



Case Study: Legal

“Data encryption is no longer a ‘nice to have’ for law firms; it’s a necessity.

Brian Focht, Attorney at Stiles Byrum & Horne

Legal Industry Needs Highlights

Breach Stats¹

Law firms with 100+ attorneys reporting a data breach incidence in 2015:

25%

All Law firms reporting a data breach incidence in 2015:

15%

Law firms who had clients request a security audit

34%

Top 3 Breach Incident Types¹

- Loss/Theft of laptops, USB drives, tablets or smartphones
- Spear phishing
- Unauthorized hardware or software use by employees or 3rd party vendors

Top 7 Breach Targets²

- Patent and insider deal (M&A) information
- Healthcare data
- Case and/or litigation strategy information
- Confidential client business trajectory information
- Attorney-client privileged communications
- Personally Identifiable Information (PII) for employees, clients, and vendors
- Financial information, including credit card numbers and PIN numbers

Sources

1. 2015 - American Bar Association – Legal Technology Survey Report

2. 2015 - What are the Top Cybersecurity Threats to Law Firms? – Optimal Networks



For companies that provide services to clients, or retain any customer data, data security is an important part of daily business, and enforced by numerous state and federal regulations. Given the sensitivity of information that lawyers and law firms are entrusted with, the need for provable bullet-proof data security is of even more critical importance.

A growing law firm, headquartered in North Carolina – herein referred to as NC Cape Law for their privacy – is just one of many companies that rely on WinMagic to protect confidential client and organizational data. The law firm was seeking a solution that could provide encryption and key management for its laptops, Self-Encrypting Drives, and removable media devices – A data security solution that could ultimately protect their valuable data wherever it resided.

Growing Data leads to growing security needs

Founded in 1998, NC Cape Law (NCCL) operates practices in 15 locations on the US east coast, with nearly 600 attorneys and 900 supporting employees. NC Cape Law is a full-service business law firm, serving a wide range of regional, national and international clients in industries that include healthcare, life sciences, financial services, commercial real estate, intellectual property/patent, telecommunications, as well as educational institutions and governmental bodies and agencies.

As the company expands their locations and client base, the inevitable volume of client data expands with it. NCCL is diligent about data security and meeting its compliance obligations. Due to the regular travel by its attorneys and staff, they needed to have an encryption management solution that could minimize or eliminate any risk of a data breach, in the event of loss or theft of a device.



Customer Overview

NC Cape Law

(Pseudonym used for privacy of the customer and its clients, because security is what we do.)

15 offices in the US southeast
1200 - 1500 employees

Industry Legal

Challenges

- Meeting compliance standards in respective jurisdictions
- Reducing risk of data loss due to lost or stolen devices
- Managing OPAL SEDs
- Introducing multi-factor authentication
- Addressing perpetually evolving data risks

WinMagic Solutions

- SecureDoc
- SecureDoc for SEDs
- SecureDoc Enterprise Server

Pain Point:

Finding the Right Solution to Protect Critical Data

According to the 2015 International Legal Technology Association (ILTA) Technology Survey, only 54% of law firms encrypt their laptops, and a mere 36% encrypt USB and removable media devices. NCCL, though, had always been aware of its data security needs and legal compliance, and well ahead of their industry peers. NCCL was perpetually dedicated to preventing unauthorized access to data, and had encrypted all company-owned desktops and laptops.

As NC Cape Law managed a client base with international interests, they were particularly diligent about taking all necessary steps required to meet compliance of U.S.-E.U. and U.S.-Swiss Safe Harbor Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information. Additionally, NCCL needed to adhere to the US Privacy Act and a number of federal and state legislations relating to data. Failing to meet any of these compliances could result in massive fines, public embarrassment, and worse.

