

## vigilancepro

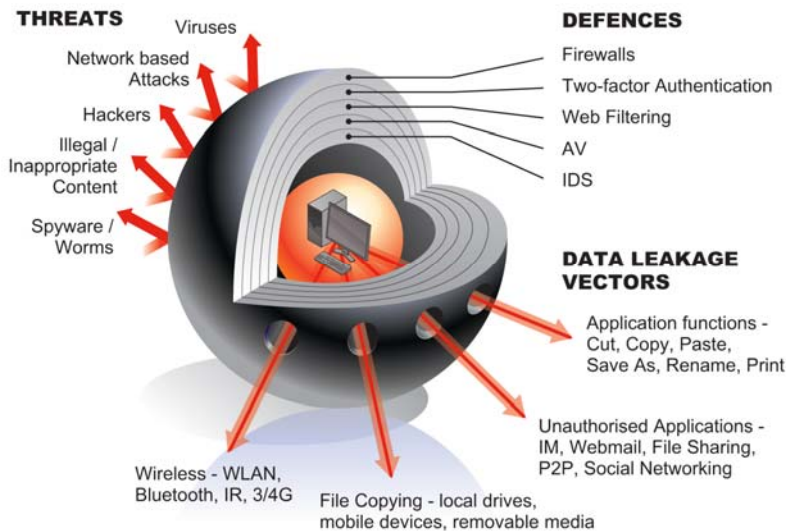
**VigilancePro<sup>®</sup> Enterprise from Overtis is a comprehensive user activity management solution that protects high value information assets and IP, preventing data loss.**

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<sup>™</sup> solution complements traditional security products and adds a much needed user-centric approach to preventing information loss.

### At Rest and In Flight

VigilancePro<sup>™</sup> can provide strong controls over how information/files are not only stored and processed - but also transmitted and shared, particularly externally.

The monitoring and protection features of each layer can be combined to provide a

powerful and flexible policy management and enforcement capability.

Policies can prevent dissemination of information via email, web mail, IM, FTP, Skype, social networking sites etc. Even printing of sensitive documents can be restricted.

Copying of files and folders to removable media (such as USB drives) - as well as local drives in mobile devices - can be fully monitored or prevented.

If copying is allowed then information transferred can be encrypted using strong algorithms (AES 256-bit) with Encrypted Vault Manager (EVM), to ensure that even if information falls into the hands of unauthorised parties it cannot be read.

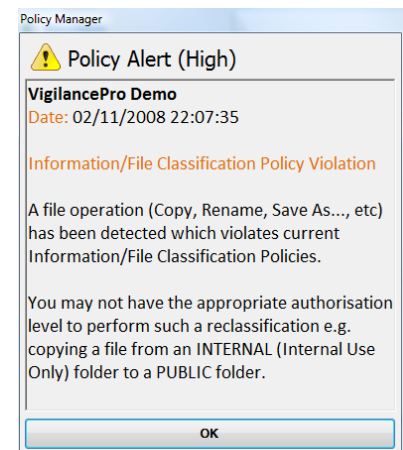
### Complete Application Control

Advanced application shaping enables specific functions in applications to be limited depending on the user, group, time, location, or a combination of attributes. Cut, copy, delete, save as, and export can all be disabled within Microsoft Excel for example.

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 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.

### Physical Security Integration

Integration of physical and logical security systems maximises existing investment, improves risk management and realises tangible security, operational and financial benefits.

VigilancePro can extend physical entry controls and policies linking them to key information assets ensuring that **even if unauthorised physical access is**

### 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<sup>™</sup> can keep users on the 'path of acceptable

## OVERVIEW

**gained, logical access to sensitive data is denied.**

VigilancePro integrates with physical security controls such as access control systems, CCTV and RFID - as well as biometric devices (including fingerprint and vein readers) - to significantly enhance the physical security perimeter.

Policies **limiting certain actions to specific monitored locations, as well as to particular individuals**, can be implemented and enforced.

Extending logical security and combining logical with physical security controls can provide powerful policy management and enforcement of:

- visitor and contractor access - and attempted access - to premises
- entry or attempted entry to computer rooms and data centres
- access to secure cages or racks within facilities
- visual monitoring of hosting environments

Integration with door entry systems enables:

- enforcement of 'low man count' policies with the option to prevent access to sensitive data, or to certain applications or application functions, if occupancy of a given area drops below pre-determined levels
- the ability to freeze user sessions if the user leaves a given area to prevent unauthorised access through session hijacking
- the ability to freeze all workstations in a secure area if the area is empty (overnight, during breaks, or as the result of a fire alarm)



### Beyond Passwords

Particular user actions that may be entirely unintentional but potentially harmful - or even malicious or fraudulent - can be monitored and prevented.

