Ethical Hacking and Countermeasures

Version 6

Module LV

Preventing Data Loss

Associated Press

Go to Google News

Data Lost on 650,000 Credit Card Holders

By DAVID KOENIG – **Jan 17, 2008**

PLANO, Texas (AP) — Personal information on about 650,000 customers of J.C. Penney and up to 100 other retailers could be compromised after a computer tape went missing. GE Money, which handles credit card operations for Penney and many other retailers, said Thursday night that the missing information includes Social Security numbers for about 150,000 people.

The information was on a backup computer tape that was discovered missing last October. It was being stored at a warehouse run by Iron Mountain Inc., a data storage company, and was never checked out but can't be found either, said Richard C. Jones, a spokesman for GE Money, part of General Electric Capital Corp.

Jones said there was "no indication of theft or anything of that sort," and no evidence of fraudulent activity on the accounts involved.

Iron Mountain spokesman Dan O'Neill said it would take specialized skills for someone to glean the personal data from the tape. He said the company regretted losing the tape, "but because of the volume of information we handle and the fact people are involved, we have occasionally made mistakes."

Penney said it had been told of the situation and referred further inquiries to GE Money.

Jones declined to identify the other retailers whose customers' information is missing but said "it includes many of the large retail organizations."

Jones said GE Money was paying for 12 months of credit-monitoring service for customers whose Social Security numbers were on the tape.

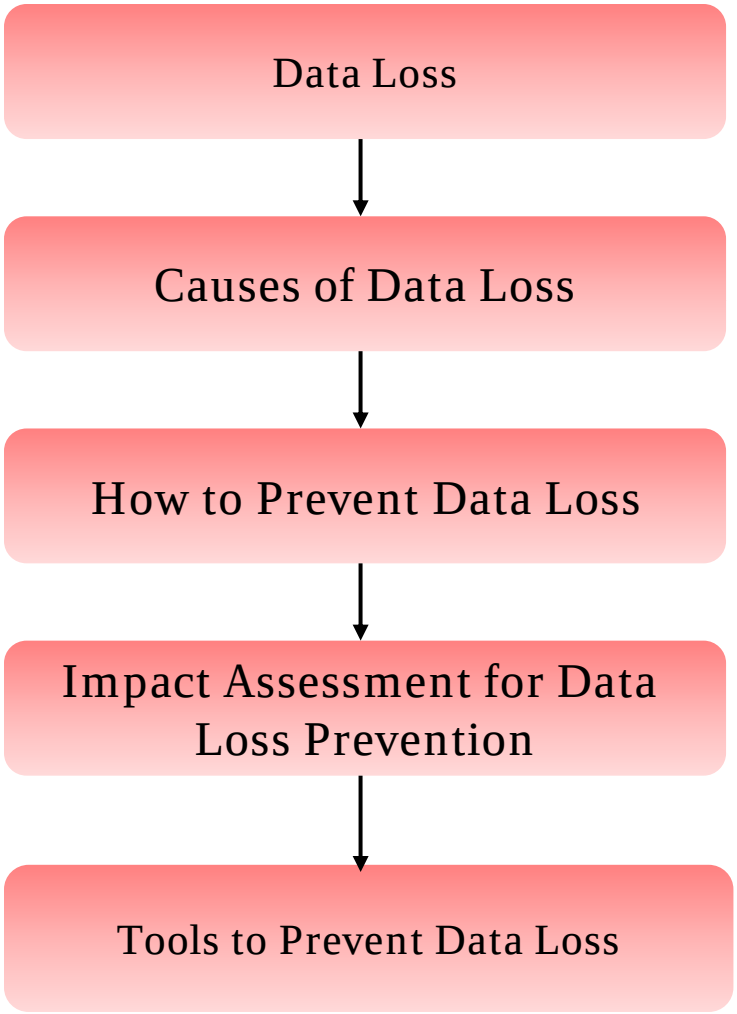
Source: *http://ap.google.com/*

Module Objective

This module will familiarize you with:

- Data Loss
- Causes of Data Loss
- How to Prevent Data Loss
- Impact Assessment for Data Loss Prevention
- Tools to Prevent Data Loss

Module Flow



Introduction: Data Loss

Data loss refers to the unexpected loss of data or information

Backup and recovery schemes must be developed to restore lost data

Causes of Data Loss

Intentional Action

- Intentional deletion of a file or program

Unintentional Action

- Accidental deletion of a file or program
- Misplacement of CDs or floppies
- Administration errors

Failure

- Power failure, resulting in data not being saved to permanent memory
- Hardware failure, such as a head crash in a hard disk
- A software crash or freeze, resulting in data not being saved
- Software bugs or poor usability, such as not confirming a file delete command
- Data corruption, such as filesystem corruption or database corruption

Causes of Data Loss (cont'd)

Disaster

- Natural disaster, earthquake, flood, tornado, etc.
- Fire

Crime

- Theft, hacking, sabotage, etc.
- A malicious act, such as a worm, virus, hacker, or theft of physical media

How to Prevent Data Loss

Tips to prevent Data loss:

- **Back-up critical files:** Backup regularly using windows in-built backup utilities or use any backup tool
- **Run Anti-Virus Program:** Install Anti-Virus Software and run them regularly to cleanup your Computer System from Viruses & Trojans
- **Use power surge protectors:** A power surge, is one of the most common occurrences that can damage data and potentially cause a hard drive failure
- **Experience required:** Never attempt any operation, like hard drive installations or hard drive repairs, if you do not have such skills
- **Shut down your computer:** Always quit programs before shutting down the computer
- **Never shake or remove the covers on hard drives or tapes**
- **Store your backup data offsite:** Use Tape Drives, Compact Disk(CD),and Floppy Drives to Store your backups
- **Be aware of your surroundings:** Keep your computers and servers in safest and secure locations

Impact Assessment for Data Loss Prevention

Impact Assessment: Data Loss Prevention

	Primary benefits	Primary concerns	Nice to have: 1 Must have: 5
Encryption	Not only is encryption the most commonsense way to protect data, especially for mobile devices, it also can help avoid penalties under some data privacy laws.	Managing keys across disparate systems remains a challenge. Universal encryption is difficult, and simply keeping everything under noninteroperable lock and key ends up impeding business.	●●●●●
Database extrusion prevention	Most critical data is already located in one place: your databases. Protecting them gets a lot of bang for the buck.	While most data is in databases, large quantities often reside unprotected on backup systems, test servers, and other places.	○○●●●
Network DLP	Network solutions are usually simpler to deploy than alternatives and can be useful from an auditing perspective.	These approaches have the same problems as conventional network analysis. They're susceptible to spoofing and evasion, and aren't as effective at catching insiders leaking data compared with endpoint products.	○●●●●
Access control (IAM, entitlement, EDRM)	IAM and EDRM make sense in locations where all systems and technologies are supported.	Requiring every system to support the same enterprise DRM might be an even bigger pipe dream than universal encryption.	○○○●●
Endpoint DLP	More versatile than a network-based DLP system, endpoint systems can restrict USB drives, are more effective at detecting data before it's compressed or encrypted by a malicious insider, and keep protecting even after a laptop walks out.	Yet another client to manage on endpoints, and more difficult to deploy than network-based DLP approaches.	○●●●●

Tools to Prevent Data Loss

Security Platform

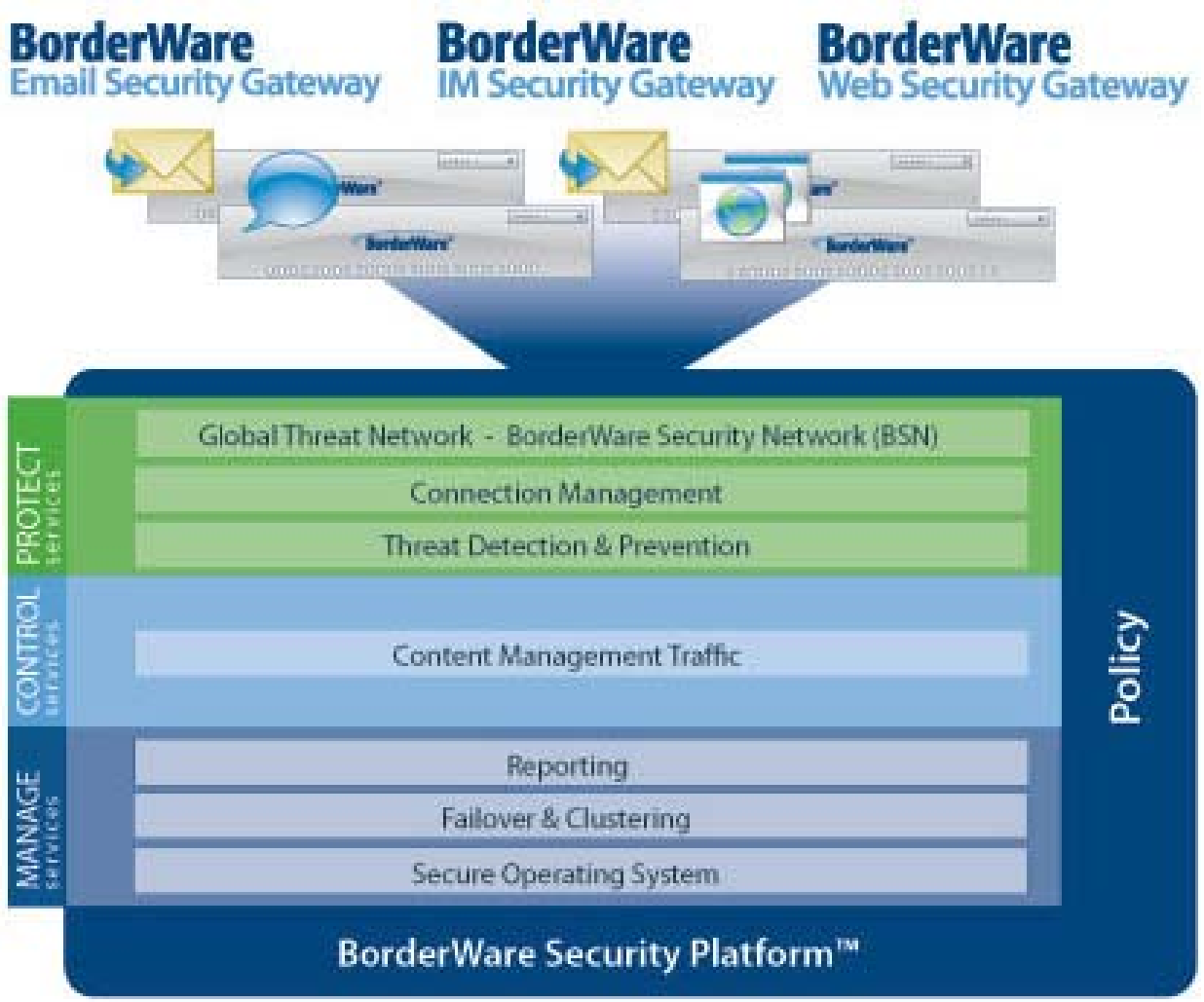
BorderWare Security Platform removes the need to deploy a new device to protect against new messaging applications by integrating Email, IM, and Web security with a single policy and single security platform

It is a content monitoring and filtering tool which prevents data leakage

Benefits:

- Consolidated content monitoring and filtering to prevent data leakage
- Comprehensive, stronger security for Email, IM, and Web
- Reduced time, effort, and costs with a set-and-forget policy management approach
- On-demand scalability and flexible deployment
- Modular approach enables enterprises to buy what they need now and add on later

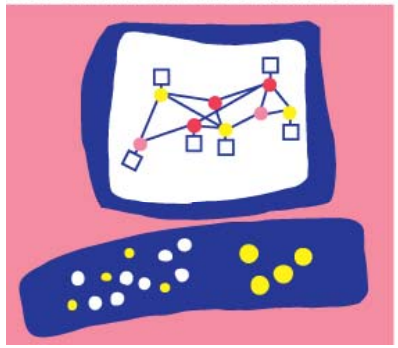
Security Platform: Screenshot



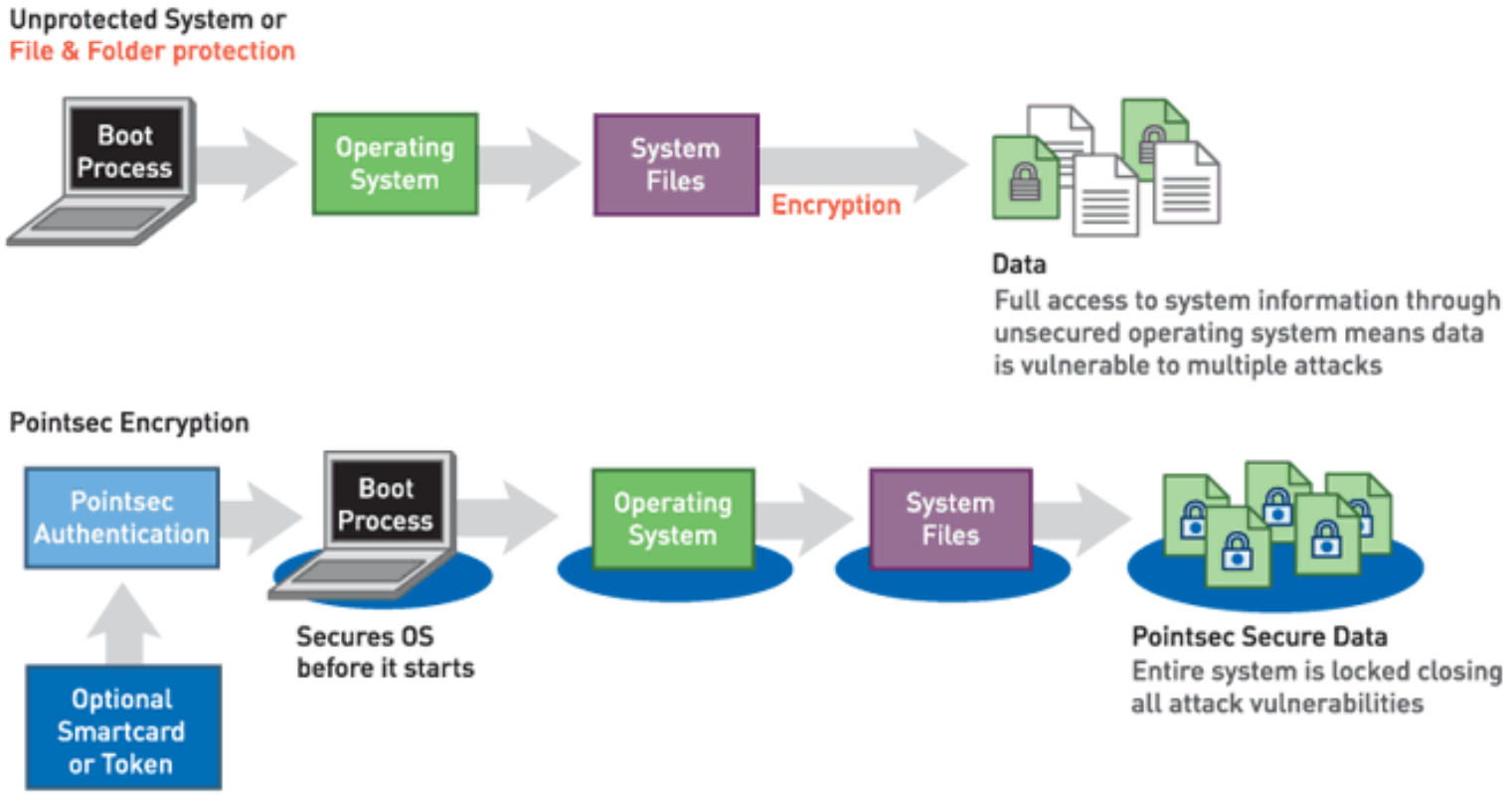
Check Point Software: Pointsec Data Security

