

vigilancepro

ACTIVITY ANALYSIS & PRE-FORENSICS

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.

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.

Notification Data

Notification data is held on the VigilancePro™ Server within an SQL database – either Microsoft SQL Server 2005 Express with Advanced Services, or SQL Server 2005 for larger deployments.

In addition to the built-in reporting capabilities within VigilancePro™ industry standard reporting tools can be used to query the database directly. Notifications can also be exported to Microsoft Excel.

Archiving & Standalone Exports

The VigilancePro™ Manager can be configured to automatically archive notifications from the database daily, weekly or monthly to efficiently manage local storage.

Data overwriting (with a fixed amount of storage) combined with automated archiving allows 'set and forget' style operation.

In addition to archiving, Standalone Exports of events can be created from the VigilancePro™ Manager - to CD or DVD media for example.

Each Export includes not only full notification details but also a light version of the VigilancePro™ Manager software so that information within the Export can be viewed on any PC platform.

Pre-Forensics

VigilancePro™ can identify user behaviour associated with security breaches, providing the ability to see and stop problems before they occur.

In support of evidence handling procedures Standalone Exports feature the ability to enter a free text description of why a particular Export is being created.

Realising Compliance

The rich reporting features and full visual audit trail of all user interaction with critical files and folders satisfy the requirements of a wide range of standards, regulations and legislation, and enable organisations to demonstrate due diligence and prove attestation levels at any stage of the compliance lifecycle.

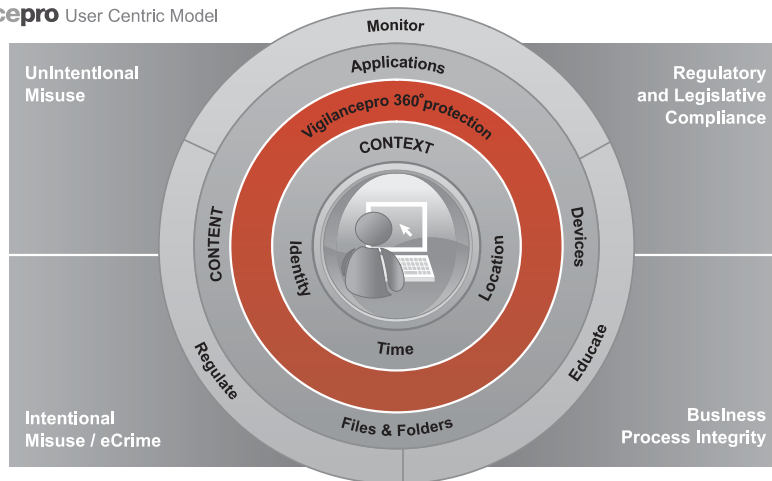
VigilancePro™ provides the ability to identify the occurrence of particular data formats, such as credit card PANs, social security and National Insurance numbers, NHS or other health service IDs, in real-time.

Any exceptions - instances of data outside of authorised applications or locations – are highlighted.

The Endpoint, Server and Terminal Server agents combined provide comprehensive coverage of the enterprise – including third parties with access to systems remotely.

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.





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 point 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

