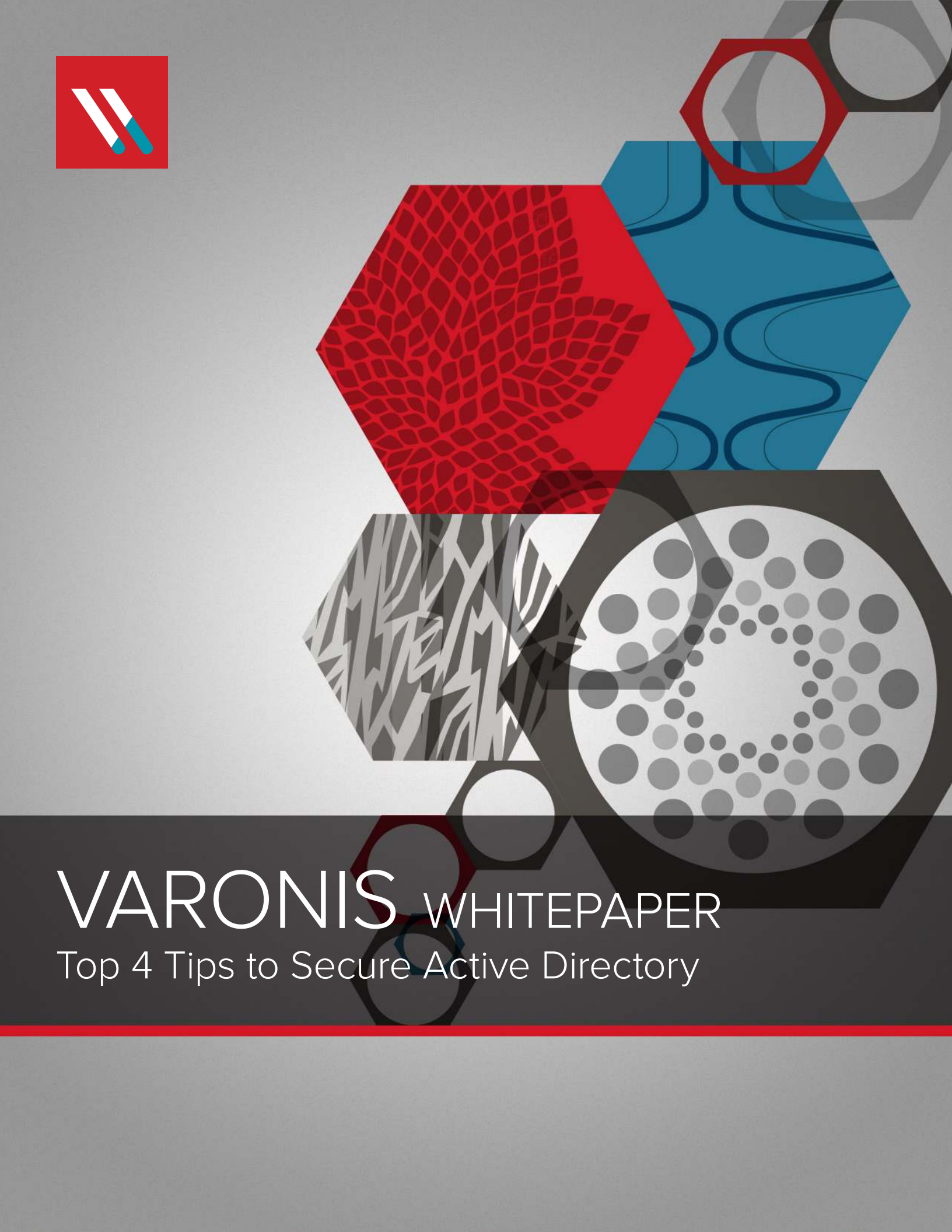

VARONIS WHITEPAPER

Top 4 Tips to Secure Active Directory

CONTENTS

OVERVIEW ____ 3

BASELINE ____ 4

RESTRICT ____ 6

CLEAN UP ____ 8

MONITOR ____ 10

ABOUT VARONIS ____ 13

TOP 4 TIPS TO SECURE ACTIVE DIRECTORY

OVERVIEW

Active Directory is at the heart of the IT infrastructure for nearly every organization. In companies of any size, sysadmins rely upon Active Directory (AD) to help manage and authenticate user accounts, control access to workstations, servers, or applications, and enforce policies across a wide range of devices.

