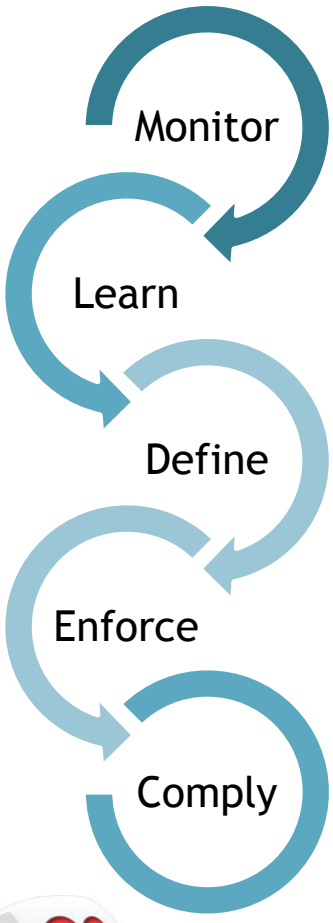
WhiteOPS™ for File Services

Securing the Big Data: The Challenge

Today more than 80% of the organizational data is unstructured. Most of this data usually resides within file-servers, NAS devices, portals and mailboxes. The most common form of unstructured data is files. The challenge is to manage and protect this vast data across an enterprise's unstructured data stores. A solution should answer: **Who accessed the resources? When? Where from? Who can access them? Who should not have access?** Etc. Conventional audit solutions have failed to deliver a holistic solution, due to high performance costs, lack of forensics and classification capabilities, and ignorance in the field of entitlements analysis and management.

The WhiteOPS™ Solution



Monitor

Begin by monitoring **who is accessing what information**? **Is that information sensitive**? Get a **full audit trail** for every activity, using the WhiteOPS™ patent-pending activity enrichment mechanism. Retrieve information, literally by asking questions. **No native auditing involved**.

Learn

Learn **who has access to what**, **who's using their access rights** and most importantly, **who is not**. Learn **where your sensitive information resides**. Be enlightened with **actual usage patterns** and **identify data owners**. Detect **unused folders and stale entitlements**.

Define

Assign data owners. Control access with real-time access policies. Use negative (blacklist) or positive (whitelist) rules, or a combination of both. Use WhiteOPS™ **smart data classification** to **define and locate organization-specific data types** and start evaluating risks.

Enforce

Use the WhiteOPS™ flexible response mechanism to **respond to violations in real-time**. Everything from **real-time notification,** through the **exporting of violations to SIEM systems,** or execution of a **tailor-made user exit,** can be configured with ease.

Comply

Automate access certification processes and **streamline access requests**. **Manage regulatory-related compliance controls**. Use WhiteOPS™ out-of-the-box, comprehensive controls bank or create your own custom ones.

Whitebox Security is?

Whitebox Security is a leader in the field of Identity and Access Governance. The company pioneered **Intelligent Access Governance**, which combines the best of identity intelligence, and identity & access governance in WhiteOPS™, its Access Governance solution. Whitebox Security has been named one of the ten most innovative security companies by the RSA® innovation sandbox, has been awarded Gartner's cool vendor and was shortlisted for 'best IAM product' category by the SC-Magazine Europe awards in 2012.

Access Governance is?

A technology to answer the following questions:

Who did what?

Who accessed files and folders? When? Where from? Where to? How? What happened?

Who can do what?

Who can access which files and folders? Granted by which role? Is it effective?

Who needs to do what?

Who should and should not have access? Who didn't use their permissions? Since when?

Who approved what?

Who has violated access policies? How? Who approved access requests? Who certified access? Based on what?

Key Capabilities

Activity & Identity Monitoring With Data Enrichment

WhiteOPS™ is the only data governance platform to offer both agent-based and agentless (network-based) monitoring solutions. Both solutions can monitor all types of file-servers (Windows, NAS, etc.) and protocols (SMB, SMB2, NFS, etc.). It is also the only solution to enrich every monitored activity with details regarding the executing user, machine and session. These details are taken from existing security and HR systems such as: IDM, FW, EPS, HR, etc. within the organization.

Roles & Entitlements Analytics

WhiteOPS™ automatically collects and analyzes all the granted entitlements on your file-servers' folders and shares. For every entitlement, WhiteOPS™ reports its' last usage time and whether it is effective (allowed by both NTFS and Share entitlements) or not.

Real-Time Unified Access Policies

You can use WhiteOPS™ to ensure no violations are incurred while accessing resources on your file-servers. WhiteOPS™ access policy is real-time and unified, meaning that you can integrate every monitored and enriched security-attribute, as many as you need, into policies. Violations will trigger customizable real-time responses, to make sure you are informed and responding at the most crucial time for response.

Data Classification

WhiteOPS™ Data Classification helps categorize and order your data, and locate your valuable, highly confidential information (HCI), which maybe hidden amongst millions of files distributed across the enterprise. WhiteOPS™ can also answer more complicated questions, such as: who accessed sensitive finance/legal/HR related data or where there is HCI data that is over-exposed (across all of the organizational unstructured data stores).

Access Certification

Access Certification, a common requirement across many regulations, is the process of making sure that granted entitlements are actually needed, and of removing excessive entitlements. WhiteOPS™ is delivered with built-in usage-aware Access Certification capabilities. The usage-aware certification process enables the reviewer to get an actual usage analysis for all pending-certification entitlements.

Access Requests automation

WhiteOPS™ is delivered with a built-in self-service that enables users across the organization to request access. These requests go through a flexible review-process which will accompany the request from start to the grant on the relevant resource.

