



Vericept Data Loss Prevention Solution

Identify Sensitive Data and Enforce Controls to Prevent Data Leakage

Overview

The key to effective data loss prevention (DLP) is the ability to enforce control over sensitive data with accuracy and precision. Regardless of what types of data are being monitored (in-motion, at-rest, or in-use), Vericept's unparalleled classification technology discovers sensitive information based on content relevant to each company's specific data security and compliance policies. Vericept's patented classification suite and pre-defined Risk Categories allow organizations to define, identify, and enforce the protection of sensitive information while minimizing false positives and false negatives. All findings are centrally recorded and presented in configurable and summary detail, including details on policy violations.

To provide extensive visibility and maximum protection over information assets, the Vericept Data Loss Prevention solution includes four main components: Vericept Monitor, Discover, Protect, and Edge. In addition, the Vericept DLP Solution Management Console provides an easy-to-use interface that streamlines workflow and policy management. This capability expands the flexibility of the Vericept solution and allows organizations to tailor the DLP solution to fit their specific needs.

Key Benefits

- ▶ Single solution for identification of sensitive content, in-use, at-rest, and in-motion
- ▶ Automatic blocking of data leakage over email, webmail, HTTP, and HTTPS
- ▶ Centralized compliance reports, dashboards, and event details of all policy violations
- ▶ Enterprise class workflow, case management, and SIM integration
- ▶ Unmatched accuracy and breadth of content detection capabilities
- ▶ Customization of content policies to detect unique business information
- ▶ Pre-configured categories and reports to help meet compliance mandates


VERICEPT™

Vericept Corporation

800.262.0274 www.vericept.com

The Vericept Data Loss Prevention Solution includes:

- ▶ **Vericept Management Console** provides a user interface that makes workflow and policy management easy with a customizable, graphical dashboard for straightforward analysis and one-click administration.
- ▶ **Vericept Monitor** analyzes all data in motion on your network for compliance violations and sensitive data regardless of port or protocol. When used in conjunction with a proxy server, Vericept Monitor-CAB can block traffic sent via HTTP, HTTPS, and FTP.
- ▶ **Vericept Protect** provides email control to defend against unauthorized loss of data. Protect can initialize a self-compliance policy or automatically encrypt, block, or quarantine email communications and attachments. Vericept Protect provides active feedback to users to educate them on the proper handling of sensitive data.
- ▶ **Vericept Discover** investigates data-at-rest to find and protect sensitive information residing in stored data on desktops, laptops, and file servers.
- ▶ **Vericept Edge** controls information leakage on desktops and endpoints with three major attributes: *Content Visibility* to discover and maintain an up-to-the minute inventory of sensitive data; *Device Control* to prevent data loss on removable media and drives; *Content Control* for real-time, content-aware controls over file access and saves.



Define Sensitive Data

The first step in an effective data loss prevention program is to define what data is sensitive. The Vericept patented classification engine has a suite of content detection technologies that provide multi-level content analysis for defining sensitive information in both structured and unstructured data. As information is generated on desktops and laptops, Vericept can classify new and multiple generations of sensitive information and initiate automatic controls based on corporate policy. Information identification at all levels of a network allows organizations to gain insight into who is accessing information and how sensitive this type of information is within the company. Vericept's classification suite minimizes false positives, increases the accuracy of sensitive data discovery and scales effectively to large enterprise environments. Once classified, information can be regulated by initiating more extensive security measures to mitigate the risk of loss.

Policy Management

Once sensitive data has been defined, organizations can set security policies based on their specific needs. Vericept has over 70 pre-configured policies that help protect against compliance violations, customer data loss, and the leakage of intellectual property assets. These policies include:

- ▶ **PCI DSS:** This category detects the transmission of cardholder data that is considered a violation of the Payment Card Industry Data Security Standard (PCI DSS 1.1), including instances where the cardholder data embedded in the card's magnetic strip is transmitted in clear text.
- ▶ **Personal Information:** This category is designed to identify information that could lead to a violation of the State Data Privacy Laws such as CA SB 1386, including driver's license information.
- ▶ **GLBA:** This category helps organizations detect violations of the Gramm-Leach-Bliley Act. It is specifically designed to search for credit card numbers, Social Security numbers, expiry dates, security code, access code or password, home addresses, mother's maiden names, and bank account information.
- ▶ **HIPAA:** This category detects possible violations of the Health Insurance Portability and Accountability Act by recognizing such things as Social Security number, telephone number, address, city, or zip code, medical account number, date of birth, and date of admission or release.



