www.cyberoam.com

Cyberoam Endpoint Data Protection

Data Protection & Encryption

Device Management

Application Control

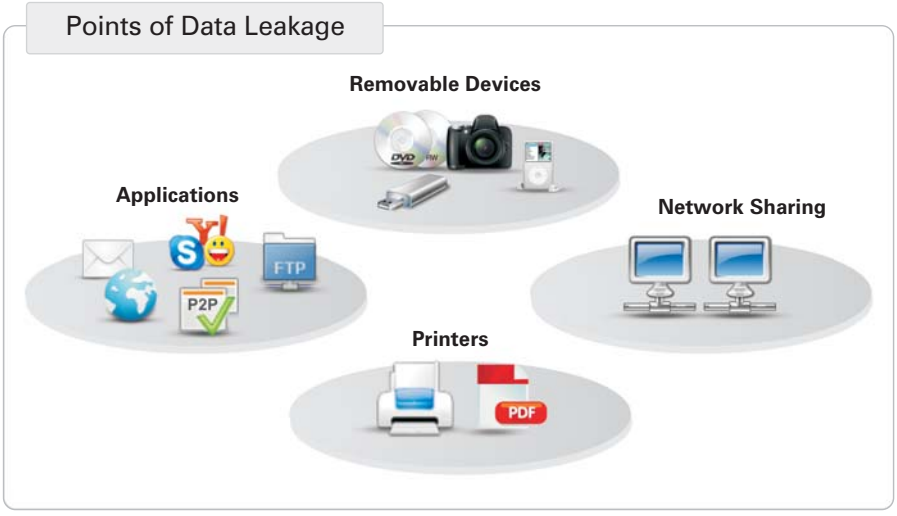
Asset Management

Protect your Data. Protect your Assets.

Cyberoam®

Overview - Data Leakage

More than half of corporate data lies unprotected over endpoints in organizations. Sensitive information like customer data, trade secrets, intellectual property, and legal documents reside over endpoints for their productive use by authorized users. However, easy access by users to portable devices and applications like USBs, DVDs, MP3s, file-sharing applications, Instant Messengers, and more, make it easy for them to maliciously or accidentally leak this data. Today, the cost of lost/stolen data to an organization is massive with lost business resulting in 65% of breach costs, according to research. Hence, organizations need to protect their corporate data at endpoints from unauthorized sharing or leakage by insiders.



Besides, centralized, automated Asset Management is necessary at the endpoint due to the presence of large number of users, branch offices, rise in sophisticated attacks and the resultant bugs and vulnerabilities.

Hence, securing the endpoint to protect corporate data and assets has become critical, with a rapidly rising number of organizations deploying dedicated data protection suites that offer user-level controls when handling data.

Cyberoam - Endpoint Data Protection

Cyberoam Endpoint Data Protection protects the organization's endpoints from data leakage through Identity and group-based policy controls, encryption, shadow copies, logging, reporting and archiving. Cyberoam offers data protection and asset management in four easy-to-deploy and use modules -

- **Data Protection and Encryption**
- **Application Control**
- **Device Management**
- **Asset Management**

These modules enable organizations to limit access only to trusted devices, applications and recipients while sharing data. Asset Management eliminates the IT burden on organizations with reduced support calls due to malware attacks, system recovery and performance issues. The easy-to-manage Cyberoam Endpoint Data Protection allows organizations to prevent data loss, enhance security, employee productivity and efficient management of IT assets while retaining business flexibility. In addition, organizations can meet regulatory and security compliance requirements.

Benefits

- Prevent endpoint data leakage
- Extend data security beyond the network
- Enhance employee productivity by blocking unauthorized applications
- Streamline IT infrastructure management
- Lower Total Cost of Ownership of IT infrastructure
- Reduce malware penetration through patch management
- Meet security compliance with IT asset management
- Reduce legal liability and business losses

