

WHITE PAPER



FAIL-SAFE MODERNISATION:

HOW **ALCHEMY** SHIELDS
MANUFACTURING
FROM HIDDEN LEGACY THREATS

Cloudhouse Technologies Limited

📍 1 Ariel Way, London, W12 7SL

☎ +44 (0) 203 51 51 505

🌐 www.cloudhouse.com

Executive Summary

In manufacturing, legacy systems are often the backbone of operations. The applications teams use every day are reliable, familiar and deeply integrated into workflows. They are still doing the job and doing it well.

But running them on outdated operating systems poses serious risks. When it comes to modernising infrastructure, these trusted tools can become incompatible or unsupported, leading to disruption, retraining or costly redevelopment.

In particular, legacy operating systems (OSs) and app vulnerabilities can result in complete line shutdowns or security breaches — risks no manufacturing board can afford to ignore.

In February 2025, a global study found that **80%** of manufacturing companies “experienced a significant increase in overall cybersecurity incidents or breaches last year”. Clearly, not securing these applications could lead to major financial, reputational and operational damage, especially in light of the recent high-profile attacks on several retailers.



However, the motives behind legacy application modernisation can be misguided. Organisations can often view the process as a cost-saving or compliance-led activity rather than a critical business continuity decision. This is what this white paper sets out to reframe.

True modernisation is not a one-time event: it's an ongoing process. As such, manufacturers should see their modernisation projects as one large step in an ongoing journey of digital transformation.

Cloudhouse Alchemy provides a cost-effective, vendor-neutral solution with no code or application changes. It enables critical legacy applications to remain secure and functional on modern platforms with minimal disruption to live environments. This ensures operational continuity, compliance and, crucially, reduces risks.



Unmanaged legacy risks: A ticking time bomb in manufacturing

Legacy applications – often running on unsupported operating systems – still underpin key functions in many factories. These aren't just back-office apps; they're tightly integrated into production lines, logistics and control systems.

Imagine: a 20-year-old calibration tool goes offline due to a **Windows 11 upgrade attempt** – no compatible version exists, halting quality assurance processes for days. This could cause **line stoppages, missed deliveries and operational chaos for this period.**

When a legacy control app fails or is compromised, the cost is not IT overhead – it's idle lines, missed orders and tarnished trust. It's why vulnerabilities in legacy systems aren't just an IT issue: they are a **risk to production, IP and reputation.**



Risk to production

Legacy systems are often embedded in the core of manufacturing operations. Think control systems, calibration tools, scheduling apps, and so on. Any failure in these systems can lead to several risks, including:

- check or registry misconfiguration, can stop production.

- **Downtime exposure:**

Unpatched systems are vulnerable to ransomware or failure. If a critical app fails, entire production lines may grind to a halt.

- **No hot-swap capability:** Many legacy apps are so tightly coupled with their environment that there's no quick way to restore service.

- **Dependency chain failure:** Hidden dependencies (see later section) mean that even indirect failures, like a license check or registry misconfiguration, can stop production.



Risk to IP

The legacy systems that manufacturers rely on handle a whole range of sensitive data, from source code and product formulas to design specs and machine configurations. These systems are prime targets for attackers precisely because they are unprotected.

- **Weak security posture:** Legacy apps often lack encryption, have limited access control or minimal audit logging.
- **Easy targets:** Attackers look for legacy OSs known to be exploitable (e.g., EternalBlue for Windows Server 2003).
- **IP leakage risk:** Compromised legacy systems can expose proprietary product designs or operational processes to competitors or bad actors.



Risk to reputation

Even if production and IP are unaffected, a breach or failure can severely impact customer confidence, regulatory trust and market standing.

- **Customer trust erosion:** Customers expect reliability and data protection – a visible failure or breach undermines credibility.
- **Regulatory scrutiny:** Many sectors like pharma or automotive have strict compliance mandates. Operating unsupported software can trigger fines or lost certifications.
- **Media fallout:** A cyberattack traced back to a legacy app makes headlines — and the brand damage can far outlast the incident that took place.



The cost of doing nothing

Modernisation projects have often been positioned as a cost-saving or compliance-driven initiative — nice to have, but easy to defer. Yet, quite simply, the cost of doing nothing is far more than an IT 'inconvenience'.



From crippling **downtime costs** to the **severe cybercrime risks** that emerge from unsupported systems, the industry numbers paint a vivid picture.

