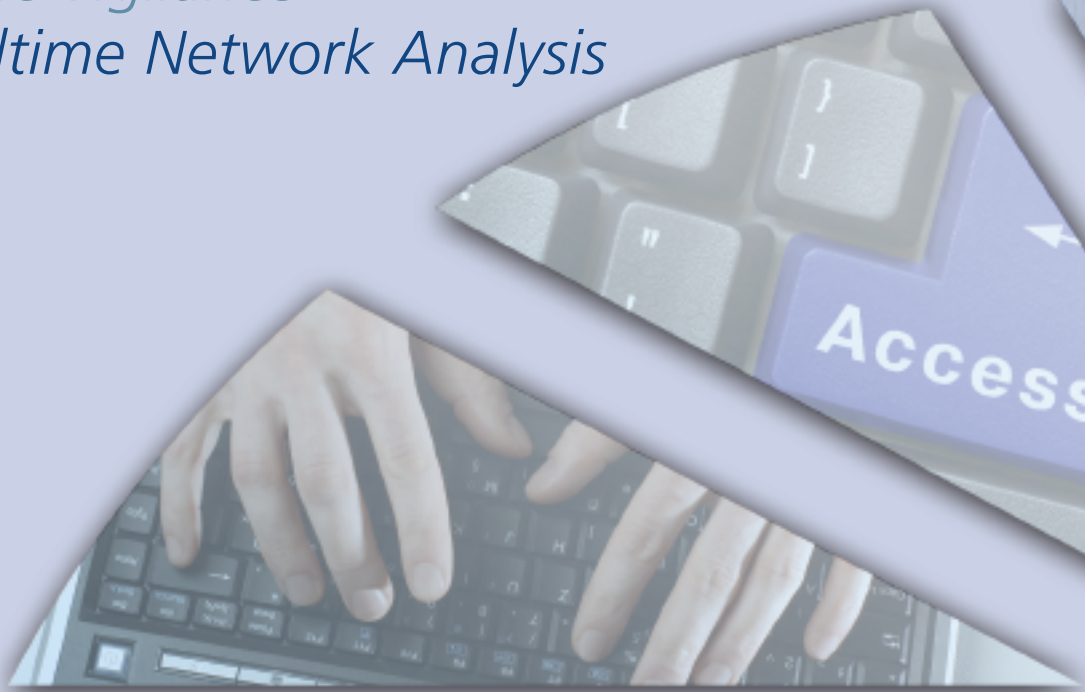


opticvision

Optic Vigilance

Realtime Network Analysis



"From the instant it is switched on, Optic Vigilance software allows any organisation to ring-fence and protect their most sensitive information."

Overview

Optic Vigilance is a unique software application designed to counter the twin threats of deliberate commercial espionage, the equally devastating accidental loss of sensitive data and equipment, and the subsequent effect on that organisation's reputation.

Optic Vigilance software allows any organisation, for example: academic establishments, armed forces, banks, business, the medical profession, police or even governments to ring-fence and protect their most sensitive information, their most critical assets and most important transactions from the instant it is switched on, and to safeguard them every second of every day.

Every electronic transaction, and especially those out of the ordinary, is immediately identified, recorded and reported upon. And those making the transaction are immediately identified and monitored.

Optic Vigilance is like an all-seeing electronic sentry with a clear and simple but nonetheless vital set of orders: stop critical information and indeed equipment - like laptops and PCs - from leaving your organisation without you knowing.

Threats to Business

The catalyst for the creation of Optic Vigilance was an analysis of the threat to sensitive information; which is significant and growing. Statistically, the biggest threat to business or official secrets is by individuals actually inside the company or institution who are willing to betray their organisation or to commit fraud or insider trading; the annual cost of such acts is estimated at £100 billion. Given the vast electronic network that is now our academic, business, diplomatic, financial and political world, it has become much easier to betray confidences and secrets, and to undermine credibility and reputation.

Regrettably, recent high profile incidents demonstrate only too clearly that many organisations clearly see information security as being an optional extra rather than a core function and this attitude threatens every business activity of that organisation.

Serious security breaches in particular across Europe and the US have arisen from accidental data leakage and loss of customer information from networks and laptops. These acts have brought into sharp focus the severe impact of such transgressions on companies' and individuals' financial well-being and reputations.

Threats identified and analysed include:

- Industrial espionage by competitors or insiders
- Leaking of official documents
- Commercial data loss or data leakage
- System tampering or loss
- Identity theft
- Intellectual Property theft
- Financial fraud
- Insider Trading
- Product Shrinkage
- Freight loss
- Careless information management
- Poor electronic document security
- Improper use of company networks
- Deliberate acts of electronic sabotage

In each case, the use of Optic Vigilance software could have monitored and prevented the incident from taking place.