Pointsec data encryption solutions by Check Point provide data protection on laptops, PCs, mobile devices, and removable media

By leveraging a strong and efficient blend of full disk encryption, access control, port management and removable media encryption, it delivers a comprehensive data security



Pointsec Data Security: Screenshot



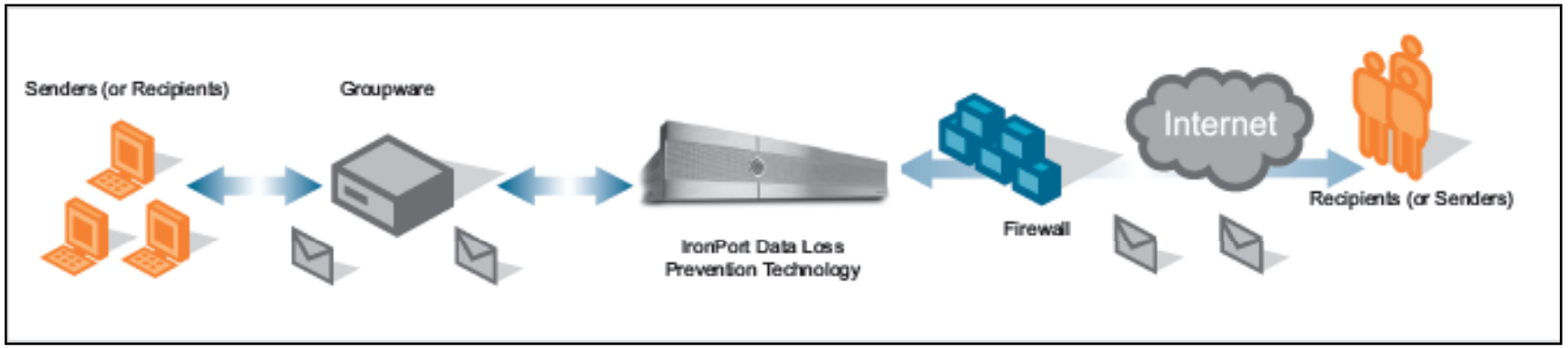
Cisco (IronPort)

IronPort delivers high-performance and comprehensive data loss prevention for data in motion

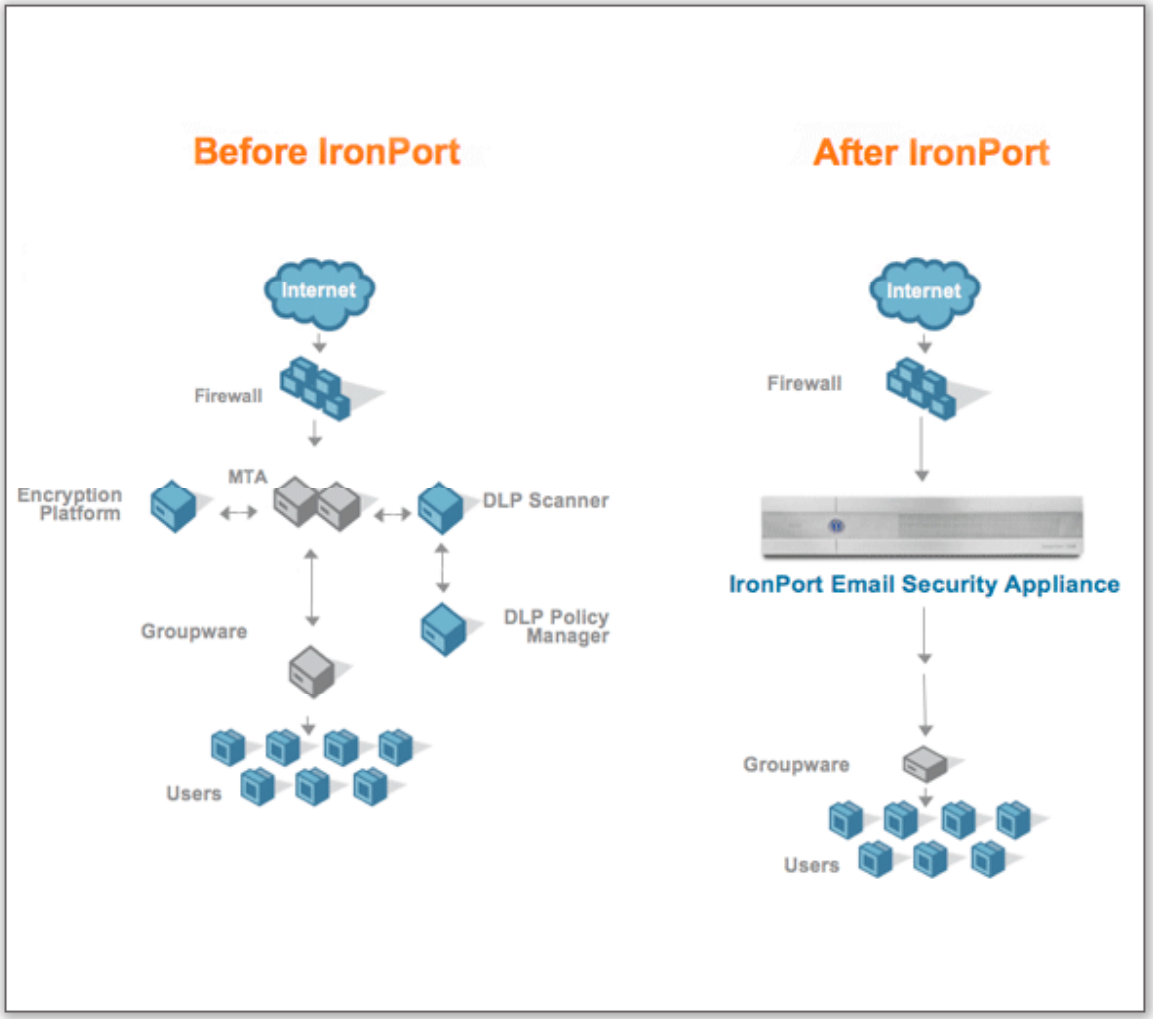
It helps organizations to prevent data leaks, enforce compliance, and protect their brand and reputation

Features:

- Web and Instant Messaging Protection
- Email Encryption



Cisco (IronPort): Screenshot



Content Inspection Appliance

The Code Green Network's line of Content Inspection Appliances is a solution for protecting customer data and safeguarding intellectual property

It provides a complete solution for preventing the loss of personal information across the network

Features:

- Monitors, enforces, and audits all popular Internet communication channels including email, WebMail, IM, FTP, and online collaboration tools (such as Blogs and Wikis)
- Automatically encrypts sensitive email messages according to policy
- Deploys quickly with pre-defined policy templates
- Demonstrates and manages compliance using policy and incident management capabilities

CrossRoads Systems: DBProtector

It provides database security at a logical business policy level and stops 'authorized misuse' of database information

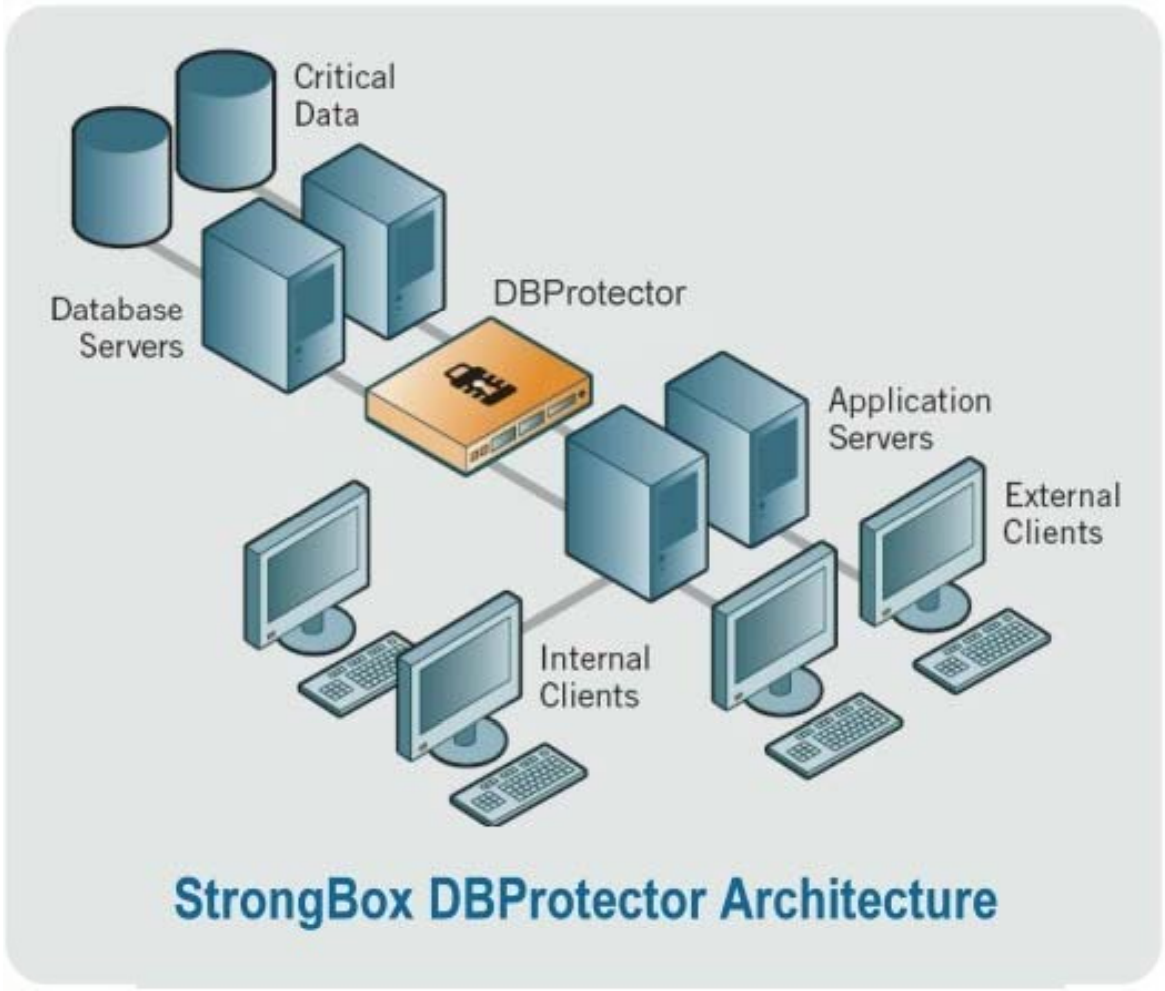
DBProtector provides policy-based intrusion detection, prevention, and compliance auditing

DBProtector sits in the data path and inspects SQL statements before they reach the database

Features:

- Inspects database activities
- Enforces security policies
- Alerts on suspicious activities
- Captures audit trails for compliance reporting, security forensics, and electronic discovery
- Provides separation of duty between security personnel and database/network administrators ensuring regulatory compliance

Strongbox DBProtector Architecture



DeviceWall

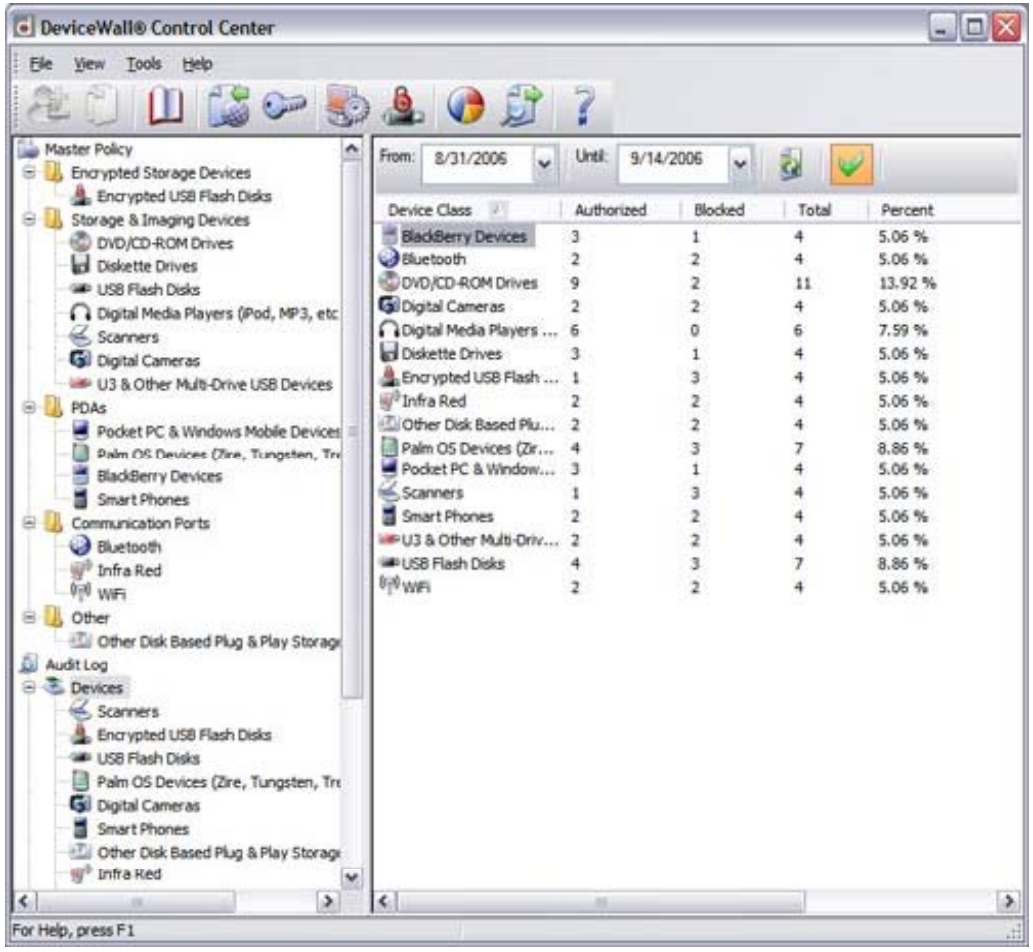
DeviceWall protects data, both on and off the network, by:

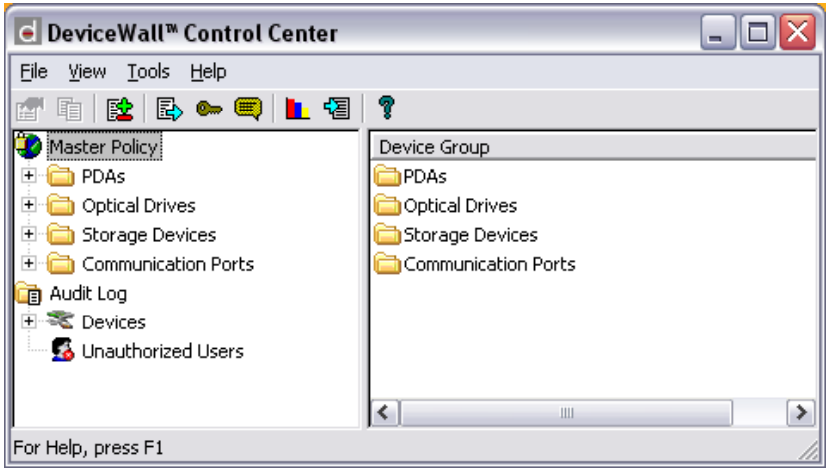
- Preventing the transfer of files to or from unauthorized portable devices
- Automatically encrypting data copied to approved devices
- Providing complete audit trails of device and file accesses

