

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.

Overcoming Complexity

Compliance covers a broad spectrum of both internal and external activity - understanding processes, mapping key data flows, designing policies, selecting appropriate controls, executing/implementing those controls, monitoring control effectiveness, gathering evidence, identifying risks, raising issues, monitoring the progress of remediation work, understanding dependencies and mitigating circumstances.

Choosing solutions that address a broad range of controls and requirements is critical in simplifying complex compliance programs and minimising associated costs.

Compliance In Depth

VigilancePro™ provides immediate compliance with many of the requirements and controls within a range of regulations and legislation.

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.

It also addresses many of the key requirements of Payment Card Industry Data Security Standard (PCI DSS).

Visual Audit Trails

To have a significant impact on compliance program efficiency and effectiveness solutions should enable organisations to prove due diligence and attestation levels at any stage in the compliance lifecycle, supporting both the internal and external audit processes.

VigilancePro™ provides a comprehensive visual audit trail of events across all user

activity providing a unique insight into how users interact with sensitive information. Individual alerts may optionally include desktop screenshots, a screenshot of the relevant application window, all foreground window text, and even CCTV footage.

Each event is assigned a severity and date and time stamped, with user details.

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. 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. 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

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.

360° Negative Assurance

A great deal of the compliance effort concentrates on segregating information such as cardholder data and personal

identification information (personal data) into well protected and defined areas within the overall infrastructure.

Outside of these defined areas, or zones, there is often limited detection for the occurrence of regulated or sensitive data. Often the only outbound filtering on traffic for sensitive content leaving a logical zone is limited to obvious channels such as email, web mail and IM. This presents a multitude of data leakage vectors to people inside the organisation.

The constant is the user, who has a need to access information from different directions, locations and therefore through a variety of applications.

VigilancePro™ provides complete 360° visibility across the entire information estate for the occurrence of specific keywords and phrases, such as sensitive project and product codenames, or particular data formats or types.

Physical Security Integration

Integration with physical security systems including CCTV, access control & RFID, ensures that even if physical access is gained, logical access to information is denied.

Many of the standards and regulations include strong physical security controls. VigilancePro™ assists organisations by realising physical and logical security system convergence, simplifying compliance.

Least Restrictive Response

Action in response to a particular event is configurable. Any intervention is least-restrictive, intelligent and appropriate – minimising operational impact.

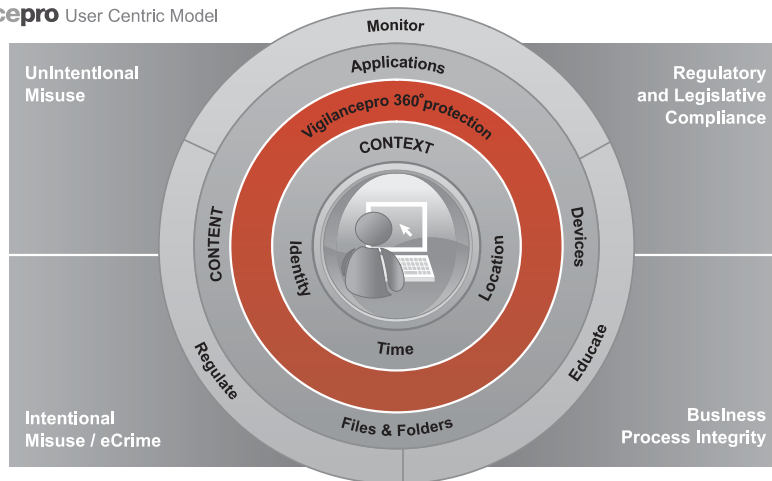
Legitimate information flow is improved whilst at the same time data leaks are prevented.

Responses include monitor, alert user, justify (requires the user to enter a valid business reason for a given action), authenticate, prevent and freeze workstation.

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.

COMPLIANCE IN DEPTH



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