“Current systems cannot defend against individuals leaving laptops in taxis or, indeed, identity theft - currently one of the fastest growing IT security threats. This system can.”

Why is Optic Vigilance Different?

Currently, information security depends largely on a mix of products to protect against the external and internal threats:

- **To protect the network from external attack, organisations typically use firewalls, content filters, antivirus and anti-spyware systems.**
- **To defend against the internal threat, the latest outbound network traffic content filtering applications help protect an organisation.**

To complement the software and hardware is what we call 'thinkware': the organisational policies and procedures which must be written and enforced to deal with the complexities of the real world. These can sometimes be conspicuous by their absence. Even when they do exist, making sure that employees conform to them can be extremely difficult.

Generally speaking, the first time a company knows that its policies and procedures have been ignored is either when they suffer a serious financial loss; when a competitor steals an unexpected march on them; or when a catastrophic security breach leads to customer exposure and unwanted media attention. Having procedures is one thing; enforcing and ensuring continuous compliance is quite another.

Current software and hardware tools do not as yet constitute a fully-integrated security solution. Content filtering software has at best limited and, at worst, no ability to guard against encrypted information leaving the system or to identify deliberately fraudulent transactions. Similarly, current systems cannot defend against individuals leaving laptops in taxis or, indeed identity theft - currently one of the fastest growing IT security threats. This system can.

Finally, you do not need to use technology to attack a system or the intellectual property of a company. Information can leave unobtrusively (and illegally) in pockets, backpacks or handbags on discs, on memory bars, or as printed documents - as well as quietly disappearing into the network by perhaps being emailed to a home address or an anonymous email account. The end result is the same: loss of information, loss of profit, loss of reputation. In some cases the loss of sensitive personal data has led to massive fines for the companies which lost the data as well as the inevitable reputationally damaging questions about organisational capability, efficiency, and management competence. Optic Vigilance can protect you from this dangerous situation.



“Optic Vigilance protects against the external and internal threats by a unique integrated approach, combining software, hardware and thinkware in one application.”

How does it Work?

Optic Vigilance protects against the external and internal threats by a unique integrated approach, combining software, hardware and thinkware in one application. This integration provides powerful overlapping layers of security which both ring-fence and protect your vital information and critical transactions - and of course ultimately your reputation; your continued success and your profitability.

Optic Vigilance in its most basic configuration is a software application which is installed on a dedicated Optic Vigilance server. This server is then connected to the organisation's computer terminals. The programme then propagates out from the Optic Vigilance server to the users chosen by the company and installs itself on the user terminal.

The application is completely invisible and undetectable (we have had it tested by computer forensics experts) and will not impact on company personnel's ability to work. Optic Vigilance has also been very carefully designed not to be a drain on either power or resources: it uses less than 5% of the CPU capacity for 95% of the time, which is considerably less than some ordinary processing applications.

To ensure Optic Vigilance is configured precisely the way you want it, a rule set is decided by the organisation's management; for example: it may wish to be alerted whenever financial spreadsheets are opened, emailed, or printed.

Or it may be that the management team want to know when someone accesses next year's price or product list; or the latest sales brochure, proposals or exam questions; or the Holy Grail: the customer database.

In the medical profession we can protect patient records and Doctors' notes; for the police we can protect the names of sensitive sources or current operations. Optic Vigilance will alert you that someone has accessed such information, and will also alert the user that they may be in breach of company or official policy and should remind

themselves of the correct procedures. Optic Vigilance can therefore be used for staff education as well as compliance. It can also alert management when inappropriate surfing or activity takes place in breach of company or organisational policy, or when someone is spending too much time on the internet, and not enough time at work.

Optic Vigilance therefore works on five different levels; monitoring the following:

- **Activity - what people are doing**
- **Application - what they are using**
- **Content - what they are looking at, modifying, saving, or emailing**
- **Device - what are they doing it with**
- **File - the location of the item**

However, for a much more sophisticated approach, by integrating Optic Vigilance with existing security systems, for example: CCTV or access control, then we can ensure that information and equipment stays where it is meant to. This integrated approach will allow the capture of CCTV images of users, who may be doing something you do not want them to do, to be stored for later analysis on a Digital Video Recorder.