To increase its security posture, NCCL wished to introduce smart cards as part of a new multi-factor authentication process for its attorneys and employees. Unfortunately, their current vendor could not and would not support smart cards. NCCL remained committed to their plan to integrate smart cards into their authentication requirements. They began the search for a vendor and solution that could provide them with the multi-factor authentication support that they required. The new solution needed to be simple to implement, administer, manage, and use. And, it needed to provide a unified and comprehensive solution for all its devices.

Finding one vendor that could do it all? Well, that proved difficult – until NC Cape Law discovered WinMagic.

Customer Solution Highlights

SecureDoc Full Disk Encryption

- Automatically secured endpoints where no native encryption exists, or is insufficient or unmanageable

Support for Multiple Operating Systems

- Supports NCCL's OS mix including Microsoft Windows 8 and Win 7 Professional, and Linux

Self-Encrypting Drive (SED) Management

- Supports the Opal SEDs operating on NCCL's Lenovo laptops
- Offers OS-Agnostic support for any SED

Multi-Factor Authentication

- SecureDoc supported NCCL's need for multi-factor authentication on a number of its endpoints.

Removable Media Encryption

- Protected NNCL's sensitive data on USBs and flash drives by fully encrypting these media on a sector-by-sector basis

File and Folder Encryption

- Utilizes the same AES 256-bit used for FDE to manually encrypt individual files and folders that they wish to protect
- Permits email file attachment encryption

The Solution:

SecureDoc – Everything Encryption

When NC Cape Law first discussed their requirements with WinMagic they were feeling frustrated and overwhelmed with the thought of having to switch encryption vendors. Would it all be worth it in order to simply adhere to their requirements of smart cards? Would it really add the extra protection they desired? The answer was a resounding, yes – it would be worth it. And, WinMagic and its suite of SecureDoc solutions would make the migration process painless.

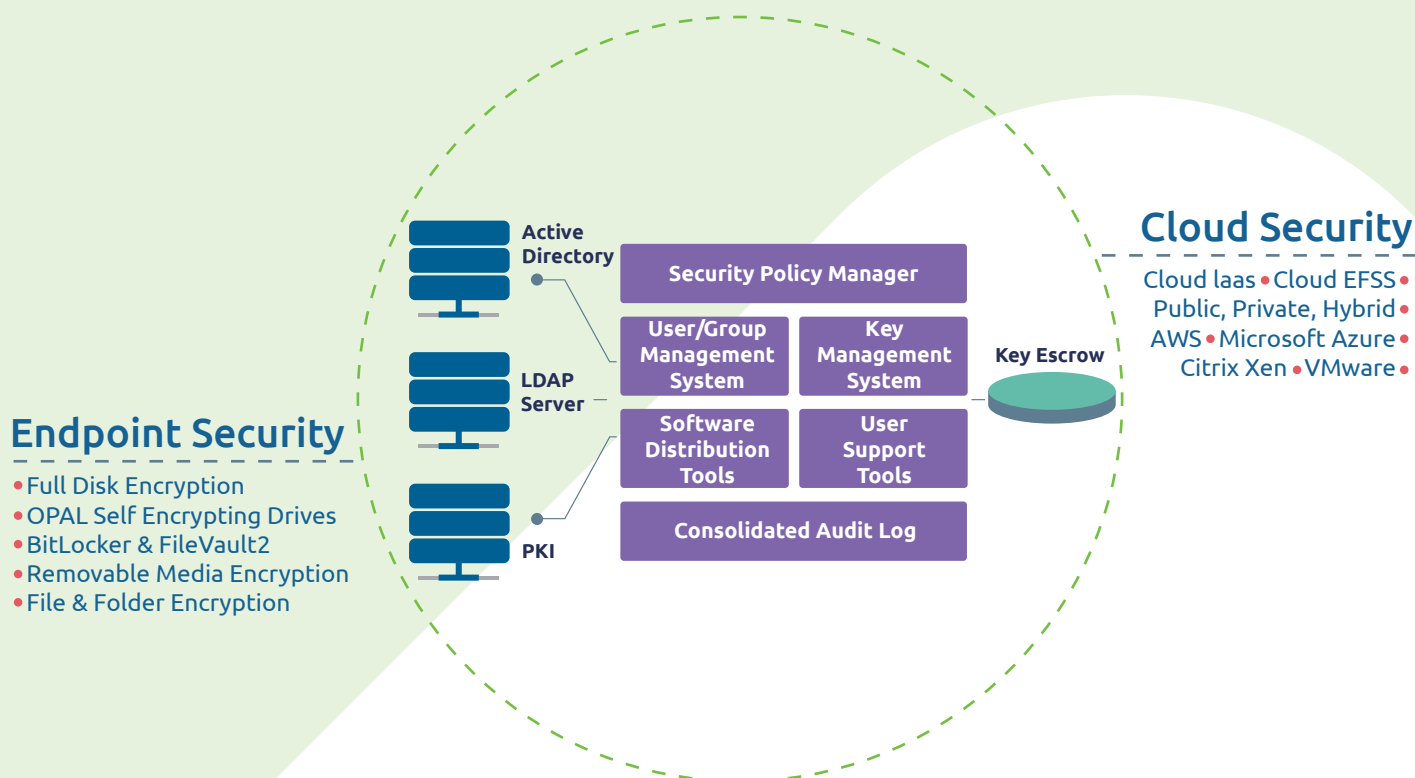
SecureDoc's full-disk encryption software uses certified and accelerated AES 256-bit encryption. Beyond FDE, SecureDoc also protects removable media, files and folders, and manages SEDs. SecureDoc was the ideal solution to meet NC Cape Law's strict data security requirements in terms of simplicity, manageability, and value; plus offers support for multi-factor authentication. As NC Cape Law deploys Lenovo laptops with OPAL SEDs, SecureDoc was a logical solution given WinMagic's status as a Lenovo integrated partner, and offers the broadest support for Trusted Computing Group (TCG) Opal and Enterprise compliant self-encrypting drives.