Irregular actions might include a high quantity or other unusual stock movement, a transaction above a certain value, or a large number of repeated transactions in a short period of time.

**Integration with biometric devices enables policies requiring users to prove who they are before completing certain tasks**, preventing password sharing or the use of another user's account on a sensitive system if left unattended.

Biometric information - with photographic evidence in the form of CCTV images - combine to provide compelling evidence of the individual that carried out a particular transaction, action or operation. Equally CCTV sequences can prove that a user was absent when a particular task was carried out.

### Content & Context Awareness

VigilancePro is both content and context aware. Context might refer to user, time, application, specific application function, file or folder location, media or device, or transaction value or frequency.

Specific data formats - such as credit card PANs, bank account numbers and sort codes, social security and National Insurance numbers, tax codes and NHS or other health service numbers - can be identified in real-time and secured to protect employees and consumers and ensure compliance with the ever increasing amount of legislation and regulations.

### Flexible Information Classification

VigilancePro provides the basis for the rapid introduction of simple yet highly effective information classification programs.

Folders can be classified very simply by folder name.

A simple classification scheme with three levels - Public, Internal Use, and Confidential - can be introduced by creating corresponding rule sets for each of the levels, eliminating the typical complexity associated with implementing a classification program.

Using wizards rules can be created that ensure only certain users can read, change or copy confidential information.

### Low Impact Day Zero Implementation

At the point of introducing a classification scheme folders and shares become 'classified zones' for different types of information - often aligned by department, division or function.

Specific additional levels can be created - associated with information relating to particularly high value or high sensitivity projects as needed.

### Document Classification

For Microsoft® Office applications (Word, Excel and Powerpoint) VigilancePro can extend classification to files. Users are automatically prompted to select a classification for every document,

spreadsheet or presentation on Save (or Save As). The protective marking is inserted into the metadata of the file and can be optionally added anywhere in the header or footer.

### Extending Classification to Email

With increasing amounts of corporate information contained or distributed in emails, VigilancePro can extend file and folder classification programs to email messages.

Using a remote handler (or plug-in) for Microsoft Outlook the same classification levels that can be applied to files can be applied to emails - with users prompted to select a classification level for each message from a simple pop-up on clicking Send (or use of Alt-S).

Recipient lists can be limited based on the classification level selected. Internal Use may limit recipients to the same or trusted domains. Confidential emails may only be sent to pre-defined recipient lists. File attachments can be limited to encrypted files created with the integrated Encrypted Vault Manager (EVM).

### 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. 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

### Compliance In Depth

VigilancePro provides immediate compliance with many of the requirements and controls within a range of regulations and legislation by providing detailed visual audit trails of interaction with information, linked to content and context.

Organisations that adopt standards to help navigate through the legislative and regulatory minefield derive significant benefits - most notably through increases in productivity, efficiency, effectiveness, agility and a reduction in risk.

VigilancePro provides a sophisticated framework directly addressing more than 60 of the 133 controls within ISO/IEC 27001 - the global standard for information security best practice.

## Legacy Applications

Integrated OCR capability within VigilancePro enables content and activity analysis for legacy 'green screen' applications - many of which were written before detailed logging and auditing of user actions was required. VigilancePro can extend the life of many older applications avoiding costly alternatives.

## In Depth Reporting

VigilancePro provides a comprehensive visual audit trail of events across all user activity. Individual alerts may optionally include desktop screenshots, a screenshot of the relevant application window, all foreground window text, and CCTV footage. Each event is assigned a severity and date and time stamped with user details.

Events, or notifications, are viewed centrally within the VigilancePro Notification Viewer, a powerful interface that displays all individual notification details along with any attachments.

Detailed incident trend reporting can be run on demand or at specified intervals (daily, weekly, monthly). Powerful multi-dimensional analysis (based on asset, information classification level, application, user, department, group etc) highlights unusual or suspicious - as well as malicious - user or administrator activity quickly.

Interactive 3D charting provides rapid drill down to specific actions.

## Automated Executive Summaries

Summary and executive dashboard reports, providing at-a-glance change and short term trend analysis, can be automatically emailed to key stakeholders at configurable intervals.

