

VigilancePro™ -- Guarding Against Data Loss

VigilancePro™ provides organisations with protection from both internal and external threats; it allows organisations to decide and implement security and alert policies; it integrates with existing software security systems; and it uniquely connects physical and logical security systems to fill the gaps in existing IT security infrastructures.

The protection of information, whether for commercial or compliance reasons, is one of the greatest challenges today facing businesses and organisations of all sizes. A key challenge in all business sectors is how to address the needs of security without adversely impacting on day to day operations, and, equally as important, to do so without contravening an individual's civil rights and personal privacy.

VigilancePro gives a company the ability to cope with the whole spectrum of national and international compliance regulations, legislation and best practice ranging from the Payment Card Industry Data Standards, to Sarbanes Oxley and ISO 27001.

VigilancePro™ mitigates threats to IT systems such as:

- **Fraudulent and Unauthorised Transactions**
- **Insider Trading**
- **Financial Fraud**
- **Identity Theft**
- **Social Engineering**
- **Shrinkage (Inventory Loss)**
- **Freight Loss**

Key Benefits

VigilancePro™ has the following key benefits:

- The protection of selected endpoints and information on a network, regardless of size
- The transparent and effective enforcement of company policy, ensuring legitimacy of transactions
- Interactive, learn as you work user education through on screen alerts, prompts and questionnaires
- Ensuring users are more accountable for their actions through;
 - Transaction level authentication
 - Keeping audit trails of confidential information changes and movement
 - Guarding against accidental data loss
 - Providing user authentication / alerts before information is written to public folders or removable devices such as CDs, DVDs or USB memory sticks
- 'Laptop Lost' capability - protecting laptops and their contents once removed from the network

VigilancePro™ monitors and manages:

Activity Both on and off-line activity

Applications Including: MS Office, Web Browsers, Instant Messenger, etc

Content Data at Rest, Data in motion

Device Including (but not exclusively) USBs, CD or DVD, Bluetooth, COM and LPT ports

File File classification and movement

VigilancePro's™ on screen guidance and questionnaires help users become part of the solution rather than part of the problem

System Requirements

Supported Platforms

The VigilancePro™ Client runs on the following Microsoft Windows NT-derived operating systems:

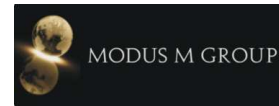
- Microsoft Windows 2000
- Microsoft Windows XP Professional
- Microsoft Windows Vista (Business or above).

The client computer must also have a fully patched .NET Framework 2 (or above) installed.

Client (endpoint) systems require a minimum of 512MB main memory (1GB recommended) and at least 10MB of fixed disc space.

Server Requirements

The VigilancePro™ server software requires Microsoft Windows Server 2003 or Microsoft Windows XP Professional with IIS and .NET Framework 2 (or above) which must be installed prior to installing any of the VigilancePro™ Server applications. A minimum of 1GB (2 GB recommended) of main memory is required, plus a recommended minimum of 40GB of fixed disc space.



Availability/Reliability

VigilancePro™ has the following attributes (or provides features) to support availability and reliability:

- Client systems are not dependant on network connections to the server with configuration and notification data being cached locally on the client (endpoint) system.
- Laptops operate independently when not connected to the server via a LAN connection.

VigilancePro™ Key Features

- Patent pending, next generation technology featuring unique IT and physical security integration
- Checks user and system activity against current policies, in real-time, to create regulatory compliance audit trails, report and/or prevent undesirable actions.
- Highly scalable client(endpoint)/server web-service based architecture
- Core functionality based on managed code(.NET) for greater ease of deployment, management control and security
- Centralized Control and Reporting
- Customizable end user policies
 - Policies based on user groups
 - Time-dependent policies
 - Location-dependent policies
- Single screen reporting dashboard
 - Notification filtering
 - Segmentation and drill-down
 - Trend analysis
 - Report definition
- Daily/weekly/monthly emailed reports
- Daily/weekly/monthly automatic archives

Physical Security System Integration

With unique patents-pending technology, VigilancePro™ is able to integrate with other compatible thirty party systems such as physical security systems, including Finger Vein Biometrics, digital video recorders (DVR) and access control systems delivering a unique, exceptionally robust security environment.

Key Security Benefits

- Freeze logged on user sessions if the user has left the room or building to prevent session hijacking
- Freeze user sessions if room occupancy counts have dropped below pre-determined levels
- Freeze user sessions in the event of fire alarm or other security alerts
- Authenticate application use and critical transactions based on the user's location
- Detect and provide visual evidence through CCTV imagery of hardware tampering and theft, including potential hardware key logger placement
- Provide immediate alerts that can be used directly by security guards so that they can apprehend perpetrators before they leave the building
- Provide automated audit trails and secondary authentication for 'dumb terminal' systems such as IBM AS400 or VAX, or indeed others.

System Highlights

- **eForm Transaction Recorder (Audit Trail)** Point of input electronic "carbon copy" ensures transaction integrity
- **Confidential Information Usage Screening** Pre/post encryption identifies data leakage
- **Device and File Usage Audit Trails** Both end-point (client) and server are monitored to identify and report data leakage
- **"Learn-As-You-Work" User Education and Mentoring** Real-time user alerts help prevent/curb undesirable behaviour and explain policy or procedure breaches to users
- **Device Control** Electronic 'superglue' locks down legacy connections, undesirable devices, removable media and network shares
- **Laptop AWOL** A range of pre-defined actions to be executed in a system or laptop if it goes missing
- **File, Application and Content Control** Blocks access to or time lock files, applications and/or content; blocks commands which may cause security concern, for example: Save As, Import, Export, Print, Window Minimize
- **Integration** Record individuals attempting to tamper with hardware, verify operator identity, lock vulnerable workstations and verify user location. Integration with Finger Vein biometric systems will guarantee user authentication, counter identity theft, and session hijacking. Integration with RFID technology ensures total asset traceability and management and prevents unauthorised removal of hardware and hardcopy.