Since access to almost all critical data and systems relies on AD, it is one of the most important technologies to protect. Below are tried-and-true tips, tricks, and best practices based upon years of experience and distilled into four primary steps, culled from the collective knowledge of the AD Admins and security professionals who are in the trenches with us every day.

Four steps to secure Active Directory:

1. Baseline
2. Restrict
3. Clean-up
4. Monitor

STEP ONE: BASELINE

Everyone needs a place to start: a baseline against which they can track progress. This baseline is the foundation for the rest of the steps – so it's important to get it right.

RIGHTS IN AD

Only certain individuals require elevated rights to AD, and even so, they only need enough to do their jobs. However, figuring out who has rights to make changes to AD objects can be tough without automation.

You can make some headway with the native Windows interface and PowerShell[1], however you'll likely need to enumerate group members (and nested group members, and don't forget to take delegation into account). There are commercial solutions available that make reporting on Active Directory permissions a breeze.

GPOS

It's especially critical to baseline GPOs. GPOs can enforce a broad range of policies, but can result in disaster if improperly changed. If you start with a "known good" state, and closely monitor all subsequent changes, you limit the exposure if something goes wrong, and you can recover more quickly when know what's been changed.

[1] *http://blogs.technet.com/b/heyscriptingguy/archive/2012/03/12/use-powershell-to-explore-active-directory-security.aspx*

ADMINISTRATIVE ACCOUNTS

Administrative accounts require special consideration. With elevated rights, administrative accounts can be susceptible to abuse of power by authorized users, and are valuable targets to an attacker. It is imperative to map out which accounts hold administrative rights and what resources can be accessed by those accounts – and to monitor them closely.

Creating an approved list of administrative accounts lays a secure foundation upon which to build a strong security practice. Not only will it let you manage change within the environment – by limiting it to specific accounts, people, and roles – but it also makes it easier to spot when something is not right. Much like identifying permissions within AD itself, there are a few go-to items to watch, such as members of the Domain Admins group, but it can get a bit more difficult to identify users/groups in "local" administrator groups.

Some solutions let you grant administrative access temporarily, even to local administrator accounts. Consider this kind of approach for added security – even your admins probably don't need to have administrative access all of the time.

SERVICE ACCOUNTS

Almost every application makes use of service accounts. These accounts run all sorts of important processes, and may even have elevated rights to perform some required operations. Enumerate service accounts and make sure that they're monitored for account lockouts, password changes, and unusual access patterns. naming conventions (Ex: all service accounts start with SVC_), and/or keep them in designated OU's to help track them. It is highly recommended to avoid using the same service account for multiple different applications. Benefits of using one service account per application are ease of maintenance and manageability. Sharing service accounts between applications can cause headaches if the account is compromised or locked out, and an attacker could compromise more systems or cause wide-spread application outages.

STEP TWO: RESTRICT "HIGH-VALUE TARGETS"

LIMIT AND CONTROL ACCOUNTS THAT HAVE ELEVATED ACCESS AND ACCESS TO SENSITIVE DATA.

Make sure implement a least privilege model, so that only legitimate people have administrative access to AD and that they have only enough privileges to perform their required tasks. These accounts should be periodically reviewed to ensure access is correct and required.

Additionally, these accounts should be monitored closely for signs that they have been compromised. Tell-tale signs can include administrative accounts logging in from many systems in a short period of time, unusual locations, and making changes to systems not normally associated with them or outside of change control windows.

Keep in mind, however, that administrative accounts are not the only high-value only targets. Many users have access to sensitive information like PII/PHI, financial data/PCI information, the recipe for your secret sauce, or even your CEO's inbox. Attackers can exploit these accounts to go after valuable information within an organization. Regularly reviewing who has, does, and should have access to sensitive information significantly reduces the exposure to potential data breaches.

As organizations are becoming (painfully) aware after breaches at Sony and the NSA, sensitive data can often be found in file shares, SharePoint, and email. Remember to review and control access to unstructured data as well.

SEPARATE ADMINISTRATIVE ACCOUNTS FROM NORMAL USER ACCOUNTS

Make sure elevated accounts are only used for the right tasks, and not for daily use. This makes approved administrative access easier to track and document, and unusual administrative access easier to spot and flag.

ENFORCE SEGREGATION OF DUTIES

Some administrative accounts should be used exclusively for administering AD, and other should only be used for file system operations. With this type of segregation, it's easy to spot abuse if an AD-administration account is added to a group that administers the file system and is then used to start accessing data.