- **Downtime costs:** Downtime costs can vary significantly, but manufacturers can face losing on average \$22,000 (£17,000) per minute when the production line stops. Every unplanned outage will far outweigh the costs of investing in modernisation.
- **Cyber risk exposure:** According to the 2024 IBM Cost of a Data Breach (CODB) report, the average total cost of a data breach in the industrial sector was \$5.56 million. Given many industrial control systems run on outdated OSs, with no path to vendor support or patching, this threat is very real.
- **Insurance & compliance impacts:** Companies may face higher premiums — or even be denied coverage — if critical systems remain on unsupported platforms.
- **Opportunity cost:** Every hour spent firefighting legacy issues is an hour not spent innovating or scaling production.



Yet these legacy apps are still critical to operations. **Downtime is not an option.** So, while the cost of doing nothing is significant, the wrong modernisation project can also cause notable disruption by not accounting for the hidden dependencies of these applications.

Hidden dependencies traditional containerisation or virtualisation can't address

Legacy applications often rely on a complex web of underlying components. These can be specific dynamic link libraries, registry settings, component object model objects, hardcoded file paths, or legacy system drivers — components that were never designed to be portable.

These dependencies are typically tightly coupled to the original OS and hardware environment. As such, they make legacy apps notoriously difficult to modernise with conventional tools like traditional containerisation (e.g., Docker) or virtualisation (e.g., VMware, Hyper-V).



Why both fall short for legacy systems

Both containerisation and virtualisation assume a clean, modular architecture – and they work well for modern apps built with portability in mind. But while they help in moving away from physical infrastructure, neither solves the real problem for manufacturers using legacy apps.

Essentially, they don't reduce risk — they just move the old environment into a new wrapper. This is because they struggle when faced with:

- **Hardcoded, OS-specific dependencies** (e.g., apps that only run on Windows XP)
- **Custom integrations with legacy industrial systems** that don't expose APIs or standard interfaces
- **Software components** that rely on outdated system functions
- **Interdependent services** that break when separated or moved to new environments

As a result, containerising or virtualising legacy apps can lead to partial functionality, instability, or outright failure, especially in complex manufacturing environments where uptime is critical.

That's where **Alchemy** offers an **alternative**: it isolates and intercepts those legacy dependencies while redirecting data flows so apps can run unchanged in modern, supported environments — without requiring containers or virtual machines at all.





Alchemy in action

Traditional modernisation methods assume the app and its dependencies are modular, replaceable, and OS-agnostic — but legacy apps aren't.

The use of software like **Alchemy by Cloudhouse** addresses this gap by capturing and packaging not just the application, but all of its environment-specific dependencies. It preserves the exact behaviour of the original system while allowing it to run securely on modern infrastructure, all without extensively rewriting or refactoring the code.

Testing the rigs of an automotive company



We worked with an automotive company that faced a tough decision: its critical component testing rigs were connected to **Windows XP machines** running **16-bit testing applications**. These rigs were worth millions and still essential to their processes – but the software couldn't run on modern Windows systems.

Did the company need to replace the rigs? Rebuild the applications?
Or was there another way?

Rather than replace the rigs or rebuild the applications, they decided to use Alchemy. Cloudhouse packaged the apps from their **XP environment** and redeployed them on **the latest Windows desktops**, preserving both their investment and their testing capability.



Enhancing operational flexibility

The customer was also dealing with the limitations of being tied to specific **Windows XP machines** due to a lack of knowledge of the application and missing install media. Specifically, they had an application that was only installed on a single machine.

With Cloudhouse's packaging solution, this application could now be deployed using standard Windows deployment software like Intune across all machines in the room, including laptops. This meant that multiple operators could use the software simultaneously, significantly enhancing operational flexibility and efficiency.

And by having increased accessibility, employees could now work from different locations and devices, ensuring that the necessary tools were always available when needed.



Reframing modernisation: From optional upgrade to business continuity imperative

Legacy applications are critical to manufacturers and their operations. But the risks of running them on unsupported OSs means the cost of doing nothing and not modernising systems is a ticking time bomb.

With these risks crossing into operational, financial and reputational domains, this is now a C-suite priority. Modernisation has to be positioned as a business continuity imperative, not just a cost-saving, compliance-driven initiative. But with so many hidden dependencies, these legacy apps need to be modernised while keeping them running and secure.

Alchemy by Cloudhouse empowers manufacturers to upgrade their infrastructure without replacing what still works. By redeploying existing applications onto modern OSs without the need for containerisation, virtualisation or code changes, manufacturers can keep vital operations ticking over while, crucially, securing their systems.

Modernisation is no longer about chasing the latest tech — it's about defending what matters most: uptime, security and customer trust.

Alchemy offers manufacturers a fail-safe path to securing legacy systems without disruption. The stakes are too high to delay.

Contact us today to explore how Alchemy can help your company manage hidden legacy threats securely, efficiently, and affordably.

