A Comprehensive Plan to Simplify Endpoint Encryption

Managing SEDs, BitLocker, and FileVault Together from the Cloud

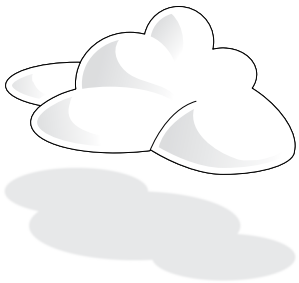
Executive Summary

Encryption is an essential component of any information security plan. When a company computer is lost or stolen, the loss places corporate data beyond the control of IT. If files were encrypted at the time of the loss, the data is considered safe, and the organization is saved the potentially devastating financial and reputational damage of a data breach. Encryption is increasingly required by data protection regulations, and is widely considered a best practice. Why is it, then, that many companies have been slow to deploy endpoint full disk encryption?

The deployment of encryption is commonly perceived as a complicated and expensive undertaking. IT is concerned firstly with the complexity of deploying encryption to a diversity of devices, and secondly with the challenge of managing encryption once is has been enabled. Though most IT departments attempt to standardize on the equipment used by employees, the recent Bring Your Own Device (BYOD) trend has forced almost every company to support multiple devices. Naturally, different devices have different encryption capabilities, meaning that IT must deploy and manage multiple encryption solutions. Faced with the need to encrypt endpoints with different types of drives, running different operating systems, obvious concerns arise. This paper describes how cloud-based security management can make it easier and more affordable for companies to deploy self-encrypting drives (SEDs) and software-based full disk encryption (FDE). It describes the barriers, both perceived and real, to disk encryption deployment, and how using cloud-based management accelerates deployment and reduces operational costs.

wave®

Background: The Need for Encryption



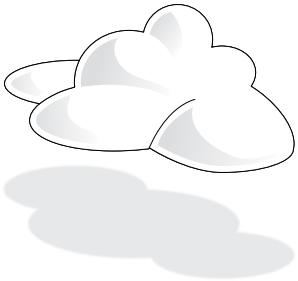
Organizations of all kinds face a growing need to encrypt data on desktops and mobile laptops. In the U.S., most states have implemented data breach disclosure laws to protect consumer privacy. The 2014 Cost of Data Breach Study by the Ponemon Institute found that the average organizational cost of a data breach has grown to $3.5 million. Further, according to Ponemon's 2014 Cost of Cyber Crime study, the average annual cost of cybercrime per company in the US is $12.7 million. The average US company is hit with 122 successful attacks per year. Of course, the cost of incident response is just part of the problem. The harmful ramifications of a successful data breach can include loss of customers, brand degradation, and the loss of intellectual property, ultimately resulting in the erosion of competitive advantage and corporate value.

The trend towards a mobile workforce has been shadowed by a sharp increase in device theft. As employees become more mobile, the potential for data being lost, stolen or misplaced increases significantly. Each new publicized data breach involving a lost/stolen laptop highlights the vulnerability of data residing on the desktops and laptops where people work every day.

Analysts and security experts all agree that encrypting data on laptops and desktops is a priority. Gartner, for example, recommends that all companies deploy encryption broadly across all workstations. Despite this consensus, many organizations lack a consistent encryption strategy. Without such a strategy, securing data from loss and demonstrating compliance is an almost impossible challenge.

Why Desktop and Laptop Encryption Isn't Widespread

An InformationWeek survey, Data Encryption: Ushering in a New Era, found that "lack of interoperability" was cited as the most significant factor deterring people from deploying encryption. Concerns about deployment and management costs are the next two factors listed. While these concerns are legitimate, they are often clouded by misperceptions and misunderstandings, or based solely on experiences with legacy, software-based FDE technologies.



Interoperability concerns: Most enterprise environments consist of a mix of hardware brands, operating systems, and software applications. Cloud-based encryption management solutions tend to be more OS-neutral and support a wider variety of platforms than on-premise management solutions. SEDs are also OS- and platform-neutral – encryption is completely transparent to the application and operating system.

