



NewRedo

Full Strength Security, Zero Frustration

The Clear Guide to Compliant IT for Normal Humans

Table of Contents

Table of Contents	1
Executive Summary	2
The Hidden Cost of Outdated IT	2
The Solution: A Unified Control Hub	2
Why This Matters to the Board	3
1. Fostering a Productive and Secure Workplace	3
2. Streamlined Business Expansion and Acquisitions	3
3. Enhanced Compliance and Streamlined Audits	4
4. Flexibility and Future-Proofing	4
Implementing Change Seamlessly	4
Next Steps	4
Contact Details	5

Executive Summary

Technology should be a mostly invisible driver of company progress. Today, businesses can choose from a wide range of software tools and services, but this flexibility often leads to a fragmented array of tools, each demanding separate login credentials. *This daily frustration for employees hampers operational growth and introduces avoidable security vulnerabilities.*

This guide explains how an Open Directory platform, such as JumpCloud, solves this issue through cross platform authentication and synchronisation. It guarantees that every employee needs only a single user ID, while simultaneously upholding robust, industry-standard security without needless complexity. It works by securing users, data, and their devices, across hardware platforms and operating systems (including Windows, Mac, Linux, or mobile), from a unified, secure location. Businesses can enhance security, streamline acquisitions, and cultivate a smoother working environment for their staff.

The Hidden Cost of Outdated IT

Work has fundamentally changed. The traditional model of corporate IT, centered on the physical office, desktop computers, and local servers, no longer fits today's reality. Modern teams operate from offices, homes and client sites, and depend heavily on multiple web applications.

This reliance on outdated, office-centric technology to manage a modern, distributed workforce leads to significant operational problems. Employees can struggle with multiple login prompts and password resets, leading to frustration and a loss of productivity. Simultaneously, IT teams are bogged down with repetitive administrative tasks, diverting their focus from more valuable work.

Crucially, the use of disconnected systems especially across a mix of Windows, Mac, Linux and mobile devices undermines security, making it extremely difficult to guarantee the safety of company data.

The Solution: A Unified Control Hub

The growing complexity of IT requires a shift from merely layering on more security software to simplifying the underlying foundations of IT management. This modern solution in the technology industry is called an Open Directory Platform.

Essentially, this platform functions as a single, secure control hub for the entire business. It unifies the management of laptops, software applications, and office Wi-Fi, within a single system.

Crucially, an Open Directory Platform makes everyday work simpler for staff by providing every employee with one secure user ID and password. This single login grants access to workstations, cloud systems, and legacy business applications, eliminating the need for employees to manage countless passwords or overcome unnecessary technical hurdles.



Why This Matters to the Board

Adopting a unified platform is more than a simple IT upgrade; it is a strategic business decision that delivers several important benefits.

A Productive and Secure Workplace

A unified system can significantly streamline the employee experience, starting with an easier onboarding process. New hires can receive a laptop that is pre-configured and ready to go. On

their first day, a single sign-in provides immediate, secure access to all necessary tools, files, and systems.

By dramatically reducing common technology disruptions like forgotten passwords or locked accounts, staff can remain focused on their core responsibilities.

And because the system offers native support for Apple, Windows, and Linux, employees can use their preferred equipment without compromising essential security standards.

Streamlined Business Expansion and Acquisitions

Growing a company through acquisition often creates significant operational friction, particularly when integrating newly acquired entities. These companies frequently operate with a patchwork of disparate systems, including various email platforms, outdated network infrastructure and inconsistent security protocols.

An Open Directory platform offers a cohesive, unifying answer to this growing problem.. Instead of needing an immediate, disruptive overhaul of technology, the platform allows existing systems to connect securely to a central management environment. This delivers instant visibility and control to leadership teams and facilitates collaboration and coherence between staff from both organisations. The process of achieving long-term technical alignment can be managed incrementally, with significantly less disruption to ongoing daily operations.

Enhanced Compliance and Streamlined Audits

For businesses in regulated industries or those serving major enterprise clients, demonstrating robust security compliance is non-negotiable. Fragmented IT systems turn the preparation of evidence for standards like GDPR or ISO 27001 into a slow, manual chore.

By contrast, a centralised platform ensures audit readiness by automatically logging all login activity and monitoring the security posture of all company devices. If auditors ask for data on system access or device encryption, the platform can generate accurate, trustworthy reports both quickly and efficiently.

