

## vigilancepro

**VigilancePro® from Overtis is a comprehensive user activity management solution that protects high value information assets and IP.**

Through the use of a unique integrated and layered approach to information security, VigilancePro™ enables organisations to visually identify and manage exactly how users access, process, store and transmit sensitive information.

### Promoting Positive User Behaviour

VigilancePro™ implements and encourages positive user behaviours in line with information security policies to comprehensively prevent unintentional - as well as malicious - data loss, by implementing controls where they are most effective, between the user and the information. Any intervention is least-restrictive, intelligent and appropriate - minimising operational impact.

Legitimate information flow is improved whilst at the same time data leaks are prevented.

The VigilancePro™ solution complements traditional security products and adds a much needed user-centric approach to preventing information loss.

### Transparent Effective Enforcement

VigilancePro™ uniquely provides transparent and effective enforcement of a company's security policies based on the understanding that the majority of data losses are unintentional and due to a lack of security awareness and education.

According to research around 77% of leaks are the result of the actions of undisciplined employees. In combination with Security Awareness programs (mandated by standards including PCI DSS and ISO 27001) VigilancePro™ can keep users on the 'path of acceptable use', driving and promoting positive user behaviour around the secure handling of confidential information.

### Customisable On Screen Prompts

Initially in response to specific actions - such as copying a file to a removable drive, or attaching a key financial spreadsheet to an email - warning dialog boxes can be presented to the user reminding them of their obligations when handling sensitive or regulated information. Dialog boxes can be customised to include links to Intranet sites containing relevant policy documentation. Dialog boxes can also

## USER EDUCATION & AWARENESS

allow the user to input a free text description of a valid business reason for a particular action, minimising operational impact.

These features provide 'user mentoring', specifically designed to reinforce user awareness training, before moving to more stringent blocking and prevention of actions. On screen alerts and prompts provide softer 'learn as you work' user education.

The ability to present the user with multiple choices in response to particular actions provides a non-intrusive powerful feedback mechanism for ongoing policy development.

### Least Restrictive Response

Action in response to a particular event is configurable. Intervention is least-restrictive, intelligent and appropriate. Minimal operational impact leads to increased efficiency.

Legitimate information flow is improved whilst at the same time data leaks are prevented.

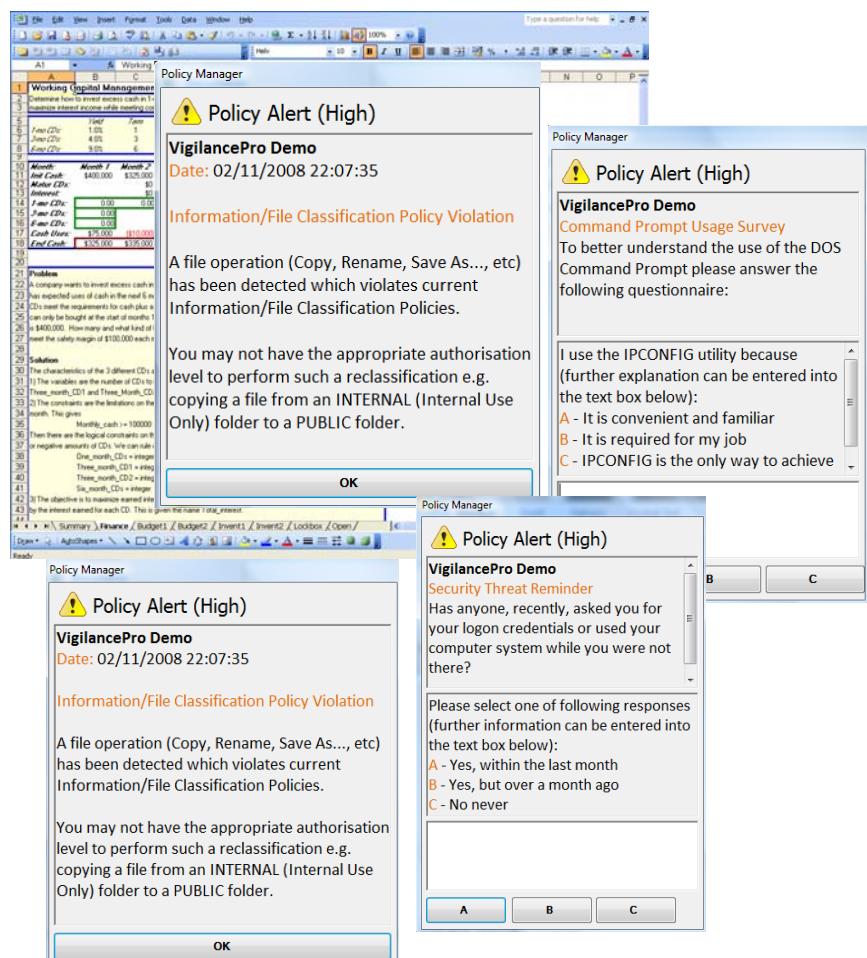
Responses include:

