

vigilancepro

MOBILE USER & DEVICE MANAGEMENT

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.

Unique Security Model

VigilancePro™ uses a layered approach that not only allows companies to manage devices, file and folder access and application use, but also analyse instances of keywords and phrases.

Additional layers provide:

- User Guidance – ensuring that interaction with sensitive information is in line with security policies – through softer “learn as you work” on screen alerts, dialog boxes and prompts.
- Physical Security – a dedicated layer manages integration with physical security systems
- Transaction Layer – mandates authentication to complete specific actions

The monitoring and protection features of each layer can be combined to provide a powerful – and flexible - policy management and enforcement capability

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.

Intentional - or unintentional - user activity continues to be monitored and prevented. Different rules and policies can be applied dependent on location as well as connection type.

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.

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.

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 (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.

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.

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

Content & Context Awareness

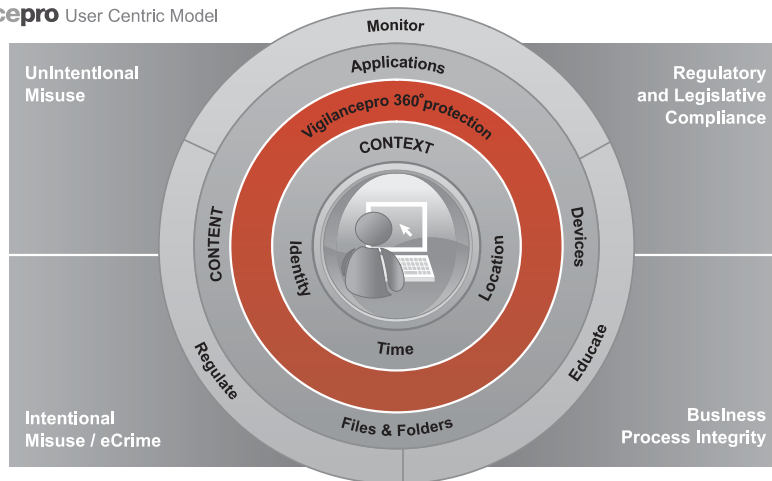
VigilancePro™ is both content and context aware. Context might refer to user, time, application, specific application function, file or folder location, media or device, or transaction value or frequency.

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.

Compliance In Depth

VigilancePro™ can dramatically improve an organisation's overall corporate governance posture and compliance with the requirements of the Data Protection Act, PCI DSS, FISMA, HIPAA, GLBA, and SOX.

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 – including those relating specifically to mobile devices (A.11.7.1).



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

