SecureCARE™

Capture And Record Events

the ultimate data loss prevention (dlp) solution

Content Profiling
Sophisticated content analysis capabilities (keyword and pattern matching with boolean search, login times, system activities, and location) to detect credit card numbers, bank routing numbers, social security/EIN numbers and other insider threats

Policy Alerting
Provides immediate alerts when policies are violated via an email, database log or text message

Policy Enforcement
Provides immediate feedback to users when policies are violated and enforcing desired user behavior

Detailed Reporting
Creates customized reports depicting user security violations, behavioral analytics and file operations

Mobile Workforce
Secure policies on and off the network insuring mobile devices are protected remotely.

Enterprise Scalability
SecureCARE uses a redundant middleware architecture to scale with large enterprises and prevent service outages

- U.S. Businesses lose over 12 Billion per year due to data loss
- On average it costs a company $218 per data record lost
- 85% of all companies experienced a data breach

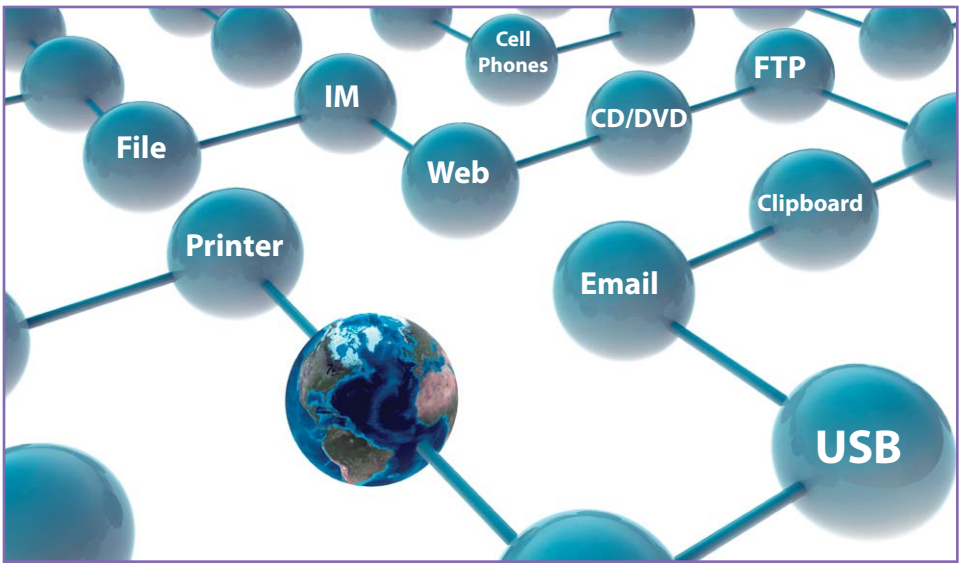
The Problem

Today's organizations face information protection challenges which no one could have envisioned in the days when mainframes were common. The average laptop can carry up to a ½ terabyte of storage, while keychain sized USB devices can hold entire customer databases. The ability for users to connect to any network within wireless range of their laptop, emailing or exchanging company confidential data via a mix of private and public services, leaves your organization wide open to data breaches. Just by locking down users, is no longer the answer. Companies need enabling technologies that secure their information while having policies allow or restrict user actions. Instead of broadly restricting user activity, companies want to only block those actions that could result in a damaging data breach. Organizations need this solution to be mobile, adaptive, and minimally intrusive.

Challenges around data protection and insider threats have changed dramatically over the past few years. The increased volumes of data breaches which occur on a yearly basis are staggering. The build out of digital business to encompass outsourcing workers, partners, and offshore centers, combined with the motivation of sophisticated hackers, disgruntled employees and identity thieves, puts more sensitive information at risk than ever before.

The Solution (DLP)

Endpoint security has been evolving over the past few years; Traditional appliances which sit on the fringe of your network have severe holes within their protection capabilities. Agent based DLP solutions have become the "must have" within the corporate world today. Endpoint devices like thumb drives, cell phones, mp3 players and cd's have forced companies to really focus at the user level. The agent solution must be able to scan for sensitive content, encrypt specified data, block external devices, monitor print jobs and track user activities at the desktop level, preventing someone from walking out your door with vital company information.



www.cthtech.com 630.613.7070 sales@cthtech.com

protect data-in-use, in-motion and at-rest

- Over 70% of corporate data breaches occur internally versus external threats
- 253 million records of U.S. residents have been exposed due to security breaches

The Real ROI

The unfortunate truth is that one data leak can result in ongoing costs to your company. Even after your operations have recovered, effects of the leak could continue to impact your business for years after. When realizing what is at stake, the decision should be simple.

