

Protection against data leakage with extrusion software, involves understanding of hackers' practices and knowing forms in which data is monitored. By **Justin Peltier**

Computer hackers and bank robbers have a lot in common. Both begin by performing a reconnaissance of the potential target. With a bank robber, this means a trip to the bank to understand the layout.

When penetrating a computer, the hacker begins with data

gathering techniques such as Google hacking. Once this is complete, the hacker performs a remote port scan to see what the potential avenues of entrance to the computer system are.

Once the ports have been identified the next step is to look for vulnerabilities in the open

applications discovered in the port scan. The hacker is ready for the heist and launches an exploit against a vulnerable system.

Clearly the best option is not to have the vulnerability exist in the first place, but catching every vulnerability in any organisation is a daunting task.

Trend Micro LeakProof



Supplier Trend Micro
Contact www.trendmicro.com

The Trend Micro offering is an all-in-one appliance that comes with everything preloaded. All the administrator needs to do is configure the device. The initial configuration

is done by attaching a power cord, PS/2 keyboard and VGA cable to the device.

The underlying operating system is Linux, but the configuration is completely menu driven and no command line commands are necessary. Once the initial set-up is complete the machine will have an IP address and you can configure the device using http, https or ssh.

In most environments LeakProof is installed with the

help of an engineer. The main purpose of the engineer is to assist the company in defining exactly what sensitive information is and what to look out for. There are pre-built templates for policies such as SOX and GLBA, and these rules can be customised or created using a wizard interface.

The client-side software is very well done and runs without an icon in the system tray.

The client can be removed or disabled using anti-rootkit technology, but the administrative console will immediately report the system as offline and notify the system administrator.

One of the biggest challenges to this solution is getting the client out to all of the client machines. The program can be made to an msi file and distributed using SMS on zenworks or any other popular software deployment package.

LeakProof provides many means to protect data, including a critical document feature.

As opposed to appending a digital signature the DLP program uses a grouping of letters in several places in the document to create the fingerprint. This speeds up security processing.

LeakProof can block suspicious activity and warn the user. It can also redirect users to the corporate site on internet usage. Lastly the DLP can provide a window, which

allows the user to justify the action being taken.

The documentation was a PDF file broken into easy to find sections. Free support is offered for the first year of the product and additional years and features such as 24/7 support are available for an extra fee.

SC MAGAZINE RATING

Features	★★★★★
Performance	★★★★★
Ease of Use	★★★★★
Documentation	★★★☆☆
Support	★★★★☆
Value for Money	★★★★★

OVERALL RATING ★★★★★

For An easy to use, excellent performing product with too many features to be covered in this review

Against The deployment of the client software may require some planning

Verdict A very solid product with very well done client-side software, all put together at a great price. Our Best Buy

Contact details:



A very solid product with very well done client-side software, all put together at a great price

Justin Peltier

