Vision Statement

SecureDoc™ by WinMagic

# WinMagic – our vision for better data security in a complex world.

AUGUST 2019

WINMAGIC®

For more than twenty one years, WinMagic has maintained a well-earned reputation for thought leadership and innovation in the field of data encryption. Throughout our history, we have achieved a number of industry 'firsts', helping to raise the bar for security and manageability for enterprises everywhere. Looking ahead, our goal is to provide uniquely powerful, **intelligent solutions for everything encryption**, simplifying security for even the most complex environments.

### WinMagic's vision – the simple way to optimize data protection

As the race for data security becomes ever more urgent in the modern digital world, WinMagic believes it has answered an important piece of the enterprise data security puzzle. Our vision focuses on three key points:

1. **Cryptography** (of which encryption is a key part) should be the **foundation of data – and IT security** moving forward.
2. **Effective data security starts with secure workloads**. Once all the endpoints are protected, it's very hard for intruders to reach your critical data, even in the cloud. Yet most security strategies continue to focus on the server and neglect the ongoing vulnerabilities at the endpoint. WinMagic's approach is unique and addresses a critical gap in today's security market. By focusing on securing the endpoint, we're helping extend, improve and integrate data security for the organization as a whole.
3. **Encryption and key management should be cross-platform**. A leader in data security is needed to deliver truly platform-agnostic solutions that work for everyone.

## Challenges and Opportunities in the Data Security Landscape

New technologies like cloud and other innovations continue to increase the attack surface and open up data to newer and bigger threats. To combat these threats, more technologies are introduced – from AI to big data. But this 'arms race' only equips the attackers further. The result: ever more security vendors and products entering the market without securing data at the most fundamental level – more long-term pain for a short-term gain.

WinMagic's view focuses on **cryptography**. When executed properly, cryptography prevents outside attack by significantly reducing the attack surface – restoring trust in data confidentiality. This reduced attack surface simplifies and improves protection, requires fewer products and provides greater reassurance against the ever-growing threat landscape.

a. **Most encryption products are afterthoughts, perhaps still in some infancy state**. Let's ask ourselves two basic/obvious questions: When and where should sensitive data be encrypted; and with what key, e.g. who should have access to the key and thus can access plaintext data? Ideally, sensitive data should always be encrypted except when it is being processed (used by an application, which processes plaintext data). Ideally, only authorized users should have the key for the encryption of that data. Most current offerings are not that sophisticated. Appliances sitting on the network might not encrypt the data before it leaves the endpoint, and more importantly, the data is encrypted with keys available to the appliance, the admin or even the service providers. Most common offerings today – even the sexy ones like CASB – are easier to implement but there are better solutions!

b. **Built-in encryption has become de facto**. Unlike the early days of our operation, today's platform vendors have mostly built encryption into their OS or platform environments. Encryption products like BitLocker for Windows, dm-crypt for Linux and FileVault2 for Mac are popular, as are AWS and VMWare built-in encryption. However, because they're not focused on encryption, platform vendors only offer minimal key management and manageability features, if at all.

   What's more, some encryption solutions require the encryption key to be accessed by the managed service provider (MSP) – introducing an inherent weakness to the system. For example, while promoting "bring your own key BYOK", in the end the MSP needs the key to run the system, and thus

has possession of the key anyway. A laptop owner wouldn't expect the vendor to have access to their data. But cloud enterprises have had to accept this unhappy compromise, with no choice but to hand over the key to all their cloud data. Now, WinMagic is offering another way. Note that the notion of the encryption keys exposed to the service providers here is different than the key management issue discussed in a. In a. we discuss key management issue. Here it is about the encryption methods. Here the encryption is performed by the MSP and thus it has to have the key; no key management solution can change it!

c. **The IT security market would benefit from an encryption leader**. One that can bring compatibility to the security ecosystem for the benefit of everyone – both vendors and customers. Specifically, the market needs a unified, platform-independent suite of solutions that secures data wherever it resides. In other words, a universal solution with full interoperability between all platforms – from IoT to datacenters and cloud. We believe WinMagic's products are well designed to lead the way in the future of encryption.

d. **The importance of virtualization and cloud**. It is well known that enterprises are moving away from traditional IT infrastructure towards virtualization and cloud computing. Indeed, if the security aspect can be taken care of – this process will only accelerate. Security is much more challenging now workloads run off-premise, in the cloud, and out of your control. Data moving between endpoint and cloud, on-premise to cloud, or even between clouds, all need complete end-to-end protection.

   WinMagic's focus has been on transferring traditional endpoint encryption principles to the cloud – and this concept is rather unique. We're building on years of offline knowledge and expertise, rather than reinventing the wheel for a new era of cloud.

e. **Legal compliance and policy**. GDPR, HIPAA and more mean encryption is now a 'must-have' for most enterprises and government agencies. At WinMagic, we are well positioned to help policy makers with sensible technological solutions that focus on cryptography and other expertise.

## Why our vision is key

**The foundation of our vision is what we call our 'techno-logical' approach – clear, sound reasoning grounded in high-tech principles.**

WinMagic can play a key role in the global encryption market providing intelligent solutions for 'Everything Encryption' in both the near and distant future.

**Encryption consists of two distinct parts**. Encryption and key management need to be kept separate. While the platform vendor is well positioned to create a robust, transparent encryption solution for its own environment, the key management component (KMC) is a completely different story. A good KMC needs to work independently across a number of different platforms, securing the organization's data wherever it resides.