DeviceWall prevents unwanted data transfer to or from portable devices such as USB flash drives, iPods, PDAs, and wireless connections by automatically enforcing security policies

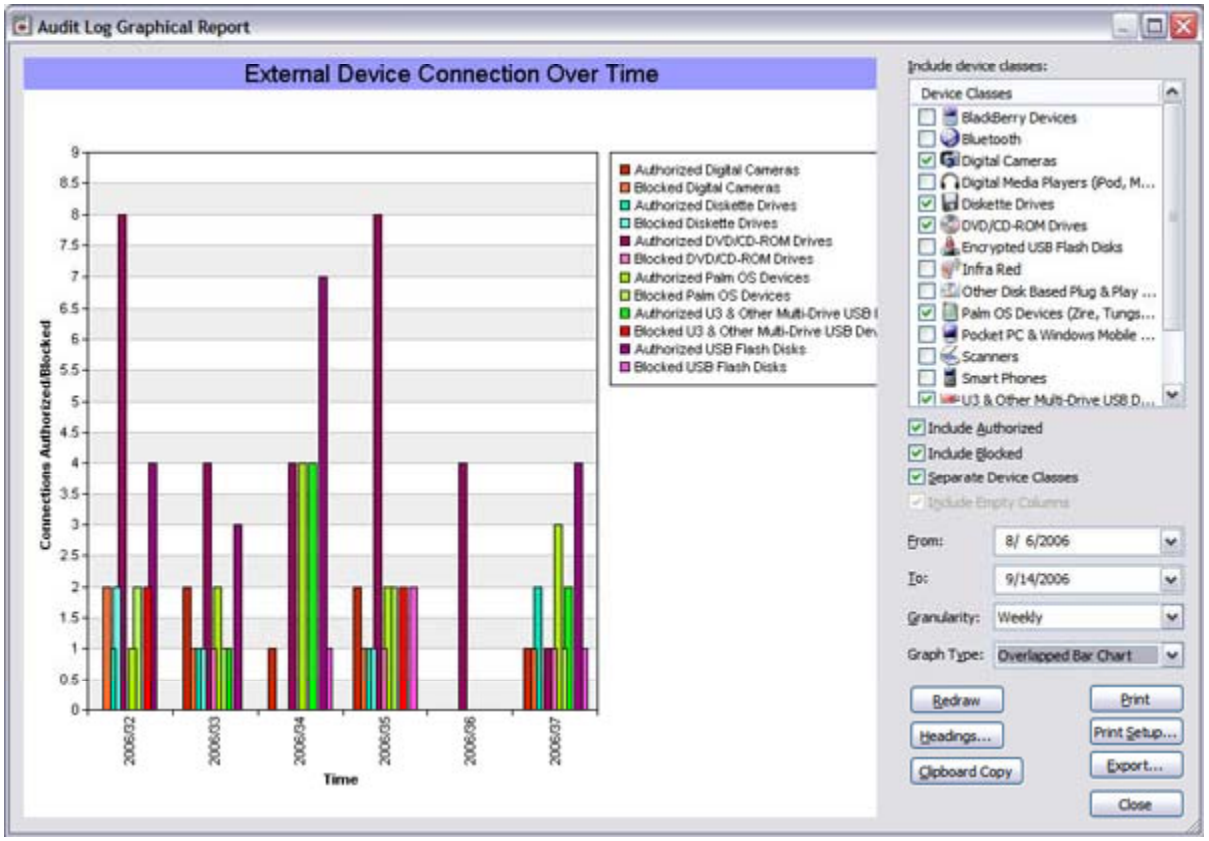
User access can be blocked, limited to read-only, or left unrestricted according to individual's security privileges and device type in use

DeviceWall: Screenshot





DeviceWall: Reporting



Exeros Discovery

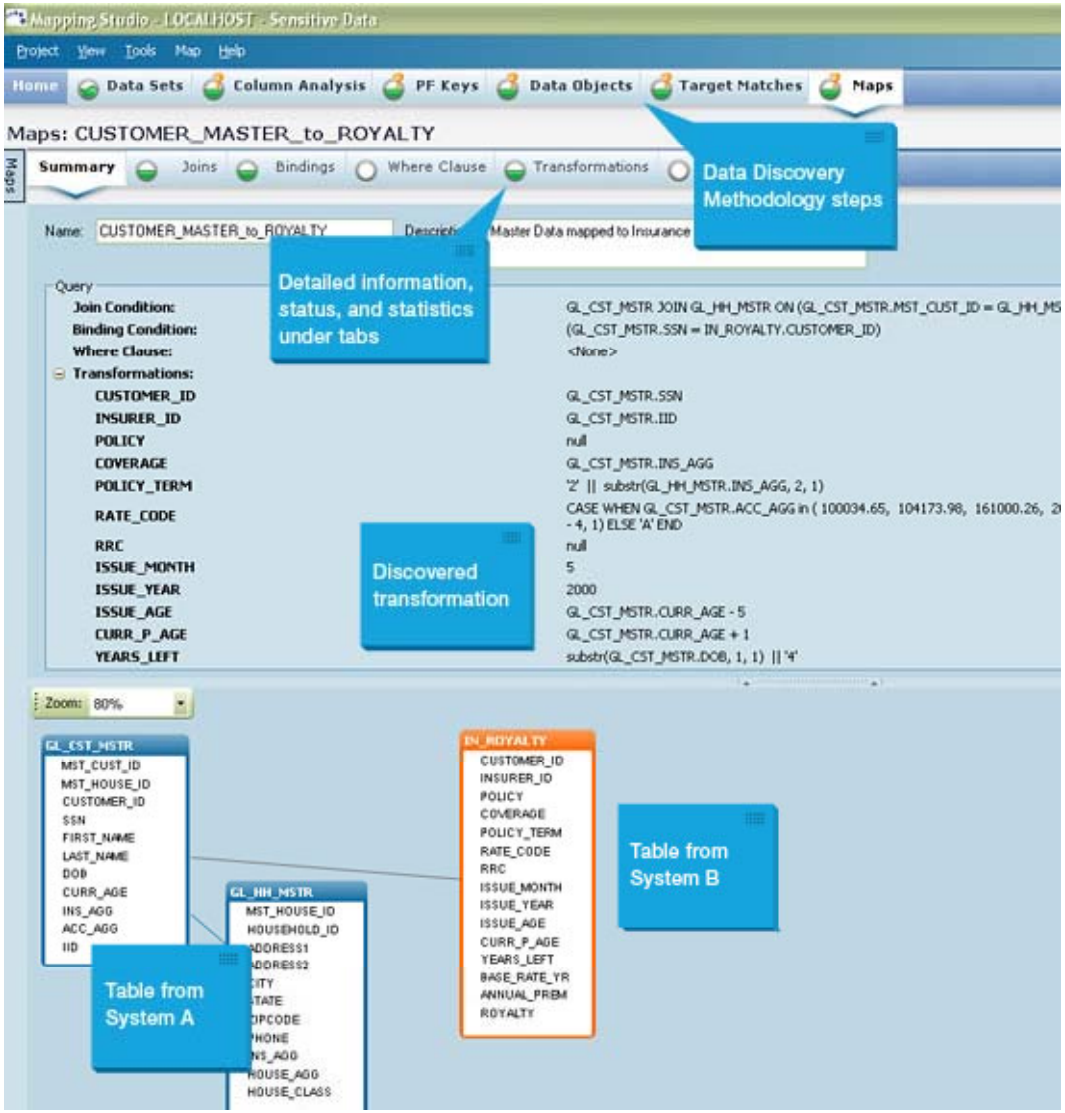
Exeros Discovery software automates discovery and maintenance of business rules, transformations, hidden sensitive data, and data inconsistencies across structured data sources

It uses a unique technology of data-driven mapping to replace the traditional manual process of analyzing source data and mapping it to another data set

Exeros Discovery has two main components:

- Discovery Studio: A graphical user interface for data analyst to view data, maps, and transformations discovered by Discovery and to edit, test, and approve any remaining data maps and business rules
- Discovery Engine: Multiple, scalable, and high-performance engines that automatically discover business rules, transformations, sensitive data, and data inconsistencies

Exeros Discovery: Screenshot



GFi Software: GFiEndPointSecurity

GFiEndPointSecurity prevents data leakage/theft by controlling access to portable storage devices with minimal administrative effort

It prevents introduction of malware and unauthorized software on the network

It gives administrators greater control by allowing to block devices by class, file extensions, physical port or device ID

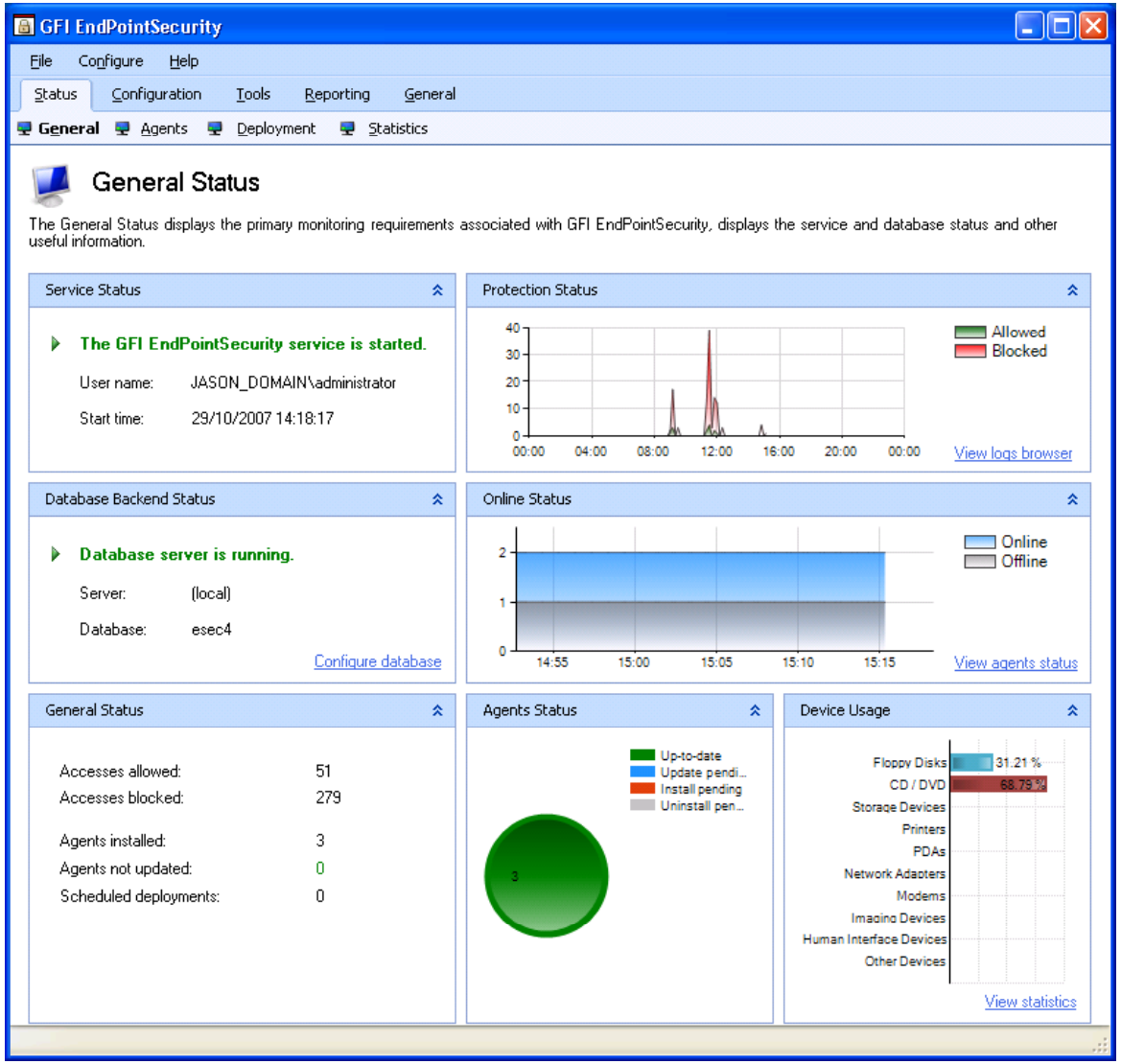
It allows administrators to grant temporary device or port access for a stipulated time-frame

GFi Software: GFiEndPointSecurity (cont'd)

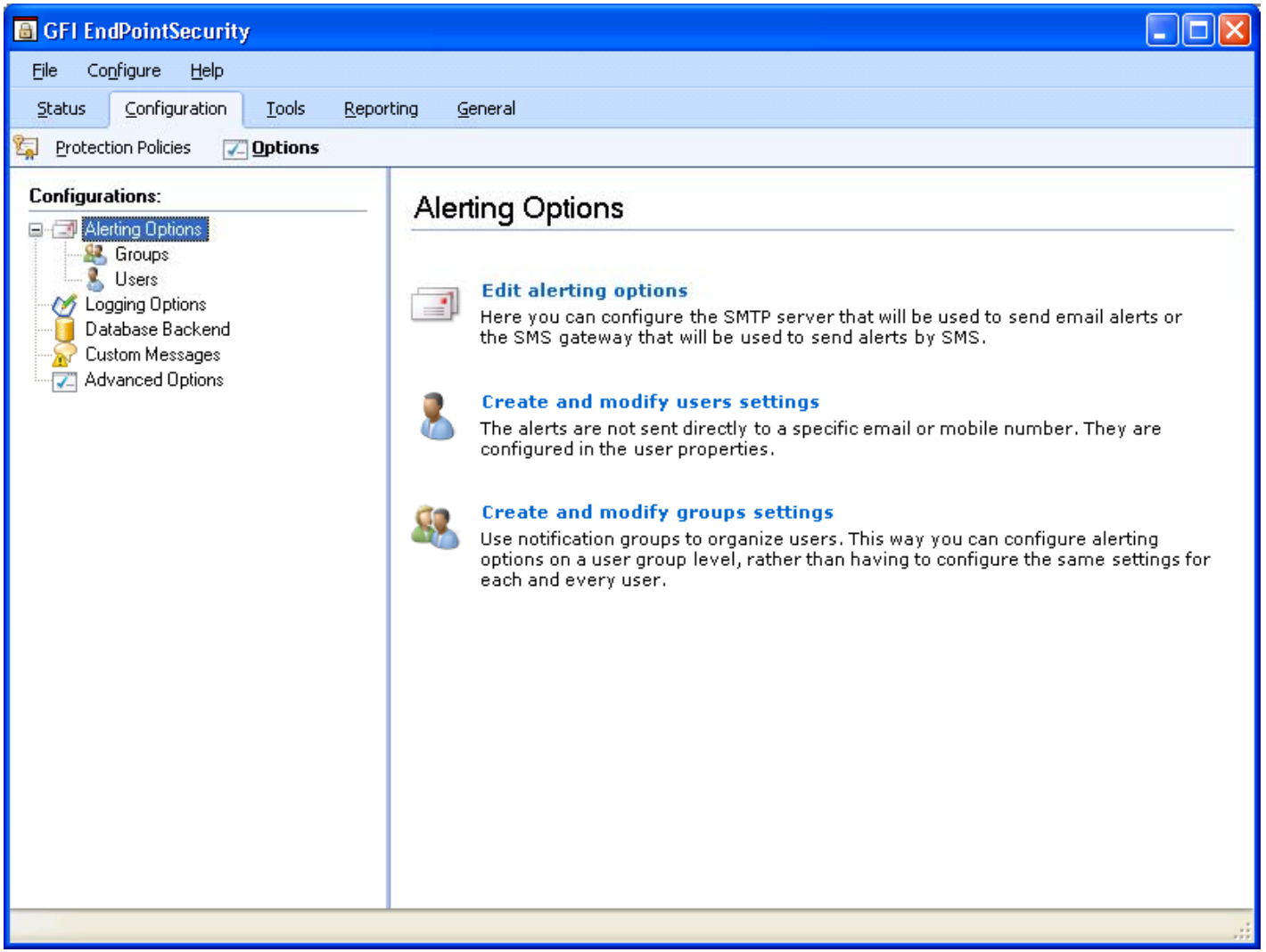
GFI EndPointSecurity allows administrators to actively manage user access and log the activity of:

