SPHERE TECHNOLOGY SOLUTIONS

Automation Nation: Success in Data Governance with Smart Remediation

The data security landscape is evolving at breakneck speed as cyber threats and technology advances reshape the security framework of firms across verticals. In the course of only a few years, cybersecurity costs have grown by over 20% with an average cost to firms of nearly $12 million. Likewise, the annual rise in data breaches inches up by nearly 30% year-to-year. Accenture's latest cost study on cybercrime also shows an unprecedented scale of investment in security in response to evolving information security threats, yet current spend is often misdirected toward a handful of capabilities that fail to deliver efficiency and data governance success.

Being at the forefront of successful data management means making efficient use of your security investment and processes in the long term -- from a time, resource and dollar perspective.

The Risk is in the Unstructured Data

Data growth is accelerating in unprecedented ways. IDC predicts that global data will reach 44 zettabytes, or 44 trillion gigabytes, by 2020. By comparison, data measured in at only 4 zettabytes in 2013. Cloud-based databases, email systems and IoT devices have opened the floodgates for even larger scale data and risk, but unstructured data remains a huge vulnerability. Unstructured data repositories lack the control and predictability of traditional databases. Yet, they remain a huge chunk of organizational data -- Forrester reports that firms hold 100 TB of unstructured data on average.

How do you solve for the unstructured data risk at your firm in the long term?

Unpacking Remediation

Successful data remediation requires dramatic increase in control, while reducing enterprise risk and costs. After identifying the risks in your data environment, you need a plan of action. For the uninitiated, traditional remediation can translate into a tedious, time-consuming and costly process for firms. Removing open access, pruning privileged access, certifying ownership or performing other asset reviews can all be complex operational cogs in the remediation wheel.

Trial by Fire, Pilot Remediations

It's a good idea to perform a smaller scale pilot remediation to understand the complexities your organization presents and how to best handle them. Also, this will give you a sense of how long a full remediation will take:

- Identify the responsibilities across operational teams
- Document the steps of the process using a swim lane diagram
- Provide recommended communications to be used during entitlement reviews and remediation
- Document the entire process for use across the broader environment
- Communicate to the associated ownership with remediation requirements
- Implement the controls to ensure the environment does not go back to the pre-remediated state.

Making Remediation Smarter

Advanced analytics and automation are integral for smarter, more cost-effective remediation, powering intelligent risk reporting to create a data-driven action plan for your most valuable assets, and ultimately reducing risk. This means going beyond reporting on risk, to initiate action on assets (i.e. emailing the data owner, opening a ticket and starting an asset review workflow as well as adjusting permissions and removing access). Adding automation to every step of the workflow enables you to automatically fix the issues, schedule updates, and remediate areas of high risk:

1. Find out what exists -- Identify and understand your most critical open access to sensitive data through automated file discovery and classification of file content.

2. Categorize data as active or stale --- Map your data to delineate redundant or stale data that is ready for remediation.
    - For stale data, remove all permissions for immediate risk reduction.
    - For active data, identify owners.

3. Identify who needs to maintain access -- Power access management with analytics to define, certify and validate ownership of unstructured data automatically.

4. Implement changes -- Develop standardized groups where group membership and other metadata can be updated and access controls for resources can be streamlined.

Know Your Roles

Understanding data permissions helps achieve successful access management and ongoing remediation. There are many different people involved in any one remediation – here's a quick guide to some data personas you need to know:

- Data seward – one of your more important data roles, this is your in-house team or vendor serving as the data SME (subject matter expert) responsible for spearheading data quality and remediation work
- Data owners – department heads or executives responsible for specific datasets
- Data custodians – your team or vendor responsible for enforcing business rules about data access, custody or exchange
- Data producers – this role runs the gamut of staff, clients, and partners whose business activities generate data
- Data users – employees tasked with conducting analyses and producing outputs from your data

5. Remove open access and replace with standardized access controls -- Set and manage unstructured data permissions, remove security issues such as open access, and update permissions to support a Least Privileged Access model.

Action, Not Just Reporting

Smart remediation mobilizes typical actions to clean up and standardize a target unstructured data collection, decreasing the overall risk to your organization:

- Create RO Group (if it doesn't exist)
- Create RW Group (if it doesn't exist)
- Remove the Open Group
- Remove Direct Users
- Remove Non-Standard Users

Driving Successful Data Governance

Actionable intelligence and automation are quickly becoming the pillars of successful data governance. According to Cisco's 2018 Annual Cybersecurity report, 39% of companies report their reliance on automation to mitigate cyber threats -- advanced security technologies that include machine learning and artificial intelligence capabilities are becoming increasingly important. 34% of firms are completely reliant on machine learning; while 32% said they are completely reliant on artificial intelligence.

Smart remediation, leveraging predictive analytics and automation, helps solve the unstructured data risk at your firm in the long term; automatically fixing issues and doing the heavy lifting for you. Achieving a true depth of automation is vital to ensure that information security and governance are significantly less time-consuming and costly processes, to make your firm more secure in a shorter period of time with less resources.

About SPHERE

SPHERE is an award-winning woman-owned cybersecurity company focused on unstructured data security, Privileged Access Management and Identity and Access Management solutions. SPHERE has created a technology-enabled service model leveraging:

Leading Edge Products

SPHEREai: Our enterprise-ready architecture is built for top 100 firms but used by companies of all sizes. We love data and our architecture allows us to ingest, correlate, analyze and report on all types of data so we can provide critical security and risk reporting for all your governance needs.

SPHEREboard: When it comes to unstructured data, wrong permissions are a major danger for your organization. SPHEREboard focuses heavily on many different access control issues across your file shares and other unstructured data repositories.

Subject Matter Expertise

Ranging from strategic security advisory to SWAT-team remediation projects, SPHERE provides solutions to help companies understand their risks, create policies for a target end state, and remediate major vulnerabilities. We have experience remediating nearly 1 million AD groups, 26 million file shares, and 60,000 privileged accounts.