



# Protect sensitive data and intervene to prevent data loss

## KEY BENEFITS

- Detect sophisticated threats from internal or external actors
- Reduce risk of data breaches
- Accelerate forensic investigations
- Reduce false positives, ensuring that resources are spent on alerts most likely to be fraudulent

## SECURITY + RISK MANAGEMENT + INFORMATION GOVERNANCE

- **iManage Security Policy Manager:**  
Need-to-know security policies at scale
- **iManage Threat Manager:**  
Data protection from internal and external threats
- **iManage Records Manager:**  
Electronic and physical records management without professional user burden
- **iManage Conflicts Manager:**  
Single view of ethical and business conflicts
- **iManage Business Intake Manager:**  
Automated management of business intake procedures

## SUPPORTED SYSTEMS:

- iManage Work

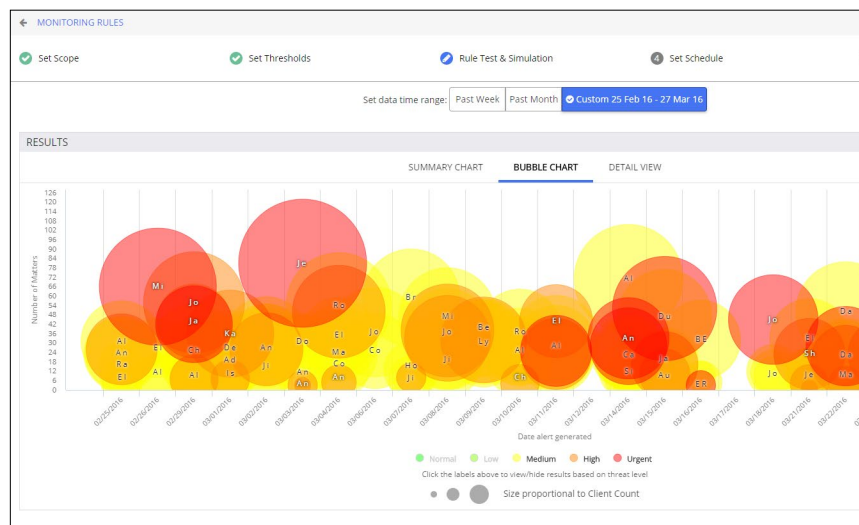
## iManage Threat Manager — Protect your sensitive data

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.

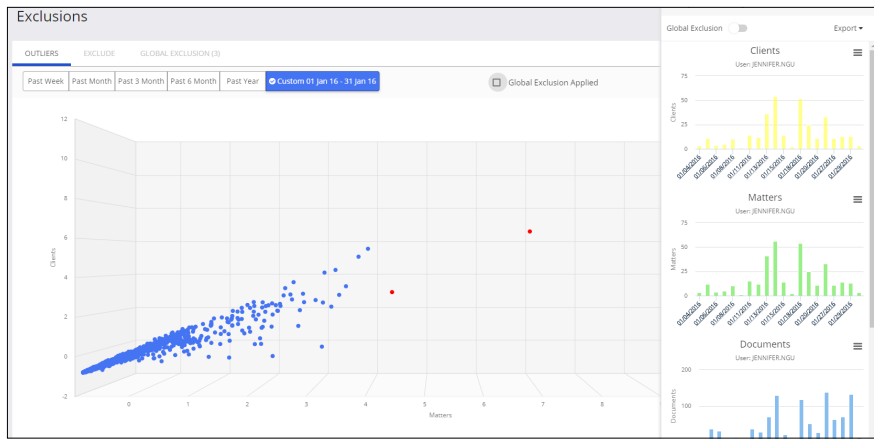
iManage Threat Manager is designed to meet the needs of CIOs, CSOs and compliance officers looking for advanced solutions to protect sensitive data. Threat Manager leverages historical and contextual information in the iManage system to provide faster identification of both external and internal threats, and avoids pitfalls such as “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, and matters 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 gives you the capabilities to exceed the demands of even the most challenging clients.

### 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, matters, 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 deployed as an on-premises software appliance or is available as a SaaS service in the iManage Cloud. Its self-learning algorithms minimize administration and ensure that alerts remain accurate over time. Integration with SIEM tools enables the SOC to see Threat Manager alerts in their application of choice.

### 24/7 Continuous threat protection

Once configured Threat Manager scans for threats 24/7 continuously enabling you to detect and neutralize threats as soon as they manifest themselves.

#### Follow iManage via:

-  [twitter.com/imanageinc](https://twitter.com/imanageinc)
  -  [facebook.com/imanageinc/](https://facebook.com/imanageinc/)
  -  [vimeo.com/imanage](https://vimeo.com/imanage)
  -  [linkedin.com/company/imanage](https://linkedin.com/company/imanage)
- Blog:** [imanage.com/blog/](https://imanage.com/blog/)



#### 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.