



The Information Leak Detection & Prevention Guide

Essential Requirements for a Comprehensive Data Leak Prevention System

April 2007

GTB Technologies
4685 MacArthur Court
Newport Beach, CA 92660
WWW.GTTB.COM
949-863-9254

The Insider Threat

By now you're so familiar with network security problems that you've got a complete arsenal of hardware and software, encryption and firewalls, IDS and IPS, to prevent any hacker, virus, worm, malware or spyware from penetrating your defenses. From the outside you are impregnable.

Inside is a different story.

Inside, your email server may become a superhighway for sending classified data to the outside world. A Blackberry can be as dangerous as an internal spy. An HTTP link can be a pipeline to the competition.

Your vaunted security may look like a fortress from the outside, but from the inside information is leaking through the cracks. And unless you can detect it, you can't stop it.

According to Deloitte's *2006 Global Security Survey*, 49 percent of companies reported they experienced an internal security breach in the past year. 31 percent of breaches came from virus and worms, 28 percent through insider fraud and 18 percent from data leakage. In addition, 96 percent of companies surveyed were concerned that employees might do something untoward with their information systems.

The research indicated that only 37 percent of companies surveyed believe their company effectively prevents breaches. More specifically:

For large data breaches (10,000+ customers)

43% of companies detect breaches 80% of the time

76% of companies detect breaches 60% of the time

For small data breaches (100 customers or less)

17% of companies detect breaches 80% of the time

38% of companies detect breaches 60% of the time

Carelessness is Expensive

Finding data breaches, discovering what happened and who was responsible, is expensive. According to a Ponemon Institute report, *"Lost Customer Information: What Does a data breach Cost Companies?"* which surveyed 14 organizations, the cost of recovering from a single security breach averaged \$4 million per company, per breach (about \$140 per lost customer record).

Direct costs—outside legal counsel, increased call-center costs and related items—were \$5 million.

According to the Aberdeen Group's *2006 The Insider Threat Benchmark Report*, companies that include ILP strategies in their risk planning report a 13 percent reduction in their security events. Companies without an ILP solution experience a 35 percent *increase* in security events.

In light of this, it becomes obvious that an ILD&P (information leak detection and prevention) solution is essential to any company's risk prevention framework. The question is: which solution is best for you?

7 + 1 Criteria for Evaluating ILD&P Solutions

1 Appliance, not Software

Any ILD&P solution consists of two components – network protection (data in motion) and data at rest protection. The network protection component must be a specialized appliance, not software, like a firewall, a router or a switch. Therefore, just as you don't buy "router software", you should not buy ILD&P software and try to integrate it with hardware, as it is a waste of resources and a deployment risk. It is recommended to buy only an appliance, which has software and hardware integrated (not 'pre-installed') and guaranteed by the vendor.

2 Security

It may be obvious that a data security product should increase data protection and not decrease it; therefore it is crucial that under no circumstance should an ILD&P solution copy secured content to its own internal storage. Such methodology would constitute a security breach in itself; still it is surprising to find that some ILD&P vendors disregard this principle.

3 Comprehensive Channels Coverage

An ILD&P solution must scan and be able to block all potential avenues (protocols) of data leaks over the Internet; not be limited to just scanning and blocking of SMTP and HTTP or some other popular protocols.

Every enterprise network uses encrypted protocols such as VPNs, secure SMTP, secure IM, FTPS, HTTPS, etc. The content inspection should cover encrypted traffic also. It is not enough to simply recognize the encryption and to make a “go / no go” decision, or to limit the inspection to HTTPS.

An ILD&P solution should not be dependent on the tight integration with other devices such as mail servers or web proxies. One reason is the difficulty and risks in the deployment and maintenance. Additionally, the mail server or web access configuration may not be supported. More importantly, the products dependent on such integration will not be able to inspect traffic without using those devices. For example, if an ILD&P product requires integration with the enterprise mail server, it will not be able to inspect emails sent by an employee using their personal webmail.