Identify Sensitive Data

A fundamental challenge facing all companies is to locate where sensitive data exists and classify it by business risk. Vericept provides an automated solution to this problem by finding and classifying sensitive data wherever it may reside in the enterprise. Whether the information is stored on servers, desktops, laptops, or databases, Vericept finds the sensitive data and classifies it with the most accurate suite of detection and classification methods. The Vericept Content Detection Suite includes:

- ▶ Full and Partial File Matching of important documents
- ▶ Exact Content Match of large structured data sets to protect customer data
- ▶ Time-tested pre-defined Risk Categories
- ▶ Rules-based engine that enables users to combine Vericept's detection methods to create highly customized policies for detecting and preventing information loss and insider risk
- ▶ Intelligent content analysis through semantic patterns, linguistic constructs, data classification, and modeling of abstract concepts via Vericept's unique Content Analysis Description Language™ (CANDL)



Enforce the Protection of Sensitive Data

Vericept provides multiple ways to prevent sensitive traffic from leaving an enterprise:

- ▶ **Vericept Protect** can block, encrypt, quarantine, or send back for reconsideration email messages (SMTP traffic)
- ▶ **Vericept Monitor**, working in conjunction with a proxy server, can prevent data leakage over HTTP, HTTPS, or FTP.
- ▶ **Vericept Edge** can block access to removable media and USB drives and enforce real-time, content-aware controls over file opens and saves to and from local drives, removable media, and removable drives.

The screenshot shows the Vericept web interface with the following details:

- Page Header:** VERICEPT, Home, Reports, Search, Categories, Policies, Workflow, Administration, Help, Administrator, Logout, Preferences, Help.
- Event Detail:** Events: Event Detail. Actions: Back to Results, False Hit, Transfer to Self.
- Overview Tab:**
 - Attributes:** Severity: High; Directionality: Outgoing; Match Count: 56; Category: VCPT/pcidis; Date/Time: 2008-01-23 21:42:14.914270; Protocol: smtp; From Account: amarkov; To Account(s): vrept@le@yahoo.com; From Host: amar-es.vracme.com; To Host: mail.shch.org; From IP: 192.168.1.2; To IP: 10.3.2.3; From Port: 25; To Port: 32964; Has Attachments: true; Log size: 0.
 - Matches:**
 - form-data; name="subj" customer credit card numbers content-disposition: fo
 - s.txt" content-type: text/plain mastercard 5389733663647952 52438039803047
 - american express 347266715839899 372892857861561
 - discover 601142621017113 601134044450478
 - diners club 30270183534976 30336780692
 - Workflow State:** state: VIEWED; priority: 1; organization: InfoSec; reviewer: unassigned; hasAnnotations: false; eventAction: EMAIL_QUA.
 - Workflow Summary:**
 - 2008-01-23 22:22:22 Chang
 - 2008-01-23 21:42:14 NEW
 - Email Protect Actions:**
 - Reject E-mail
 - Release E-mail
 - Notify Sender
 - Notify Reviewer
 - Not

Vericept's easy-to-use Event Detail allows for rapid risk analysis and remediation

Key Features

- ▶ Customizable Portal
- ▶ Automatic severity assignment using custom policy settings
- ▶ Automatic highlighting of sensitive data, even for custom categories
- ▶ Dashboards pinpoint most critical event attributes for rapid identification of violations
- ▶ Customizable reports, embedded reporting package

