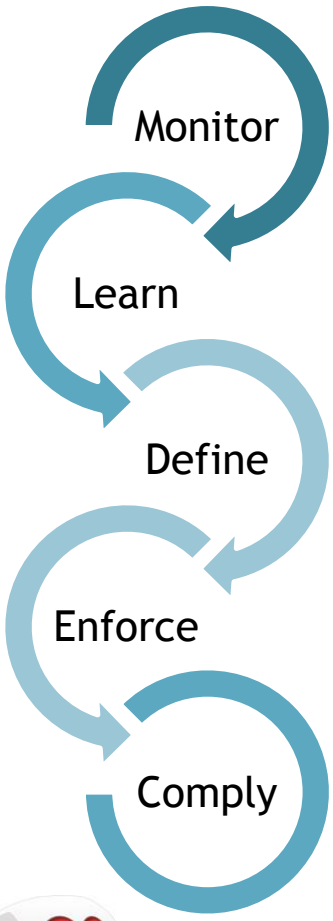
WhiteOPS™ for Microsoft® Active Directory

The Challenges in Microsoft® Active Directory Security

Active directory is one of the most critical IT infrastructures, as it provides one of the key cornerstones of security: authentication. But with great power, comes great responsibility, and next in line are the risks. E.g. minor configuration changes could cause hours or even days of critical infrastructure outage. To effectively manage these risks, vast amounts of data needs to be considered. Data such as: **who changed, moved or deleted objects? Who has access to what?** Etc. Conventional audit solutions have failed to deliver this due to their lack of forensics capabilities, and complete ignorance in the field of entitlements management.

The WhiteOPS™ Solution



Monitor

Begin by monitoring **who is changing or deleting objects? Who is changing memberships of groups? Who reset passwords?** Get a **full audit trail** for every activity, using the WhiteOPS™ patent-pending activity enrichment mechanism. Retrieve the information you need by asking simple questions.

Learn

Learn **who has access to which objects? Who's using access rights** and most importantly, **who is not. Which objects are over-exposed? Identify owners of your groups, containers and other objects.** Detect **unused objects and stale entitlements.**

Define

Assign owners. Control access with real-time access policies. Use negative (blacklist) or positive (whitelist) rules, or a combination of both. Use WhiteOPS™ **smart usage-patterns** to **define real-time unified rules 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,** is 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 changed or deleted what? When? Where from? How? What has been done?

Who can do what?

Who can access which objects? Granted by which group? 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 in your directory objects such as: users, computers, all types of groups, etc. For each entitlement, WhiteOPS™ shows the last usage time and whether or not it is effective.

Real-Time Unified Access Policies

You can use WhiteOPS™ to make sure no violations are incurred while accessing your Active Directory infrastructure. 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.

Automated Compliance Controls

Organizations typically have many compliance controls that require periodic execution. Whether regulatory-related or not, it's no simple to meet audit requirements. WhiteOPS™ makes easy work of audit reporting; simply schedule the best-practice, out-of-the-box controls (supporting SoX, PCI, HIPPA, ISO 27001, etc.), or easily create your own custom controls. Trends and statistics are automatically generated to track and report improvements or deterioration in compliance level.

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.

WhiteOPS™ for Microsoft® Active Directory

www.whiteboxsecurity.com

whitebox Protect what you value most™

Technical Capabilities

Capability	Points To Remember
Identity & Activity Monitoring	- Monitoring is done in real-time. - Detect what is happening to your users, groups, computers, group policies and any other object type, together with the changes' before and after values where applicable. - Each activity is enriched with data from in-place 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.
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	- Access policies are being evaluated in real-time. - 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 flexible responses in real-time. - Automate compliance controls to detect and manage security anomalies and configuration changes (Best practices compliance controls are delivered out-of-the-box).
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 workflows knowledge required to create highly flexible review-processes.
Rapid Return of Investment	- Detect orphan accounts, empty groups, infinite nested groups, and many more entitlements anomalies that can easily be removed to reduce capital and operational expenditure. - Automate compliance, from controls executions to handling of rejects and even automated responses. Everything, to lower the response times, and save precious work-hours.
Scalability & Investment Protection	- Fully scalable, enterprise-ready, to support the most demanding environments. - WhiteOPS™ is a platform, all of the above capabilities are supported other than for Microsoft® Active Directory, also for: File-Servers, NAS Devices, Microsoft® SharePoint®, Microsoft® Exchange, 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 Admin' group members across all the organizational forests and domains.

Completely Real-Time with Flexible Responses

Response time and actual responses are of the essence when dealing with access policy enforcement. WhiteOPS™ allows you to respond 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

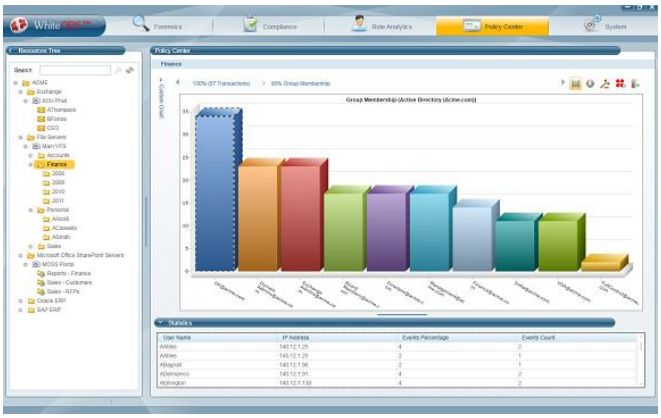
Within one day of installation, WhiteOPS™ will start monitoring your Active Directory infrastructure, collecting and analyzing entitlements, and evaluating out-of-the-box access policies.

Within a week of installation, having generated usage-patterns, WhiteOPS™, will demonstrate how your resources are being used and by whom, who can use them? Unused accounts and groups will be reported.

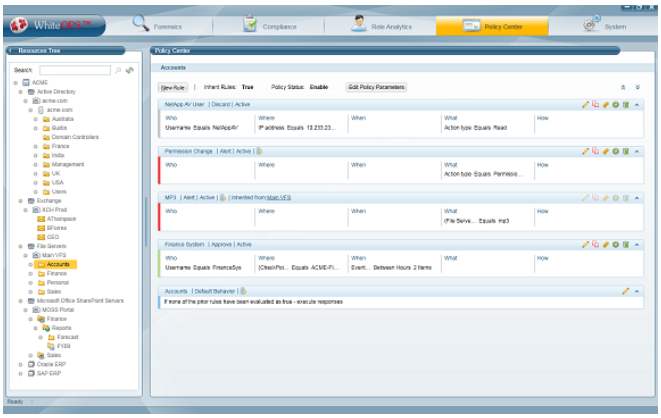
Within a month of installation, custom usage-based access rules can be created. Trends of policy violations and compliance controls will be reported.

Latest word in User Experience

Interactive Usage-Pattern Analysis



Real-Time Unified Access Policies



Data Owners & Casual Users Website