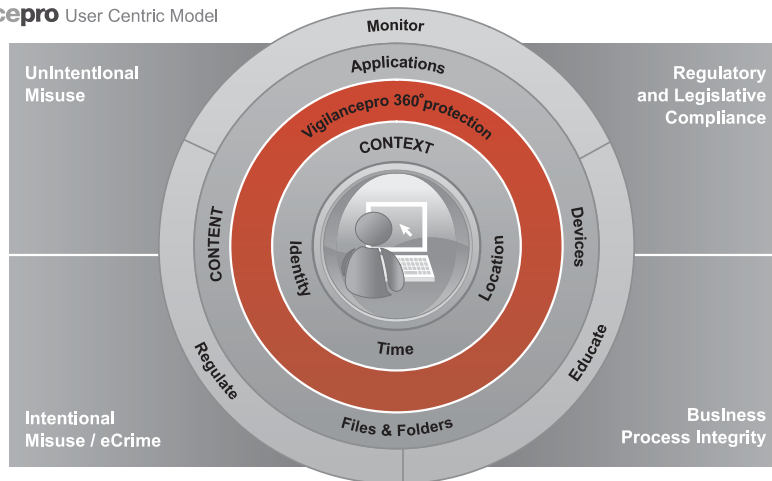
- Monitor
- Monitor and Alert User
- Monitor, Alert and Justify (requires the user to enter a valid business reason for a given action)
- Monitor, Alert and Authenticate – requiring the user to use a fingerprint or finger vein reader to prove *who* they are
- Prevent and optionally freeze workstation

### Realising Compliance

The unique on screen user education features within VigilancePro™ reinforce security education programs through continuous communication of policy and acceptable use guidelines, meeting the on-going training requirements within standards such as ISO/IEC 27001.

Combined with advanced visual audit trail and reporting features VigilancePro™ enables organisations to rapidly prove compliance, or non-compliance, with a range of regulations and legislation.





**Key Features**

- Patented next generation endpoint security software solution
- Unique user-centric framework enabling transparent and highly effective security policy management and enforcement
- Fully customisable policies may be applied to individual users, groups, or across the organisation – leveraging Microsoft® Active Directory structures
- Advanced rules engine – fully content and context aware (including time and location)
- Registry and Windows event log watchers included
- Integrated OCR capability for content and activity analysis of legacy 'green screen' applications
- Complementary to other endpoint products (including AV, anti-spyware and personal firewalls)
- Real-time monitoring of user and system activity and events
- Protection of fixed and mobile endpoints
- Agents for servers and terminal servers
- Integration with physical security systems (including CCTV, access control, and RFID)
- Integration with biometric devices enabling transaction authentication
- Centralised management of agents and policies
- Centralised summary (dashboard), detail and trend reporting
- Full visual audit trail (optional desktop screen shots and CCTV images with local playback)
- Optional support for two-factor authentication for VigilancePro® Manager access as well as requirement for two people to enter passwords to access certain views
- Fully configurable response as a result of an event (alert, notify user, require justification, prevent, freeze system)
- Automated email alerts as well as daily, weekly, monthly reports
- Automated archiving of events
- Highly scaleable (Web Services based architecture)
- Software core based on managed code (.NET) for ease of deployment and security.

**Key Benefits**

- Prevention of unintentional as well as malicious data loss
- Unique user-centric multi-layered approach to protection of sensitive information assets
- Integration of physical and logical security systems to maximise existing investment, improve risk management and realise tangible operational and financial benefits.
- Physical security integration - with CCTV, access control systems and RFID – enables implementation of powerful location based policies
- Comprehensive IT security policy management and enforcement, without impact to approved business processes and information flows
- Reinforcement of user education and awareness programs through on screen prompts, dialog boxes and alerts, providing softer "learn as you work guidance, raising awareness to the risks associated with certain actions (or attempted actions)
- Flexible least restrictive intervention in response to actions promotes positive user behaviour combined with increased user accountability
- Transaction Layer Authentication requires users to authenticate to complete specific transactions - proving who completed an action (even if passwords are shared or compromised)
- Mobile Device and Mobile User Management delivers added protection of lost or stolen laptops - with the ability to remotely delete information securely for example
- 360 degree coverage across the entire information estate for the occurrence of specific keywords and phrases, or particular data formats or types - such as credit card PANs, social security and NI numbers, NHS or other health service numbers – simplifying compliance
- Terminal Server Agent provides strong security for outsourced third party access as well as enabling the creation of highly secure zones within the network
- Support for Syslog/SNMP for integration with other management consoles and SIM/SEM solutions

- Support for multiple VigilancePro® servers provides enterprise scalability and separation of events by type, location, business unit, role etc.
- Advanced application shaping enables specific functions in applications – such as Cut, Copy, Paste, Rename, Save As, Print - to be limited depending on the user, group, time, and location
- Management of unauthorised transfer of sensitive information to local hard drives, public folders and removable media
- Option to encrypt files using Encrypted Vault Manager (EVM) and ensure only encrypted data is copied to removable media or attached to emails
- Comprehensive visual audit trails provide evidence of compliance (or non-compliance) with policy, best practice, standards, regulations and legislation

**System Requirements**

**Agents**

VigilancePro® agents are available for:

Microsoft® Windows XP Professional, Windows Server 2003 & 2008 (including Terminal Server)(32-bit only), Windows Vista, Windows 7

**Agent Pre-requisites**

.NET Framework version 2.0

Windows Installer 3.1 or later

512MB memory (1GB recommended)

Minimum 10MB of free disk space

**VigilancePro® Server**

Microsoft® Windows Server 2003, or Microsoft® Windows XP Professional with IIS\*

.NET Framework version 2.0\*

1GB memory (2GB recommended)

Minimum 40GB of free disk space

\* IIS and .NET must be installed prior to installing VigilancePro® Server software

