

vigilancepro

INFORMATION CLASSIFICATION

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 unique 'user-centric' approach to preventing information loss.

Flexible 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 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.

Implementation can be phased over time with initial focus on information that can be readily identified as Confidential - such as financial, HR and customer personal or account data.

Monitored & Controlled Classification

VigilancePro™ supports two different types of classification - Monitored and Controlled.

With Monitored Classification detailed audit trails are provided of classifications and re-classifications, as well as actions on classified files (such as open, modify, delete and print).

Moving a file from one folder to another may re-classify the file if the destination folder has a different classification level to the original.

Controlled Classification adds restriction of file movement based on user group membership.

Full audit trails are provided of file classifications and re-classifications - brought about by relocating files - with users prompted and reminded of the implications through on-screen dialog boxes.

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).

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 corporate perimeter.

The VigilancePro™ Terminal Server agent provides protection when third parties - such as outsourcing partners, vendors and offshore staff - access sensitive systems remotely. If access is over terminal services the same threat management is achieved as if an endpoint agent was installed on the remote clients.

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

At Rest and In Flight

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

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, linked to classification levels.

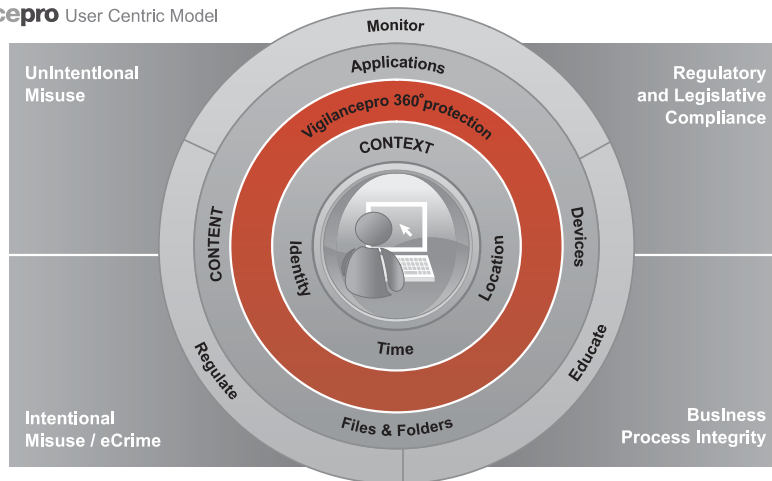
If copying is allowed then information transferred can be encrypted using strong algorithms (256-bit AES) with Encrypted Vault Manager (EVM), to ensure that even if information falls into the hands of unauthorised parties it cannot be read.

Realising Compliance

The implementation of simple yet powerful classification schemes can have a dramatic impact to the overall levels of protection of key information assets.

VigilancePro™ provides the foundations for classification schemes recommended or mandated in multiple standards.

Combining Information Classification capabilities with other features of VigilancePro™ enables organisations to directly address more than 60 of the 133 controls within ISO/IEC 27001 - the global standard for information security best practice.



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

