iManage Threat Manager

PROTECT SENSITIVE DATA AND INTERVENE TO PREVENT DATA LOSS

Key Benefits

- Advanced technologies detect and neutralize sophisticated attacks

- Identify outliers, reduce the risk of a data breach

- Streamline forensic Investigation, drive efficiencies

- Manage information with better visibility and control

- Accelerate compliance by detecting non-filers

- Integrates with enterprise IT security stack

Security + Risk Management + Information Governance

- **iManage Business Intake Manager:** Automated management of business intake procedures

- **iManage Conflicts Manager:** Single view of ethical and business conflicts

- **iManage Security Policy Manager:** Need-to-know security policies and information barriers at scale

- **iManage Threat Manager:** Data protection from internal and external threats

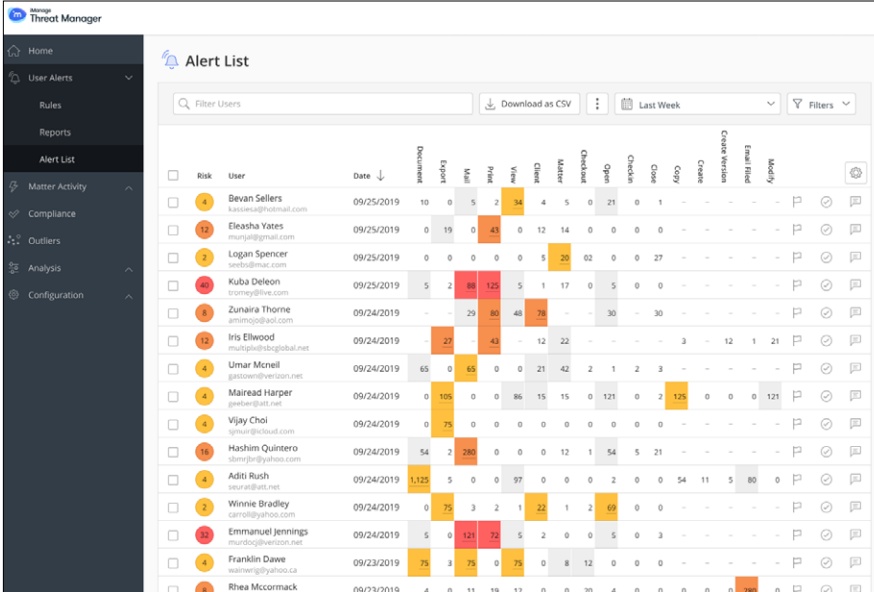- **iManage Records Manager:** Electronic and physical records management

iManage Threat Manager — protect your sensitive data

Clients entrust professional services firms with their most privileged information. But many firms continue to be the targets of high profile phishing attacks, or insider malfeasance, which render the traditional security stack that protects the network perimeter ineffective.

iManage Threat Manager is designed to meet the needs of CIOs, CSOs and compliance officers looking for advanced solutions to protect sensitive data. Threat Manager leverages historical and contextual information in the iManage system to provide faster identification of both external and internal threats, and avoids "false positives" that plague many other approaches. iManage Threat Manager delivers threat detection, monitoring, investigative capabilities, alerts, and reporting to protect sensitive information in your iManage system 24/7 across any device, anywhere.

Modern information security and governance controls

iManage Threat Manager offers granular reporting across multiple entities including users, clients/projects, and matters/engagements to ensure that appropriate controls can be applied holistically to deliver visibility into the access and flow of sensitive data. Further, its adoption analysis allows firms to quantify the risk associated when data isn't being properly filed.

Threat Manager provides 24/7 continuous threat protection enabling you to detect and neutralize threats as soon as they manifest themselves
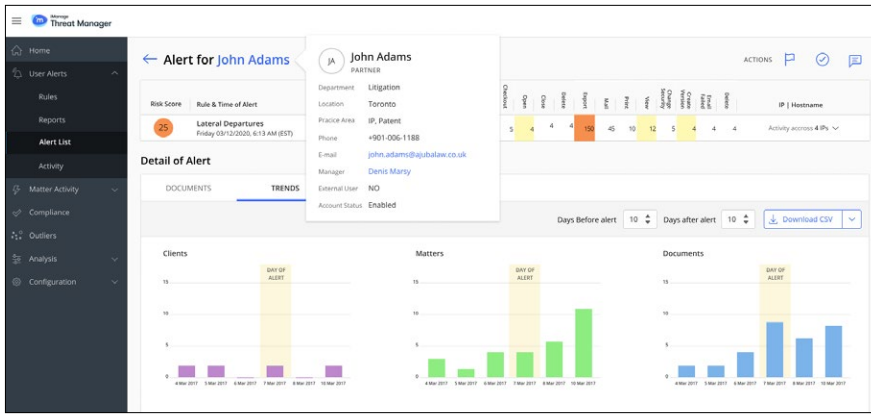
Quickly investigate and neutralize threats with built in reports, advanced forensics and granular event reconstruction

Comply with client obligations

Clients now contractually require firms to demonstrate proper controls to protect sensitive information. It's not uncommon for clients to audit systems and require notification when malicious behavioral patterns are detected. Regulations now require that affected parties be notified within stipulated periods of breach discovery. iManage Threat Manager delivers the threat detection, mitigation and information governance controls that gives clients the confidence that their sensitive data is protected.

Detect threats with the highest levels of accuracy

iManage Threat Manager understands the unique context in which professionals operate — practice areas, clients, and projects — and applies state-of-the-art machine learning against data with high value, such as engagements accessed where no time is billed, or matters accessed outside a practitioner's area of expertise. This ensures that overburdened resources only investigate alerts that have the highest probability of being malicious.

Reduce investigation time with comprehensive forensics

Threat Manager provides advanced forensics and granular event reconstruction to ensure rapid detection and investigation of an alert. Rich contextual information like clients/projects, matters/ engagements and documents allow you to quickly assess the scope of any breach.

Intervene to prevent data loss

The ability to detect and neutralize a threat early before it escalates to a full blown attack is critical. Threat Manager allows you to define custom actions, such as alerting a user or supervisor, escalating to a manager, or disabling an account based on the severity of a threat.

Deploy easily in the iManage Cloud or on-premises

Threat Manager is available as a SaaS service in the iManage Cloud or as an on-premise software appliance. Within hours, an organization can safeguard information with Threat Manager.

Integration with the enterprise IT security stack

SIEM frameworks have become an industry standard for security conscious organizations. REST APIs enable the display of alerts generated by Threat Manager in SIEM dashboards giving the SOC enhanced visibility into malicious activity in the DMS.

Advanced role-based reporting and usage analytics

Protecting sensitive information must go beyond alerting to provide systematic controls to manage information at every level. Threat Manager provides comprehensive user, client, and matter activity reports. Additionally, analytics allows organizations to measure adoption and pinpoint incorrect usage or export patterns.

About iManage™

iManage transforms how professionals get work done by combining artificial intelligence, security, and risk mitigation with market-leading document and email management. iManage automates routine cognitive tasks, provides powerful insights and streamlines how professionals work, while maintaining the highest level of security and governance over critical client and corporate data. Over one million professionals at over 3,000 organizations in over 65 countries – including more than 2,000 law firms and 500 corporate legal departments – rely on iManage to deliver great client work – securely.

iManage
Making knowledge work

Blog: imanage.com/blog