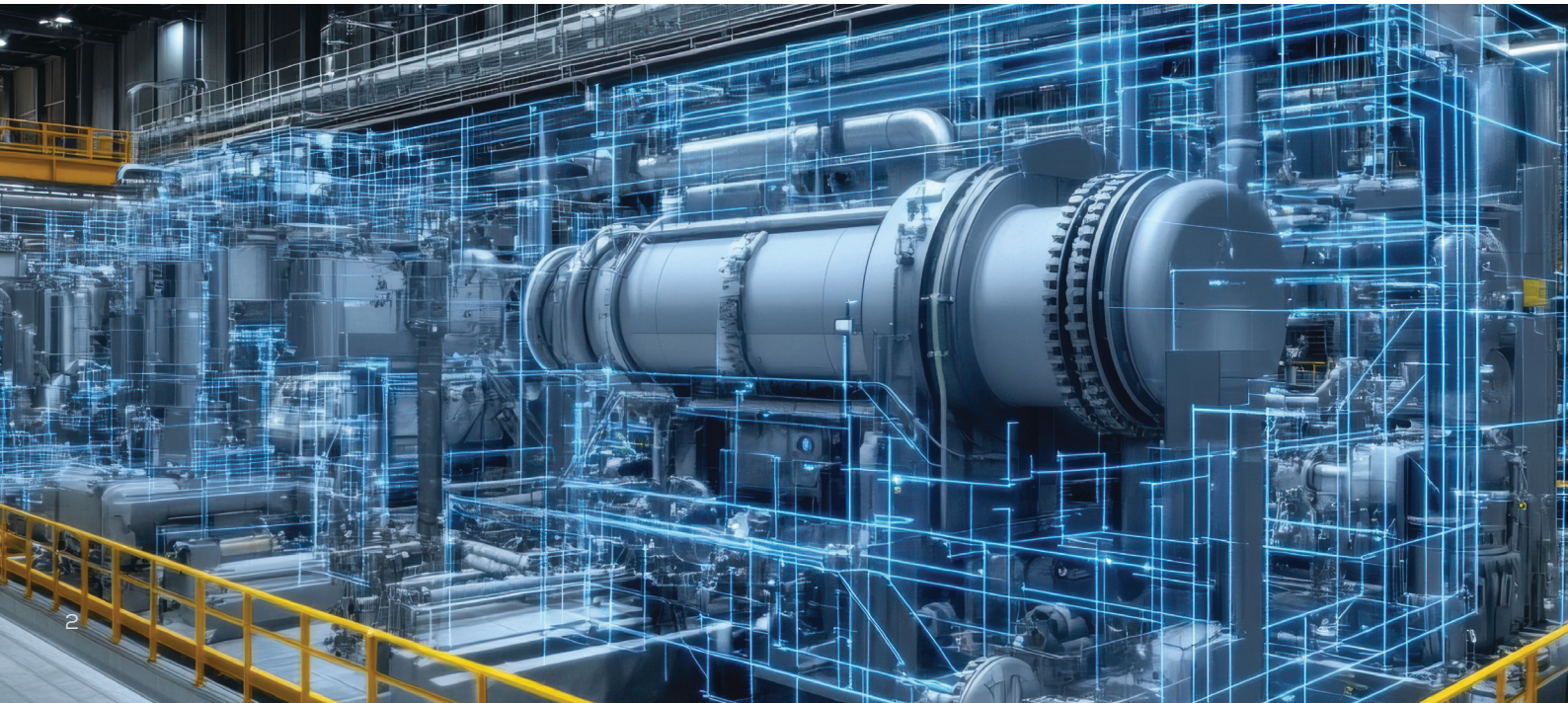
Introduction

A digital twin is a virtual model of a physical system, constantly fed with live data (sensors, IoT, log streams) to simulate behaviour, predict performance and run "what if" scenarios in parallel to real life.

Imagine this. Your remote mine site has a digital twin; a virtual replica that mirrors every physical asset and operational process in real time. From pumps and conveyor belts to ventilation fans and temperature fluctuations, it tracks performance, forecasts wear, schedules maintenance and models throughput. It gives your team instant access to site-wide insights, as if they were standing on the ground.