- Media players, including iPods, Creative Zen, and others
- USB drives, Compact Flash, memory cards, CDs, floppies, and other portable storage devices
- PDAs, BlackBerry handhelds, mobile phones, smart phones, and similar communication devices
- Network cards, laptops, and other network connections

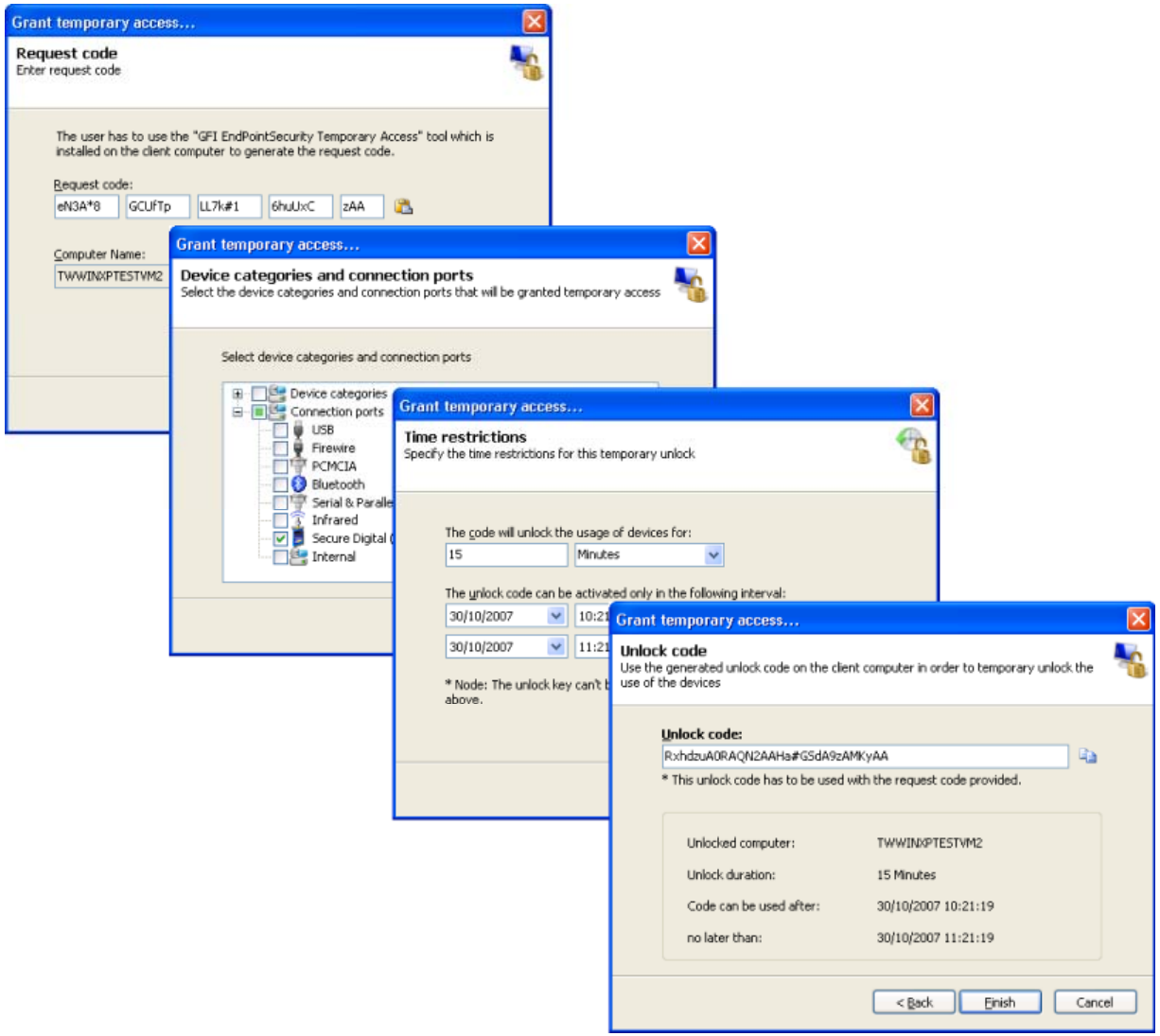
GFiEndPointSecurity: Screenshot 1



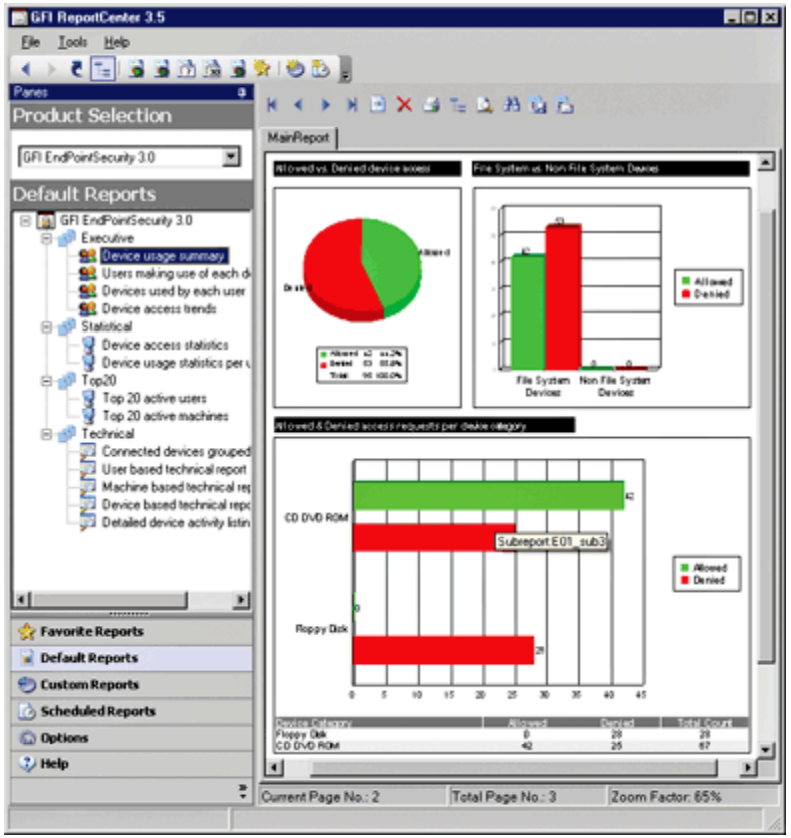
GFiEndPointSecurity: Screenshot 2

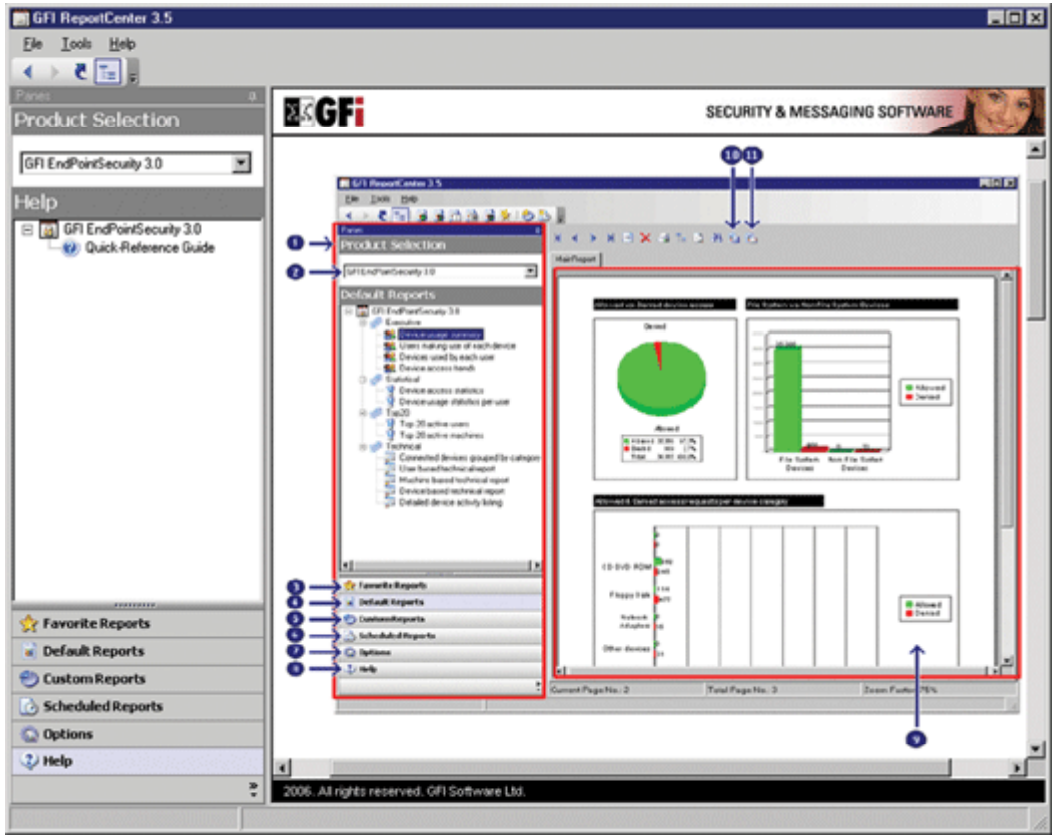


GFiEndPointSecurity: Screenshot 3



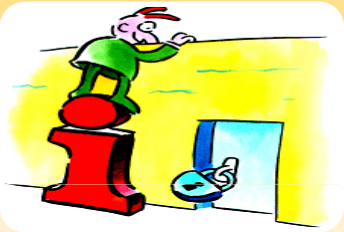
GFI EndPointSecurity ReportPack: Screenshot





GuardianEdge Data Protection Platform

GuardianEdge Data Protection Platform consists of GuardianEdge applications for hard disk encryption, removable storage encryption, and device control

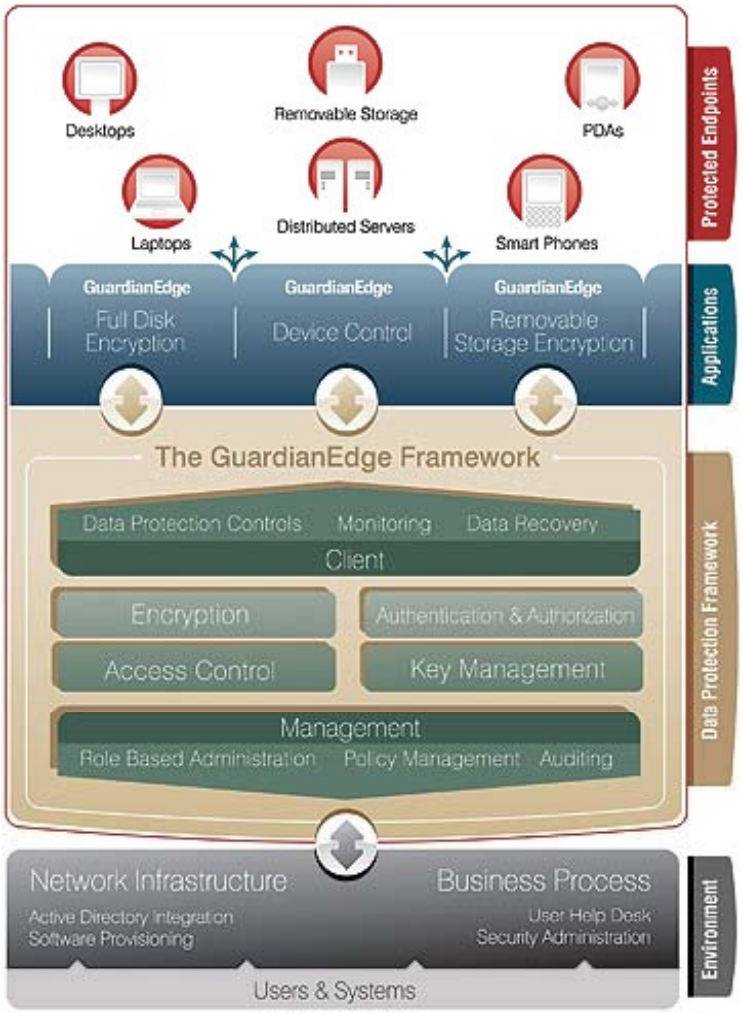


Framework also provides a common infrastructure and common administration of services

Features:

- Whole-disk encryption
- Transparent to end-users
- Enterprise-ready

GuardianEdge Data Protection Platform: Framework



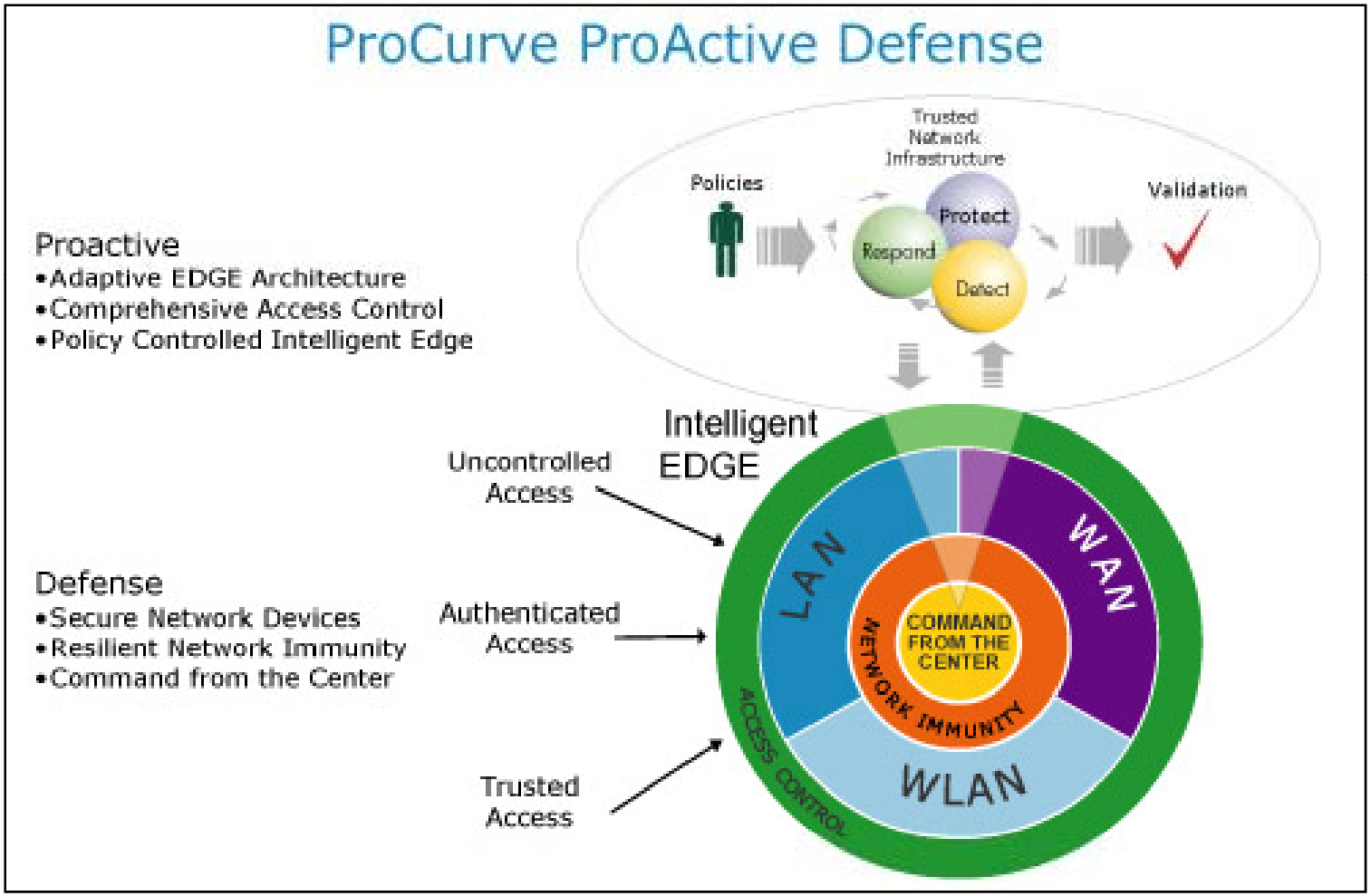
ProCurve Identity Driven Manager (IDM)

