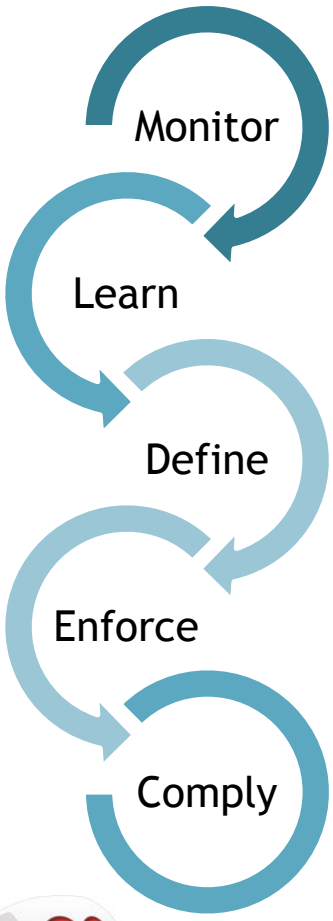
WhiteOPS™ for Microsoft® Exchange

The Challenges in Microsoft® Exchange Security

Email is the most common way of communication between organizations and the outside world. As storage became cheaper, mailboxes and public folders became bigger, much bigger. With the increase in size, came the increase of risk. Mailboxes and public folders have turned into personal folders, in which the user aggregates vast amounts of unstructured data. A solution needs to answer: **Who holds what data**? **Who accessed it**? **Who can**? **Who should not?** Etc. Conventional audit solutions have failed to deliver this due to their 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 which mailboxes**? **Who sent email as or on behalf of others?** Get **full audit trail** for every activity, using the WhiteOPS™ patent-pending activity enrichment mechanism. Retrieve this information, simply by asking questions.

Learn

Learn **who has access to which mailboxes and folders**? **Who is using their access rights** and most importantly, **who is not**? Learn **where your sensitive information resides. Identify data owners** of your public folders. Detect **unused resources and stale permissions**.

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 even executing 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 which mailboxes? When? Where from? How? What has been done?

Who can do what?

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

Who needs to do what?

Who should and shouldn't have access? Who didn't use his granted access? 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 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 within the organization, such as IAM, firewalls, endpoint security, HR systems, etc. To ensure the most relevant and comprehensive information is available when asked, all monitored activities, that including their data enrichment attributes from the execution point-in-time, are kept and forever retrieved together.

Roles & Entitlements Analytics

WhiteOPS™ automatically collects and analyzes all the granted entitlements on your mailboxes, mailbox's folders, public folders, etc. For every entitlement, WhiteOPS™ is able to report the last usage time and whether it's effective or not.

Real-Time Unified Access Policies

You can use WhiteOPS™ to make sure no violations are incurred while accessing your Exchange resources. WhiteOPS™ access policy is real-time and unified, means that you can integrate every monitored and enriched security-attribute, as many as needed, into policies. Violations can trigger 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 Exchange infrastructure. 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 tracks the request from start to the grant on the relevant resource.

Technical Capabilities

Capability	Points To Remember
Identity & Activity Monitoring	- Monitoring is done in real-time. - Each activity is enriched with data from existing security systems (Directory Services, Identity Management, Endpoint Security, Firewalls, Anti-Viruses, HR applications, etc.). - The complete activity's information will always be kept 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. - Analyzing entitlements to detect and alert on ineffective entitlements. - Fine-grained views including recursive group membership, etc.
Forensics Capabilities	- Information is retrieved by asking questions. Literally. - Sophisticated queries which combine as many security-attributes as needed, 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.

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. - No workflow knowledge needed to create highly-flexible review processes.
Rapid Return of Investment	- Detect unused resources on Exchange servers like mailboxes and public folders 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 easily be 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 Microsoft® Exchange, also for: File-Servers, NAS Devices, Microsoft® SharePoint®, Microsoft® Active Directory, SAP®, Oracle® EBS 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 will make the fastest and most accurate decisions with ease.

Rapid Time-to-Value

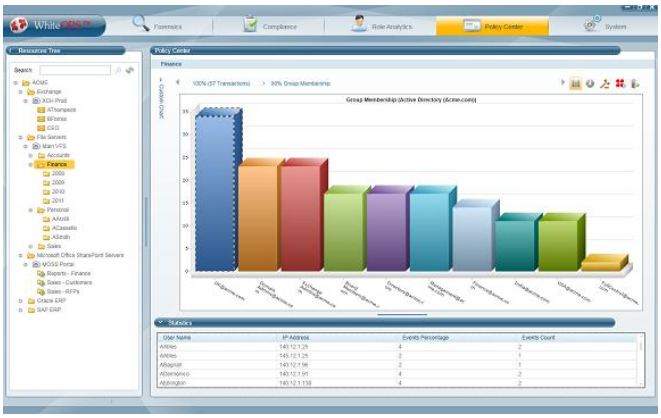
Within one day of installation, WhiteOPS™ will start monitoring your Exchange infrastructure, collecting and analyzing entitlements, creating usage patterns, and evaluating out-of-the-box access policies.

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

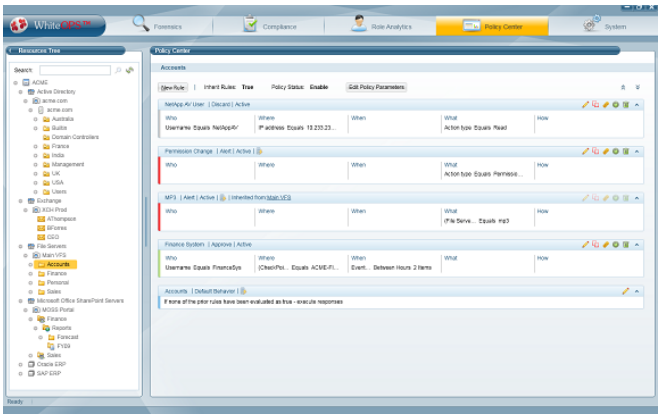
Within a month of installation, custom usage-based access rules can be created. Usage-aware access certification campaigns can start. Incremental data classification processes will ensure you will not lose track of your sensitive data ever again.

Latest word in User Experience

Interactive Usage-Pattern Analysis



Real-Time Unified Access Policies



Data Owners & Casual Users Website