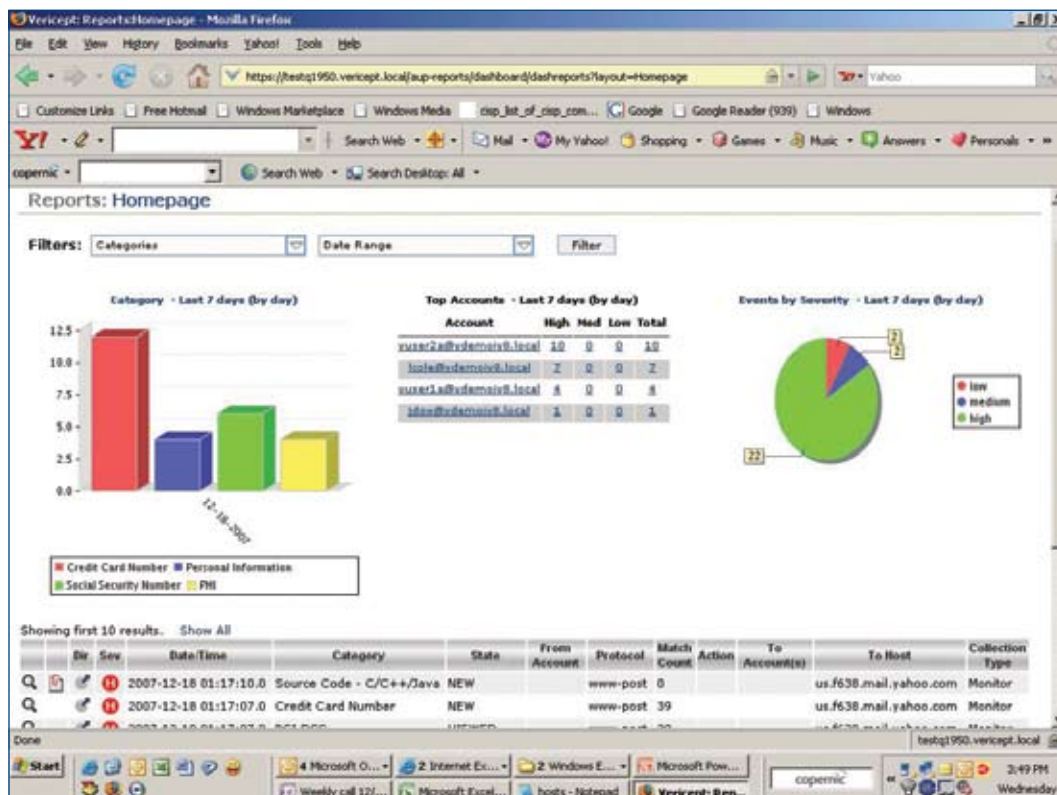
Vericept Protect provides email enforcement based on policy to stop sensitive information leaving the enterprise.

- ▶ **Protect Blocking** stops communication that should not be leaving the organization, based on the categories selected. A log of the event is captured as an evidence trail.
- ▶ **Protect Quarantine** intercepts email delivery and allows independent review and approval before email release or deletion. A user alert can be sent to the sender informing him/her of the policy violation and that the communication was quarantined.
- ▶ **Protect Self-Compliance** allows the sender to decide whether an email should proceed, by alerting the sender that the message violates company policy. The sender can decide to continue sending the message, to send the message with encryption, or not send the message at all. Email self-compliance helps to train and remind employees of corporate policy. The violation is logged for the Vericept Reviewer.
- ▶ **Protect Encryption** automatically encrypts the email without any user interaction and without impeding the flow of business. Protect's encryption is a cost-effective way for an enterprise to encrypt all sensitive information (PII, CCN, etc.) that must be protected in transit.

Vericept Monitor provides blocking of HTTP, HTTPS, and FTP traffic that is sent to it via ICAP from a proxy server.

- ▶ **Monitor Content Aware Blocking (CAB)** looks at the content of ICAP traffic and sends a message to the proxy server to block any violations of policy. A notification is sent to the sender that the message has been blocked. This content aware and blocking capability extends to all web-mail protocols and attachments that are using Port 80 as a channel.

Monitor's blocking capability extends to SSL/TLS traffic. The proxy server decrypts the encrypted tunnel, and sends the traffic to Monitor – CAB for analysis and action. The sender is notified if the traffic is blocked. Encrypted traffic evaluation can be restricted to specific reviewers through permissions set by administrators.



