



## information protection and data governance

### Recent Data Breaches

#### Sony

77 million records of personal customer information and possible credit card data was breached

#### Wikileaks

A government employee secretly downloaded 750,000 files from a US Defense department network and provided confidential information to outside sources

#### Bank of America

A former bank employee provided sensitive customer information to people outside the bank, who used the data to steal money from around 300 Bank of America customers

#### Citigroup

The largest breach to a US financial institution as 360,000 credit card holders information was stolen off the Citigroup network online banking platform

### Features

- Email Encryption
- Email Archive
- Hardware Control
- Document Management
- Website Filtering
- Data Discovery
- Clipboard Monitoring
- Application Access
- Fingerprinting
- File Shadowing
- Screen Capture
- Print Control
- Content Profiling



### The Challenge: Minimize the Risk... Stop the Breach

If you have data, you have problems. Your information is at greater risk than ever, evidenced by the recent high profile attacks that involve theft of confidential and proprietary data from large organizations. No one needs to tell you that customer names, credit card numbers, and transaction records must be protected. Governments, insurance companies and many different agencies make you follow rules that regulate your data. Data security is becoming more difficult with constantly changing regulations, exorbitant fines, and ever evolving attack vectors. Mobile computing, peripheral devices, and file sharing software compound the problem.

### What's at Risk?

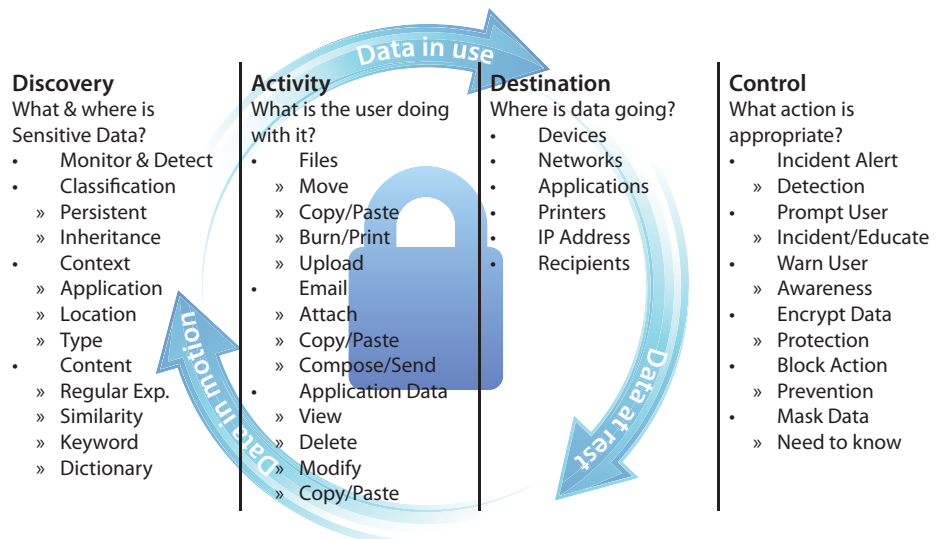
- Compliance fines - Non-compliance equals stiff penalties and costly law suits
- Workforce productivity - Enforcing data security rules can create confusing business processes and restricts employees from using tools to increase productivity
- Company credibility - Disparaging posts or any security breaches must be made public allowing millions of people to read about the negative publicity

### The Solution: Agent based approach to integrated DLP

CTH Technologies revolutionizes Data Loss Prevention (DLP) by combining technology and process to move businesses from passive detection to active enterprise information protection. While other vendors might have you believe that DLP is costly and complex, with many separate modules to purchase, the CTH Technologies solution is easy to install, deploy and implement with a minimum amount of resources to manage. Our all-in-one information protection and content inspection software security solution provides a total cost of ownership advantage to all of our clients within any size organization.

