



Over 250 million confidential records were reported lost or stolen within the past two years. And each day, there are more stories of data theft or of accidental or intentional privacy breaches.

Why has data loss become so prevalent? First, business data is growing. According to Forrester Research, data volumes double approximately every three years, and by 2010, data will be in zettabyte sizes (1 ZB=1021=1 trillion GB). In addition, approximately 80 percent of the world's data is unstructured, which means the vast majority of information is contained in documents, spreadsheets, or email.

Also, large amounts of data are more accessible than ever. Organizations allow for easy access to databases for information sharing, and storage and compression technology has allowed for more powerful (and risk-laden) endpoints. An 80-MB mobile device now holds 6000 Microsoft Word documents or 720,000 emails, and new 64-GB removable devices allow for an entire hard drive to be copied onto a device the size of a pack of gum. This means that employees, business partners, or even data thieves can access and transmit intellectual property or customer private data easier and faster than ever before.

### What Is Data Loss Prevention?

Data loss prevention (DLP) technology is content-level inspection and control of confidential and private data. This technology was designed to protect against accidental data loss and to provide visibility into and enforce policies on information usage and communication. When used in conjunction with other security technology, DLP can also help to protect against intentional data loss and data theft.

### Why Data Loss Prevention?

Protecting intellectual property, complying with regulations to protect private data (such as the PCI regulation), and ensuring that employees are adhering to corporate communication policies are among the main business objectives that can be addressed with data loss prevention technology. But it's not just business objectives that are driving the need for DLP—it's also the staggering number and size of reported losses.

### The Cisco Data Loss Prevention Solution

The Cisco® Data Loss Prevention Solution offers an integrated approach to preventing data loss through enhanced data protection and content control.

- Enhanced data protection: Cisco offers a vast portfolio of security products to build a Self-Defending Network and strengthen your data protection policy, such as:
  - Ensuring that clients with the right credentials and security posture are securely accessing the corporate network, whether onsite or remote or connecting via wired or wireless
  - Ensuring that points of sensitive data use, rest, or transit, such as databases, applications, clients, and communication protocols, are properly secured and free from data threats

- Content control: Cisco integrates data loss prevention content control into its security devices to:
  - Protect against data loss where it is most needed, focusing on key areas of risk
  - Classify, audit, and enforce policies on the use and transmission of a company's most critical data, such as credit card numbers or Social Security numbers

With this integrated approach, the Cisco Data Loss Prevention Solution enables organizations to:

- Increase efficiency and optimize expenditures by leveraging the existing Cisco security infrastructure
- Protect against a broader spectrum of data loss avenues, such as unauthorized access, unencrypted connections, malware, or end-user actions
- Decrease the time to implement and operate DLP technology
- Reduce the "noise" associated with large-scale DLP deployments by focusing on key areas of risk

### Key Areas of Protection

The key areas of protection for the Cisco Data Loss Prevention Solution are data in motion (in transit), data at rest, and data in use. The following table addresses common data loss risk areas and how they can be addressed:

Vector	Areas of Risk	Protection
<b>Data in Motion</b>	Email, instant messaging, web, FTP, wireless	<ul style="list-style-type: none"> <li>Monitor for sensitive information and acceptable use</li> <li>Encrypt data as it moves</li> <li>Apply conditional blocking</li> <li>Educate employees</li> <li>Control rogue communications</li> </ul>
<b>Data at Rest</b>	Storage, databases, tapes	<ul style="list-style-type: none"> <li>Encrypt tapes or storage</li> <li>Prevent unauthorized access to back-end systems</li> </ul>
<b>Data in Use</b>	Endpoints (clients, servers)	<ul style="list-style-type: none"> <li>Prevent sensitive information from leaving (i.e., USB)</li> <li>Discover data on endpoint</li> <li>Protect offline</li> <li>Educate employees</li> </ul>

### How the Cisco Data Loss Prevention Solution Works

The Cisco Data Loss Prevention Solution incorporates a strategy and architecture for protecting against data loss. The first step in protecting against data loss is knowing what content you want to protect, and where that content is located.

Once you have identified what you want to protect, you can consider implementing the following solutions to protect against data loss:

- Establish a data protection policy: Verify and augment your data security policy to prevent against accidental or intentional data loss

