

Ophir Optronics takes a Measured Approach to Information Security

Background

Ophir Optronics (est. 1976) is an international leader in precision IR optic, laser measurement equipment and 3-D non contact measurement scanning. Ophir's team, including its subsidiaries (USA, Japan, Germany), consists of more than 300 scientists, engineers and technical support personnel, providing service to thousands of customers worldwide. Ophir Optronics Ltd. has been publicly traded since 1991.

Ophir Groups operate three primary lines of business: The Laser Measurement Group produces a complete line of laser measurement instruments for analysing, profiling and measuring laser power, energy, laser wavelength and other sources of light; the Optics Group produces optical components, lenses and telescopes for sophisticated electro-optics systems with expertise in IR; Optical Metrology (Optimet), one of Ophir's subsidiaries, provides sophisticated Non-Contact measurement sensors for distance and Non-Contact 3-D measurement systems for a wide range of markets: automotive, aerospace, quality control, in-process inspection and reverse engineering applications.

The Challenge

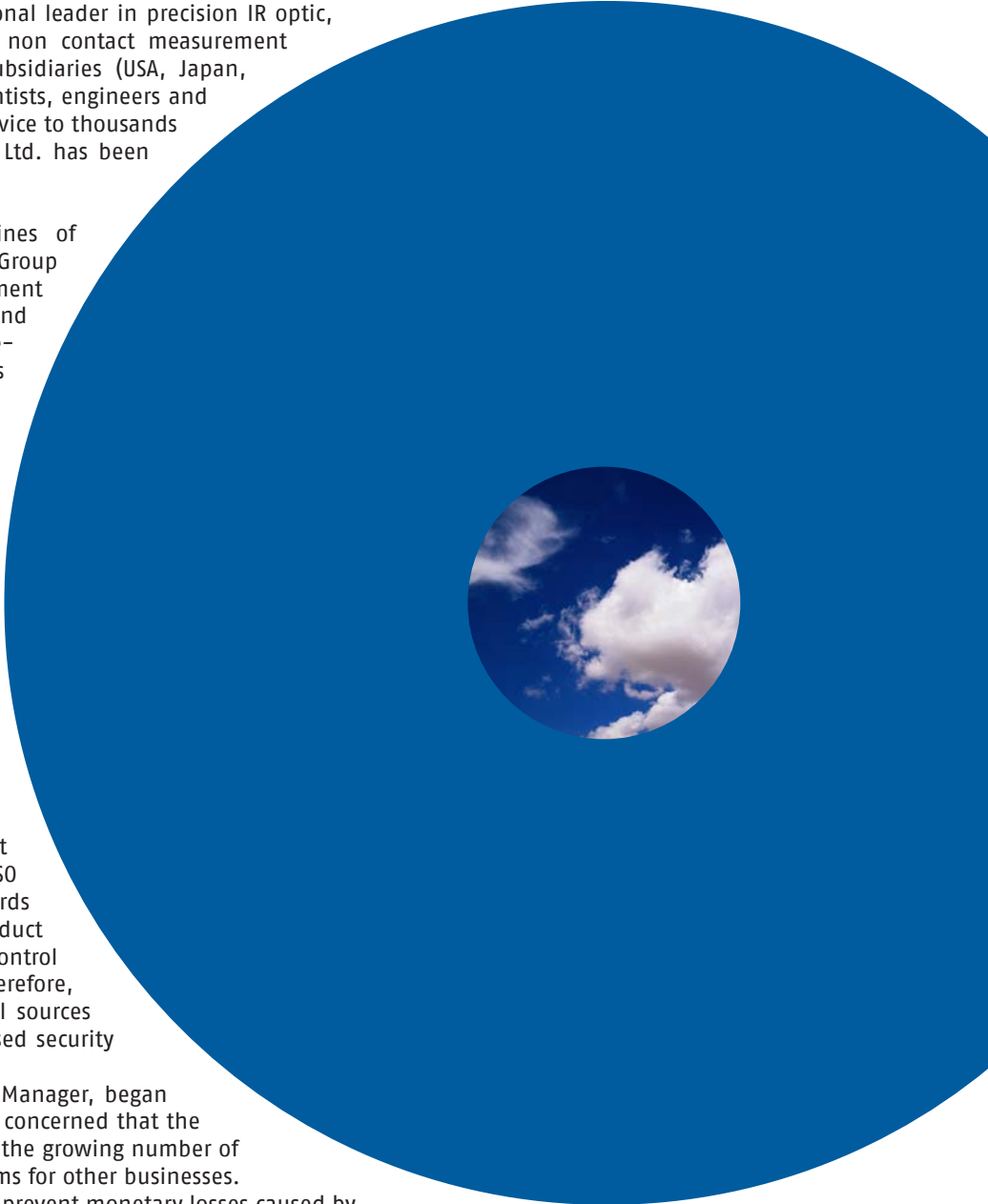
Production at Ophir Optronics' three groups involves high-tech development and manufacturing facilities. Ophir's ISO 9001:2000 certification and quality standards require extensive quality control of all product lines and products. Some product control processes do not tolerate interruption. Therefore, the company must minimise all potential sources of downtime, including those from IT-based security intrusions.