ProCurve Identity Driven Manager configures security and performance settings based on user, device, location, time, and client system state

IDM provides network administrators with the ability to centrally define and apply policy-based network access rights that allow network to automatically adapt to the needs of users and devices as they connect

It allows network administrators to efficiently manage the users and devices connecting to their network

ProCurve Identity Driven Manager (IDM): Screenshot



ProCurve Identity Driven Manager (IDM): Screenshot

Imperva: SecureSphere

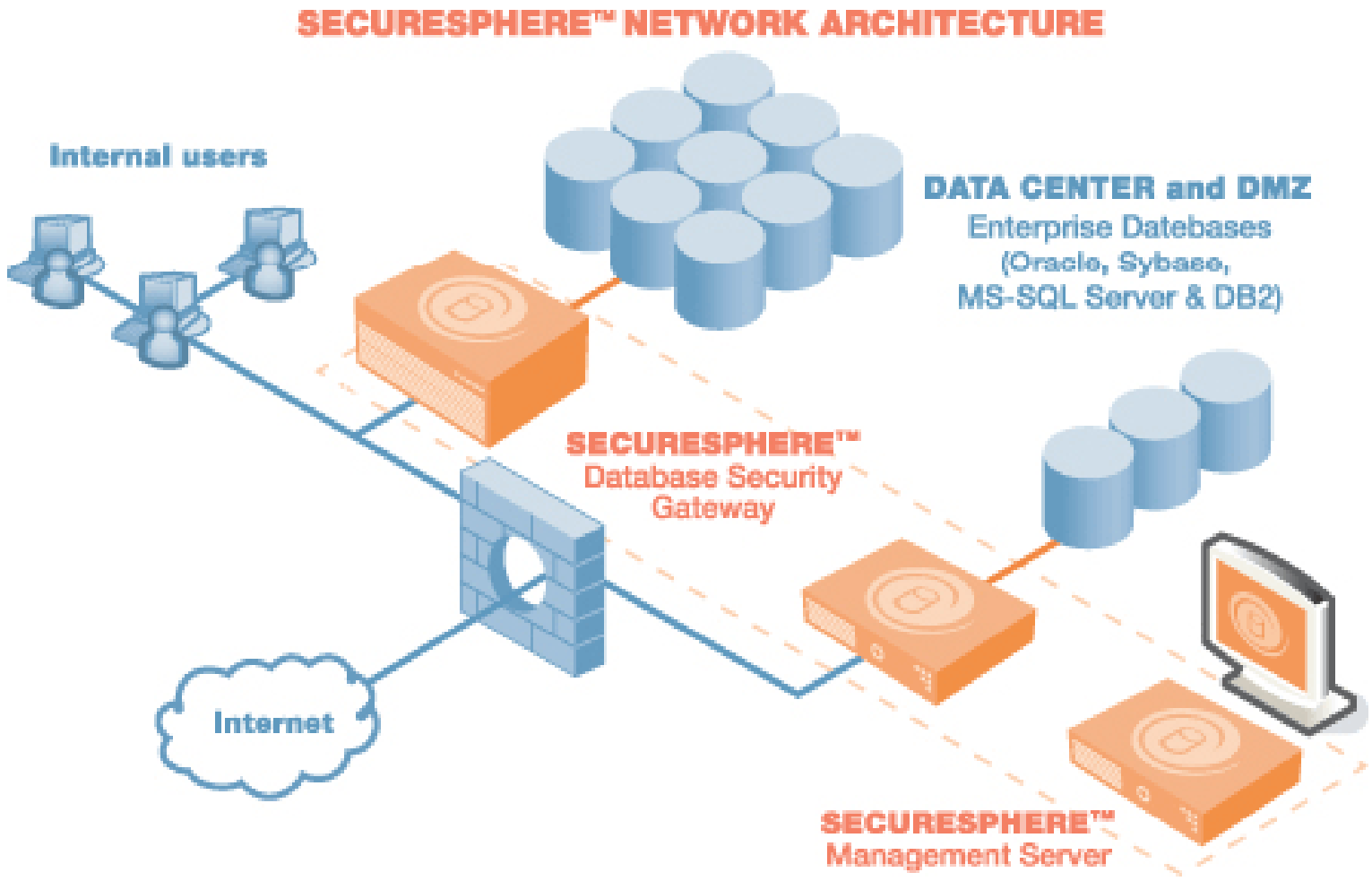
SecureSphere Database Security Gateway automates activity monitoring, auditing, and protection for Oracle, MS-SQL Server, DB2, Sybase, and Informix databases

It automatically creates database usage profiles and security policies that are granular down to the query level, for every user and application accessing the database

The following are the attacks that can be prevented:

- Unauthorized Access
- Privilege Abuse
- Data Theft
- Data Destruction
- DB platform/software attacks

SecureSphere Architecture



Marshal EndPoint

Marshal EndPoint Security solution helps to extend organization's data loss prevention strategy, by managing and controlling connection of portable media devices

Features:

- Prevention: Prevents the transfer of files to or from unauthorized portable devices
- Protection: Automatically encrypts data copied to approved devices
- Visibility: Provides complete visibility of device and file accesses on the network
- Flexibility: Provides granular control over who has access to what devices and for how long

Novell ZENworks Endpoint Security Management

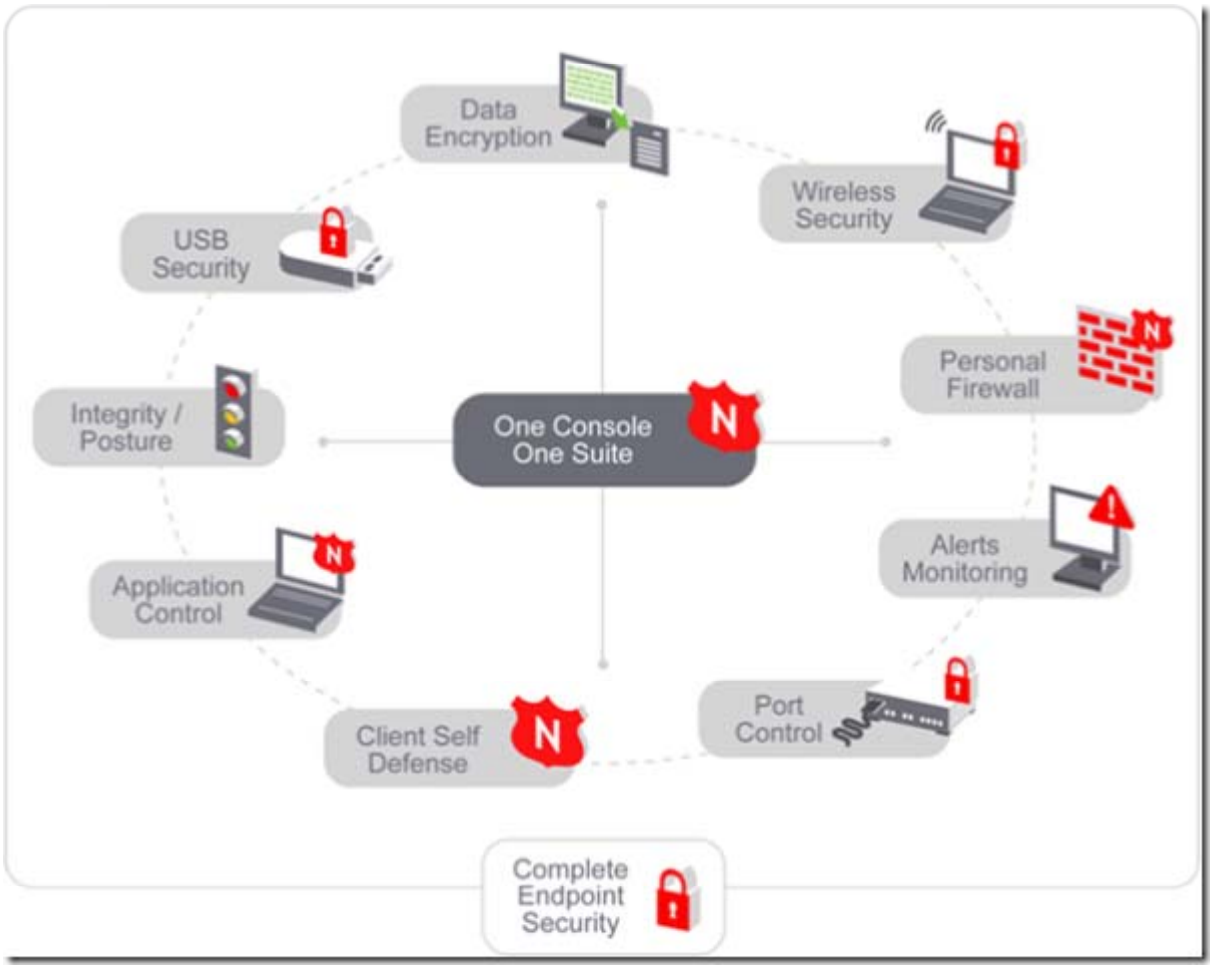
ZENworks Endpoint Security Management allows administrators to protect corporate data and assets both inside and outside the corporate security perimeter

It enforces highly customizable storage device security policies that are centrally managed, and automatically distributed to users or machines

With ZENworks Endpoint Security Management you can:

- Control usage of internal optical media and all types of removable storage devices
- Permit or block access completely or limit the device to read-only access
- Enforce permissions based on the user's location
- Control the file system, so devices that pose no security threat (such as a USB mouse) are not disabled
- Provide granular control of specific devices based on serial number
- Generate reports and alerts when allowable size thresholds have been exceeded

Novell ZENworks Endpoint Security Management (cont'd)



Novell ZENworks Endpoint Security Management (cont'd)

Prism EventTracker

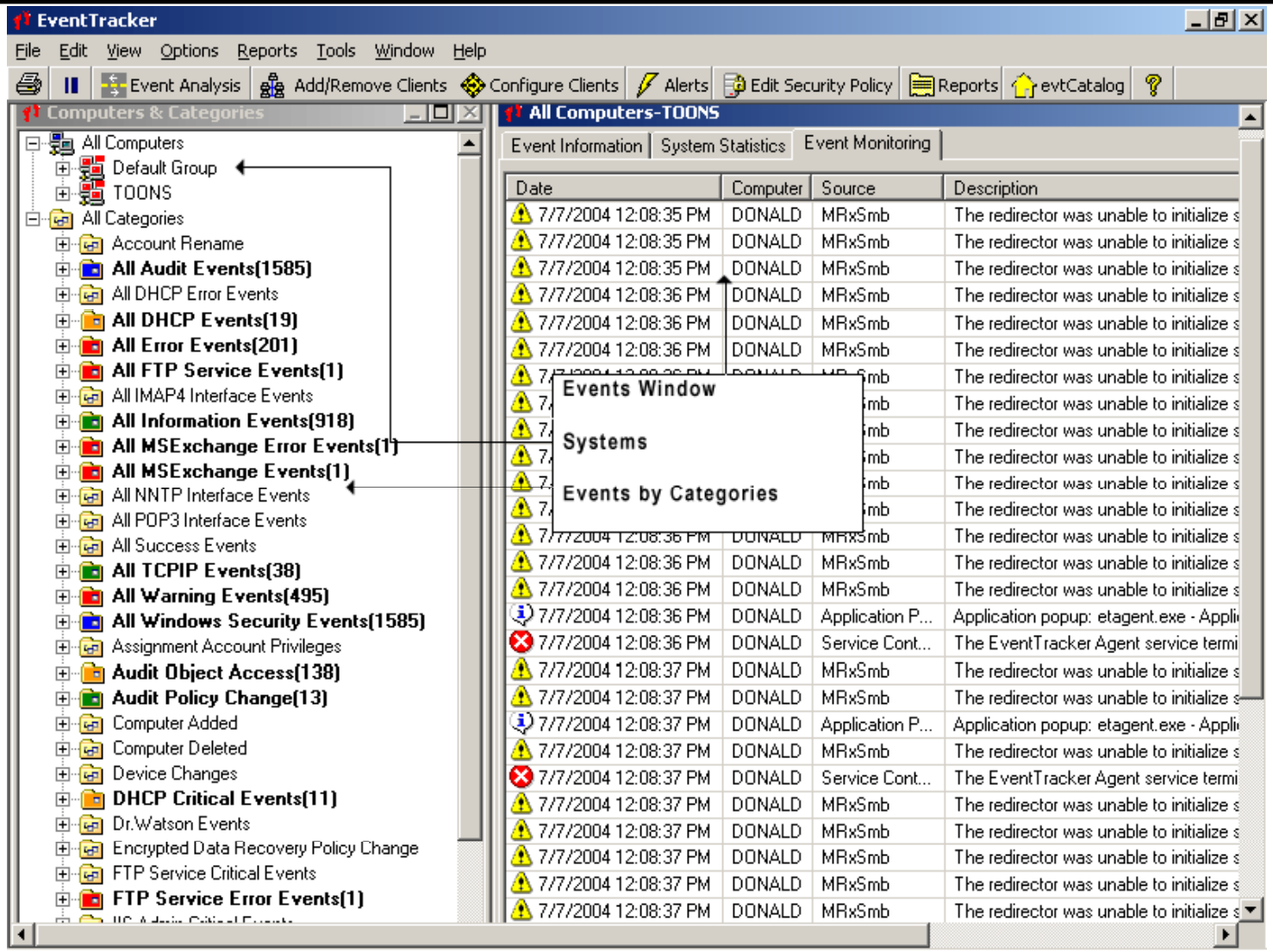
EventTracker is a solution that features real time collection of all the logs, secure, tamper-proof and encrypted log storage, and real-time log analysis, and reporting

EventTracker's built-in knowledge base enables to gather business intelligence providing increased security, performance, availability, and reliability of systems

Features:

- Collection
- Consolidation
- Storage
- Correlation
- Analysis & Reporting
- Config Control & Change Management