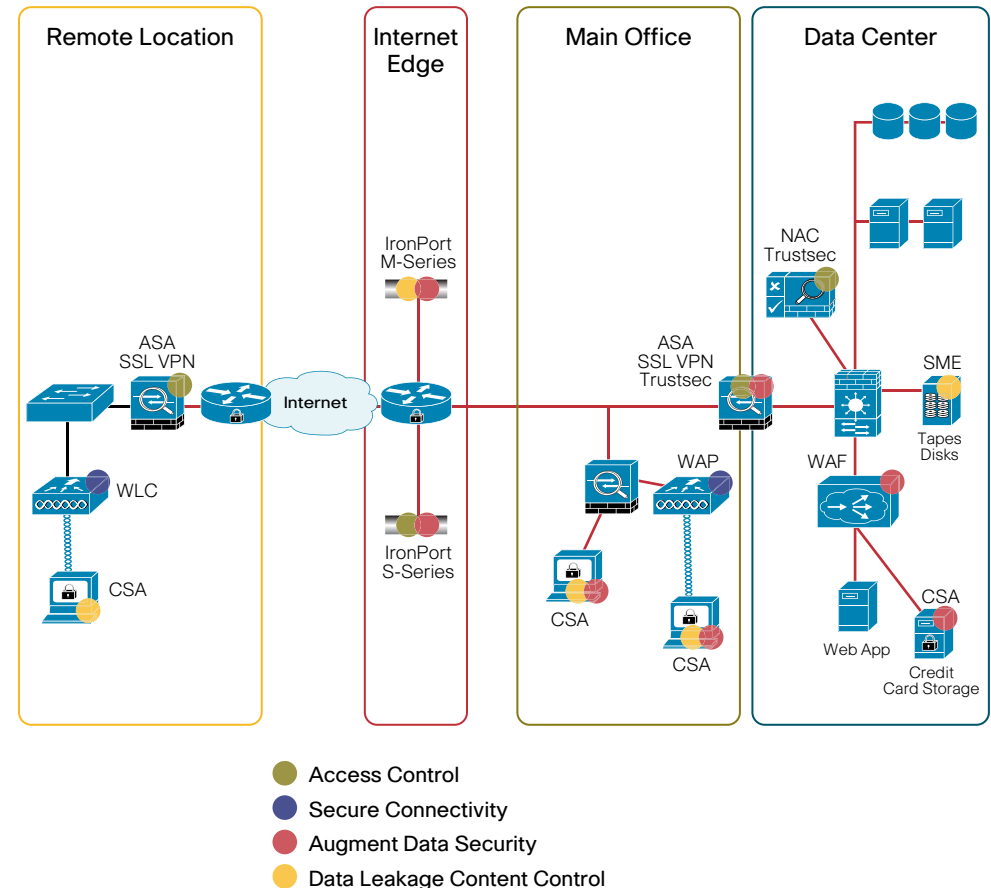
- Secure connectivity: Mitigate rogue access points, control wireless access, and encrypt remote connectivity
- Control access: Ensure that only authorized people are accessing sensitive networks and files
- Implement DLP technology: Control sensitive data at high-risk points with policy-based content inspection and enforcement

## Cisco Data Loss Prevention Solution Portfolio

The following table outlines the core Cisco Data Loss Prevention Solution portfolio.

Objective	Product	Benefits
<b>Data loss Prevention Technology</b>	IronPort C-Series	Prevents sensitive data loss that can occur via email, by using content inspection at the email gateway: <ul style="list-style-type: none"> <li>• A policy-based email gateway solution with integrated DLP full-body and attachment scanning</li> <li>• Flexible rule engine includes prepackaged dictionaries and Smart Identifiers (e.g., SSNs, credit card numbers) and remediation capabilities, such as blocking, quarantine, and encryption</li> </ul>
	Cisco Security Agent	Prevents sensitive data loss that can occur at the endpoint: <ul style="list-style-type: none"> <li>• A single agent, single console, endpoint protection solution with DLP capabilities</li> <li>• Discovers, audits, and enforces policies on sensitive file access and data use, such as credit card numbers, SSNs, and user-defined terms</li> </ul>
	Cisco Storage Media Encryption	Prevents sensitive data loss that can occur through lost backup tapes: <ul style="list-style-type: none"> <li>• Encrypts data at rest on heterogeneous, SAN-attached tape devices and virtual tape libraries (secure AES-256)</li> <li>• Fully integrated with the Cisco MDS 9000 family hardware</li> </ul>
<b>Control Access</b>	Cisco Network Admission Control	Prevents data loss that can occur through unauthorized access to networks, as well as data loss that can occur through malware from insufficient security policies: <ul style="list-style-type: none"> <li>• Provides guest access and prevents unauthorized access</li> <li>• Helps ensure that systems connecting to the network have the correct security posture</li> </ul>
<b>Secure Connectivity</b>	Cisco SSL VPN	Prevents data loss that can occur through unauthorized or unencrypted remote access: <ul style="list-style-type: none"> <li>• Remote access based on SSL VPN delivers secure access to network resources by establishing an encrypted tunnel across the Internet. Available on Cisco ASA 5500 Series Security Appliances and Cisco Integrated Services Routers</li> </ul>
	Cisco Unified Wireless Network	Prevents data loss that can occur through unauthorized wireless access and threats: <ul style="list-style-type: none"> <li>• Offers access points, client devices, wireless controllers, and network management with integrated security and granular policy management</li> <li>• Integrates threat and intrusion detection to prevent wireless attacks</li> <li>• Single-user identity and policy protects against unauthorized access</li> <li>• Detects rogue access points, tracks users, and monitors security</li> </ul>
<b>Augment Data Security</b>	Cisco ACE Web Application Firewall	Prevents data loss that can occur through web applications: <ul style="list-style-type: none"> <li>• Helps ensure that credit card information and SSNs are not accidentally disclosed or stolen through web applications</li> </ul>
	IronPort S-Series	Prevents data loss that can occur from clients accessing infected sites: <ul style="list-style-type: none"> <li>• Protects against web-based threats to data, such as data-stealing malware or phone home traffic</li> </ul>

Figure 1.



## Why Cisco for Data Loss Prevention?

The Cisco Data Loss Prevention Solution protects your most critical data at the highest points of risk within your network. Integrated into security devices, the solution optimizes the purchase, deployment, and operational time required to protect high-value content. In addition, through the integrated approach, a Cisco Data Loss Prevention Solution covers a broader spectrum of data loss avenues, including malware and end-user actions.

## More Information

For more information on the Cisco Data Loss Prevention Solution, please visit [www.cisco.com/go/dlp](http://www.cisco.com/go/dlp).