Wave Encryption Service

Centralized Endpoint Encryption Management Delivered from the Cloud

Key Benefits:

- ✓ **On-demand encryption management**: Monitor and control data encryption on all network endpoints through a simple, point-and-click web interface. No on-premise servers or training necessary
- ✓ **Hassle-free configuration**: Encryption is automatically configured, whether a laptop relies on a self-encrypting hard drive, Microsoft BitLocker or Microsoft EFS
- ✓ **Business ready**: Achieve data security compliance in minutes not days, with preconfigured security policies, and automatic software and policy updates to all managed clients. Automated event reports and integrated email alerts keep you up-to-date
- ✓ **Transparent encryption**: Implement strong encryption that is invisible to end-users, and has zero impact on the performance of their systems
- ✓ **Intelligent data security**: Policy-based anti-theft features allow for data to be automatically wiped-clean in the event a PC is lost, stolen or otherwise deemed unresponsive

wave®
Simplifying Encryption and Authentication

Wave Encryption Service (WES)

Until you secure your network's endpoints against attack, your business intelligence, reputation and bottom line remain at risk. The experts agree: It's no longer a question of whether or not you need encryption, but rather how best to implement managed encryption across your organization — quickly and efficiently.

Wave Encryption Service (WES) is the answer. From the cloud, it lets you rapidly deploy, manage and enforce encryption policies across your entire organization without the need to maintain your own dedicated servers, software or other IT resources. WES supports commonly available legacy encryption solutions, like Microsoft® Encrypting File System (EFS) and BitLocker®, as well as industry-leading hardware-based solutions, such as self-encrypting drives (SEDs). Once downloaded onto a laptop, WES automatically detects the device's resident encryption capabilities and seamlessly adapts them to the service's online management interface. In short, your organization receives compliance-grade managed encryption in minutes rather than days, and with minimal IT overhead.

Centralized Security Management

Organizations both large and small understand that centralized management of end-point security is essential to protecting their networks and data. WES provides the policy-based access controls, easy-to-use reporting and audit logging, centralized control and end-user access recovery that companies require to cost effectively implement and manage the security of network endpoints. Most importantly, it gives IT the assurance that data will remain protected in the event that a computer (or its hard drive) is lost or stolen.

Wave Encryption Service (WES)

Strong Encryption Policy for Network Endpoints

WES allows you to intelligently encrypt data on your organization's scattered laptops, and automatically eliminate encryption keys from the device if and when the service detects a threat. It specifically monitors two main threats: failed logon attempts and Active Omission®. By automatically monitoring laptop activity, WES lets you establish online and offline policies that block unauthorized access to PCs that fail to adhere to those policies. Further, access can be easily, immediately and remotely restored at will.

WES for Self-Encrypting Drives (SEDs)

SEDs are the most secure, best performing and most transparent encryption option for protecting data on laptops. Put simply, they comprise a closed and independent architecture — including their own processor, memory and RAM — and impose very strict limits on the code that can run within this environment. Encryption and decryption of data occurs in the drive controller itself, rather than relying on the PC's host CPU — making them impervious to conventional software attacks.

WES is the only cloud-based management solution that supports all Opal-based, proprietary and solid-state SEDs, offering drive initialization, user management, drive locking, user recovery and crypto erase features for each. Further, the service supports the use of file and folder encryption even when the drive is fully encrypted — providing data protection even after the encrypting drive is unlocked. This layered protection is especially important in shared workstation environments, as it ensures that users with SED credentials can only access their user files.

Microsoft BitLocker: Wave's cloud service also provides a comprehensive set of tools to automate and secure the configuration and administration of Microsoft BitLocker, the volume encryption technology embedded into Windows7®. The WES intelligent agent automatically identifies PCs that are BitLocker-ready and then remotely configures them for BitLocker encryption. In addition, Wave Encryption Service enhances BitLocker security through the automation of the Trusted Platform Module (TPM), for strong key protection and cloud-based management of BitLocker recovery passwords. WES reporting capabilities allow administrators to quickly and easily identify which of their PCs have BitLocker turned-on.

WES for Microsoft Encrypting File System (EFS): For legacy PCs, WES implements powerful data protection using Microsoft EFS complimented with an intelligent file filter. This layer of encryption is integrated into the Microsoft OS using EFS encryption keys directly tied to the user's login. That means when a user logs in, the keys are automatically used to decrypt files for that particular user. The WES intelligent file filter automatically finds and encrypts all instances of a particular file on the system, eliminating the risk of intentional or unintentional data loss. In addition, WES enhances EFS by providing recovery services for the centrally managed encryption keys.

03-000301/version 1.00 Release date: 09-12-2011

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

wave®
Simplifying Encryption and Authentication