Cyberoam Endpoint Data Protection - Modules

Data Protection and Encryption

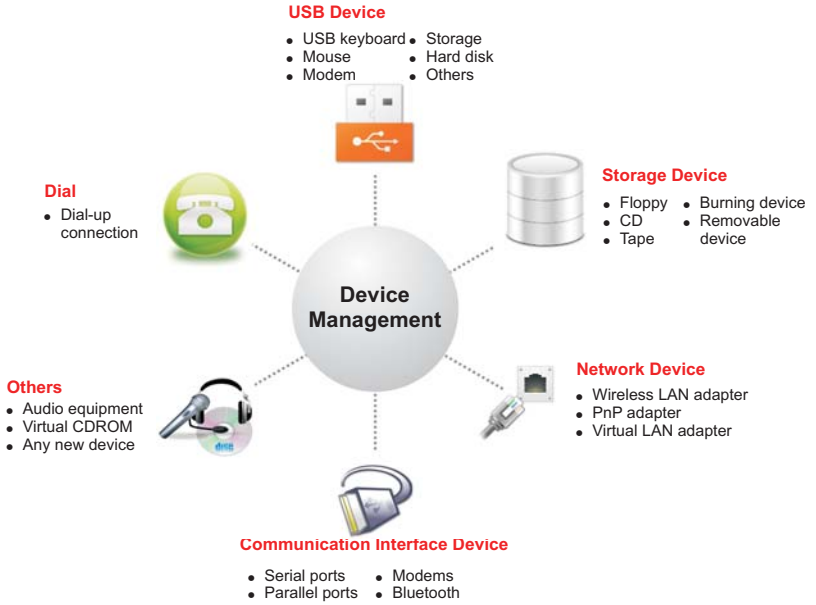
Insider access to sensitive documents and accidental or malicious file transfer is a major cause of data loss. With the Cyberoam Data Protection and Encryption, organizations can control data transferred to removable devices, printers, or attachments in emails or over Instant Messengers. They can control document operations, document sharing and save shadow copies at the time of specified actions to the document. Organizations can eliminate the risk of data loss on account of lost removable devices by encrypting removable devices and files at the time of copying them to a device. They can ensure that data in devices is accessible only to authorized users through decryption requirement for encrypted files.

Features

- Block file transfer by filename or extension over -
  - Removable devices
  - Chat, email, file sharing applications and more
  - Network sharing
  - Printers
- Specify read-write access to white-listed removable devices
- Offer encryption and decryption for files and removable devices
- Control file transfer via email and Instant Messengers based on file name, extension, size, within and outside the network
- Control access to printers
- Create shadow copies of files during creation, modification, transfer, print
- Offer customizable alerts to administrators and warning to users
- Create logs-reports of access, usage, modification, transfer and deletion of files.

Device Management

Removable devices are the most common routes to data leakage because of their small size, considerable storage capability and difficulty in tracing. Cyberoam's Device Management module allows organizations to trace and control all removable devices at their endpoints. Organizations can allow access only to whitelisted devices - USB devices, storage ports, network/Wi-Fi devices, communication interface devices, dial-up devices and others.

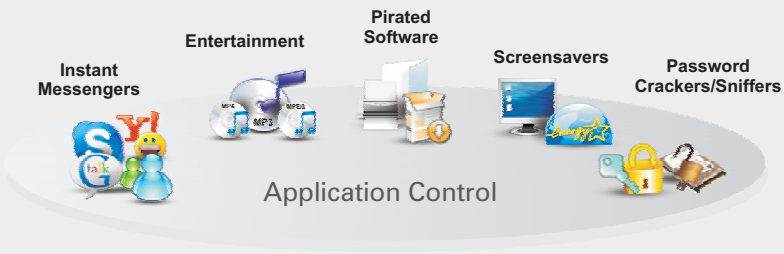


Features

- Allow/block access to classified removable devices
- Apply device control policy even when offline
- Set expiry time to disable policies automatically

Application Control

Unrestricted application usage can result in the use of unauthorized, illegal and malware-laden applications, causing data loss, productivity loss, legal liability and network outages. The Application Control module allows organizations to prevent data loss by allowing or blocking access to specified applications. Application logs allow them to view the type and time of applications used at endpoints across the organization.



Features

- Offer granular, policy-based application controls for chat, webmail, gaming, file sharing, FTP and more
- Apply policies even when offline
- Set alerts and their levels for unauthorized application access
- Customize warning messages to users
- Set expiry time to disable temporary policies

Asset Management

Distributed offices and rise in malware attacks are opening organizations to higher levels of threats, leaving IT teams in a fire-fighting mode. Cyberoam's Asset Management module for Windows® enables organizations to streamline their IT infrastructure management with centralized and automated hardware and software asset management that includes inventory, patch and update management. This allows organizations to control hardware and software costs while lowering malware penetration and meeting the requirements of security compliance.

Features

- Hardware and software inventory
- Hardware/ software asset location, configuration, version tracking, historical information
- Automated patch management, updates of Microsoft Operating System and its applications
- Centralized management
- Remote deployment of Microsoft Software Installation (MSI) packages

Cyberoam Product Portfolio

Cyberoam offers complete security to your organization.
Cyberoam's product range includes:

- Unified Threat Management
- Cyberoam Central Console
- Cyberoam iView
- SSL VPN
- Endpoint Data Protection

Toll Free Numbers
USA : +1-877-777-0368 | **India :** 1-800-301-00013
APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958

Cyberoam®