Executive Summary

Define Unstructured Data
Unstructured data is everything we store in files: documents, spreadsheets, video, voice and images. It is spread across files servers, NAS (Network attached storage) devices, application servers and even organizational portals (like Microsoft® SharePoint) and Email servers. Unstructured data is everywhere and exploding. In modern organizations, unstructured data takes part in almost any mission critical business process. In most organizations it will contain sensitive information, trade secrets, internal financial data and other types of information that should be kept protected.

Securing Unstructured Data - Key Challenges
Unlike application oriented data, which is usually well mapped and has means of protection, unstructured data is loose and out of control. Organizations are now facing tremendous challenges:

✓ Map existing stores of unstructured data.
✓ Find data (folders, files, sites) owners and map key user groups.
✓ Classify sensitive data.
✓ Define and enforce authorization policies on data stores.

The Complete Picture - Structured & Unstructured Data Eco-Systems
Unstructured data, in most cases, is only a subset of a more complete information collection. A quote document that is attached to a CRM record is more valuable and meaningful in that context. For that reason, some of these key challenges should be looked at from a complete, holistic approach. Keeping that concept in mind, organizations should not try to meet the unstructured data challenges with niche, isolated, tools that will evidently lead to a partial, incomplete solution.

Requirements for an Effective Solution
The road to a complete solution that will provide actionable intelligence should contain the following milestones, at least:

✓ Complete monitoring solution for a broad portfolio of data stores.
✓ Real-time, complete audit which includes IT Information integration and identity identification ability.
✓ Automatic classification of data owners and user groups, based on variety of information sources.
✓ Complete authorization policy life-cycle management, including user permissions review automation and role engineering.
✓ Ability to define cross-domain, unified security policies and to respond to policy violations in real-time.
✓ A platform based solution that will allow monitoring additional business application domains, such as ERP, CRM, Billing and home grown / 3rd party applications.

Whitebox Security’s WhiteOPS™ Data Governance Bundle
Whitebox Security, a leader in the field of Identity Intelligence provides a complete, end-to-end solution for unstructured data governance. The WhiteOPS™ Data Governance Bundle is a packaged solution, designed to provide a complete solution at a highly effective price/performance ratio.
Background

Data governance, for both structured and unstructured data, is at top priority for enterprises today. Technologies like DLP, Identity Intelligence and even classic audit solutions are targeted and learned by organizations who wish to tackle this important initiative. Unlike past security and risk challenges, with data governance, a "patch" solution will not do the work. The data is in-fact everywhere and a broad solution with a modular architecture is strongly needed. The discussion should begin, though, by understanding why this enterprise-wide view of the organization's data is needed. First, enterprises strive to decrease the risk of data misuse and leakage. Second, a visibility of data access from simple audit to complex ownership analysis is required. Third, business leaders need to control and monitor access privileges in a straight-forward and automatic approach (as regulatory compliance often requires them to sign and approve these privileges). In the past, these issues were considered at low priority as business leaders assumed that access controls over sensitive data are in place. Recent studies accompanied with a rapid rise of unfortunate data misuse incidents has led executives to understand that their sensitive data is not as secured as they once believed it to be (Source: Symantec, Global Internet Security Threat Report for 2009).

The business drivers for Data Governance

It is clear today that a crucial part of the organization business related digital information is unstructured data. Almost a decade ago Merrill-Lynch estimated that “..More than 85 percent of all business information exists as unstructured data” (Source: DM Review Magazine). Now, as business leaders realize that their data is exposed and out of control, immediate actions are required:

- Audit actual data access.
- Map data owners, users groups and usage patterns.
- Analyze the permissions of users and groups to data.
- Recommend entitlement changes to meet business and regulatory policy.
- Support user permissions review & grant process.

Obviously, these business requirements translate to numerous complex technical requirements which we will discuss further but some additional notes should be made on data governance business requirements first. Business leaders are required to gain complete ownership on their entire underlying digital data and assets. In most cases this requirement unfolds a maze of files, emails, enterprise applications records (such as ERP and CRM) - to name a few. Though these types of digital assets are different in nature their users are basically the same. For instance, a reasonable assumption on an employee from an HR department will be that he or she can access HR related folders on the NAS device, HR related collaboration sites on the enterprise portal and HR related function on the ERP application. This creates an important common ground that substantially simplifies crossing this maze. This is the reason why data governance solution must take a holistic approach that will allow business leader to gradually cover all aspects of their business rules and policy.
**Data Governance - Key Requirements**

*Why Existing Solutions Fall Short*

As unstructured data governance needs evolved and organizations came to realize that the exploding unstructured data must be kept in check, first generation of data governance solutions came to life. These solutions aimed to solve the “File Server” problem. They are neither designed to meet the data governance challenge with a holistic approach nor takes into account other data sources and existing IT infrastructure that must be integrated in-order to provide a complete solution.

