

With many different routes it can take to escape the enterprise, keeping your data where it belongs involves more than blocking points of exploit, says **Justin Peltier**.

Computer crackers and bank robbers have much in common. Both types of ner-do-wells begin by performing a reconnaissance of the potential target. With a bank robber, recon usually means a trip to the bank to understand the physical layout, where the cameras are located and

placement of the guards. Also, the ultimate prize is to find the location of the vault.

When penetrating a computer, the cracker begins with data-gathering techniques, using Google hacking and other informational sites. Once this is complete, the cracker typically begins by performing a remote

port scan to see which are the potential avenues of entrance to the computer system or network.

Once the ports have been identified, the next step is to find vulnerabilities in the open applications discovered in the port scan. Now, the cracker is finally ready for the heist and launches an exploit.

## LeakProof



**Vendor** Trend Micro  
**Price** \$45-\$85  
**Contact** [us.trendmicro.com](http://us.trendmicro.com)

Trend Micro LeakProof is an all-in-one appliance that comes with everything preloaded. All the admin needs to do is configure the device. The initial configuration is done by attaching a power cord, a PS/2 keyboard and a VGA cable to the device. The underlying operating system is Linux, but have no fear if you are a Linux novice – the configuration is completely menu-driven and no command line commands are necessary. Once the initial setup is complete, the machine will have an IP address

and you can configure the device using HTTP, HTTPS or SSH. Unless you are a Linux pro, I would stick with the HTTPS install.

In most environments, the DLP product is installed with the help of an engineer. This helps identify data whether it be personal clients' information, intellectual property, personnel information, classified information (which has not been classified as public) and industry secrets. By knowing what information needs to be protected, you can configure the unit to watch out for sensitive information. As mentioned before, the install is quite simple and the main purpose of the engineer is to assist the company in defining exactly what sensitive information is to be protected. There are pre-built templates for standards such as SOX and GLBA, etc., and these rules can be customized or created using a wizard interface. LeakProof can also use regular expressions (regex), keyword and metadata for each file as search vectors.

The client-side software is very well done. In essence, the client is a well-intentioned rootkit. The client runs without an icon in the system

tray, the process does not show up in the process list, and the utilities directory is hidden from Windows Explorer. It basically comes down to this: if the client doesn't know it's there, they are less likely to tamper with it.

The documentation was industry standard PDF files broken into easy-to-find pieces.

At \$45-\$85 per seat, the Trend Micro LeakProof offering is at the low end of the price range.

Trend offers free support for the first year, and additional years and features are available for an additional fee. It is our Best Buy.

SC MAGAZINE RATING	
Features	★★★★★
Performance	★★★★★
Ease of use	★★★★★
Documentation	★★★☆☆
Support	★★★★☆
Value for money	★★★★★
<b>OVERALL</b>	<b>★★★★★</b>
<b>Strengths</b> A product with too many features to be covered in this review.	
<b>Weaknesses</b> The deployment of the client software may require some advance planning.	
<b>Verdict</b> A very solid product at a great price.	



A very solid product at a great price. Our Best Buy.

**Justin Peltier**



**Small & Medium Business (SMB)** (888) SMB-TREND, (888) 762-8736

**Enterprise** (877) 21 TREND, (877) 218-7363

For more information: [DLPIInfo@trendmicro.com](mailto:DLPIInfo@trendmicro.com)