Technical Capabilities

Capability	Features
Identity & Activity Monitoring	- Two monitoring methods supported: Network-based and agent-based. - Real time monitoring. No native auditing required. - Each activity is enriched with data from existing security systems (Directory Services, Identity Management, Endpoint Security, Firewalls, Anti-Viruses, HR applications, etc.). - The activity's details will always be kept and retrieved relevant to its execution time.
Data Classification	- Data types definitions support keywords, regular expressions, patterns like SSN or credit card numbers and file system metadata including: file type, size, etc. - Incremental classification processes are fully supported. - Out-of-the-box best-practice classification rules are supplied.
Entitlements Analytics	- Schedulable and automated collection of entitlements. - Cross-checking entitlements with activities to detect unused entitlements. - Analysis of entitlements to detect and alert on ineffective entitlements. - Fine-grained views including recursive group memberships, etc.
Forensics Capabilities	- Information is retrieved by asking questions. Literally. - Sophisticated queries combine as many security-attributes as necessary, can be easily created, saved and reused. - Dynamic reports can be easily produced and scheduled.
Policy Compliance	- Real time evaluation of access policies. - Rules can integrate security-attributes from different security systems (e.g. Department = R&D, endpoint policy = no removable media allowed, and smart card auth. required = True). - Policy violations will trigger one or more definable responses in real-time.
Access Certification	- Usage-aware, smart UI with bulk-operations support, to reduce work-time. - Closed loop: automatically creates access revoke requests.
Self-Service Access Requests Automation	- Request one or more entitlements, for yourself, or on behalf of others. - Highly customizable and easy-to-define review processes. No workflows knowledge required.

Business Benefits

Benefit	Description
Business Processes Support & Ease of Use	- Authority delegation fully supported. - Business-friendly language, presentation and interface. - Intuitive UI, designed to support every monitored system in the same way. - Multilingual end-user interfaces with RTL fully supported..
Rapid Return of Investment	- Detect unused resources on file-servers such as: files, folders and whole shares that can easily be removed or backed-up to save expensive, high-end disk storage. - Detect orphan accounts, empty groups, infinite nested groups, and many more entitlements anomalies that can be easily removed to reduce capital and operational expenditure.
Scalability & Investment Protection	- Fully scalable, enterprise-ready, to support the most demanding environments. - WhiteOPS™ is a platform, and therefore, it can deliver all the above capabilities, other than for file-servers and NAS devices, also for: Microsoft® SharePoint®, Microsoft® Exchange, Microsoft® Active Directory, SAP® and for every homegrown or COTS application.

The WhiteOPS™ Advantages

WhiteOPS™ is a platform

WhiteOPS™ delivers all the benefits of purpose-built software in a platform. All business-critical applications covered by the same console, in the same way, and at the same time.

True Full Audit-Trail

As each activity is enriched with security-attributes from in-place security systems, all necessary information is available for investigation at any time, relevant to the activity's execution point-in-time.

Fine-Grained Forensics

WhiteOPS™ allows you to ask anything, literally. Using the advanced forensics mechanism you can ask, for example, for all the activities made by the 'Domain Admins' group members across all the organizational unstructured data stores.

Completely Real-Time with Flexible Responses

Response time and actual responses are of the essence when dealing with access policy enforcement. WhiteOPS™ is responding to violations in a timely manner to prevent harm to the business.

Usage-Aware Access Certification

Supplied with the usage pattern of every review-pending entitlement, the reviewer is empowered with access context to support effective decision making.

Rapid Time-to-Value

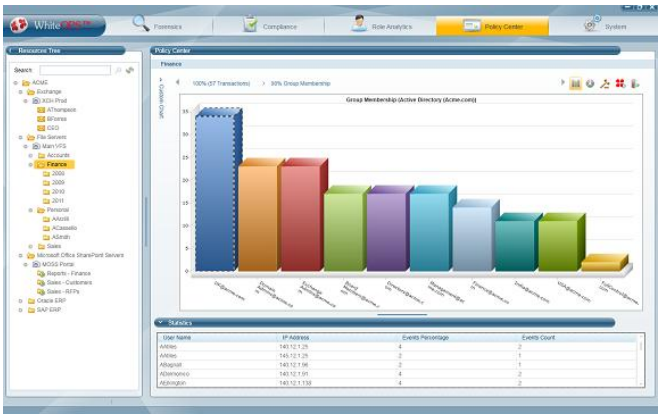
Within one day of installation, WhiteOPS™ will start monitoring your file-servers, collecting and analyzing entitlements, creating usage patterns, and evaluating out-of-the-box access policies.

Within a week of installation, WhiteOPS™ will find out where the organization's most sensitive and valuable data resides and who can, and has, accessed it. Unused resources and accounts will be reported.

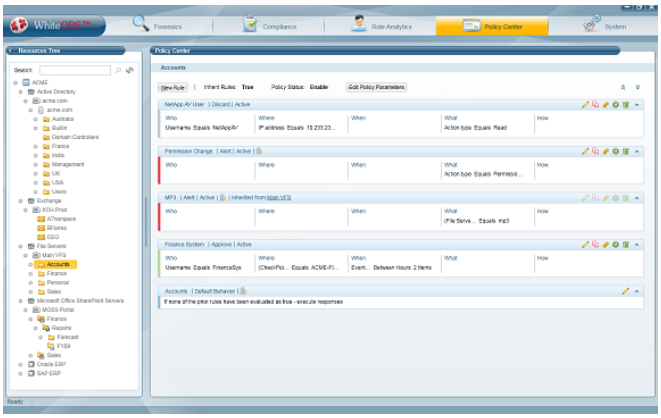
Within a month of installation, custom usage-based access rules can be created. Usage-aware access certification campaigns can start. Incremental data classification processes will ensure you won't lose track of your sensitive data ever again.

Latest word in User Experience

Interactive Usage-Pattern Analysis



Real-Time Unified Access Policies



Data Owners & Casual Users Website