

A variety of products attempt to close escape routes to stop unauthorized transfer of files or information based on a set of rules, says Peter Stephenson.

One of the most important security functions today is protecting organizational secrets. We finally have entered a world where everything important is on a server or workstation somewhere in our organizations. Certainly we're nowhere near paperless, but the really

important stuff lives happily in our systems as data bits and bytes. It also travels around — on our networks, in email, on thumb drives, on CDs, etc. How do we ensure that critical data, intellectual property and the like don't grow wings and fly our nicely protected coop?

Today we cannot offer that assurance. But we can close many escape routes effectively. As always, there is the beginning of a convergence in this market space. Two years ago, the term extrusion prevention was hardly known. Today, it is a major piece of the enterprise security tool kit.

SureView, v5.0



Vendor	Raytheon Oakley Systems
Price	\$100,000
Contact	www.raytheon.com/oakley

Raytheon Oakley Systems SureView appliance offers very complete extrusion prevention with a twist. Along with the usual event reports, the appliance can replay the actual event, including pre-encryption data. As an investigative tool, this capability is unsurpassed by any other product feature we've seen.

Because SureView uses agents at the endpoints (user workstations), virtually all data leakage policies can be monitored, including the use of peripherals such as thumb drives. The product comes with over 200 pre-made policies and making new ones is not difficult.

Installing the appliance was easy using the installation guide provided. We found that it installed like

most other types of appliances with which we are familiar. The installation guide takes you through the installation, setup and configuration processes and other documentation takes over from that. The entire process is fairly intuitive.

SureView performed very well and it was easy to replay an entire incident. The replay feature behaves like a DVD player and every action by the offending user is recorded as a set of screen shots. As a forensic evidence tool this capability really shines. Using the replay feature, you can see exactly what the violator did to cause an alarm. Usually, this is enough to encourage the violator to admit their act. For accidental behavior, this function is an excellent teaching tool. For deliberate violators, this provides all of the forensic evidence you will need.

Documentation for the product is very good, but we found the web site a bit thin, mostly consisting of marketing materials. There are extra-cost support packages available and documentation is available online for those users with a support contract.

The product is very expensive

with a price tag of \$100,000. This, however, is for unlimited users, so for a large enterprise this product is a good value.

We liked this product for its forensic capability, but as a straightforward extrusion prevention product, it did quite nicely as well. However, at its high price it will most likely find its best application either in large organizations or in applications where extremely high control of internal information leakage is important.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★☆
Value for money	★★★★☆
OVERALL RATING	★★★★★
Strengths	Extremely powerful, exceptional forensic capabilities.
Weaknesses	High price.
Verdict	If you need very strong data leakage protections with powerful forensics, this is the product for you. For its unique approach to forensics, we designate this product Recommended.



Extremely powerful, exceptional forensic capabilities.

Peter Stephenson

Raytheon
Oakley Systems

For more information, contact:
Raytheon Oakley Systems, Inc.
2755 East Cottonwood Parkway, Suite 600
Salt Lake City, Utah, 84121 USA
1.800.662.9120
info@oakleynetworks.com • www.raytheon.com/oakley