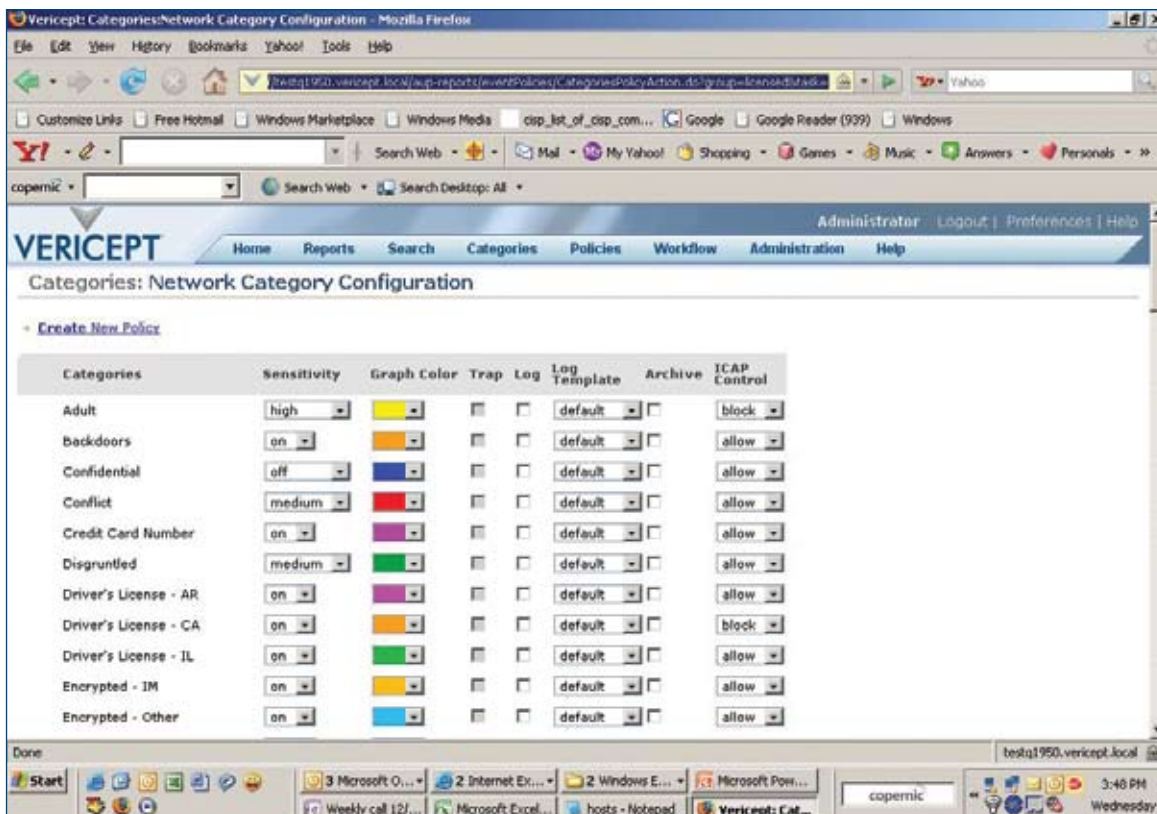
Vericept Monitor's powerful reporting tools enable you to pinpoint trends, identify top offenders, and assign severity levels to each threat

Vericept Edge controls information leakage on desktops and at endpoints.

- ▶ **Edge Content Visibility** uses a client to scan for sensitive files by performing a complete scan when the client is loaded onto a system and subsequently incrementally monitors any files created, edited, or deleted. System-based policies allow monitoring of individual groups of users for specific categories of sensitive data that pose the greatest risk to information loss.
- ▶ **Edge Device Control** prevents data leakage via removable media and drives. With device visibility, Edge captures information on device type, vendor ID, product ID, serial number, and blocking actions. System and policy administrators can report on device usage to understand where corporate policies are being violated and assess the associated risks. Device control policies are used to block specific users' access to removable drives (such as USB drives) and removable media (such as CDs, DVDs, and floppies).

Policies can be configured as combinations of restrictions and allow access to media and drives by groups of systems, individual users, or Active Directory groups. This gives policy makers flexibility in enforcing corporate controls on device usage while allowing access to privileged users to maximize efficiency and productivity. Device control also prevents data loss resulting from lost or stolen USB drives. For those users who are permitted USB access, drive usage is restricted by vendor ID and product ID, thereby permitting only corporate-approved and encrypted USB drives.

