ManageEngine DataSecurity Plus

CASE STUDY

About the customer

Steadfast Group is one of Australasia's largest general insurance broker network and underwriting agency groups, providing a wide range of insurance services and solutions to businesses and individuals across Australia, New Zealand, and other neighboring islands. Operating within the highly regulated insurance sector, the organization manages vast volumes of sensitive customer information, financial records, policy documents, claims data, internal reports, and compliance-related documentation on its file servers.

With a workforce of around 1,000 to 5,000 employees distributed across multiple offices, Steadfast Group relies heavily on shared file environments to support daily operations, collaboration, and customer service. As Sofia Basnet, a system administrator at Steadfast Group, explains, maintaining strict control over who accesses and modifies critical files is essential to reduce insider risks and meet compliance requirements.

Challenges

Before implementing DataSecurity Plus, Steadfast Group faced growing difficulties in monitoring file activity across its expanding IT environment.

With multiple file servers and thousands of users accessing shared folders daily, Basnet and her team struggled to gain a clear and centralized view of:

- Who was accessing business-critical files
- What changes were being made
- When those activities occurred

This lack of centralized visibility created several key risks, such as delayed detection of unauthorized or suspicious accesses, limited ability to investigate incidents quickly, and increased pressure during audits and compliance reviews.

Without consistent, real-time monitoring and alerting, potentially risky file activity could go unnoticed. For an organization operating in the insurance industry, that level of uncertainty was not sustainable.

Why DataSecurity Plus stood out

When Basnet and her team decided to evaluate a comprehensive data security solutions for Steadfast Group, her primary focus was finding a platform that could:

- Provide centralized file activity visibility
- Enhance their security posture
- Provide timely alerts to address incidents as early as possible.
- Simplify compliance reporting
- Be deployed quickly without complex configurations
- Offer reliable technical support when needed

Ease of setup was a major consideration. The team needed a solution that would integrate smoothly without long implementation timelines or heavy administrative overhead. Strong technical support was equally important. Given the critical nature of file auditing in a regulated industry, Steadfast Group wanted assurance that expert assistance would be available whenever issues arose or advanced configurations were required.

ManageEngine DataSecurity Plus stood out by delivering:

- A straightforward and quick deployment process
- Out-of-the-box audit reports tailored for compliance and security use cases
- Responsive and knowledgeable technical support

> According to Basnet, the combination of simplicity and support played a key role in their decision. *"Ease of setup and strong technical support were key factors [in choosing DataSecurity Plus]," Basnet said.*

Rather than spending weeks configuring custom scripts or complex monitoring tools, the IT team was able to quickly start tracking file access and changes across their environment with DataSecurity Plus.

How ManageEngine DataSecurity Plus helped

Once deployed, DataSecurity Plus transformed how Steadfast Group monitored and managed their file activity.

Centralized file auditing across the environment

The platform provided a single, unified dashboard that helped improve operational efficiency and reduced blind spots across all monitored servers and critical folders.

The team could clearly see:

- File read, write, delete, and modification events
- User identities associated with each action
- Time-stamped activity trails for investigations

> As Basnet rightly pointed out, *"[DataSecurity Plus] provided centralized visibility into file access and changes."*

Real-time alerts for faster threat response

DataSecurity Plus automatically notified administrators when suspicious or policy-violating activity occurred, such as:

- Unauthorized access to sensitive folders
- Mass file deletions or modifications that could point to a potential ransomware attack
- Unusual access patterns outside normal business hours

This allowed the IT team to respond immediately instead of discovering issues long after the fact.

> Basnet highlighted this by saying, *"The real-time alerts and audit reports improved our security posture significantly."*

Simplified compliance and audit reporting

Compliance requirements in the insurance industry demand detailed and accurate records of filer access and changes. With DataSecurity Plus, Steadfast Group leveraged built-in File Audit reports to:

- Track access to critical files
- Demonstrate compliance
- Quickly answer questions about historical file activity

These reports eliminated the need for manual data collection and significantly reduced preparation time for audits. Instead of compiling logs over several days, administrators could generate comprehensive reports within minutes.

> "The feature we use most is File Audit reports for tracking access and modifications across sensitive folders. [It helps us] meet compliance requirements and reduce insider threat risks," Basnet said.

Conclusion

For Steadfast Group, file activity is no longer a blind spot.

By implementing ManageEngine DataSecurity Plus, what was once difficult to track is now centralized. What required manual effort is now visible in real time. What carried insider threat risk is now actively monitored. Instead of reacting after the fact, the team can now act as file activity happens.

Like Steadfast Group, you can also deploy specific modules of DataSecurity Plus to address specific needs or integrate all the capabilities of DataSecurity Plus to enhance your data security posture.

From file server auditing and data risk assessment to DLP and cloud protection, DataSecurity Plus can serve as a one-stop data security posture management platform. To try these capabilities for yourself, schedule a free, guided demo. Alternatively, you can download DataSecurity Plus and use it for 30 days with no limits to preview all the features in your environment.

Request a Demo | Download a fully functional, Free trial

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, check out the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore DataSecurity Plus' capabilities

File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment

Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention

Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more