Misperceptions about SED acquisition cost: Those IT executives who are aware of the SED alternative for endpoint encryption often believe that SED technology is expensive or uncommon. Only recently has production and support for SEDs become widespread in the PC industry, so they still have an outdated reputation for being expensive and scarce. SEDs are now available from a wide range of PC suppliers, including Lenovo, HP, Samsung, Dell, and others, for little to no incremental cost over comparable standard drives. SEDs are available as both hard disk drives (HDDs) and solid-state drives (SSDs).

Cost and Complexity: Enterprise management of disk encryption solutions has historically required server infrastructure and maintenance. Emerging cloud-based management solutions obviate the need for these fixed costs and simplify the path to deployment.

Cloud-based disk encryption management solutions and SEDs address many of these key concerns, and are worth further investigation for any organization looking to address the security of data on desktops and laptops.

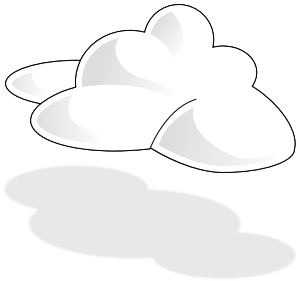
Introducing a Hybrid Approach: Cloud-Based Management of Hardware- and Software-Based Endpoint Encryption

Wave Cloud is a cloud-based endpoint encryption management solution that can manage software-based FDE on Windows and Mac platforms, as well as hardware-based self-encrypting drives on Windows. This enables IT to support the most popular platforms in corporate use today, while providing a smooth upgrade path to the advantages of SEDs.

IT needs central visibility and management of devices and control over the security policies that govern them. If a user forgets their password, for example, the PC is unusable until the password can be reset. Endpoint encryption is typically a part of a compliance effort, and thus requires audit and reporting capabilities. If a laptop is lost or stolen, organizations

need to be able to demonstrate that the data remains protected. Wave Cloud offers cloud-based management of self-encrypting drives and software FDE, including:

- User and password management
- Windows password synchronization and Single Sign-On (SSO) for self-encrypting drives
- Centralized policy enforcement
- Visibility and reporting
- Automatic initialization of self-encrypting drives
- Automatic provisioning of self-encrypting drive users



As a cloud-based service, Wave Cloud does not require any server infrastructure, so deployments can be accomplished in minutes.

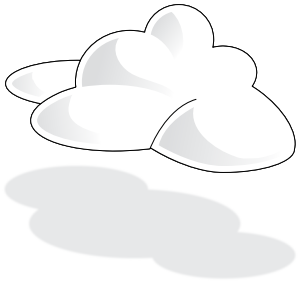
Wave Systems has been pioneering encryption management since 2007. Since then, the Trusted Computing Group (TCG) has defined an SED standard called Opal. Leading drive manufacturers like Seagate and Hitachi, flash vendors including Micron and Samsung and external drive leaders such as CMS have built a wide-range of Opal-based SEDs. PC vendors like Dell, HP and Lenovo offer these SEDs on a variety of systems, for little to no additional cost.

Self-Encrypting Drives

An SED embeds encryption processing within the drive's micro-controller chip so that encryption is always on, offering certainty that data is encrypted and the ability to confirm encryption for compliance reasons. SEDs offer significant advantages over software-based encryption alternatives, including:

- ***Better performance:*** Because encryption happens on a chip within the drive, it doesn't compete for processing cycles with the laptop's CPU or slow down running applications. Encryption is completely transparent to the OS as well as its applications. As a result, end-user satisfaction is higher than with software-based encryption.
- ***Faster deployment:*** SEDs do not require an initial encryption cycle, which can take up to 24 hours using software-based solutions. IT can provision data encryption in far less time, typically minutes.
- ***Enhanced security:*** When using SEDs, encryption is always on and cannot be turned off or otherwise compromised by the end user. SEDs are also impervious to cold-boot attacks.

From the end user's perspective, hardware-based encryption simply works and never interferes with their productivity. From the administrator/management perspective, there's no lengthy initial encryption process, and no software installation/configuration cycle of encryption software. Companies in search of an endpoint encryption strategy or struggling with the effort of software-based encryption should evaluate the SED alternative for its lower long-term costs and improved ease-of-use when compared with software encryption.