*Why is this important?*
As OS-specific encryption becomes more widely available, enterprises want the best of both worlds – the platform vendors' encryption solution, managed by a best-of-breed key management solution. WinMagic continues to develop KMC solutions that are fully compatible with BitLocker, FileVault2, dm-crypt and self-encrypting drives (SED) – as opposed to encryption components that compete with them. Our KMC does much more than manage BitLocker. It takes over its pre-boot authentication (PBA) function, enabling it to run a powerful KMC.

**Better than built-in OS encryption – the self-encrypting drive (SED)**. The best technology innovations are smart, simple and efficient. Which is exactly how we'd describe the SED. While OS encryption requires compatibility with numerous conflicting kernel drivers, as well as precious CPU time – drive-based encryption is simple and secure. In many ways, we believe SED is the foundational solution for disk encryption. Though recent virtualization technology and secure workloads have rendered them less suitable in some areas, we believe SEDs should be the data-at-rest foundation for IT systems

*Why is this important?*
Enterprises continue to invest heavily in FDE despite the availability of OS-level encryption. While SEDs resolve their teething problems (compatibility issues, BIOS and more), WinMagic stands out as a true pioneer in this area. Our reputation and strong relationships with both SED and PC vendors bode well going forward.

**Secure Virtualized workloads – a game-changing technology**. Enterprises are often hesitant to move their most sensitive data to the cloud because of confidentiality concerns, exposure risks, Cloud Service Provider (CSP) access, infrastructure vulnerabilities and the risk of undisclosed government access. Similarly, CSPs are concerned about their liability in the event of a data breach and in keeping the trust that their customers put in them.

Part of the solution to this problem is memory encryption technology such as Secure Encrypted Virtualization (SEV) to protect data in use. In the case of SEV access to unencrypted, plain text, memory is only available to the customer's (i.e. "guest") virtual machine and not to the CSP hypervisor, management software or administrators.

*Why is this important?*
Protecting the confidentiality of data in use without protecting data at rest is not a complete solution. In general a workload starts from disk, processes data in memory (data in use) and writes it out to disk (data at rest). In-guest FDE encryption uses the CPU and memory to protect data at rest and can benefit from the protection that SEV provides.

This is where WinMagic's approach is critical. We enable the customer (guest owner) to verify that their guest virtual workload is protected with SEV BEFORE unlocking any confidential data stored on the disk and loading the work load. We believe secure workload technology, utilizing SEV alongside WinMagic FDE and enterprise-class key management, will revolutionize the way data is secured in the cloud and beyond – changing the data security game completely for Cloud Service Providers and SaaS providers.

**Secure data sharing leveraging Blockchain-based DPKI –** Sharing data securely and easily within the enterprise and with outside partners is difficult and comes with a high administrative cost. Existing solutions rely on passwords which are fraught with problems and require users to create themselves accounts or use a specific method such as eMail or Dropbox as the transport medium.

*Why is this important?*
We can solve this problem with a combination of existing WinMagic file encryption and symmetric key management know how combined with emerging blockchain-based Decentralized Public Key Infrastructure (DPKI) technology. Our vision is to enable users (vs. administrators) to create and manage share groups. These groups combine symmetric key encryption keys for intra-enterprise sharing and public key cryptography for external sharing. Blockchain-based DPKI is the repository for the public keys addressing many of the deficiencies of traditional centralized PKI systems. Encrypted files can be shared by any method (USB, eMail, Box, …) and the recipients do not need a password to access the data. However if the file falls into the wrong hands it cannot be read because they do not have the key.

**Unified Intelligent Key Management – the answer to today's data security crisis**. Compared to traditional key managers that function as a simple repository of keys, our intelligent key management solution is smart and context-aware. Taking user, device and authentication methods into account, it can intelligently determine if access should be granted to the key requestor. It also takes care of secure key storage on the endpoint, ensuring data remains secure even in the case of theft or breach, and securing key delivery – even before the OS starts. The benefit for application vendors is significant, resulting in better, more secure products for customers.

*Why is this important?*
SecureDoc from WinMagic is the only product to offer encryption and key management for disk, file, container for Windows, Linux and Mac, from endpoint, IoT, servers, datacenters and cloud – all from a single pane of glass. Since key management is complex, other vendors could benefit from our key management if we had a toolkit for them to use. Encryption is inherently difficult, but it became "easy" once there was a toolkit for it and the same would apply to key management.

SecureDoc™ by WinMagic

## Looking Ahead

For the last 21 years, we have prided ourselves in producing solutions that are cryptographically superior and easy to use. This design philosophy, combining computer science with a user-friendly mindset, has served the market well – enabling us to help improve and simplify data security for organizations everywhere. WinMagic's product portfolio continues to offer a comprehensive data security solution unlike any other. Through dedication, focus and hard work, we will stay true to our mission statement: securing data globally with high standards and strong ethics.

We hope this statement has shown why we believe our vision in Unified Intelligent Encryption Solutions will provide the industry with better security, and we are delighted and excited about the journey ahead.

Thi Nguyen-Huu
*Founder & CEO, WinMagic*

info@winmagic.com www.winmagic.com

WINMAGIC®

**US & Canada** +1 888 879 5879 | **United Kingdom** +44 0148 334 3020 | **Germany** +49 69 175 370 530 | **Japan** +03 5403 6950 | **APAC** +65 9634 5197