

SecureDoc OS Lifecycle Management

Technology trust is a good thing, but control is a better one.

Stephane Nappo, Chief Information Officer at IBFS

| Continuous Device and OS Lifecycle Management Causing Chaos

It's been said that companies that adopt change quickly remain more secure, profitable, and competitive. However, managing the lifecycle of devices and operating systems can become a nuisance, particularly in large businesses. For many businesses, existing processes are highly inefficient. Often, they are a cobbled mix of department-driven policies, dated tools, manually intense, lacking in consistent coordination, and are heavily reliant on end-users. User downtime is of immense concern to businesses. Where once "maintenance windows" could be considered a reasonable need in IT, there is no longer time for system downtime. Businesses are reliant on their systems and data being available around the clock.

These challenges result in some of the biggest and most expensive pain points a company goes through: downtime, wasted resource efforts, cost overruns, and significant data security issues, including loss of data, breach, and even compliance failure.

| Data in Movement is Data in Jeopardy

How frequently does your company complete application or OS migrations? Device deployment, updates, or maintenance? Data security has become an increasingly large issue over the past number of years in the IT field, especially given the number of high-profile data breaches that have been reported. Data loss or breach risk isn't relegated to attacks, theft, or lost devices. Accidental data loss or exposure also frequently occurs with daily OS upgrades, acquisitions, and computer replacements. But how can you balance the needs of both migrations and security without one suffering?

When carrying out data migration, sensitive and business critical data is often exposed to IT staff, 3rd party support professionals, or worse – bad actors. Migrating secure, encrypted data can be problematic or incorrectly completed, causing the data to be unreadable after the migration. Most systems also require the PC to decrypt prior to the migration, resulting in the end user needing to re-encrypt after the migration is complete – leaving a potential gap in data security. Security cannot be put on the backburner.

It is critical that with any device or OS deployment or migration that all data must be treated with respect. All sensitive information, including customer information, should have absolute security in place.

Businesses can migrate devices and operating systems while safely eliminating the challenges of inefficient PC and OS lifecycle management. Here's how.

| Secure OS Lifecycle Management Overview

By joining forces to co-deploy the [SWIMAGE](#) and SecureDoc offerings, [LogicDS](#) and WinMagic significantly reduce the headaches and security concerns businesses have when deploying new devices into their network, performing OS migration, and handling maintenance issues.

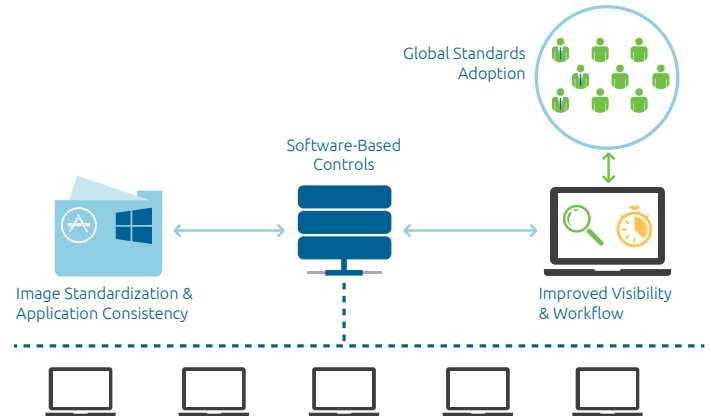
SWIMAGE empowers users or IT administrators to expeditiously migrate devices from Windows 7 to Windows 10 – a prominent challenge most businesses currently face – often in less than an hour. SWIMAGE minimizes the downtime typically associated with OS migrations by simplifying the migration process, allowing for self-migration for those on the network, or via a USB migration kit for those in remote or home-based offices. Users, domains and applications are all provisioned automatically in the process, enabling greater control over which applications users can have installed on their device. And for greater certainty, OS migrations are completely reversible if something goes wrong.

WinMagic's SecureDoc provides enterprises with a flexible and high-performing data security solution that manages data wherever it is stored – on laptops, desktops, self-encrypting drives, USBs, physical and virtualized servers, and in the cloud. By jointly deploying SWIMAGE and SecureDoc, companies can ensure that all of their data is protected during imaging and re-imaging processes, with complete visibility to the encryption status of their devices at all times.

