ManageEngine
DataSecurity Plus

Case Study

How Eastern Virginia Medical School **secures sensitive data with DataSecurity Plus**

Company: Eastern Virginia Medical School | Industry: Education | Organization size: 1000-5000

About Eastern Virginia Medical School

Eastern Virginia Medical School (EVMS) is a public medical school in Virginia, USA. It caters to more than 1,000 doctoral and postgraduate students and employs more than 500 professionals as faculty. The school campus includes affiliated hospitals, private practice medical offices, research facilities, and libraries. The extensive scope of education and healthcare services rendered on campus involves large amounts of personal health data (PHI) and personally identifiable information (PII).

Data security challenge faced by EVMS

Any healthcare organization—similar in scope to EVMS or otherwise—needs to implement a data visibility and security solution. Such a solution is required not just for safeguarding data privacy but also to comply with important mandates like the Health Insurance Portability and Accountability Act (HIPAA), the GDPR, and others. This is exactly what EVMS sought.

Using only native Windows tools to comb through multiple file servers is a tall task for any sysadmin. Rosemarie Deronne, a systems engineer III with decades of experience, faced the same issue at EVMS.

Deronne was looking for a tool to pinpoint exactly where PHI and PII were located in the institution's systems. The goal was to obtain actionable insights on where at-risk data was stored, how vulnerable it was, secure it within a reasonable timeframe, and allow remediation steps to be taken before a serious breach occurred.

These were the main questions that were put forth to DataSecurity Plus:

- Which files contain sensitive data and where are they located?
- Which users performed what kind of actions on the files, including unauthorized move or delete events?
- Which of these files were publicly accessible and had permission inconsistencies?
- Which of these files were redundant, trivial, or obsolete?

Why DataSecurity Plus stood out to EVMS

The three reasons why EVMS chose DataSecurity Plus over other data risk assessment solutions:

The **extensive data visibility features** for discovering and securing healthcare data and other personal information

Ease of setup with data discovery scans kick-starting within just minutes of download and initial configuration

Reasonably priced data security tool that offered more than just the intended use and includes robust features, like granular security controls, and responsive tech support

EVMS assessed DataSecurity Plus to screen its approach towards enhancing data security. It took the institution only 30 days to finalize DataSecurity Plus as part of its security tools. During the free and fully equipped trial that DataSecurity Plus offers, Deronne got to test the data discovery solution first hand. Her primary goal was to test what types of regular expression patterns DataSecurity Plus can scan. The scores of built-in data discovery rules for specific types of sensitive data along with the extensive audit reports convinced Deronne to finalize the decision to purchase the three core components of DataSecurity Plus: file server auditing, file analysis, and data risk assessment.

DataSecurity Plus can be up and running within few minutes of installation, and Deronne was able to quickly navigate through its user-friendly interface. When the need arose to confirm the setup, our tech support team was just a chat away. The setup, including the tech support session, was completed within 30 minutes.

After the purchase, we asked Deronne how DataSecurity Plus helps make her job easier and she had this to say:

“It provides insight into the types of data being stored on our servers so we can better protect it.”

Why DataSecurity Plus?

Ease of setup

Cost-effectiveness

Capabilities currently deployed

Data Risk Assessment

File server auditing

File Analysis

How DataSecurity Plus helped EVMS understand its data

The primary solution to EVMS' needs was the data risk assessment tool. It's a crucial tool in any IT admin's kit, but combined with corresponding functions like file event auditing and permissions hygiene analysis, data risk assessment completes the security arsenal of the SOC team. Some of the highlights of DataSecurity Plus' data risk assessment tool that EVMS employed include:

- Identifying sensitive information to comply with the GDPR, HIPAA, the PCI DSS, and many other data security regulations.
- Classifying files on a multi-hierarchical labeling system to streamline security policies. Which of these files were publicly accessible and had permission inconsistencies?
- Customizing data discovery scans by specifying regular expression patterns or keyword sets in tailor-made discovery policies.
- Managing files that contain sensitive data occurrences directly from the report interface.
- Setting up dynamic alerts with script responses or email notifications as remediation actions when a file matches the rules in a discovery policy.

Like Deronne, you can integrate all the capabilities of DataSecurity Plus to create an airtight data visibility and security mechanism, from sensitive data discovery to thwarting unauthorized file transfers.

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.

Get personalized demo

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

Monitor endpoint file activities, and detect and disrupt data leaks via USBs, email, web applications, and printers.

LEARN MORE

Cloud protection

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

LEARN MORE