### Why the SecureCARE solution?

- Agent based security tool
- Provides protection for Data at Rest, in Motion and in Use
- Easy to manage, create and customize user security policies
- 24/7 policy enforcement on or off the network
- Realtime alerting and reporting as incidents occur
- Manage compliance requirements and audits worry free
- 40+ built in reports
- Checklist configurable dashboard
- Secure the mobile workforce



# key components and differentiators

## Agent vs. Appliance

Companies today need to deal with the emergence of new end point technologies, which have put all organizations on alert for insider malicious or accidental theft or breach. These incidents have made it paramount that if you want to truly secure your organization you need an agent based solution.

- Realtime Enforcement of Policies
- Encrypt or block emails if sensitive data is discovered
- Monitor or block print jobs
- Monitor or block social networking and websites
- Secure all End-Point devices
- Laptops - Policy follows remote/mobile workforce on or off network
- Easy to deploy, manage and scalable to any size organization
- Large cost savings



### End-Point Protection

Data protection is a critical issue for all organizations today as an increasing amount of sensitive information travels across various environments and is stored on an ever growing array of endpoint devices, including PCs, laptops and removable storage devices such as hard disks and memory sticks.

#### Key Features

- Managed by one security console
- Comprehensive yet granular device and media support
- Agent will encrypt, scan, block or record screens
- Policies auto-invoke proper security enforcement depending upon user or group policy in place
- Sophisticated Content Profiling searches for keywords, numbers, etc
- Encryption is 128 or 256-bit AES password protected zip file - (Recipient inputs password to un-encrypt)
- Simplify compliance with end-point violation reports
- Block and monitor print jobs



### File Protection

Persistent insider threats and regulatory compliance mandates make protecting sensitive file data a business requirement for virtually every organization. However the sheer volume of file data and its rapid continuous growth make it a challenge to secure properly.

#### Key Features

- Agent can lock down file shares to not only read/write access but block them: copy/move, print, attach, copy/paste, rename or upload
- Sophisticated Content Profiling allows to search through all files looking for sensitive information and then enforcing the appropriate policy action.
- Agent can "file shadow" or make a copy of any file that a user has copied to a designated network location for review. This can occur when files leave via removable drives, files printed, attached to emails or even the email itself.



### Web Filtering

Protecting and managing employee access to certain URLs with inappropriate content, preventing confidential data loss over web protocols, and the explosion of social networks has put many organizations at risk of a breach or compliance violation.

#### Key Features

- 99.9% of all websites are covered and categorized
- Most up-to-date databases in industry
- Block or allow websites based on 150+ categories
- Track or block files from being uploaded or downloaded
- Block FTP
- Web policies follow mobile workforce

## Data Discovery

Corporations today need the ability to monitor all storage locations so they can understand where their sensitive data resides and who has access to it. Our agent will scan specified network file shares, desktops, and laptops to discover and classify confidential data. It automatically enforces data protection policies by applying actions including encryption, removal, notification, auditing, logging and custom scripts.

- Discovery and classification of sensitive data
- Automated remediation actions for confidential data
- Operational efficiency with minimal impact on desktop performance using off peak scheduling of scans
- Accurate scans, minimal false positives



## About CTH Technologies, Inc.

CTH Technologies now offers a unified Business Solutions Management platform that secures, simplifies, and automates IT processes. It also improves decision making, provides performance analytics and integrates data workflows across all technology platforms. Security remains the lead focal point within our solution suite offering. Our technology provides Enterprise Information Protection solutions that enable sensitive customer, patient or company data to move securely within large enterprises or small businesses, greatly increasing collaboration, enabling business processes and meeting regulatory compliance requirements for all of our customers.

