2nd August, 2011

Overview of Network Box Data Leakage Protection

For the last twenty years or more, the focus on computer security has firmly been on what might get into your systems. Hackers, viruses, computer worms, spam, undesirable content, are all obvious examples.

Now many IT managers, and indeed management in general, are beginning to worry about the need to secure their network gateways against data going in the other direction.

At Network Box, this is something we have actually been doing in terms traditional threats, for more than ten years now. Every Network Box Unified Threat Management system can block threats from coming in, or from getting out, of clients' networks.

DLP (Data Leakage Prevention) however, is not about blocking threats, in this traditional sense. It is about stopping such things as specific words, document files, credit card numbers, identity card numbers, or social security numbers, from leaving a protected network. This can, for example, help management ensure that a particular restricted set of documents, containing sensitive commercial secrets, cannot be emailed out by staff, either by accident, or on purpose.

The clear need for such functionality is easy to understand, but what has been remarkable, is the massive swing in just how important IT managers feel DLP technology is to their organization. Network Box conducts comprehensive security surveys every year, to ascertain how IT managers feel about important security issues.

In 2010, less than 16% of IT managers surveyed, thought DLP technology was important to their organization. In 2011, more than 92% of IT managers surveyed, think DLP technology is important to their organization. That is a massive swing.

The Network Box DLP (Data Leakage Protection) system is designed to protect against both the deliberate, or accidental, leakage of confidential organizational data via outgoing email.

Industry experts state that 98% of data leakage is actually accidental, so having such a system in place is extremely helpful to both the individuals who would have unintentionally leaked important confidential data from their organizations, as well as the organizations themselves who could be damaged by such leaks.

It is important to note however, Network Box can only help to enforce organizational policy. The better the policy, and the better the enforcement of those policies, the better the end results will likely be. In the end, organizational policy compliance needs to drive data leakage protection best practices.

Examples of Data Which May Be Blocked

A high degree of flexibility is built into the Network Box DLP system as standard, allowing for extensive customization by organizations. The idea is to allow the organization the tools to protect against data breaches, without limiting those organizations as to what exactly can be targeted on, and blocked.

The most common types of confidential data to be blocked typically include:

Credit Card Numbers:

- VISA, MasterCard, American Express, Discover, JCB, Diners Club, etc.

ID Card Numbers:

- ID Card Numbers, US Drivers' Licenses, US Social Security Numbers, Canadian ID Numbers, etc.

Account Numbers:

- Specific client, supplier, or other account information.

Confidential Documents:

- These can be marked as confidential using specific text or numbers, included as part of the document, for example privacy footers added to Microsoft Office documents.

In order for the system to have a high success rate for preventing sensitive data from leaving the corporate network, it is vital to have the correct policies in place, and ensure that those policies are enforced at all times.

Each organization's DLP policies should be based on that organization's compliance needs.

Organizational Policy Enforcement

The Network Box DLP system can only enforce the organizational policies which have been set. Policy creation should not be a one-time event; rules should be consistently reviewed, so that they reflect changing organizational goals and requirements.

DLP is an important tool, but like any tool, it must be used correctly in order to achieve optimal results. To be effective, it is just as important to understand the underlying requirements, as it is to understand the underlying technology.

For the Network Box DLP system to be effective, all departments within the protected organization, must collaborate, and work together on developing policies that protect the organization as a whole, while still allowing members of the organization to get their work done with the minimum of interference.

The most important single rule however, is that each organization must classify its data in the first place. If data is classified as sensitive when it is created, a lot of time and work can be saved after the fact.

Therefore, effectively marking documents, to show which contains sensitive data, is necessary to ensure the DLP system can successfully block security breaches.

Image Based DLP Security

The Network Box DLP system can stop confidential information being leaked by outbound email; and can send a warning to the sender, as well as the system administrator.

However, the system is not only restricted to working with text, and can work with images as well. This means that if you take a photograph, or screen shot of a document, it can still be blocked by the DLP system.

In addition, an electronically fingerprinted graphic could be used for all confidential documents; so adding that particular graphic to any confidential document, could stop that document from being emailed out of the network.

Such fingerprinted organizational graphics could act in exactly the same way as privacy text, with the added benefit of not being limited by language, and perhaps being even more visually obvious to users that the marked document concerned is private and confidential.

About Network Box:

Network Box Corporation is a multi-award winning managed security services company, specialising in Unified Threat Management (UTM). It continuously defends the networks of its customers using PUSH technology to instantaneously update protection, from 12 Security Operations Centres spread across the globe. Network Box Corporation has been named one of the world's Top 100 Strategic IT Vendors by MIS Asia Magazine for three years. The company's customers across the globe, include many of the world's best known corporations, organisations, and government departments.

Security Response Facebook: http://www.facebook.com/networkboxresponse
Network Box Facebook: http://www.facebook.com/networkbox

Network Box Hong Kong Limited, 16th Floor Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong
Tel: +852 2736-2083
E-mail: marketing@network-box.com.hk