



A Websense® Research Brief

Protecting the Crown Jewels: Securing Intellectual Property

It's Hard Enough to Protect IP

Data theft, piracy, and malicious employees put intellectual property (IP) at risk every day. But the greater threat to IP comes from the most reliable staff members. Accidents and seemingly trivial errors cause more IP loss than angry employees or devious hackers. Routine mistakes, from which nobody is immune, pose the greatest threat to IP, competitive positioning, and ability to effectively grow the business.

IP is the foundation of a sustainable competitive advantage. It is not limited to product specifications or proprietary research. IP can include thought leadership, strategic plans, and other internal tools used to improve a position in the market. Information regarding new products, marketing strategies, and customer analytics is fundamental to winning market share. If the competition gets a look they can advance their own product launches, learn from core strategies, and mitigate the effects of plans, significantly disrupting the business and eroding potential market share.

The Ponemon Institute estimates that one information leak can lead to a total cost of \$4.8 million. But, leaking IP is likely to be even more costly and yet potentially impossible to put a price on:

- The future value of 6 months (or more) of research and development for a new product
- “Disruptive innovation” that could reshape the market
- A market entry strategy that delivers a first-mover advantage

The loss of IP can have a downstream impact on employee morale, company reputation, and recruiting. Bottom line: If IP isn't secured, it's harder to compete.

Information leak prevention (ILP) solutions protect IP. By scanning communication protocols for sensitive data, organizations can identify a potential leak and prevent the profound consequences that could follow. ILP solutions examine data that is being used by employees to ensure that it doesn't slip into the wrong hands. Some behavior patterns indicate leaks yet are in fact routine business processes; ILP technology is designed to know the difference. By discerning between appropriate and inappropriate use, ILP solutions allow employees to use IP without putting it at risk, thereby enabling the business while securing the organization's competitive advantage.

Leaks Put IP at Risk

Not all information loss is the same. Data theft attracts the most attention. Disgruntled insiders and crafty hackers have caused businesses to implement encryption, intrusion detection, and anti-spyware solutions to protect company IP, but unintentional leaks pose the greater threat. More than 80% of data loss, according to the Ponemon Institute, comes from mistakes such as missing media and other IT mishaps. Despite the obvious disparity, businesses focus on the smaller risk, often at the expense of leaks that are in fact easier to prevent.

IP leaks happen most often in the normal course of business. Common leaks include:

- Sending data to the wrong email address (e.g. jdoe@mail.com versus jadoe@mail.com)
- Copying files to a public-facing drive
- Using a personal email account at work
- Answering external inquiries that should be directed to Public Relations or legal counsel

Seemingly innocuous activity can result in an IP leak. A simple mistake can put a competitive advantage in jeopardy.

ILP technology prevents leaks. By evaluating all communications in the enterprise, ILP solutions distinguish between the normal use of data and leaks. If the solution is too restrictive, it will disrupt the operations of the business; False positives, i.e. perceived leaks that are really business as usual, will occupy IT and business unit leaders unnecessarily. Further, false negatives (missed leaks) will continue the cost, reputation, and operational risks that the solution is supposed to prevent. Inaccurate ILP technology simply creates more expense and workload for little return.

The fundamental weakness of most ILP solutions is in how they evaluate data. Regular expression analysis is the norm; each data element is examined as an independent and distinct unit to determine if a leak is about to occur. Consider the communication of a proprietary report attached to an email message. An ILP solution is configured to intercept any email message with an attachment that contains the word “confidential”. In addition to preventing the occasional leak, the solution would have gathered a variety of personal and professional correspondence that poses no threat to the organization.

Documents Containing “Confidential”

Type	Document Examples
Personal	<ul style="list-style-type: none">• Lease or mortgage application• Insurance forms• Surprise party invitations• Legal correspondence
Business	<ul style="list-style-type: none">• Performance appraisal communications• Nondisclosure agreements• Contract drafts• Drafts of proprietary reports

An overzealous ILP solution can interrupt personal business and professional activity needlessly, creating more work for business unit leaders who have to respond to non-events. For business documents that are works in progress, it can be difficult to tell when the use of confidential IP is routine, illicit, or erroneous. Context makes the difference. To be effective and avoid disrupting the business, an ILP solution must do more than evaluate regular expressions; it has to consider the data’s meaning as well.

Plugging Information Gaps

The Websense® Content Protection Suite fuses regular expression analysis and context sensitivity to target real information leaks. Instead of examining data separately and distinctly, Websense considers additional factors such as:

- Data source and type
- Usage patterns
- Related data elements

This unique approach distinguishes between business as usual and the occasional mistakes that can put a competitive advantage at risk. “Deep Content Control” (DCC) is a proprietary technology of Websense; it uses data and context to determine meaning and prevent leaks.

DCC combines data (content) and how it is used (context) to ascertain sensitivity and identify potential leaks. When monitoring communications for data leaks, Websense uses DCC to add meaning to individual instances of data. Consider again the use of ILP rules to govern the communication of email attachments containing the word “confidential”. With DCC, organizations can do more than scan attachments for instances of that particular word. They may also:

- Look for combinations of words, such as “confidential”, the company name, and “market research” (or other pertinent language)
- Intercept only messages that contain more than one attached file that contain relevant keywords
- Note such communications directed to specific destination and from a specific user

Employees may routinely send marketing plans around the organization for review, for example. A message with one file may not signal a leak – especially if it is being sent to an outside consultant. But what happens when an employee sends twelve files containing proprietary information to an outside email address? The likelihood of a leak is much higher. In this instance, it may make sense to intercept and review the message. If the transmission is being made to a legitimate recipient (e.g., a consultant) the process owner can easily make the determination to allow the communication to continue. This simple step can keep valuable IP inside the company and prevent a catastrophic loss of data.

Leak prevention involves more than looking at bite-sized pieces of data. Context matters as much as content. The Websense approach to ILP prevents leaks, not business, delivering a high degree of accuracy, integrating with business processes for effective management, and providing comprehensive security of intellectual property.