**Key Requirements for Data Governance Solution - A Buyer’s Guide**

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
<th>WhiteOPS™ (Data Governance Bundle)</th>
<th>Other Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Monitoring</strong></td>
<td>Real time monitor of file/folder access with detailed audit trail</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real time monitor of permission changes with detailed audit trail</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source IP Identification</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source User name Identification</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support for Citrix/Terminal Services source identification</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support for any NAS platform</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Leverage solution for other business assets monitoring (ERP, Mail, etc.)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent-less monitoring</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Access Intelligence</strong></td>
<td>Complete visibility of effective folder/file permission with full visibility of groups, inheritance, etc.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Owner classification</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support for complete role (re-)engineering</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support for What-if scenarios</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Used/Unused permissions</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cross-reference with in place IT security policies and systems to better adapt access privileges to actual needs</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Policy Compliance</strong></td>
<td>Granular Definition of security policies on files/folders</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Leverage existing IT security infrastructure to define unified security rules</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Workflow</strong></td>
<td>Automatically respond to violations</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support for an end-to-end user permissions review process</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support for regulatory attestation requirements</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
The WhiteOPS™ Data Governance Bundle

About The WhiteOPS™ Product Family

The WhiteOPS™ product family is the world’s most comprehensive Identity Intelligence solution. WhiteOPS™ fully addresses the Identity Intelligence key challenges to provide answers to the following:

- Who has access to what?
- Who should have access to what?
- Who reviewed and approved what?
- Who did what?
- When, where and how did access occur?

WhiteOPS™ is based on a modular architecture which allows monitoring of common business application platforms to collect meaningful activity data. WhiteOPS™ uses the innovative Whitebox Policy Connectors to further enrich each event with data from in place security systems, such as IAM platforms, Firewalls, Enterprise Directory services, etc. This, enable WhiteOPS™ to build the most comprehensive application usage database that is leveraged to gather, analyze and manage roles and privileges in any monitored platforms. Aimed to address the emerging needs in the Identity Intelligence field, WhiteOPS™ is designed with a full support for a broad set of tasks: User Activity tracking and forensics, Role mining, User permission review workflows, IT Policy compliance for business activities with a deep support for regulatory requirements include an advances, cross-platform, Segregation of Duties engine.

WhiteOPS™ Data Governance Bundle

The WhiteOPS™ Data Governance Bundle is a cost effective package providing a complete solution for the Unstructured Data Governance in a competitive, unique, price level. The bundle includes:

1. Full support for CIFS, NFS NAS storage devices, including EMC, NetApp, IBM and HP.
2. Full Support for Windows® based file servers.
3. Complete permissions analysis, What-If scenarios and groups/role re-engineering.
4. Complete support for user permission review process, including user self-service.
5. Integrated interface to common Directory Services platforms as Microsoft® Active Directory.
6. Unlimited license with no user/server limitation.
7. Option for appliance based, plug & play, architecture.

Whitebox Security has recently announced a promotion for this bundle at the fix, unprecedented pricing which allows organization to deploy an end-to-end data governance solution with a dramatically reduced CAPEX and OPEX.
Conclusion

Holistic Approach to Key Challenges of Data Governance

Organizations today are using a variety of niche tools to fight the challenges of data governance. This approach will lead to a set of complex and costly solutions that will not provide an end-to-end solution. Organizations should tackle the Data Governance challenges with the “How can I track my user’s activities and permissions?” question in mind. Organizations that only focus on the narrow “How can I track my file servers/NAS usage and permissions?” question will create a non scalable solution that will have to be replaced, in the near future.

About Whitebox Security

Whitebox Security, a leader in the field of Identity Intelligence, provides an industry first purpose built identity intelligence platform. With the WhiteOPS™ suite, Whitebox Security has taken a technological leap to enable, alongside with the core components of IAM Intelligence, activity monitoring, role lifecycle management and policy compliance for business activities in real-time. Whitebox Security is a solution provider for retail, financial, government and telecom. For more information please visit:

www.whiteboxsecurity.com