WinMagic quickly engaged their QA team, who completed testing of the selected smart card, ensuring it would work at preboot, as required. With guidance from WinMagic, NC Cape Law was able to integrate the smart card into a multi-factor authentication process. To further enhance their authentication procedures, WinMagic enabled Pre-Boot Network Authentication via PBConnex. PBConnex provides a means for authenticating encrypted devices to the network before the operating system ever loads – meaning data is never exposed until the user credentials are verified in advance of the standard OS log-in process.

As expected, neither the integration of the encryption software with existing technologies, nor the encryption process itself created any disruption to NC Cape Law's current environment, or resulted in data loss of any form. Adding the encryption and authentication layer to endpoints proved to be seamless – users could continue to use their laptops and computers while it installed in the background, resulting in near zero down time – just as committed.

Tying the entire solution together was SecureDoc's Enterprise Server console. Administrators now had a single view of NC Cape Law's entire SecureDoc-protected environment, could manage the security keys and policies for each user, and could audit and report on compliance.

The SecureDoc Enterprise Server Environment:



Conclusion

SecureDoc: Helping ensure client-attorney confidentiality

WinMagic's encryption software and intelligent key management solution met all of NC Cape Law's data protection and multi-factor authentication requirements, and integrated easily within their business environment, without compromising the user experience. WinMagic ensures a smooth transition to SecureDoc, easily integrating smart cards with NCCL's multi-factor authentication solution. The solution allows the customer to utilize and manage the SEDs they have on their laptops, and provides a better way to protect their USBs and portable drives. WinMagic's award-winning comprehensive encryption and intelligent key management solution is the best protection against sophisticated threats and data loss – securing data wherever it is stored, and enabling a unified key management strategy across any end point, virtualized, or Cloud IaaS environment.

Authenticate. Encrypt. Achieve.



US & Canada
+1 888 879 5879

EMEA
+49 69 175 370 530

Japan
+03 5403 6950