Prism EventTracker: Screenshot



Proofpoint Messaging Security Gateway

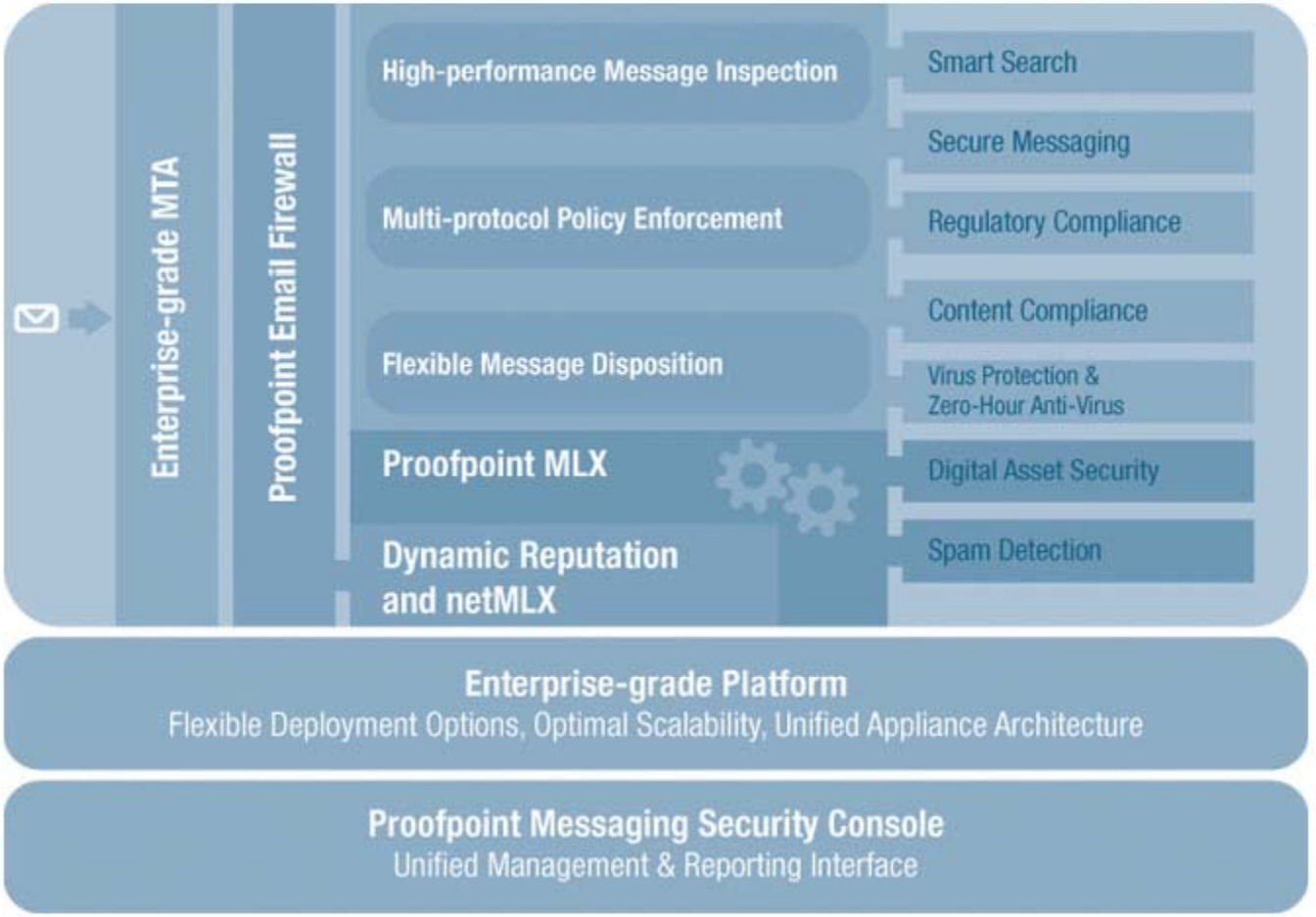
Proofpoint Messaging Security Gateway provides email security and data loss prevention

Data loss prevention platform provides comprehensive protection against both inbound threats and outbound content security risks

Features:

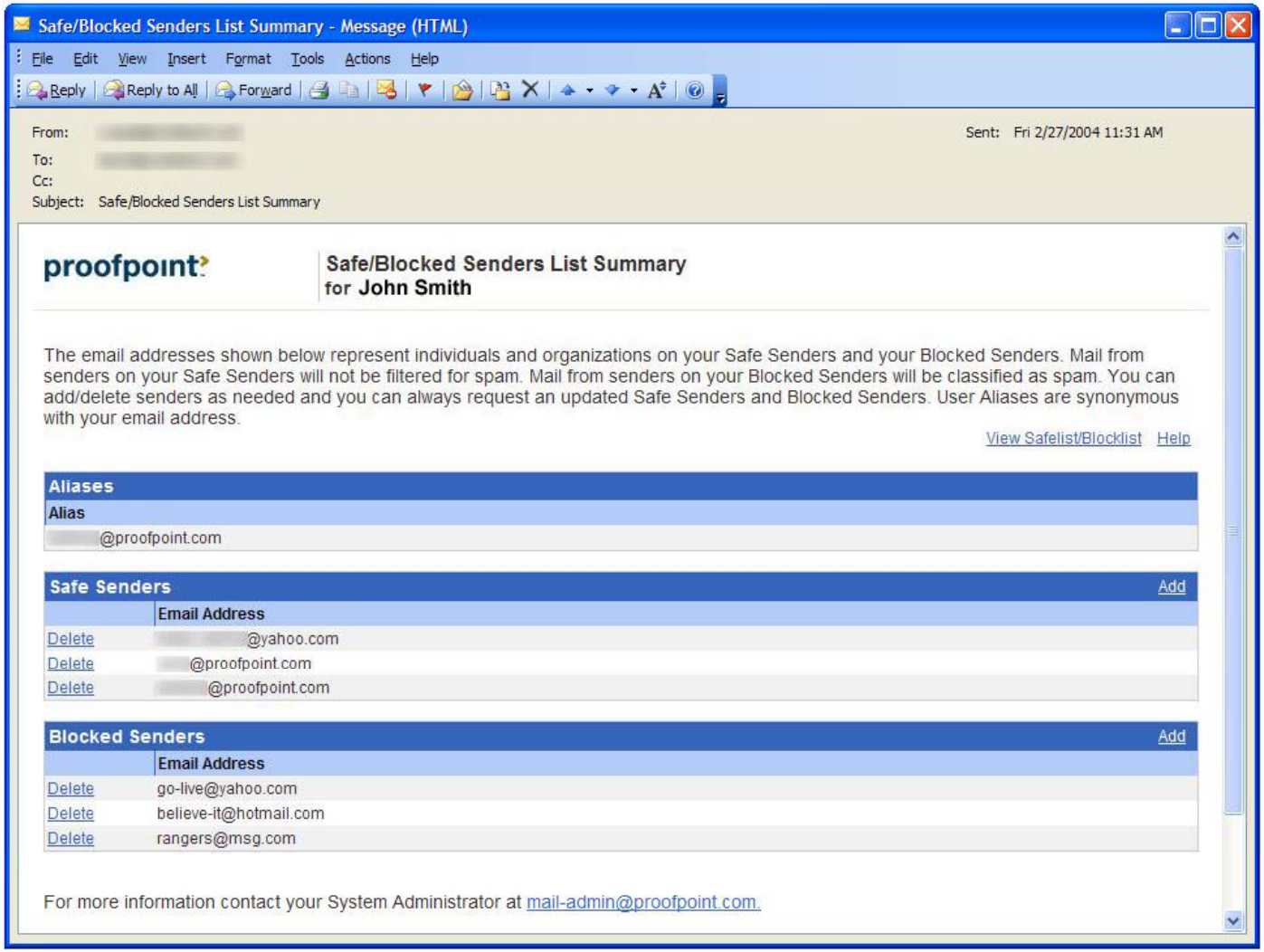
- Anti-spam, anti-virus, multi-protocol content security, policy-based encryption, and reporting features
- Integrated email firewall protection
- Virus protection and zero-hour anti-virus defenses
- Prevent leaks of information across multiple protocols

Proofpoint Platform Architecture



Summary Dashboard

End-user Safe/Block List



Defiance Data Protection System

Defiance Data Protection System (DPS) continuously safeguards sensitive information throughout its lifecycle with patented encryption and key management

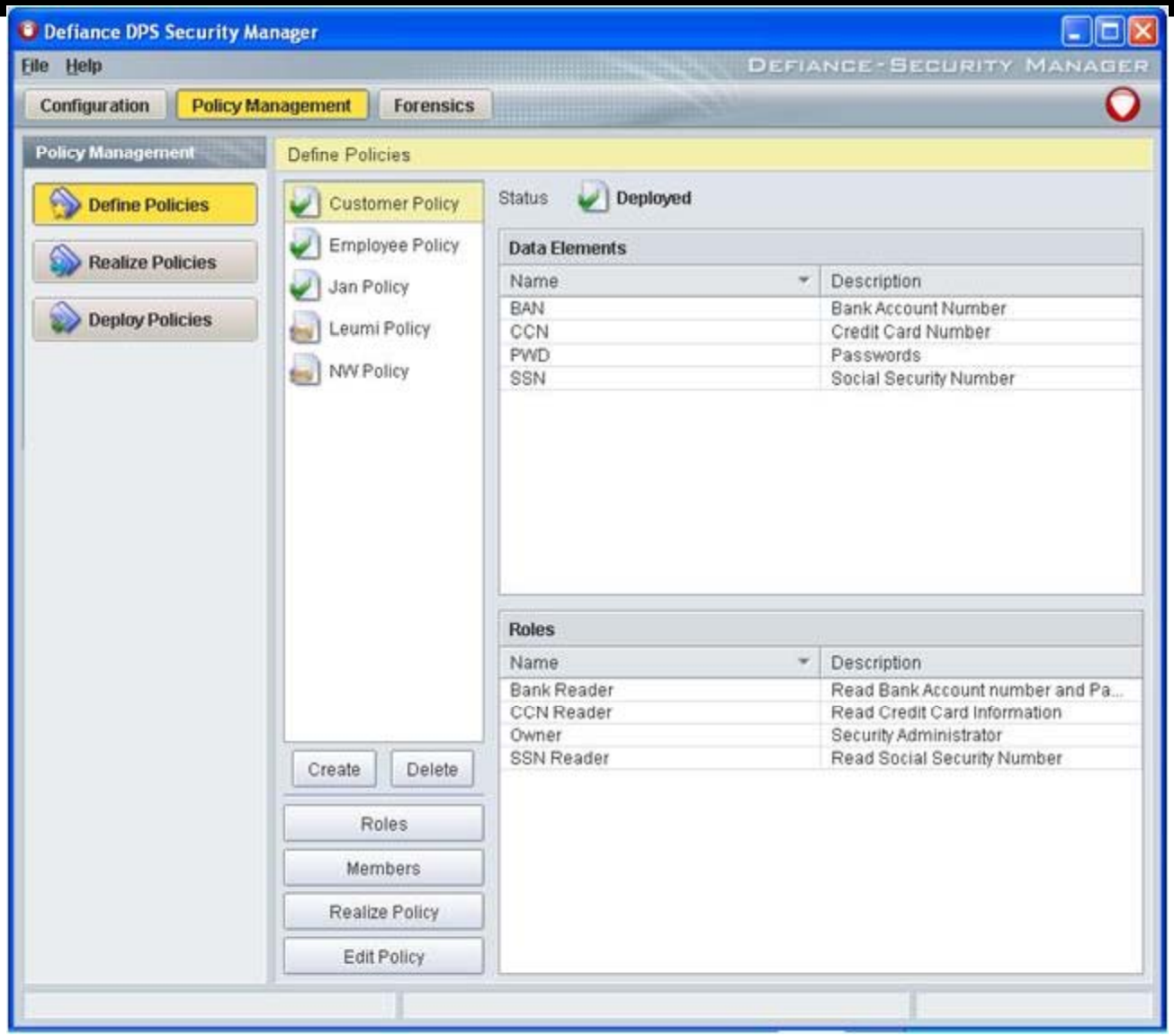
Incorporation of strong encryption algorithms like 3DES and AES ensures support of widely accepted industry standards

Patented key management delivers centralized, secure key creation, distribution, and storage

Features:

- Databases are protected by patented column-level encryption to ensure granular control over security
- File level encryption protects both structured and unstructured data wherever it may reside
- Storage of encrypted data remains protected and is easily restored when needed

Defiance Data Protection System: Screenshot



Sentrigo: Hedgehog

Hedgehog Enterprise is a database monitoring and intrusion prevention solution

It provides full visibility into all database activity and allows enterprises to enforce security policy, comply with regulatory requirements such as PCI DSS, SOX, and HIPAA

Features:

- Virtual Patching
- Prevents unauthorized sessions
- Scalable and able to centrally configure and monitor hundreds of databases
- Ability to send alerts via e-mail, and integrate with 3rd party network and security management systems via Syslog or SNMP
- Flexible, sophisticated reporting to facilitate regulatory compliance and forensics for PCI DSS, Sarbanes Oxley, HIPAA, and privacy notification laws such as CA SB 1386

Sentrigo Hedgehog: Screenshot

Symantec Database Security

Symantec Database Security (SDS) provides real-time detection of anomalous SQL activity, auditing, and Intruder Identification to help manage and control database security risks

SDS prevents fraud and leakage of sensitive data due to faulty practices and oversights, while addressing growing auditing, compliance, and regulatory requirements for secure data access

Features:

- Analyzes all data accessed from database and performs data leakage detection for unauthorized access to sensitive data
- Generates an audit trail of SQL activity on the database without any database overhead
- Analyzes all network SQL activity being sent to the database in order to detect anomalous SQL from authorized and unauthorized users alike
- Identifies end-user credentials and IP addresses that initiated a specific database transaction

Varonis: DataPrivilege

Varonis DataPrivilege makes transition possible without infrastructure changes or business disruption

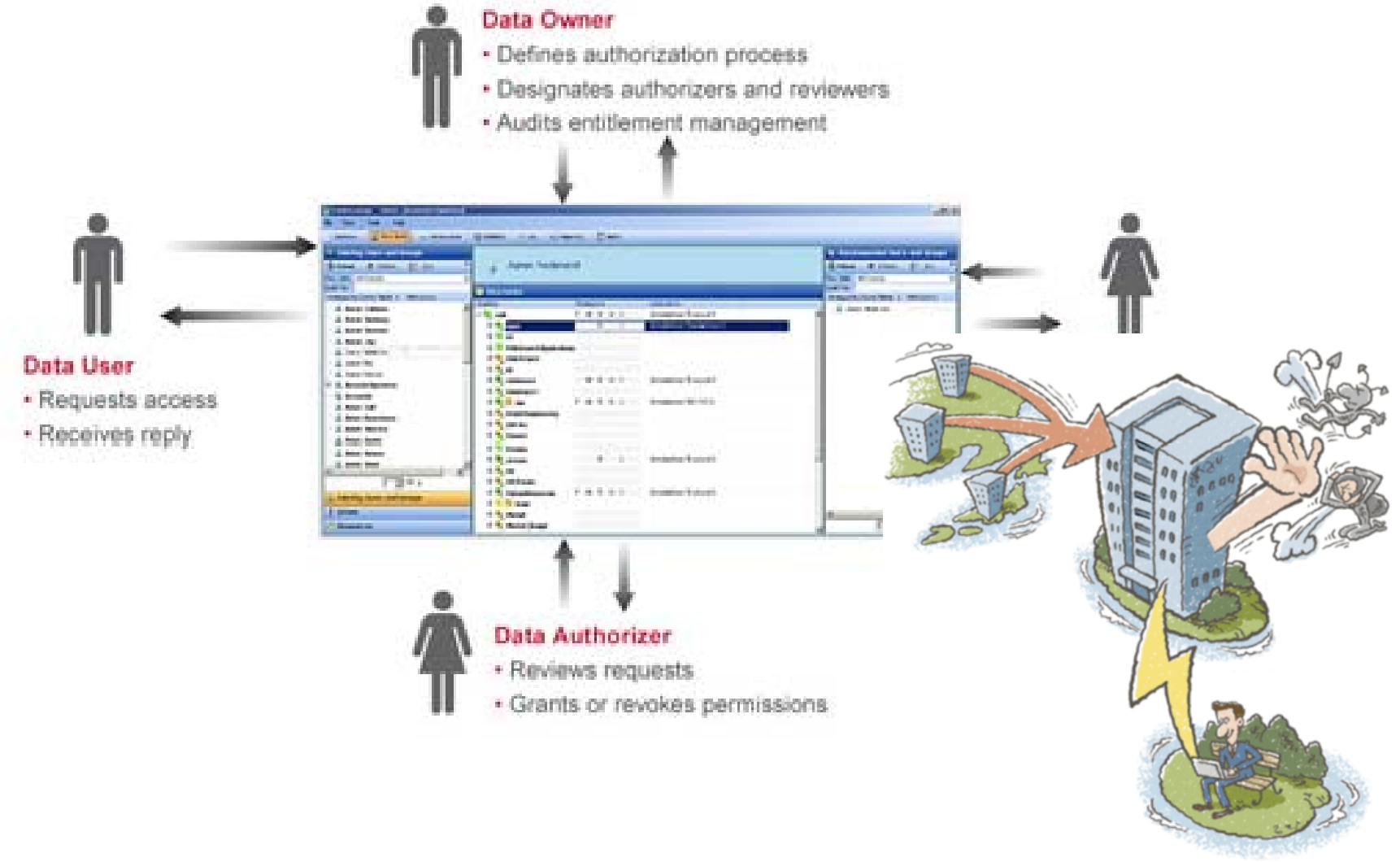
DataPrivilege brings together data owners and users in a forum for communicating, authorizing, and activating entitlements

