Quick Facts

Active Directory Quick Facts

StealthAUDIT Management Platform for Active Directory

Analysis and Remediation for Active Directory and Azure Active Directory

AD Cleanup

- Identify and Remediate Stale Users and Groups
- Detect "Toxic" Group Conditions (Circular Nesting, Deep Nesting, Large Groups)
- Determine User Last Logon Time and Password Policy
- Isolate unused Computers, Users & Groups

Cloud Support

- Ensure that accounts are successfully synced between Azure AD and on-prem AD
- Maintain Azure AD hygiene by identifying stale objects and toxic group conditions

AD Operations

- High availability monitoring
- Maintain operational integrity with daily news reports
- Alert on critical health issues
- Replication tracking and error reporting

Preventative Diagnosis

- Proactively identify potential user, group, and domain controller issues
- Identify LDAP query latency and user logon issues
- Remediate user and group issues that do not follow MS Best Practices

User Management

- Investigate Password Policy
- Discover disabled and inactive users
- Identify, Trend, and Unlock locked out accounts
- Determine last logon
- Extract and process custom user properties

Group Management

- Calculate direct and effective group membership
- Detect membership changes and remediate key groups
- Proactively prevent token bloat

Domain Consolidation

- Identify resources for consolidation
- Discover policy and schema differences before they affect users
- Ensure best practice adherence before consolidation

Compliance & Conformance

- Know who is making changes to your directory
- Launch content cleanup & entitlement reviews
- Audit security and configuration settings
- Create a baseline and a "Golden Image" standard
- Alert on changes that deviate from the standard

Group Policy

- Extract and archive policy settings
- Monitor key policy settings
- Detect differences between domain policies

Assess and Summarize Infrastructure

- Enumerate Sites, Domain Controllers, Global Catalog Server, User Accounts, and Mail-enabled Objects
- Monitor AD-dependencies like Time Synchronization, DNS configuration, FSMO Role Holders, Global Catalogue settings, and more

Domain Controller Management

- Monitor health of domain controllers in your environment
- Identify key domain controller role holders, sites, and services
- Specify the "Golden Standard" DC and ensure compliance across your enterprise

StealthINTERCEPT for Active Directory

Monitor and alert on changes and access within Active Directory in real-time

Change Monitoring & Control

- Monitor and notify on changes to any AD Object, including object creations and deletions
- Block undesired changes to critical objects, including sensitive security groups and GPOs, even when users have domain admin privileges
- Discover the source workstation that changes are made from, and the old and new values of all property changes on all objects
- Receive real-time alerts on important changes

Privileged Account Monitoring

- Identify and monitor privileged accounts
- Prevent privileged accounts from making undesired changes to critical objects
- Complement any PAM solution by ensuring privileged accounts are used appropriately

Authentication-Based Attack Detection

- Detect authentication-based attacks while in-flight (i.e. brute force attacks and horizontal/lateral account movement)
- Relieve the burden on SIEM by feeding concise, precise details of an attack through integration