In 2001 Ruth Kadmiel, Ophir Optronics IT Manager, began to seek a more effective security solution, concerned that the company be adequately protected against the growing number of viruses and Trojans causing serious problems for other businesses. There were two main motivations: one, to prevent monetary losses caused by interruptions to manufacturing and two, of equal importance, to prevent any damage to the company's brand image that might be caused by an information technology breach.

"Our company deals with leading-edge technology companies and we could not allow our IT systems to be vulnerable to compromise by malware or data theft. Of special concern was the easy availability of portable storage devices", says Kadmiel.

Initially, the company had deployed an e-mail filter in addition to two separate anti-virus solutions from different vendors. However, it became clear over time that no amount of reactive methods would be sufficient to protect the network from malware infection.

"We do have AV on our workstations, so any previously recognised virus would be found, but we also have experienced an average lag time of about 4 hours by the AV companies! That's about 3 hours, 59 minutes and 59 seconds too late to protect a network", reports Kadmiel.



Managing Remote Access The Solution

Being a global company, Ophir Optronics has a team of employees who travel all over the world. This created a need for a solution that would enable and manage secure remote access for these mobile employees while they were at customer sites, regional offices or industry shows. Similarly, Ophir needed to manage the use of removable media such as USB flash keys in a way that presentations could be taken out to a customer site, for example, without incurring the risk of data theft or of having malware imported to the system when the mobile employee reconnected to the network.

"Our people in the field represent a risk when returning to the company with no more protection than AV," complained Ophir's System Administrator Maxim Noudelman.

The Solution

Ophir Optronics had clearly defined their requirements for a security solution which would take a dual hardware and software approach to defending the network. This protection would prevent unauthorised egress of company information and thwart network infection via e-mail, internet use or removable media such as USB keys, iPods or other infected devices.

The company had initially employed SecureWave's executable file security solution to prevent execution of unauthorised programme downloads onto the corporate network and to permit integrated access to the internet. SecureWave Sanctuary® Custom Edition permits the IT manager to take complete control over execution of software and files on the corporate network. By setting up a list of known and authorised files, Sanctuary® Custom Edition enforces company security policy by creating a "default deny" environment on the network. Only authorised files can execute, everything else is prevented from running on the system. This means that spyware, Trojans, worms, viruses, or simply unauthorised software such as games or P2P file sharing programmes are prevented from running. Antivirus software is required only to clean deadware off the system, which means that most patching can be done when it is convenient to the IT manager and employees, rather than "fire fighting".

A Two Pronged Approach to InfoSecurity

Ophir Optronics examined the pros and cons of buying solutions from different vendors to tackle the dual security threat from software and removable storage media. After reviewing several solutions on the market, Maxim Noudelman demonstrated to Ruth Kadmiel the comparative effectiveness of SecureWave Sanctuary® Custom Edition

for preventing software infection on workstations and terminal services machines. After due consideration, Kadmiel also selected to deploy SecureWave Sanctuary® Device Control at Ophir Optronics for prevention of any unauthorised connection of removable media and USB devices to the corporate network. The emphasis was on its ability to manage the threat from removable storage media such as USB flash keys, iPods and digital cameras.

"We haven't found anything that installs as easily and runs as transparently as Device Control," commented Noudelman and Kadmiel.

Ophir Optronics considered the option to choose a multi-vendor solution but decided to choose both solutions from SecureWave to ensure a tight integration between Ophir's hardware and software security solutions. "We had to ensure that the security programme we installed didn't conflict with anything else on our system. SecureWave Device Control was exactly what we were looking for to control the use of removable storage media. With Custom Edition, the two products in combination give us a really tight fit," says Ruth Kadmiel.

The Deployment

300 licenses of both Sanctuary® products were purchased and the initial roll out involved 120 workstations. The deployment took around one week with a little longer to set up the authorised list of executables.

"We were encouraged by the SecureWave 'default deny' approach to software and hardware accessing the network. It's more proactive. Prior to implementing Device Control and Custom Edition, we were concerned about updating signatures in a timely fashion because of a new vulnerability being announced. We were always running after the latest threat," Noudelman said.

