Gimmal

MANAGING RIOT DATA

What is RIOT Data?

RIOT data refers to Redundant, Obsolete, *Inaccessible*, and Trivial data. These data types can clutter storage systems and inflate costs unnecessarily.

Redundant Data: Data that is duplicated across the organization, often unnecessarily.

Documents & Files — Emails

Inaccessible Data: Files that cannot be accurately read or retrieved because of old and redundant file formats.

WordPefect — Lotus — MacDraw

Obsolete Data: Data that is outdated and no longer useful for current operations.

Old Files — Legacy System Data — Outdated Reports

Trivial Data: Data that has little to no value to the organization.

Personal Files — Non-business Emails — Low-priority Info

The Impact of RIOT Data

- Redundant Data: 15-20% of company data is duplicated.

- Obsolete Data: 30% of data has not been accessed in the past year.

- Trivial Data: Up to 50% of emails are considered low-value.

Benefits of Managing RIOT Data

- Cost Reduction: Potential savings of 20-30% on storage costs.
- Improved Efficiency: Faster data retrieval and processing.
- Enhanced Security: Reduced risk of data breaches by minimizing unnecessary data.

The Cost of Inaction

- The average cost to recover from a ransomware attack is $1.85 million USD
- The average number of files ransomed per attack can be approximately 144,100 files
- Cost Per File ≈ $12.84USD/file

$1.85M

144K FILES

Gimmal's RIOT Data Management Strategy

Free Sensitive Data Assessment

Gimmal's RIOT data management strategy leverages the **Free Sensitive Data Assessment Tool** to analyze and report on sensitive and obsolete data within a subset of your Windows File Shares. Here's how it works:

- **Non-Intrusive Assessment:** The data is not moved or copied during the assessment process.
- **Risk Detection:** Focuses on detecting potential data risks and security issues, providing comprehensive data aging information.
- **Targeted Checks:** Specific checks are made for Credit Card and Social Security Numbers, along with other user-specified keywords or phrases.
- **Reporting:** The resulting report is exported to a .csv format and ingested into Power BI, generating six detailed reports. These reports do not contain any Personal Credit/Identifiable Information (PCI/PII); instead, they include basic metadata and binary values related to the sensitive data.
- **Efficiency:** The process requires less than five hours of your employees' time and is completed within two weeks. After the assessment, Gimmal Discover is uninstalled, and all data within its cloud are deleted.

Deliverables

Summary Report: Provides overall statistics for the sensitive data.

Individual Reports: Detailed statistics for Credit Card, Keyword, and Social Security Number information.

Testimonial

"Gimmal Discover has been key in helping to keep our university's data secure and reduce its exposure to outside and inside threats. University compliance and security requirements continue to evolve and expand. Having a product in our hands to quickly answer these requirements and provide proof of compliance with audit trails is of immeasurable value." **-Tim Wilson, Assistant VP IT Services, Point Park University**

www.gimmal.com