



Desktop Cop

Data Security at the Desktop

detecting and preventing insider security threats

Comprehensive Communication Coverage

Monitors all activities throughout your network

- Web based applications
- Windows based applications
- Data Transfer
- Communication
- Media
- Encryption

Policy Alerting

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

Policy Enforcement

Provides immediate feedback to users when policies are violated and enforces desired user behavior

Detailed Reporting

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

Intelligent Surveillance

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

Enterprise Scalability

Desktop Cop uses a redundant middleware architecture to scale with large enterprises and prevent service outages.

- 1 in 500 emails has confidential information
- Over 65% of security threats are from insiders who are permitted access to sensitive data
- 93 million records of U.S. residents have been exposed due to security breaches
- On average it costs a company \$182 per data record lost

Every organization has the responsibility to protect their most valuable asset, their data. Who, how and by what communication method is your organization's data being shared, both inside and outside of the company, has become a major priority for security officers. Most organizations take necessary and extreme measures to protect themselves from external threats. Now the time has come for organizations to look at ways to effectively manage and protect their data against insider threats, even with its most trusted asset, its own employees.

There are many ways trusted users can leak and remove confidential information from your enterprise; e-mail, instant messaging, printed materials and widely-used portable storage devices such as "thumb drives". The cost of confidential data loss and theft is high. It impacts your reputation, your customers, your competitive advantage and your profitability. With enterprise information leakage caused by insider threat, it's not a question of if — it's a question of when, how often, what and who.

Using traditional network-based systems, such as firewalls and email security appliances, to secure your confidential information, creates a false sense of security with managing insider threats. While these devices are easy to install, they are not as effective in detecting insider threats at the desktop level, i.e. removable media, cd/dvd burning devices and printing components. The first line of defense against insider threats is to control and manage what is happening at the desktop by capturing all keyboard and mouse movements to follow user actions. With this in mind Intellectual Dimensions, LLC has designed a desktop security solution, whose core is a proven event-based capture and record technology that has matured over seven years. During this time, we received valuable input from our clients, allowing us to evolve the core engine into a security solution that not only captures and records all activities at the desktop; but, one that helps organizations analyze, manage, and most importantly secure their most valuable asset -- their data.



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



Build Effective Security Policies

Policy based system that are enforced at 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
- ISO 17799
- PCI/PII
- FERPA
- GLBA
- SEC
- FFEIC
- HIPAA

"The first day with Desktop Cop we found sensitive internal information was being unknowingly saved to removable media"

- Desktop Cop Financial Institution Customer



Desktop Cop 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. Desktop Cop'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.

Desktop Cop provides total coverage of all activities regarding user actions that occur on the desktop. With the agent on the desktop, Desktop Cop can automatically enforce policy and regulations to enable compliance and reduce the risk of legal penalties and image damage resulting from violations. Desktop Cop uses multiple detection methods for information classification and identification. Structured or unstructured data is analyzed in-depth using a combination of rules, categories, boolean searches, lexicons, statistical analyses, and exact and partial content-matching techniques to identify protected data.

Desktop Cop protects against the misuse of:

- **Data in Use** - all file, keyboard, mouse, and clipboard activity to any local or corporate network device, such as removable device, printing, or file operation
- **Data in Motion** - all outbound and internal communication, i.e. email, web browsing, or instant messaging
- **Data at Rest** - scan all files containing sensitive information on any system within the network

About Intellectual Dimensions, LLC.

Intellectual Dimensions, LLC is a professional services group that provides business and security solutions to the financial services industry. Our team of professionals is comprised of innovative experts in the financial industry, who possess a comprehensive knowledge of Operations and Technology.

centralized policy management & reporting

Desktop Cop 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, ease of deployment

Policy Management

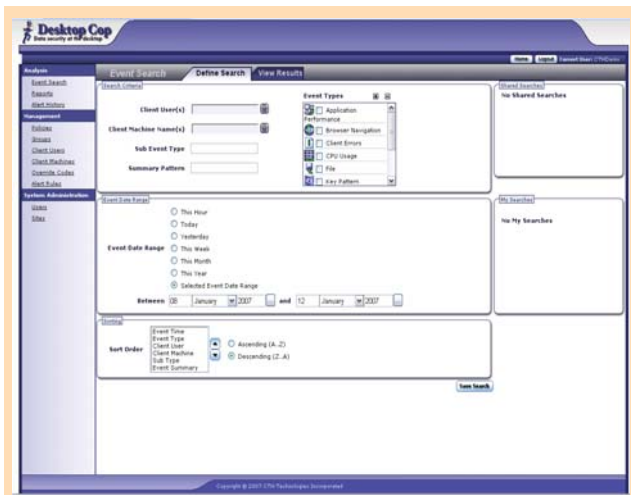
- Set policies to block content from output to various destinations including: CD/DVD, USB, Infrared, print, copy/paste, screen scrape, email, IM and FTP
- Ensure compliance with data privacy legislation for all major regulatory statutes
- Create and refine custom policies by user, group, department, 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
- Unified policy management for data-at-rest, data-in-motion and data-in-use
- 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