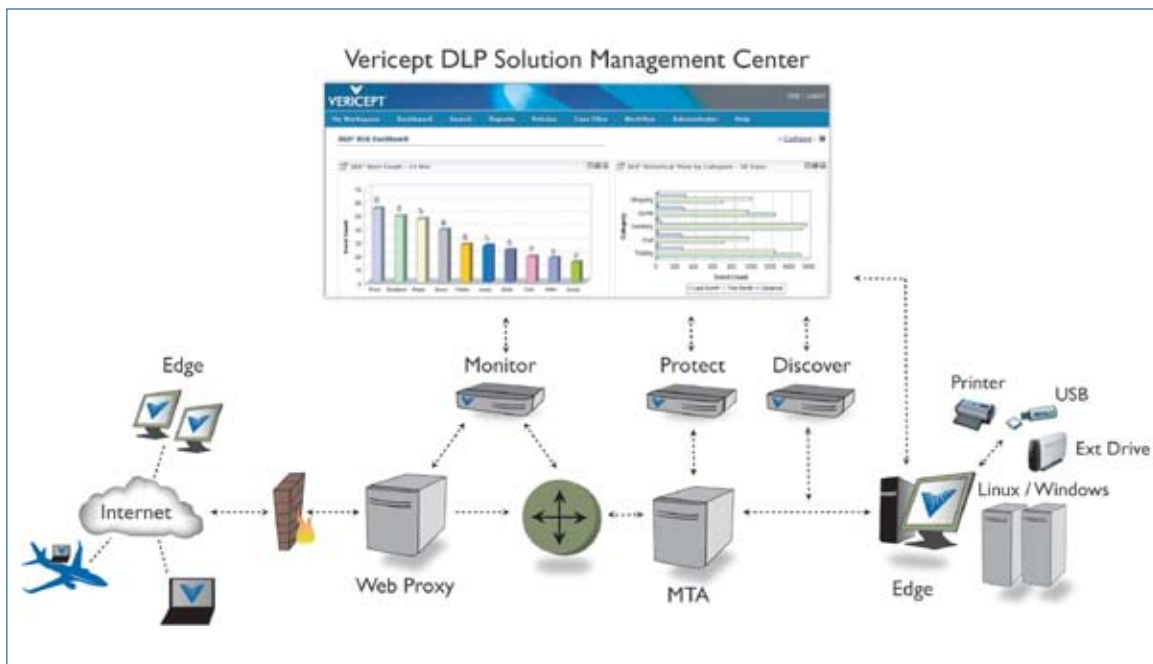
- ▶ **Edge Content Control** empowers enforcement of content security through policy actions triggered in real time when files are opened, saved, or copied by using the same highly accurate detection methods as Monitor.



Vericept Monitor includes 70 standard categories, but also enables you to configure custom categories to find and protect your unique content

Why Vericept?

Vericept Corporation is the leading provider of comprehensive compliance and data loss prevention solutions. Vericept mitigates internal risk by providing enterprise-wide discovery, classification and loss prevention of the information exchanged inside and outside an organization. Vericept's patented classification suite delivers the highest degree of accuracy and the lowest instance of false positive events available in the marketplace. Only Vericept offers comprehensive solutions for data at rest, data in motion, and data in use at the endpoint, with visibility into and control of sensitive data across all forms of traffic, including email, webmail, IM, P2P, and FTP. Vericept's technology is deployed in 800+ organizations worldwide and protects billions of pieces of communication every day.



Contact us to learn more about the Vericept Platform at 800-262-0274 or email us at info@vericept.com.

Copyright © 2008 Vericept Corporation. Vericept, Vericept Monitor, Vericept Protect, Vericept Discover, Vericept Edge and Vericept Management Console are all trademarks of Vericept Corporation. All rights reserved.



Reservoir Place
1601 Trapelo Road, Suite 140
Waltham, MA 02451

555 Seventeenth Street
Suite 1500
Denver, CO 80202

800.262.0274
www.vericept.com