Rapid Deployment of Endpoint Encryption

Deployment of Wave Cloud does not require provisioning servers, installing management servers, and training IT staff. Wave offers a free endpoint encryption pilot program. Start by selecting a modest number of pilot participants. These might include employees who travel with laptops containing sensitive corporate data or others that frequently store sensitive data on their PCs. The pilot program can use new systems equipped with SEDs or existing systems retrofitted with internal or external SEDs. To accelerate the pilot, set up Wave Cloud to centrally manage Windows BitLocker, OS X FileVault 2, or SEDs as users receive PCs equipped with them. The users can run their actual applications and devices using encrypted storage, verifying the fact that encryption is truly seamless and transparent.

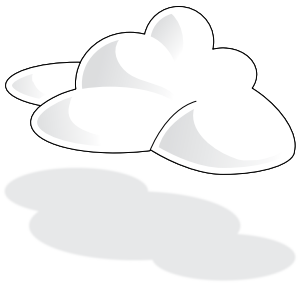
Once the devices are in place, test the basic administrative capabilities of Wave Cloud:

- Add initial users and passwords for the drives
- Synchronize drive-level passwords with Windows passwords (SED)
- Turn on Single Sign-On with the Windows login (SED)
- Reset user passwords with secure challenge/response (SED)
- Report and monitor activity to track the pilot program

Using a cloud-based management solution delivers significant benefits for the pilot project:

- Reduces the risk of the pilot by eliminating investments in server equipment or software and training management staff
- Speeds testing and assessment: The easy-to-use interface requires minimal training for administrators, and there's no waiting to purchase, install and deploy server hardware and software

Supporting Endpoint Encryption Adoption with Scalable, Subscription-Based Management



Following a successful pilot, the next step is to create your endpoint encryption policy and start deploying encryption throughout the organization.

Deployment strategies will vary according to budget, compliance requirements, and equipment refresh lifecycles. A conservative, phased deployment approach might use the following strategy:

- Retrofit SEDs on 'high-risk' devices – for example, laptops belonging to senior executives or frequent travelers and desktops containing highly sensitive data in remote or insecure areas
- Deploy BitLocker- and FileVault 2-capable operating systems where needed
- Replace existing laptops and desktops with SED-equipped systems as part of your equipment refresh policy

If SEDs are part of the equipment refresh policy, then every new desktop or laptop system deployed will have an SED. In this way, encryption is essentially built into the desktop and laptop fleet. This results in a gradual ramp-up of SEDs within the organization, with administrators adding new users and devices as they come on-line.

Wave Cloud offers a scalable platform that adjusts as needs grow. Using Wave Cloud, administrators can:

- Automatically set and enforce SED password-related policies for all new laptops and desktops
- Use role-based administration to delegate administration tasks or offer read-only access to encryption management information
- Enable Windows Active Directory synchronization and Single Sign-On
- Create reports for compliance purposes

Summary

Organizations that are struggling to secure data on laptops and desktops should seriously evaluate the advantages that a cloud-based management solution can offer. Unlike more narrow solutions, a cloud–based strategy enables a more flexible, hybrid approach to endpoint encryption. This approach results in faster deployment of endpoint encryption management across the enterprise. Wave Cloud lowers maintenance costs and reduces complexity by enabling IT to manage encrypted laptops and desktops through a single console. Selecting a solution with support for both SEDs and full disk encryption software futureproofs IT in case the corporate strategy changes in favor of one specific encryption solution. Wave believes that, in most cases, SEDs will win out over time, owing largely to the increased security and performance benefits they offer, relative to software-based alternatives.

For more information, contact your Wave representative or call (877) 228-WAVE.

wave®

About Wave
Wave Systems Corp. (NASDAQ: WAVX) reduces the complexity, cost and uncertainty of data protection by starting with the device. Wave leverages the hardware security capabilities built directly into endpoint computing platforms themselves. Wave has been among the foremost experts on this growing trend, leading the way with first-to-market solutions and helping shape standards through its work as a board member of the Trusted Computing Group.

03-000418/ version 1.01 Release Date: March 06, 2015

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com