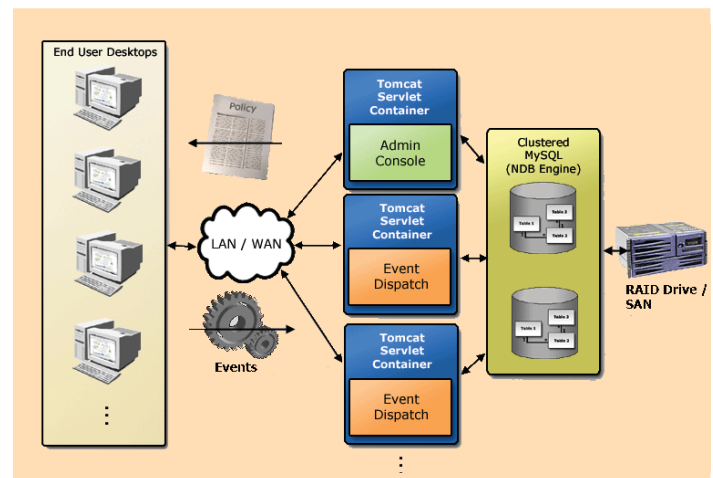
Centralized Management

- Create policies, alerts, reports or search events
- Role based administration



Scalability

- Robust architecture allows corporations to scale the technology to fit their needs
- Desktop Cop deploys into standard J2EE containers and supports persistence with most major database vendors





Desktop Cop

Data Security at the Desktop

complete desktop coverage

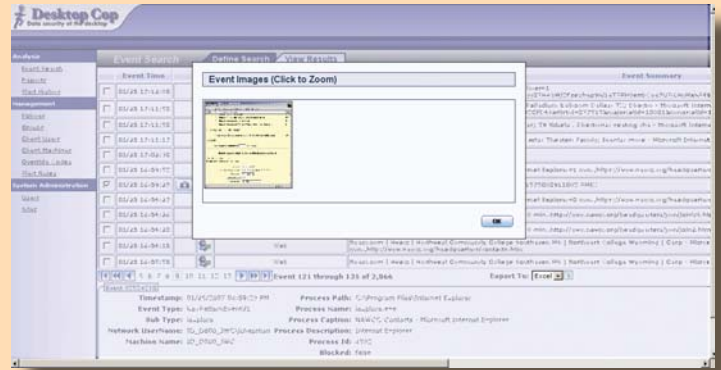
Desktop Cop Technical Features

Desktop Cop™

- 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



Email System

- Automatic or manual encryption of compressed or uncompressed file attachments
- Content profiling of attachments and email body
- Safe domain list allows internal email to be sent without encryption
- Block all attachments
- Block email transmission with content violations in email body

File System

- Monitor all file events, i.e. copy, move, paste, rename, delete, download, or save as
- Monitor all product installs and uninstalls
- Block and/or encrypt all removable device operations
- Full or partial content profiling for any device operations including compressed files
- Policy enforcement allows alerts to be created on any file operation
- Create custom events

Browser

- Block, alert or monitor URL usage by a full or partial string

Applications

- Block, alert or monitor application usage by full or partial Window caption, class or screen text
- Content profiling of application screen text
- Block, alert or monitor application usage by drive location (USB, CD, DVD, UNC or Network share)

Content Profiling

- Block, alert or monitor content within emails, files, keystrokes, clipboard or screens
- Protection against default patterns such as:
 - “99-9999999”
 - “confidential”
 - Government issued Social Security numbers
 - Credit Card numbers
 - Bank routing numbers
- Boolean search operators may be applied to any pattern (“and”, “not”, “or”)
- Block, alert or monitor based on number of instances that a pattern may occur

Hardware

- Event capture of any device addition or removal via USB or firewire (Ex: dongle, printer, storage device, camera, iPod®, and scanner)
- Block USB storage devices from being added

Monitor User Actions

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

Printing System

- Capture any printing action
- Block all files from being printed