Reactive

- Failed compliancy audits
- Stiff government fines
- 5 years of additional process & data audits
- Expensive litigation & internal investigation
- Lost revenues thru damaged brand image
- Re-establishing customer trust & loyalty
- PR costs to rebuild company reputation
- Competitors will leverage data breach

Pro-Active

- Increase customer trust & loyalty
- Protect customer's sensitive data
- Secure company IP, records & database
- One click reports for audits
- Increased scores and ratings on audits
- Secure entire network and mobile users
- Provide forensic data to legal council
- Increase user productivity

Fortunately, the threat of a data breach is significantly mitigated when the proper technology is in place, a DLP solution. Defining a clear return on investment and a manageable total cost of ownership is what CTH Technologies provides to its clients with their DLP solution, SecureCARE.

SecureCARE

CTH Technologies' believes DLP is an important information security control, with capabilities beyond those traditionally associated with monitoring tools. DLP assists management to identify and correct faulty business processes, identify and prevent accidental disclosures of sensitive data and provide a mechanism for supporting regulatory compliance and audit activities.

SecureCARE is a comprehensive data loss prevention solution with agent software installed on corporate desktops or laptops across the enterprise. Through the logging and analysis server, you deploy centrally managed policies, monitor real-time events, and generate reports. SecureCARE's intelligent surveillance system detects, manages and prevents information leakage from multiple communication activities including applications, USB devices, CD/DVD writing, printing devices, instant messaging, email, web browsing, webmail, and other file operations.

Build Effective Security Policies

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

Detect Violations

Comprehensive detection tools help detect violations to expose

- Accidental and malicious data disclosure
- Intellectual property leakage
- Vendor collusion, supplier fraud
- Financial fraud
- Compliance violations
- Customer data loss
- Confidential information

Investigate Threats

Use powerful event search engine and supplied reports depicting user security violations and behavioral analytics

Government Compliancy

Automated policy encryption satisfies privacy requirements

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

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

- SecureCARE Financial Institution Customer

- in Use - data at the user endpoint
- in Motion - data travelling across network protocols
- at Rest - data residing in storage devices

About CTH Technologies, Inc.

CTH Technologies believes that integrated network, endpoint and data discovery capabilities – coupled with a centralized management console capable of distributing a consistent set of policies, while providing usable event analysis and workflow data for alerting on and remediating violations – is the ultimate goal and destination for the DLP marketplace.

centralized policy management & reporting

SecureCARE Features

Monitoring & Enforcement
- Policies for monitoring and enforcing user behavior
- Proactive protection through real-time detection and enforcement
- Block, allow, monitor, and encrypt sensitive data
- Automate and integrate enforcement actions with existing business workflows
- Audit trails of risky behavior by groups or individuals

Detection & Identification
- All structured and unstructured text file formats supported for classification and content analysis
- Detects and identifies sensitive information in transit, in real-time, even in nested compressed files
- Scan the recycle bin, My Documents, and desktop where most sensitive data is found
- Schedule auto-scanners to run on a regular basis

Enterprise Manageability
- Centralized Administration
- Scalability to fit any business requirements
- Deploy and manage the desktop agent using any popular systems management software, speeding up the roll-out

Policy Management
- Set policies to block content from output to various destinations including: CD/DVD, USB, Bluetooth Infrared, print, copy/paste, screen scrape, email, IM and FTP
- Ensure compliance with data privacy legislation for all major regulatory statutes
- Create and refine custom policies by user, group, department, location, and domain
- Real-time push of policy changes to all agents
- Real-time alerts, event logging, and policy enforcement
- Instant notification of policy breaches

