

## Discovering, Classifying and Protecting Data at Rest Industry's First Classification-Based Encryption and Content Protection Solution



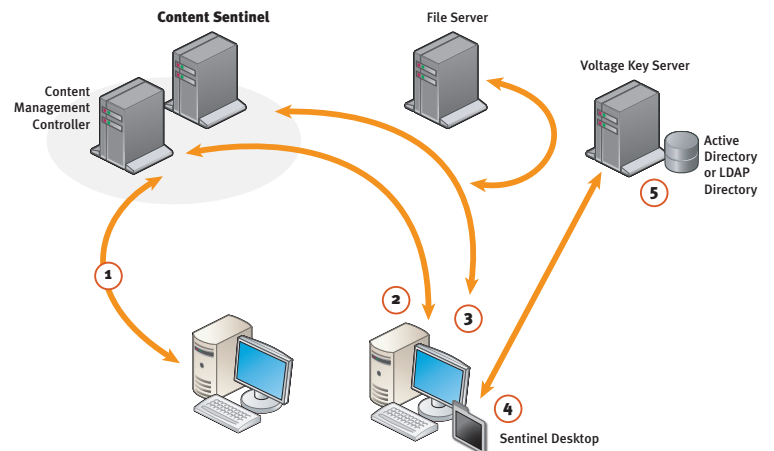
### Introduction

Voltage Security and Tablus have teamed to deliver a comprehensive classification-based encryption and content protection solution.

For the first time, enterprises will be able to automatically identify sensitive data and quarantine, delete or encrypt that data in real time based on content classification. This joint offering will integrate Voltage Identity-Based Encryption (IBE) with Tablus Content Sentinel™, Tablus Content Alarm NW™ and Tablus Content Alarm DT™.

### Content Sentinel

Content Sentinel with Voltage IBE will identify sensitive data-at-rest at network end-points, classifying it according to corporate privacy guidelines then encrypting, quarantining or deleting the data based on pre-set policies. Administrators can also control who can decrypt content by controlling the membership of a group (e.g. LDAP, Active Directory) of users. For example, if a file is encrypted to the “management” classification, then only those members of the “management” group will be able to read the file. Today, Tablus Content Sentinel accurately identifies, locates and controls sensitive information within large enterprise networks. It simultaneously scans networks, laptops, desktops and servers for data violations, and quarantines or deletes the corresponding files for immediate remediation. By integrating Content Sentinel with Voltage IBE, enterprises will gain the ability to automatically encrypt data, such as Personally Identifiable Information (PII) and credit card data to meet increasingly high compliance standards.



- 1 Sentinel scans network nodes by policy
- 2 Sentinel discovers and classifies data on individual nodes (PCI, PII)
- 3 Remediation Options: Delete, Quarantine to File Server or Encrypt with IBE immediately
- 4 Sentinel Desktop controls access to sensitive data, encrypt/decrypt functions for specific data/files after initial remediation
- 5 Data access enforced by policy to authenticated users within directory groups

## Voltage IBE

By integrating into the recently introduced Voltage Enterprise Management Platform, Tablus solutions take advantage of Voltage IBE as well as centralized policy and key management made possible by the platform. Voltage IBE differs from other encryption products on the market due to its use of any well known identity such as a common email address as the public key, enabling data to be protected without the use of certificate. This results in a powerful encryption scheme without all the management and overhead normally associated with certificate based encryption solutions.

### Key Points:

- ▶ Content Sentinel and Voltage IBE have been integrated to selectively encrypt sensitive information on desktops, laptops, servers and network shares.
- ▶ Sentinel has pre-built policies for PII and PCI related data. Other policies can be created.
- ▶ The combined product locates, classifies and encrypts data, automatically, based on a pre-set policy.
- ▶ Administrators can restrict access to sensitive data based on classification to select groups.
- ▶ IBE is easy to deploy, manage and is highly scalable unlike other encryption schemes.
- ▶ Content Sentinel supports both crawler and agent technologies to scan remote machines for sensitive data. It is highly scalable for large enterprises.
- ▶ Encryption is seamless and totally transparent to end users, requiring little or no training.
- ▶ Voltage IBE will be integrated with Tablus Content Alarm NW for data in motion on the network, and with Content Alarm DT for data in use on network desktops.

## About Tablus

Tablus, Inc. is the leading provider of content protection solutions for detecting and preventing the disclosure of confidential and privacy-related information both across network boundaries and on the desktop. Tablus offers the only comprehensive and integrated solution for locating, monitoring and protecting data at rest, in motion, and in use. By preventing such disclosures, Tablus helps organizations reduce legal and financial risk, protect against identity theft, safeguard their brand reputation and prove regulatory compliance. For more information visit [www.tablus.com](http://www.tablus.com).

## Voltage Enterprise Privacy Management Platform

Voltage Enterprise Privacy Management is a platform for consistent enforcement of privacy policies across enterprise applications and information. The Voltage Enterprise Privacy Management platform is powered by the breakthrough Voltage Identity-Based Encryption (IBE), offering the lowest administrative overhead and highest usability of any encryption solution available today.

## Identity-Based Encryption

The Voltage Enterprise Privacy Management Platform uses a breakthrough approach in cryptography known as Identity-Based Encryption (IBE). This approach uses a simple identity, such as an email address as the public key in a public/private key pair. IBE does not require the use of certificates thereby removing the usability and management problems inherent in traditional PKI based communication solutions.

### About Voltage Security

Voltage Security delivers solutions for securing the privacy of data at rest, in motion and in use anywhere within the enterprise. Voltage's Enterprise Privacy Management platform enables policy-based security of email, data on laptops/PCs, mobile devices, servers and applications. Based on an award winning breakthrough in security and usability called Identity-Based Encryption (IBE), Voltage provides solutions for data privacy to leading financial services, healthcare, government and pharmaceutical companies.

Voltage solutions provide security by making information flowing into and out of an enterprise secure.