I Streamline OS Deployments

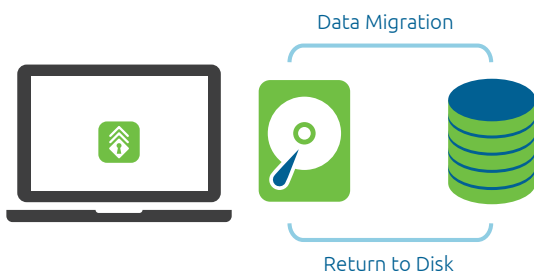
Automatically provision standardized images for devices cross-enterprise, eliminating hardware and driver dependencies, and reducing project management communications complexities

- Software-based controls for deployment standardization across departments, personas, etc. (Universal image support)
- Expedited Global standards adoption across the organization
- Application consistency and security across functional roles (ie, HR Managers get only approved applications)
- Improved communication workflow between project managers, users, etc.
- Systematic automated driver extraction process
- Security upgrades – BIOS, UEFI, MBR to GPT, TPM updates – can be implemented without the need for re-formatting
- User profiles can migrate to new domains without the need for “trust”



I Secure OS Migrations

Reduce the data security risks of OS migrations and maintenance activity in the enterprise by completely automating migration, and integrating data level encryption, ensuring data remains protected during the process



- Businesses can easily migrate from Windows 7/8 to 10 within minutes, all without compromise to security or privacy of data
- Persistent lifetime* encryption. (During re-imaging, Swimage software recognizes WinMagic Regkeys, Filter Drivers, UserData folder, etc., dropping them back on to the machine after re-image)
- Secure Snapshot and Rollback technology
- Intelligent Policy Management
- Improved project management and reporting
- Unified Encryption Reporting & Management
- Zero-touch, self-migration and remote deployments simplify OS migration/updates (SWIMAGE flash drive contains all deployment components, including the image, drivers, applications, and settings)

I Maximize User Up-time

Reduce the costs associated with non-productive user downtime and burdensome Tech support request in the enterprise by streamlining and automating device and OS deployments, migrations and maintenance

- Improvements to end user functionality and operability through automation and streamlined processes
- Real-time reporting on migration and deployment status



I Strengthen Compliance

Compliance and audit failure is a top concern for C-Suite executives. WinMagic's SecureDoc Enterprise Server helps ensure enterprises meet compliance needs by providing user-friendly audit tools to track and report that VMs and data is always in a protected state. With SecureDoc, there's no more guessing if data is secured. Instant visibility through an easy-to-read single pane of glass helps verify compliance across numerous security standards (EU-GDPR, PCI DSS, NIST, as well as HIPAA, and others) with auditing tools that report on each instance secured.

- Single pane of glass reduces risk of out of compliance devices
- Central management of all encryption keys and policies
- Simplified reporting & auditing for compliance initiatives
- Fast & comprehensive deployment reduces costs

Technical Resources

- [Secure OS Lifecycle BrightTalk Webinar](#)
- [Secure OS Lifecycle Management Blog](#)

Why Choose WinMagic?

- ✓ **Unify physical, virtualized, and cloud data security under one solution**, reducing operation & time costs associated with managing multiple data security solutions
- ✓ **Gain the visibility and control** required to strengthen data security compliance efforts through a single pane of glass providing audit, discovery, encryption and key management
- ✓ **Ease scalability** with easily deployable licenses, supporting any of a customer's growth or burst needs – no matter what speed, or scale
- ✓ **Gain Freedom of Choice** by knowing that SecureDoc can protect data on any chosen platform, or wherever it is moved
- ✓ **Support for the largest mix of public, private and hybrid cloud providers**
- ✓ **Certified for Nutanix AHV and Scale HC3 hyper-convergence platforms**
- ✓ **20 years as a leader in encryption and key management**
- ✓ **Consistently an Innovative Industry Leader:** First to: secure the data center, be FIPS 140-2 compliant, integrate with SED manufacturers

READY TO DELIVER A SECURE, COMPLIANT AND UNIFIED DATA SECURITY SOLUTION FOR YOUR CUSTOMERS? GET STARTED

WinMagic is committed to our customers' success. We offer data security solutions that can cover you from endpoints, to data center, to the cloud. To get started with unifying your data security efforts, email your WinMagic representative today.

Authenticate. Encrypt. Achieve.



US & Canada | EMEA | Japan
+1 888 879 5879 | +49 69 175 370 530 | +03 5403 6950
For more information, [click here](#) or contact WinMagic