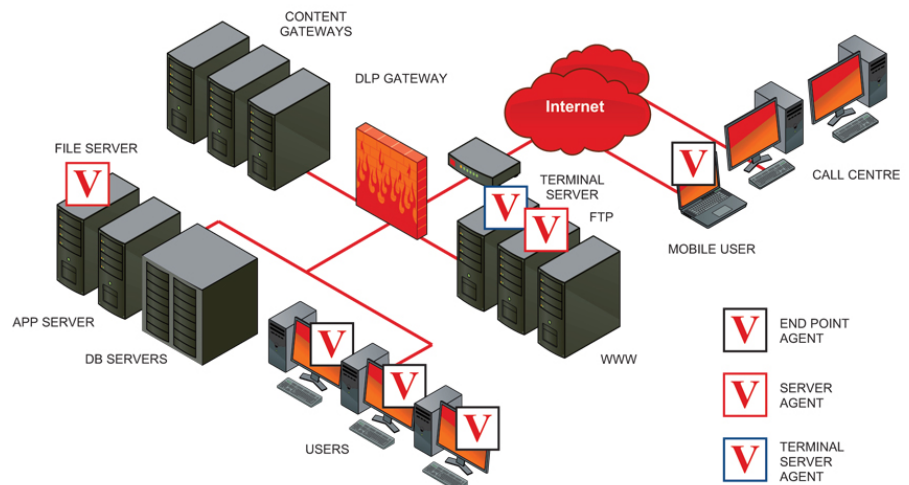
Reports provide a unique insight into user interaction with critical information and enable operational and policy fine-tuning regularly to improve or adapt security over time.

## Actionable Alerting in Real-time

Immediate email (or SMS or pager) alerts can be generated from the VigilancePro Manager as soon as a critical or severe event occurs ensuring security staff - including guards - receive timely notification of suspicious or malicious activity.

## Comprehensive Enterprise Coverage

Agents deployed on fixed and mobile endpoints, as well as terminal servers and key file servers, provide powerful protection inside and outside the blurring corporate perimeter.



If access is over terminal services the same threat management is achieved as if an endpoint agent was installed on the remote clients. The Terminal Server agent also enables the creation of highly secure zones within the network.

The VigilancePro Server agent was developed specifically for compliance applications where a full audit trail of which users accessed which key files on file servers is required. Because the server agent is installed on the server it can capture a subset of what the endpoint agent is able to monitor. Server agent notifications include:

- Username (from Active Directory)
- Date and time stamp
- File Open, Create, Modify (tied to the update of the date last modified file attribute), Rename, Delete

Centralised agent management and reporting is provided via the VigilancePro Server. Changes and updates to rules and policies are pushed out to the agents that store rules and policies locally on the endpoint.

Support for multiple VigilancePro Servers provides true enterprise scalability and separation of events by type, location, business unit, role and job function. Support for Syslog/SNMP simplifies integration with other management consoles, as well as SIM/SEM solutions.

Granular role based access to the VigilancePro Manager, along with optional enforced entry of two passwords to view particular management information as well as integration with two-factor authentication solutions, ensures access is protected and admin and ops staff only see information that is relevant to them.

## Mobile Endpoint Protection

The VigilancePro endpoint agent ensures that any policies persist outside the corporate perimeter on mobile devices. Policies are pulled down and kept locally on the endpoint.

If no connection is available to the VigilancePro Manager events are stored on the mobile device in an encrypted form and uploaded immediately a connection with the VigilancePro Server is available.

## Device Lost or Stolen

VigilancePro agents can be configured to communicate with both an internal and external (Internet facing) VigilancePro Server.

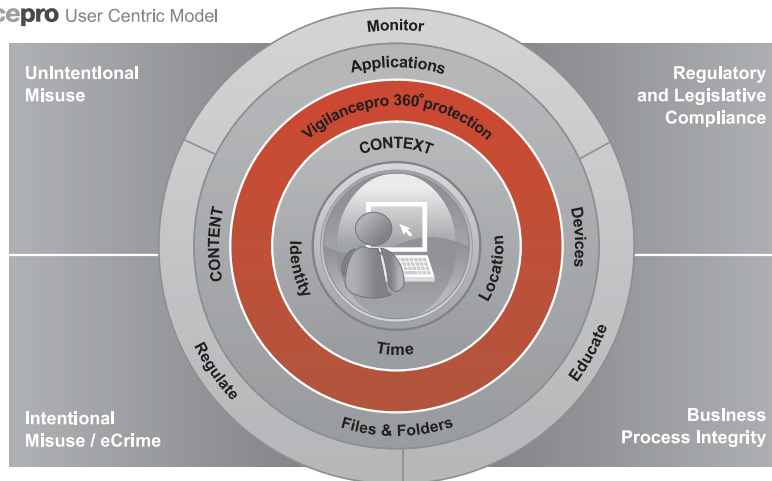
If mobile systems are lost or stolen VigilancePro agents can be configured to delete specific files and folders - or format the hard drive completely - if they fail to connect to the internal server for a period of time. Agents can be configured to run any arbitrary code on the endpoint after a set number of hours or days.

If a lost or stolen device is subsequently connected to the Internet agents can send information to the external VigilancePro Server.

## Mobile User Management

It is increasingly common for employees to continue to have access to mobile devices around the time of leaving an organisation.

VigilancePro provides complete protection during these periods enabling individual user activity to be subject to further restrictions, or their activity to be monitored more closely.



**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