# framework and reporting



*"With SecureCARE installed, our auditors were impressed with our proactiveness against data loss. With that our OCC ratings increased"*

- American National Bank

## Custom Built Security Policies

Policy based system that can be administered to the user, group or machine

## Government Compliancy

Automated policy encryption satisfies privacy requirements

- SOX
- ISO 17799
- PCI/PII
- FERPA
- FACTA
- GLBA
- SEC
- FFEIC
- HIPAA
- eDiscovery

## Security Stats

The range from least expensive to most expensive data breach ranged from \$750,000 to 31 million in 2009

75% of all organizations have experienced a data loss within the last year

70% of all employees that leave an organization take company IP with them

- Ponemon Institute

## Comprehensive Integrated DLP Framework

CTH Technologies, through its integrated all-in-one approach and multi-function agent, is the only DLP solution that eliminates multiple security products and vendors, simplifies the overall control and management of sensitive data across your organization and allows:

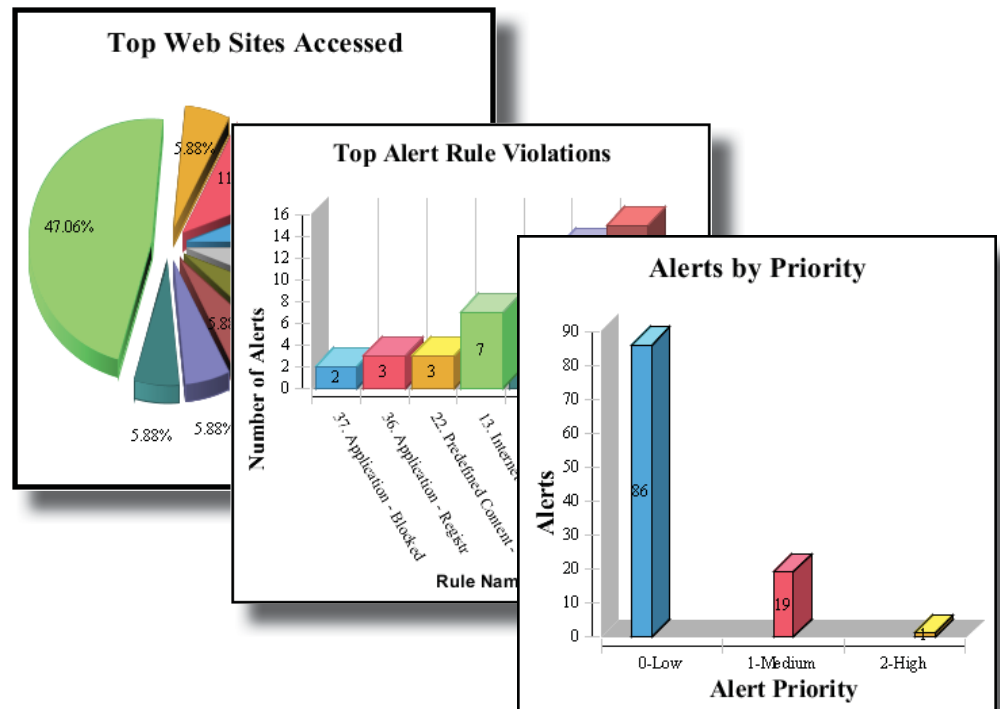
- Policy enforcement that leverages not only identity and activity, but also data classification and content analysis at the user level
- Risk appropriate responses to user activities, including warnings, encryption, blocks, scans and screenshots
- Data discovery into organizational wide data bases, files and drives to understand where your sensitive data is located
- Actionable data classification that enables policies to be enforced accurately based on the sensitivity across the content management lifecycle

## Reporting and Security Auditing

Other technology solutions provide an overwhelming amount of data in formats that are not meaningful to managers who have a critical need to acquire this information. In today's complex world of security, the display of information in meaningful and actionable formats is even more critical due to the massive amounts and differing types of sensitive data found at most organizations. These organizations need the ability to collect, aggregate, store and then mine the data to make intelligent decisions around where data is most at risk, where new threats may exist and what governing controls need to be implemented. Reports are the translation of raw data into pertinent and actionable information. SecureCARE's customizable and automated batch reporting engine provides the ability needed to deliver accurate and actionable reports for management, security/compliance officers, HR and legal department within your organization on a timely manner. These built in reports deliver:

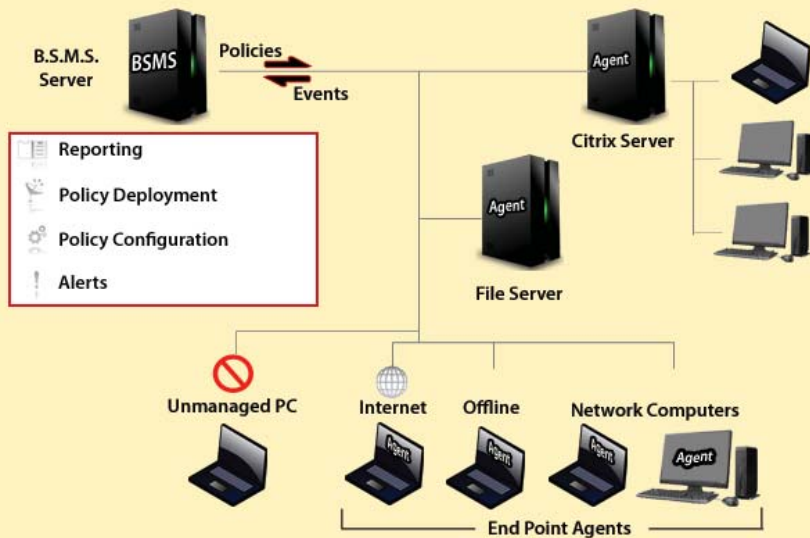
- Automated batch delivery capabilities in sending reports
- Graphical analysis and history of all warnings and alerts
- Custom query capabilities for detailed auditing
- Regulatory compliance reports

## Sample Reports





### B•S•M•S Architecture



#### Agent

The B•S•M•S Agent is installed on any desktop/laptop or server

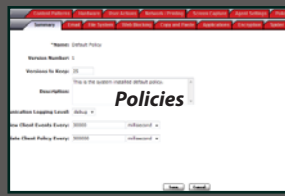
- Very small footprint (20mb hard drive space)
- Pulls down policies and pushes up events
- Hardened and tamper proof, can be ran in "stealth" mode on the host system

#### Server

The B•S•M•S Server is a Web-based application server and console that is the command center.

- Manages and monitors all B•S•M•S agents
- Captures, aggregates and stores all user activities
- Manages data security policies
- Scalable architecture for any enterprise

#### - Centralized Management -



### SecureCARE Technical Features

#### Email Monitoring & Encryption

- Monitor Email Clients - Outlook, Groupwise and Lotus Notes
- User Optional or Mandatory Encryption

#### Email Archive

- Archive incoming and outgoing emails in raw text

#### Hardware Control

- Force encryption at file level
- Block access to drives based on safe/block list

#### Document Management

- Add additional rights functionality to directories
- Block file operations via; copy, move, attach, upload, print and rename

#### Data Discovery (Spider)

- Scan directories for content or specific file types

#### Website Filtering

- Block website usage based on categorization or url patterns
- Time-based website access

#### Clipboard Monitoring

- Monitor the usage of text in the clipboard
- Block access to screenshot capabilities

#### Printing

- Control access to printers

#### Application Access

- Block access to applications based on caption, exe name and screen text
- Time-based application access

#### Fingerprinting

- Automatically tag documents based on location
- Control file operations based on tag
- Force encryption on tagged documents

#### File Shadowing

- Create shadowed copies of files for review
- Control what is shadowed

#### Screen Capture

- Capture individual screens
- DVR-like playback
- Forensic evidence

#### Content Profiling

- Protection against content patterns such as;
  - Numerical Patterns
  - Keywords
  - Table Lookups
  - Text files containing keywords
  - Regular Expressions (RegEx)
  - Default Algorithms
    - Credit Card Numbers
    - Social Security Numbers
- Boolean search operators may be applied to any pattern ("and", "not", "or")