4 Precision (Low False Positive Rate)

An ILD&P product must implement a detection methodology that minimizes false positives to zero. False positives can wreak havoc in an organization or, at the very least, increase the workload of already overworked IT Departments. For example, consider an organization with 1,000 users, each one sending 20 email messages per day. With a false positive rate of “only” 0.5% the ILD&P system will incorrectly block 100 messages per day! ILD&P solutions which base their detection method on data classification, statistical analysis, linguistic analysis, contextual analysis, keywords matching etc. are very susceptible to a high false positive rate. Precise data matching is the only methodology that ensures virtually zero false positives. Further, an ILD&P product should be able to block attempts to transmit protected data, not just report on that.

5 Resilience to Data Manipulation

An ILD&P solution must protect information (content) and not a specific representation of such data. Most importantly, the ILP&D solution should identify and protect from possible data conversions and data representation changes, such as:

- Data extracting – only a small part of a file or a subset of a database table is copied and pasted from one document to another
- File format conversion
- Compression
- Embedding
- File extension changes
- Re-typing – text is re-typed from a printed document

- Language encoding changes, especially conversion between Unicode and plain English

Different representation of the same data, i.e., a social security number may be represented in the form '777-77-7762', '777 77 7762' or '777777762'.

6 Comprehensive Coverage of Data Sources and Formats

An ILD&P product must protect structured data and unstructured data, as well as text and binary data. Experience shows that most organizations need to protect all types of data formats even if it is not evident. For example, many banks and credit unions transfer important documents such as mortgage applications, account reports, etc., over to JPEG and store them on the network. Protection of such documents requires support for binary data from the ILD&P solution. The best ILP&D solutions are those which are independent of file formats. Such solutions would support any future file formats as well as data conversions from one format to another.

7 Data at Rest Management

Confidential data can leak not only through network egress points, but there is also a risk of lost laptops, physical break-ins, etc., which gives rise to the need for Data at Rest Management. Data at Rest Management means finding confidential data in the places where it should not be (on the corporate network, employees' laptops, backup media, etc.). Once it is found, the data can be erased, moved to a secured location, or protected with access privileges by the appropriate person. A comprehensive ILD&P solution must include a Data at Rest Management module.

Data at Rest Management software will have full access to the most important files on your network. Make sure, that it is “read only” – i.e. it has no ability to delete, move or modify files on the network. Otherwise, a mistake by technical personnel can destroy the most important digital assets of your organization.

+ 1 Large Organizations

Finally, there is a criterion which is unique to large organizations that are having multiple network connection points and responsible for hundreds of Mbps outbound traffic.

Large organizations should have the following capabilities with their ILD&P solution:

- a) Load balancing
- b) Redundancy and failover
- c) Automatic data replication (ADR)

Load balancing allows multiple ILD&P devices to work as a cluster, sharing the outbound transmission load between them. Ideally, redundancy and failover would be present on two levels. On the device level, the ILD&P device must have redundant hard disk and the power supply. Further, if inline connection is desired, an ILD&P device must not interrupt the network connection even if it fails. This is usually achieved with a “bypass circuit”.

On the cluster level, an ILD&P solution should allow deployment of redundant devices. An ILD&P solution must automatically discover a failure and allow redundant devices to take over the failed devices without data flow interruption.

Since, large organizations need to deploy multiple devices for load balancing, redundancy, and protect multiple egress points; they will also need to utilize automatic data replication (ADR). ADR ensures synchronization of content between multiple ILD&P devices.

Conclusion

In today's regulated business environment, the loss of data records carries heavy penalties which can be expressed in terms of lost time, money, customer relations and ultimately lost profits. Most companies today are protected from outside threats but remain vulnerable to internal ones. A comprehensive information leak protection system is as vital to your network security as firewalls and virus protection are. The appropriate time to detect internal leaks is before they leave your network, not when a law enforcement agent shows up at your door with a subpoena.

For more information, please contact GTB Technologies at info@gttb.com or call us at 949.863.9254 x 5

GTB Technologies
4685 MacArthur Court
Newport Beach, CA 92660
WWW.GTTB.COM