Ophir Optronics was also attracted to the fact that SecureWave Sanctuary® products are sold on a single purchase, rather than a subscription basis. Once the software is purchased and installed and the list of allowed software is set up, it just keeps on working and protecting the system. Unlike AV software, there is no need to keep updating signatures and paying for new versions in response to new virus alerts or vulnerabilities being identified.

"We checked out a lot of other programmes but they didn't cover every potential threat as effectively as Sanctuary® Custom Edition and Sanctuary® Device Control together. We found some good programmes that take care of some aspects, but Sanctuary® Device Control and Sanctuary® Custom Edition cover it all," Kadmiel added.

Policy Enforcement Without Intervention

Ruth Kadmiel reports that there were some management issues to be handled when the software was rolled out because Sanctuary® absolutely enforces company security policy by allowing only known and authorised devices to be connected to the desktops and specifically authorised software to run on the company network.

"Device Control and Custom Edition are transparent, without interfering with the job of the business. For the most part, the main difficulties of the roll out were interpersonal", Ruth Kadmiel reports. "Where an employee was used to working in a certain way, we had to assist them in with reorganising the process in a more secure way. We needed to help them adjust to the fact that only specifically authorised software and removable media would be permitted on the Ophir Optronics network. The fact is that SecureWave's software is being used to enforce company policy instead of the IT Department staff trying to do it. Those employees that most objected to Sanctuary® Device Control were the ones who were also against enforced company policies. I believe that these objections will be short-lived once staff realise that the policy has been put in place to protect the business. Over the long term, Sanctuary® will reduce the conflict between those that enforce policy and those that have to live with it. We have enabled them to be secure yet remain efficient in the method they use to get their work done."

Some production managers along with their employees had meetings with Kadmiel to find out what exceptions, if any, were needed to the new user policy to allow them to work efficiently. Together they planned how best to deal with it. The sales team report that they are pleased that they are now able to use a disk on key - albeit using a specifically designated device, allocated to a named user, because they are able to download presentations and leave the USB key with the customer. Prior to deploying Sanctuary® Device Control, use of USB storage devices were not allowed, but were difficult for the IT management to control.

Sanctuary® Device Control is granular enough to allow IT management to authorise named employees to use specified removable storage devices at certain times of day, with the ability to track all data downloaded to removable media, an aspect which aids compliance with security regulations. Far from being restrictive, this granularity has enabled the IT management at Ophir to allow certain individuals more flexibility whether for in-house production efficiency and or for travel.

One company VP who recently travelled to Europe to a show reported that, due to the deployment of Sanctuary® Device Control, he found it much easier to work with clients. As an authorised user of an authorised device, he was able to store the latest company presentation on a USB flash key and leave this with his prospect. "Being able to work now this way facilitates continuity of product awareness, a positive factor for closing a sale," says Ruth Kadmiel.



Taking Security Requirements to the Board

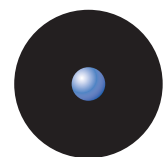
Ophir Optronics has found that the risks from malware and removable media have been reduced substantially following deployment of Sanctuary® Custom Edition and Sanctuary® Device Control. Ruth Kadmiel also values the time that Sanctuary® will free up from reactive patching because IT department technicians are able to delay some patches for more testing or patch in batches and there is no need to race against the clock whenever a new vulnerability is announced. She also values highly the fact that Sanctuary® has provided a definitive combined solution, which only requires one purchase payment, rather than paying out multiple subscriptions to multiple AV solution vendors.

"Everyone always measures the money against the risk," she reports. "Sanctuary® gives us a clear argument to present to the board: If we were to go into a meeting with a prospective customer and we lacked protection against transfer of malicious software through our removable storage, this could cause permanent loss of the account – particularly were the customer to have a high security rating."

Kadmiel goes on to explain that, because Sanctuary® Custom Edition and Sanctuary® Device Control has brought Ophir Optronics to an optimal level of protection against running application level threats such as spyware and viruses, the risk of downtime has been substantially reduced. Again this gives a potent argument to the board level executives, since a day's downtime would cost a significant amount. "If we were unable to fulfil a customer order on time because of downtime caused by malware or a denial of service attack, this could directly impact customer satisfaction and future sales," she explains.

Future Developments

Ruth Kadmiel reports that Ophir will complete the roll out of the full 300 licences within the Israel office. Following successful deployment there, the company plans to roll out the dual solution of Sanctuary® Custom Edition and Sanctuary® Device Control to the US office and other subsidiaries. This will have the added benefit of enabling the international teams to work collaboratively over the Internet, safe in the knowledge that all the offices are working to the same high standards of security as the Israel office. "By implementing a common solution, which only allows authorised devices and software to run on the corporate network, we solve the difficulties of enforcing policy across international boundaries," she says. "Best of all, no more patch updates are needed in the middle of the night! The System Administrator can get a night's sleep!"



SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com