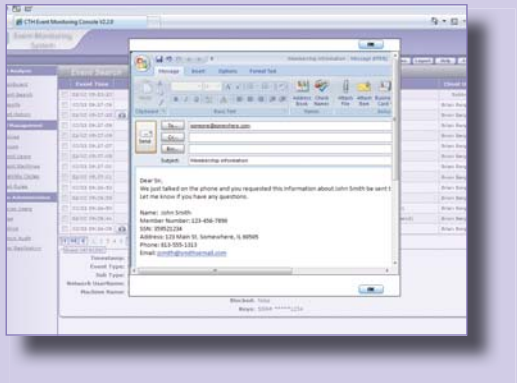
Insightful Dashboard & Reporting
- Web-based management and reporting with predefined customizable and ad-hoc report capabilities
- Create and sort event reports by date, severity, policy violation, source, destination, protected content or any combination
- Incident management includes tracking, remediation and problem resolution
- View violation status with easy to use advisory alert system

Mobile Data Protection
- Secure policies enforced on and offline to remove the "mobile user weak security link"
- Fully encrypt hard drive data
- Maintain inventory of all local files

SecureCARE Unique Features

CAREplay™
- Capture any violation with pictures
- Capture keystrokes and copy/paste activity to recognize violations in progress
- Provides evidence trail of end user activity

Scenarios
- Unauthorized application usage from USB device or CD/DVD
- Unauthorized application usage on the PC
- Unauthorized web usage
- Keyboard and Copy/Paste content violation in any application, i.e. Email or documents
- Screen content violation in any application
- User-defined actions



Protected Document Path
- Added support for individual user actions;
  - Copy/Move, Attach, Upload, Copy /Paste, Print and Rename
- Ability to exclude specific file extensions from being protected

Application Performance
- Monitor application response time based on caption, URL or exe

User Actions
- Track all user actions
- Record application usage time
- Track application violations
- Track adding/removing applications, devices or services

Spider
- Scan for only specific file types. i.e., .doc, .xls, etc.
- Scan specific hard drives and/or multiple directories
- Force Encryption if sensitive data found in scanned files
- Global encryption password support

SecureCARE™ Capture And Record Events

complete desktop coverage

SecureCARE Technical Features

Administrative Functions

- Dashboard
- Override Codes
- Alert Rules
- Alert History
- LDAP Integration
- Admin Audit
- Archival
- Policy Creation
- Centralized Management

Email System

- Automatic or manual encryption of attachments and/or body text
- Blocking of attachments and/or body text
- Content Profiling
- Safe domain list allows email to be sent without encryption
- Outlook, Lotus Notes and Groupwise support

File System

- Monitor all file events, i.e. copy, move, paste, rename, delete, download, or save as
- Monitor all product installs and uninstalls
- Automatic or manual encryption of removable drive operations
- Content profiling for any device operations including compressed files
- Track total number of fi le events for one day or Windows session
- Block, alert or monitor local hard drive file events
- Block, alert or monitor network share file events

Hardware

- Block, alert or monitor any device addition or removal via USB, Infrared, Bluetooth or Firewire
  (Ex. dongle, printer, storage device, camera, iPod®, and scanner)
- Force USB storage devices to read only
- USB Storage device safe list
- CD/DVD device safe list

Browser

- Block, alert or monitor URL usage by a full or partial string
- Block, alert or monitor URL usage by a meta content tags
- Block, alert or monitor internet file downloads
- Block, alert or monitor internet file uploads
  (Ex. Yahoo Mail, Hotmail, Gmail, Sendthisfile.com)
- Content Profiling

Printing System

- Block, alert or monitor all print activity
- Content Profiling

Policy Screens

- Customizable policy screens displayed to the end user

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")
- Block, alert or monitor based on number of instances

Applications

- Block, alert or monitor application usage
- Block, alert or monitor application usage by drive location
- Windows service start/stop monitoring and automatic restart capability
- Task Manager process termination monitoring
- Block, alert or monitor specified registry key access or changes

Screen Capture

- Block, alert or monitor screenshots for sensitive content
- Capture multiple pictures of user actions in specified application windows
- Find sensitive content in Mainframe 3270 or AS400 5250 screens

Copy & Paste

- Block, alert or monitor all text and image based clipboard actions
- Authorize clipboard actions to specific applications

File Shadowing

- Email Body archive
- Email Attachment archive
- Archive files sent to removable devices
- Auto-purge files after specified days
- Archive based on content profiling

www.cthtech.com 630.613.7070 sales@cthtech.com