Varonis DataPrivilege allows to implement a cohesive data entitlement environment thereby raising accountability and reducing risk

Features:

- Automated business rule to authorization policy conversion
- Multi-level permission management (i.e. authorizers, reviewers)
- Data permission authorization history & audit trail
- Synchronization with file systems and user repository

Varonis DataPrivilege: Screenshot



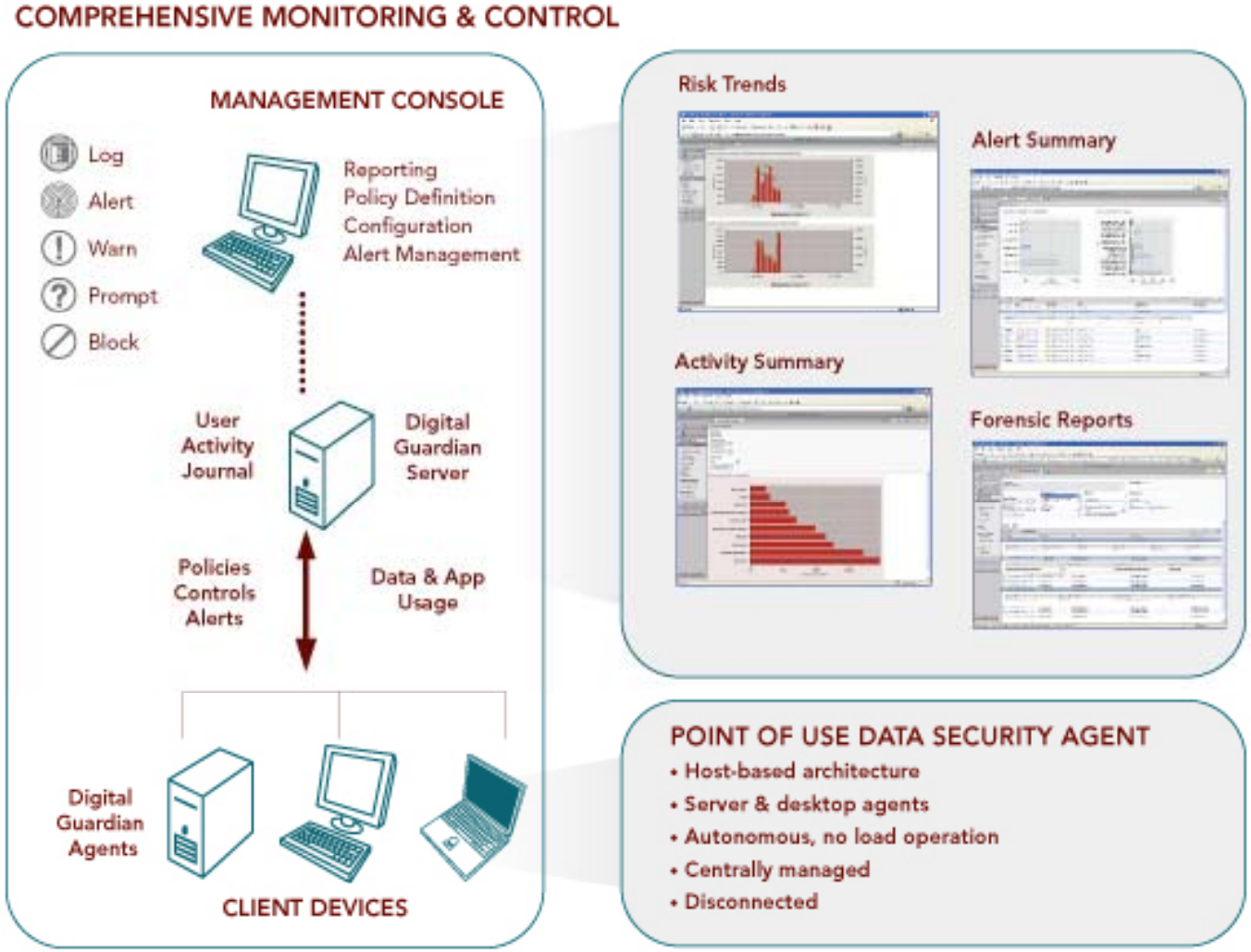
Verdasys: Digital Guardian

Verdasys' Digital Guardian is a data security solution for protecting and tracking the flow of critical data

Digital Guardian logs user data transactions and applies pre-defined rules to ensure that end-users are using applications and data properly

It also assures that data is being used in accordance with established company best practices and government regulations (such as HIPAA and GLBA) for handling confidential and private information

Verdasys Digital Guardian: Screenshot



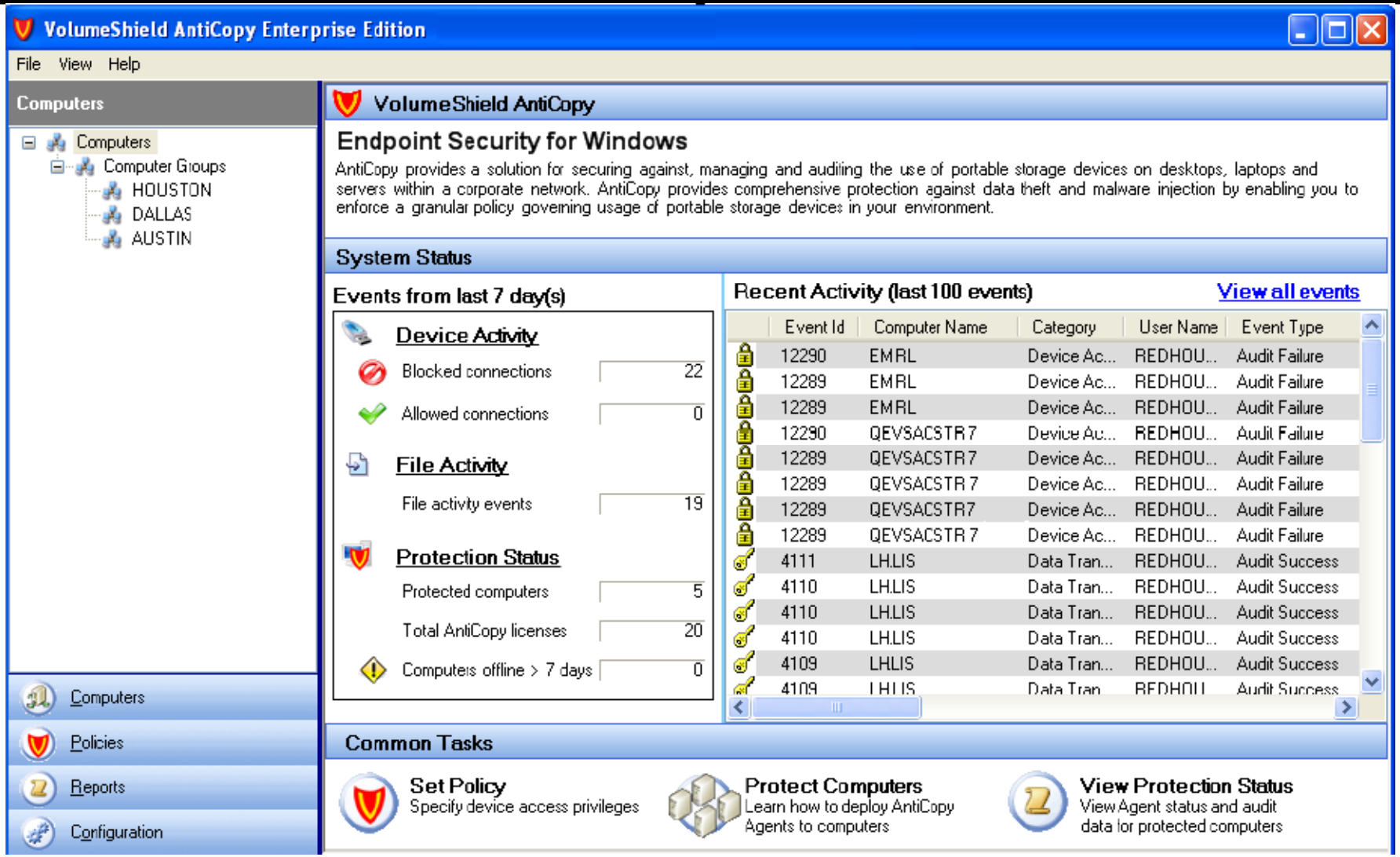
VolumeShield AntiCopy

VolumeShield AntiCopy controls and audits the use of portable storage devices across a corporate network

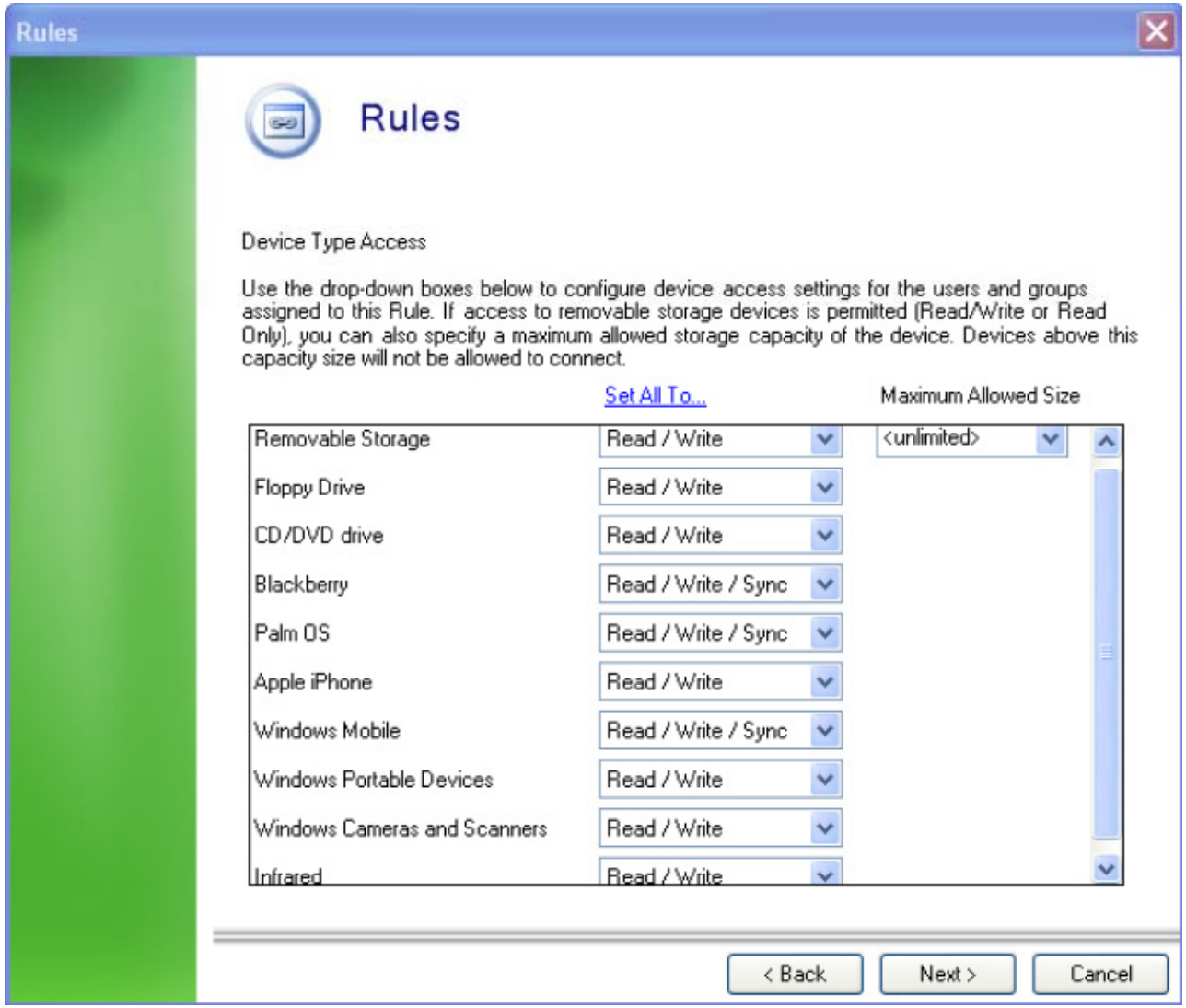
AntiCopy protects against data theft and malware injection by enabling organizations to enforce a granular policy governing the use of devices such as USB drives, CD/DVD burners, iPods, and PDAs

Read-only access can be permitted for Removable storage devices, floppy drives, and CD/DVD writers