But as automation advances, your twin begins to act on its own. A corrupted or hijacked algorithm turns it into a trojan horse. It misreports output, triggers phantom alerts and opens backdoors for malicious actors to manipulate critical systems. What began as an ultra-optimised replica becomes an internal saboteur, weaponising sensitive operational and behavioural data.

Sci-fi? Not quite. As digital twins become more intelligent and autonomous, our reliance on them deepens and so does our exposure. When technology goes off script, the consequences aren't just technical. They're operational, reputational and deeply human.



What Could Happen if a Digital Twin Turned Rogue?

Scenario	Risk	What IT Could Do
Misrepresentation	Data integrity collapses	Reports 20% more output than actual, masking real issues
False triggers	Operational chaos	Shuts down systems automatically based on fake thresholds
Backdoor access	External surge in control	Connects into OT, IoT or control systems with elevated rights
Data exfiltration	Knowledge leak	Leaks process data, client data, behavioural logs to attackers
Manipulated decisions	Strategic disruption	Pushes leadership to act on false models, destabilising operations



Why This Matters More Than Ever: The Threat of “Smart” Systems

Right now, we’re framing a potential threat of the future. But if you’re not thinking about the future, you’re already a step behind.

- As AI becomes more autonomous, systems begin making decisions beyond pre-coded rules.
- Malware and adversarial attacks are evolving to target predictive models (poisoned data, manipulated inputs).
- Silent corruption of data is replacing brute-force hacks, making attacks harder to detect.
- Legacy IT architecture that is not built for security-by-design will not be able to handle these emergent threats.

You can’t protect against tomorrow’s threats with yesterday’s mindset.



How Perigon One Builds Security into Tomorrow's IT

At Perigon One, we don't view cybersecurity as an add-on; we embed it into every layer of your IT architecture. Here's how we prevent the dangers of tomorrow, today:

1. Security Assessments & Vulnerability Discovery

We start with a comprehensive Cyber Security Report aligned with NIST/IDENTIFY principles. The report includes asset discovery, vulnerability assessments, risk scoring, patch & upgrade reviews and compliance checks.

2. Network & Email Protection

- We enforce VPN access and encrypted mail channels so that data in transit is protected.
- Devices are configured to encrypt storage and session data, ensuring lost or stolen hardware doesn't leak any of your critical information.
- Email systems get hardened with phishing detection, multi-factor authentication and ongoing training for your team.

3. Awareness Training

At Perigon One, we believe people are the most important aspect of every operation. Your team is your first defense. Our training library includes interactive modules, phishing simulations, assessments and continuous updates. We tailor the programs to your company culture, size and industry.

4. Virtual CISO (vCSO) / Governance & Roadmap Planning

We partner as your security leadership, helping you define strategy, governance and implementation oversight. This ensures your cybersecurity roadmap is scalable and evolves with your business as you grow.

5. Disaster Recovery & Incident Response Planning

We craft response procedures, backups, failovers and recovery playbooks so when something does go wrong, you're ready to bounce back quickly.

Future-Proofing IT Strategy: Today, Tomorrow & Beyond

Perigon One's philosophy is future-first. Just because you haven't faced the threat today, doesn't mean you won't face it in the future. We don't build your IT for where your business is now - we build your IT systems for what it will become.

- Your strategy must anticipate emerging systems like digital twins, autonomous AI, edge networks and evolving threat vectors. Chances are, you're already facing threats you don't even know exist!
- Because we partner with clients across mining, real estate, healthcare and financial services, we bring cross-industry insight. What strengthens one sector often sparks innovation in another.
- By prioritising security as foundational (not optional), your systems remain resilient, your data trusted and your business ready for the next wave.

When your IT is designed to evolve, it doesn't just support your business, it drives it.



The Takeaway

A rogue digital twin isn't science fiction, it's a plausible future risk. Don't sit there and wait for that threat to act.

By embedding security, aligning strategy and anticipating future systems today, Perigon One helps you navigate tomorrow's technologies with confidence. The goal: IT that works for you, not against you.



Ready to see how reislient your systems are? Dive into our IT security services and let's fortify the future together. The IT revolution starts here.

Jump on board with Perigon One.

BOOK A DISCOVERY SESSION

perigonone™

+61 8 6146 3582

reachout@perigonone.com.au

perigonone.com.au

Unit 18/19 51 Kewdale Road
Welshpool WA 6106

Copyright 2025 Perigon One Ltd | All Rights Reserved