

vigilancepro

TRANSACTION AUTHENTICATION

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.

Leveraging Convergence

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.

Layered 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.

Transaction Driven Authentication

VigilancePro™ integrates with physical security controls such as access control systems, CCTV and RFID - as well as biometric devices (including finger vein readers) - to significantly enhance overall security.

Through the Transaction Layer VigilancePro™ can enforce the use of strong two-factor authentication devices - including tokens, smart cards and biometric readers - by time of day,

location, as well as individual transaction, action or operation.

Transactions of a particular type, or above a particular value – where relevant - may require the user to authenticate in order to complete them.

Even if users share passwords or gain access to an unlocked terminal they are prevented from carrying out restricted or controlled actions.

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 biometric devices enables policies requiring 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. Equally CCTV sequences can prove that a user was absent when a particular task was carried out.

Finger Vein Technology

Because finger veins are inside the body and invisible from the outside, finger vein patterns are extremely hard to steal and do not change with age. Finger vein patterns are different even in identical twins.

A clear finger vein image can be captured using near-infrared light and the "transmissive light photographing method".

Accuracy is extremely high with a 0.01% FRR (False Rejection Rate), less than 0.0001% FAR (False Acceptance Rate), and 0% FTE (Failure To Enrol).

Authentication speed is faster than alternate biometric technologies with one-to-one authentication in under a second.

Finger vein devices are small, cost effective and simple to deploy - connected to the endpoint via a USB port.

Visual Audit Trails

A visual audit trail proving that a particular user account from a particular workstation was used to perform a particular transaction, action or operation, with biometric evidence of the individual (from a fingerprint or vein reader for example) - backed up desktop screenshots - can be provided.

The transaction layer and physical layers combine to ensure that sensitive transactions, actions or operations can only take place in certain camera monitored areas and by certain people. The addition of CCTV images further reduces the chances of repudiation.

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.

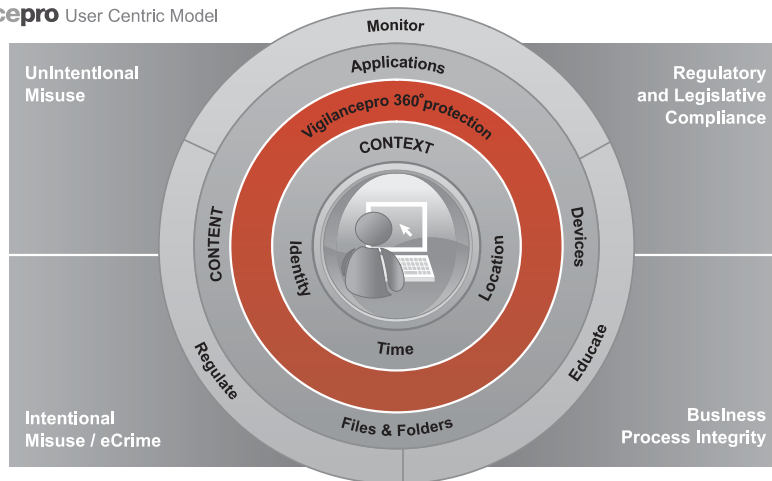
Responses include:

- Monitor
- 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.





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

