

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.

An Integrated Approach

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

Strengthening the Physical Perimeter

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

PHYSICAL SECURITY INTEGRATION

- 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)

Detailed Visual Audit Trails

A full visual audit trail of date and time stamped events is provided which include supporting log entries from access control systems.

VigilancePro™ integrates with both traditional DVR and IP-based CCTV systems with the ability to attach video frames to events - evidence that may prove invaluable in the event of hardware tampering or theft.

As well as CCTV frames, each notification sent to the VigilancePro™ Server can include desktop screen shots as well as foreground window text, to further enhance the information available centrally, assisting decision making and analysis.

Actionable Alerting in Real-time

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

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.

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 devices such as fingerprint and vein readers can require 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.

Least Restrictive Response

Action in response to a particular event is configurable. 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 time value or frequency.

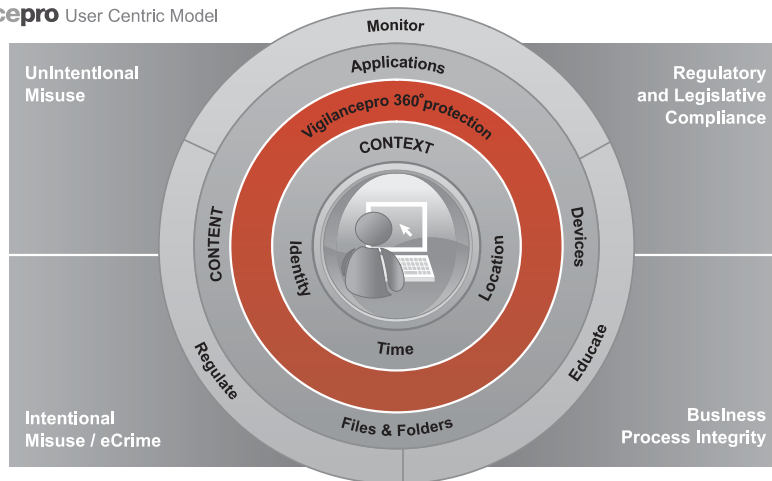
Integration with physical security systems increases the number of context variables available – most notably by adding location to policies, as well as requiring individuals to prove who they are with more than just a Windows or network login.

Compliance In Depth

VigilancePro™ can dramatically improve an organisation's overall corporate governance posture and compliance with regulatory and legislative requirements.

The unique physical and logical security integration features provide unrivalled coverage of controls recommended or mandated within standards such as PCI DSS.

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 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