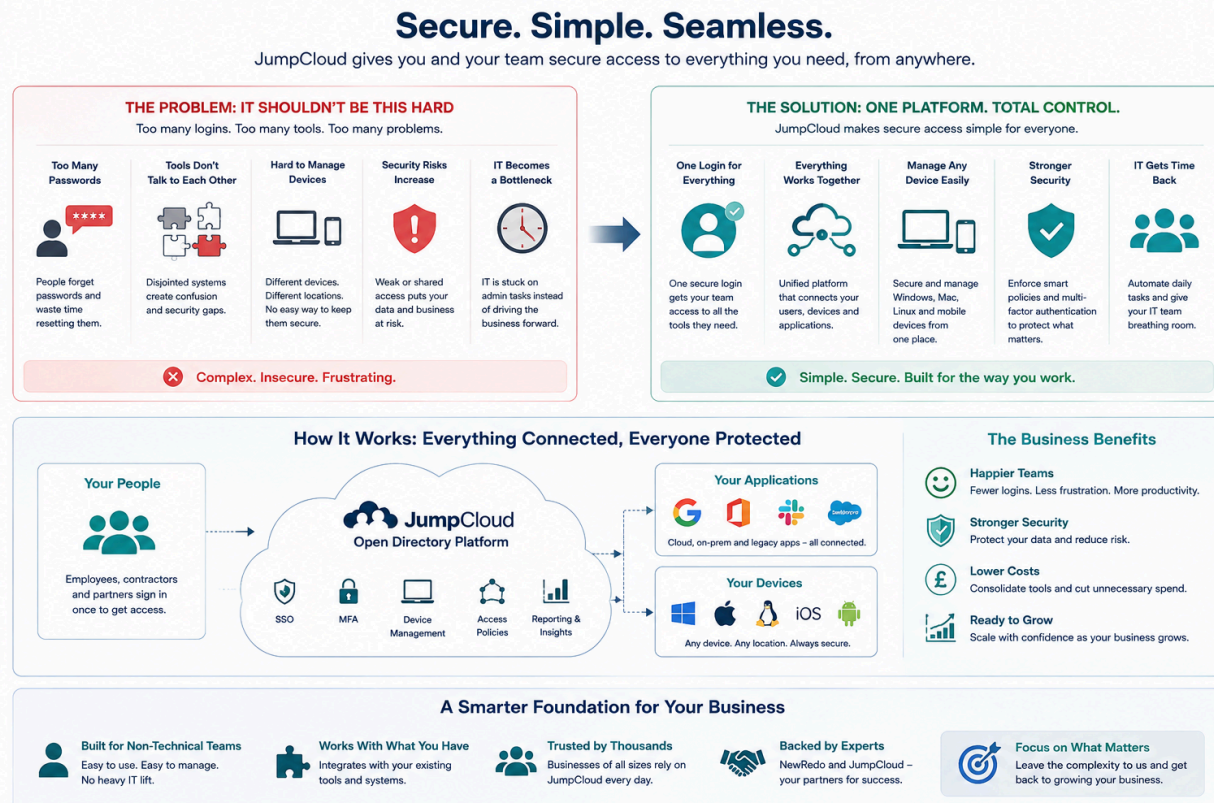
Flexibility and Future-Proofing

Businesses limit their future options by becoming overly dependent on a single technology vendor. Adopting an independent platform like JumpCloud mitigates this risk by reducing reliance on one specific ecosystem.

True cross-platform capability allows businesses to maintain the flexibility to integrate new tools and devices as markets, technologies, and regulations change, unconstrained by prior technology choices.

Implementing Change Seamlessly

While it's easy to recognise the need for change, achieving it without interrupting day-to-day operations calls for both expertise and meticulous preparation.



A successful migration process involves a three-step strategy. First, a thorough assessment of the existing infrastructure; second, developing a workable transition plan; and third, testing this approach with small, controlled pilot groups before a larger rollout. This methodology is crucial for verifying system functionality and drastically reducing operational downtime.

By employing careful planning, effective communication and a systematic phased deployment, businesses can ensure continuity and deliver predictable, low-risk project outcomes.

Next Steps

Businesses do not need to become technology experts to provide staff with a secure, modern, and frictionless working environment. A practical identity and device management assessment can help simplify technology operations, strengthen security, and support future growth.

Does this sound like something you're interested in?

Contact Details

Make contact with our expert team to discuss your challenges and explore how we could help with no obligation or timeline expectations and kick-start our collaborative partnership.

James Mitchell

E: james.mitchell@newredo.com

M: 07973735228

Jonathan Trepczyk

E: jonathan.trepczyk@newredo.com

M: 07841700058