For example: if an individual downloads data to a USB stick, or burns a DVD or CD, which just happens to be put into a pocket or handbag, then this will be caught on CCTV as the system will have been programmed to do this. Then Optic Vigilance will send an electronic warning to your IT and security staff as well as the user, or email the image to the security director. Further: if a laptop is removed from the network, after a predetermined period of time, Optic Vigilance will shut it down, and destroy the data on the hard drive. Our RFID technology could also completely prevent such removal by the use of Optic Vision RFID tags coupled with access control systems. And if you currently do not have these systems, we can install them too.

“Optic Vigilance provides an efficient, layered and cost-effective security solution that will not cost the earth, but will help you save a fortune.”

Why do I need it?



- Optic Vigilance provides a unique software application which will provide exceptional levels of electronic security to your organisation, whatever its function.
- When Optic Vigilance is integrated with other security systems, it provides an impenetrable electronic shield to protect your organisation from internal and external threats.
- Optic Vigilance allows your company to ensure that its policies and directives are followed by tracking system usage trends whilst simultaneously ring fencing and protecting critical assets and transactions.
- From the second it is installed and activated, Optic Vigilance will have a profound impact on security standards in your most critical areas.
- Optic Vigilance will keep your business or official secrets secret.

What are the Key Benefits?

Optic Vigilance provides:

- A unique way to fill the gaps in existing IT Security infrastructures.
- A system to help manage the threat from illegal insider activity, for example: the leaking of information or its physical removal from the system or premises
- An innovative software framework which provides the missing link between IT and Physical Security systems
- Complete electronic audit trails to assist regulatory compliance and subsequent investigations.

Optic Vigilance provides an efficient, layered and cost-effective security solution that will not cost the earth, but will help you save a fortune.



| | | | |
|--|--|---|--|
| TIER 1: OVERSEE MONITORS Devices, Files, Applications, Content and Activity | CAPABILITIES eFom Transaction Recorder (Audit Trail) | HIGHLIGHT The creation of an electronic "carbon copy" at the point of data input: laptop or PC | ROLES To make sure that the transaction is both safe and permitted |
| | Screening of Confidential Information Usage | Optic Vigilance captures the moment when information is manipulated, both pre and post encryption | To identify data leaking from the network; to make sure that the transaction is both safe and permitted |
| | Device and File Usage Audit Trails | To create an electronic audit trail of activity both at the point of entry: the PC or laptop, but also on the server | To identify data leaking from the network; to make sure that the transaction is both safe and permitted |
| | "Learn-As-You-Work" User Education and Mentoring | Real-time user alerts to prevent/curb undesirable behaviour | User education and training; to identify data leaking from the network; to make sure that the transaction is both safe and permitted |
| TIER 2: OVERWATCH CONTROLS Devices, Files, Applications, Content and Activity | CAPABILITIES Device Control | HIGHLIGHT OVERWATCH is the electronic equivalent of 'superglue' to prevent the introduction of external devices; it will also prevent media being removed from a device, and will stop file sharing over a network | ROLES To stop sensitive or proprietary information leaking from the network or PC |
| | Loss of Laptop/System AWOL | A range of pre-defined actions to be carried out in a system or laptop if it goes missing: for example destroying some or all of the data on the laptop. | To stop sensitive or proprietary data being obtained by those not authorised to have that data |
| | File, Application and Content Control | Block access to or time lock files, applications and/or content | To stop sensitive or proprietary data being obtained by those not authorised to have that data and to ensure it is only received by those authorised to receive it |
| | Fine Tuned Application Control | Block commands which may cause security concern, for example: Save As, Import, Export, Print, Window Minimize | To stop sensitive or proprietary information leaking from the network or PC; to stop inappropriate activity taking place on the system |
| | CAPABILITIES Integration with existing electronic security systems such as access control systems, access control systems, RFID tracking, DVR or CCTV. | HIGHLIGHT Electronically and visually record and then store the activities of individuals attempting to tamper with the system or remove media from the office. The RFID tags ensures complete traceability and management of the equipment, and integrates seamlessly with access control systems Verify the identity of those involved | ROLES To stop sensitive or proprietary information leaking from the network or PC To stop removal of equipment or hardcopy: To stop sensitive or proprietary data being obtained by those not authorised to have that data and to ensure it is only received by those authorised to receive it |
| TIER 3: OVERARCH INTEGRATE OVERSEE and OVERWATCH with CCTV, Access Control and RFID Technology | Integration with multi-factor authentication systems | To counter identify theft To control and monitor access to sensitive applications and confidential content | To stop sensitive or proprietary information leaking from the network or organisation To stop sensitive or proprietary data being obtained by those not authorised to have that data and to ensure it is only received by those authorised to receive it |