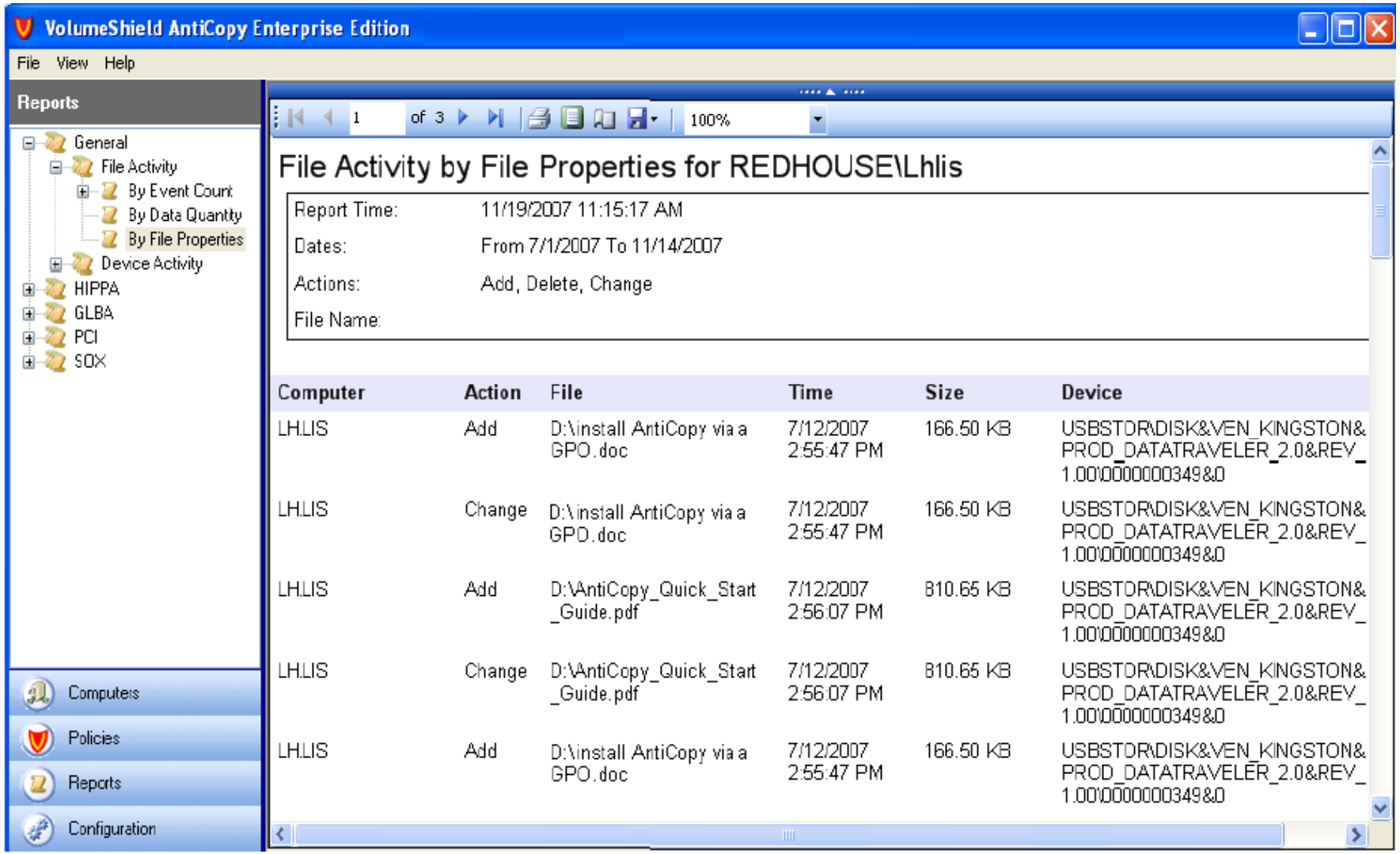
VolumeShield AntiCopy: Screenshot 1



VolumeShield AntiCopy: Screenshot 2



VolumeShield AntiCopy: Screenshot 3



Websense Content Protection Suite

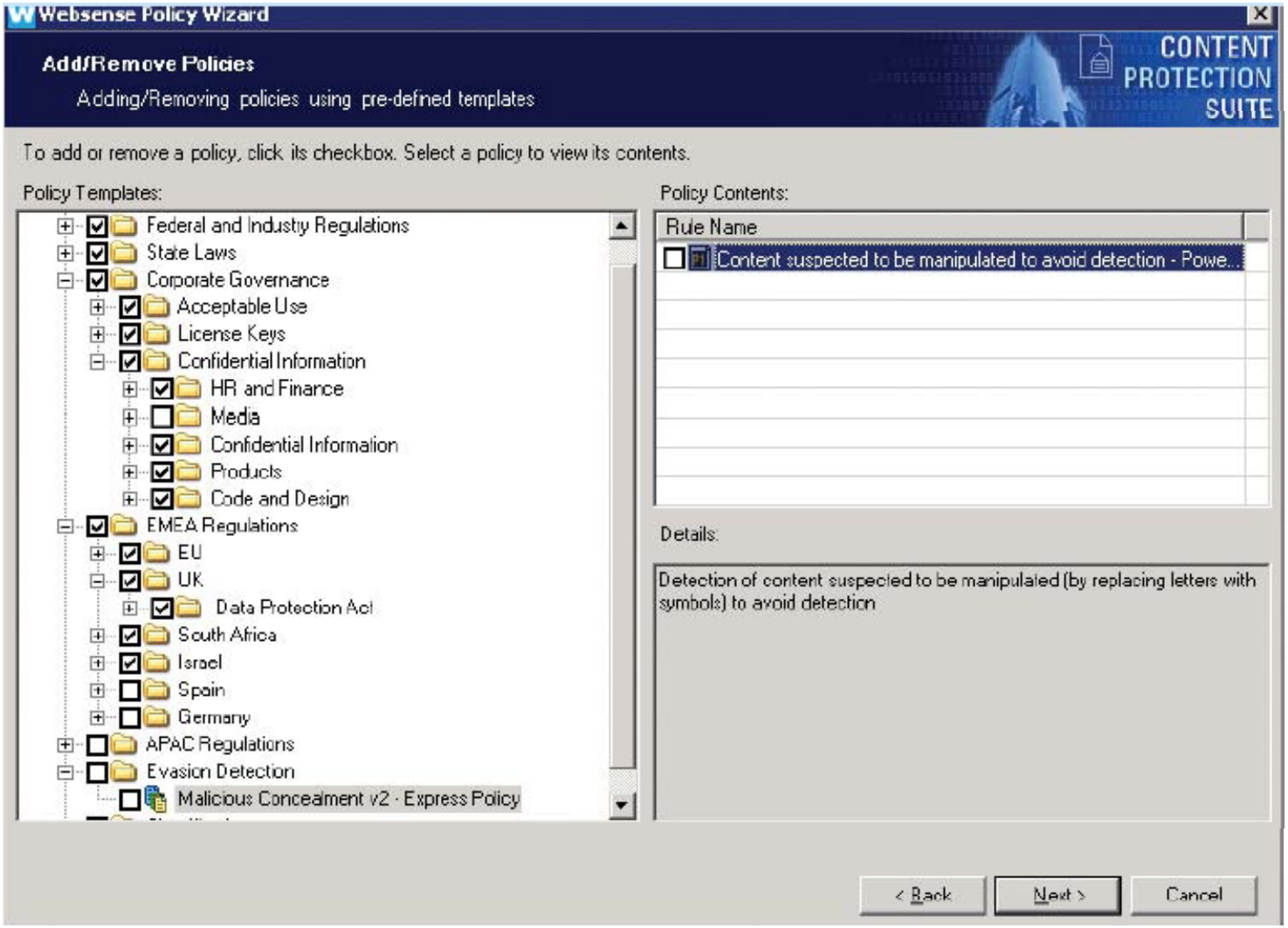
Websense Content Protection Suite is a comprehensive solution to address the growing need for robust information leak prevention

It provides superior protection to secure content and manage "Who, What, Where, and How"

Features:

- Prevents internal and external data loss
- Network and Data Recovery
- Content and Context Awareness
- Data Monitoring

Websense Content Protection Suite: Screenshot



Elcomsoft Distributed Password Recovery

Elcomsoft Distributed Password Recovery is a password recovery tool

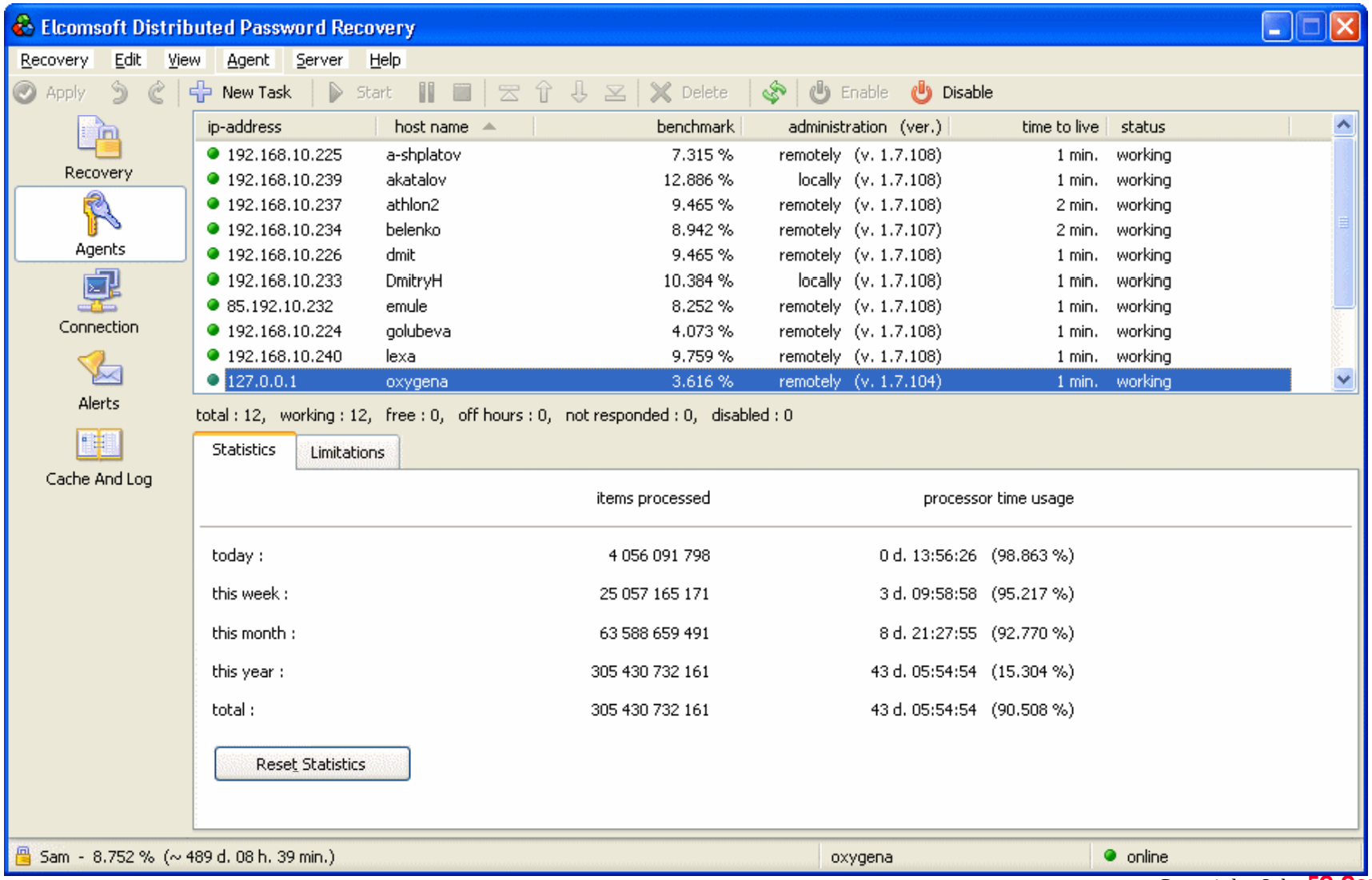
It is used to crack complex passwords, recover strong encryption keys, and unlock documents in a production environment

It is a high-end solution for forensic and government agencies, data recovery, and password recovery services

Features:

- Distributed password recovery over LAN, Internet, or both
- Console management for flexible control from any networked PC
- Plug-in architecture allows additional file formats
- Schedule support for flexible load balancing
- Encrypts all network communications between password recovery clients and the server
- Installs and removes password recovery clients remotely

Elcomsoft Distributed Password Recovery: Screenshot



Tool: Internet Password Recovery Toolbox

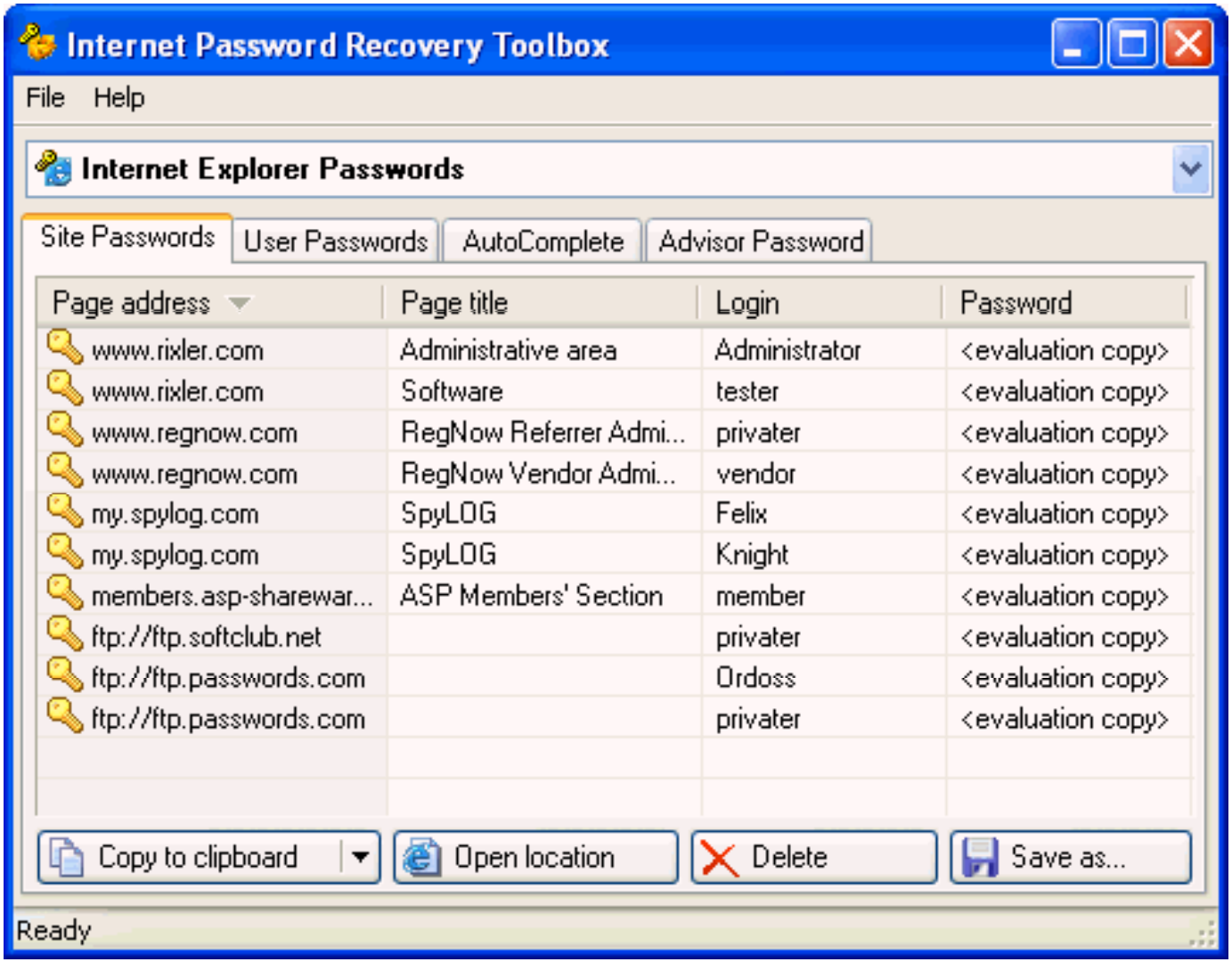
Internet Password Recovery Toolbox is a password recovery tool

It maintains browsing and deleting passwords for protected sites and user passwords for HTML forms

It recovers the following passwords:

- Internet Explorer
- Outlook Express
- Outlook
- Network and dial-up passwords
- ISDN lines
- Virtual Private Networks

Internet Password Recovery Toolbox: Screenshot



Summary

- Data loss refers to the unexpected loss of data or information
- Backup and recovery schemes must be developed to restore lost data
- Using CDs or even an external USB hard drive for data storage can potentially save from hiring a data recovery service to perform hard drive data recovery on hard drive or RAID server
- The Code Green Networks line of Content Inspection Appliances is a solution for protecting customer data and safeguarding intellectual property
- Symantec Database Security (SDS) provides real-time detection of anomalous SQL activity, auditing, and Intruder Identification to help manage and control database security risks

"The toaster pastry fits right into the floppy drive! This allows you to transfer data from your computer to your mouth. The information is stored in your fat cells, thus transforming your pot belly into a high-capacity hard drive!"

"Yesterday I changed everyone's password to 'password'. I sent it to everyone in a memo, put it on a big sign on the wall and printed it on all of the coffee cups. Guess how many people called me this morning because they forgot the password."