RESTRICT ELEVATED BUILT-IN USERS AND GROUPS

Built-in users and groups are found in every domain so they are a constant target in the attacker playbook. The first thing to do is disable Guest, and the second is to rename Administrator so attackers won't get any traction from default attacks (also limit access to this account). It is also a good practice to rename any sensitive groups.

USE SYSTEMS DESIGNATED FOR ADMINISTRATION

If administrators are supposed to use a certain machine (or set of machines) it is easy to detect and alert on misuse when they are used from other systems. If an AD administrative event comes from an incorrect machine/IP, at best, the admin needs a little education on security, and at worst, it could be an attacker compromising an admin account.

ENFORCE STRONG PASSWORDS

Humans seek patterns and meaning, so we often opt for easy-to-remember passwords, or personal details, making passwords susceptible to guessing/brute force/dictionary attacks. By enforcing a strong password policy (complexity, length, and history requirements), it becomes orders of magnitude more difficult for an attacker to batter, force, or guess their way in. Wherever possible, use multi-factor authentication

SET MANDATORY PASSWORD EXPIRATION

Given enough computing power and time, passwords can be brute-forced. By requiring users to change their passwords often (and preventing repeated use), this limits the amount of time an attacker has to attack any given password, and manages the amount of time they could be in control of an account until the password is changed.

STEP THREE: CLEAN-UP

Once your environment is base lined and high-risk items have been addressed, it's time to tackle some housecleaning. AD is complex enough as it is, so a little time spent on clean-up can pay dividends in avoided headaches and confusion down the road. Here are some starting points:

LOOPED NESTED GROUPS

Looped nested groups can be annoying at best and performance-degrading at worst. Some applications may get stuck in an infinite loop if they try to enumerate the members of a group which loops in on itself. Removing looped nested groups improves the overall health of your AD environment.

DUPLICATE SAM ACCOUNTS

A duplicate SAM account is when the same First Name, Last Name and SamAccoutnName appear in accounts in multiple domains. Duplicate SAM accounts can sometimes result in inconsistent provisioning of access. Try to find and eliminate these to ensure smooth operations and a consistent experience for end-users.

EXPIRED ACCOUNTS

Expired accounts look like disabled users because they become disabled when the expiration date passes (the setting can be configured in the object Accounts tab). The downside with using expiring accounts is when the account is used for an automated process or to run an application -- you won't find out it's disabled until someone stumbles upon an issue, or an application breaks. Knowing which accounts are expired and reporting on upcoming expirations can help you both eliminate clutter from AD and preempt any service interruptions

STALE ACCOUNTS

If an account has not been used in several months, it may not be valid anymore. You get a two-fold benefit from eliminating these accounts: first, the environment is more clean and manageable, and second, it reduces the attack surface because attackers can't hijack them and use them to move around within your organization.

ACCOUNTS WITH INCOMPLETE DATA

AD serves as the hub for your digital identity within your network. Having complete and accurate information will make for a better experience in the services or solutions that rely on this data. With few exceptions (such as service accounts) all business users should have certain key fields complete. These include the given name and surname fields, a department, location, and email address and/and telephone number.

ACCOUNTS WITH PASSWORDS THAT NEVER EXPIRE

Very few (if any) accounts should have passwords that never expire. In all but the most extreme cases, these accounts should be found and reconfigured to have a password that changes periodically. If it does require a static password, make sure it is extremely long, complex, and random, to help protect from brute-force attacks.

STEP FOUR: MONITOR (AND MAINTAIN!)

In addition to ongoing monitoring and reporting, some events in AD require immediate attention. Below are a few items that you may want to be notified about immediately:

GPO CHANGES

GPOs changes are not typically a frequent occurrence in most organizations, and when they are modified, they should be managed by a change control process. By alerting on any changes to GPOs, you can validate them with your change control process, spot potentially unwanted behavior, and quickly recover should a mistake be made.

FAILED AUTHENTICATION/ACCOUNT LOCKOUTS

Sometimes we forget or mistype our passwords, but a spike in these occurrences could indicate more serious issues. By tracking authentication attempts, or account lockouts, you get deeper insight into the health of your environment, and can identify potential attackers trying to compromise your network or elevate their rights

ACCESS REQUESTS

Are your application service accounts trying to access your user home drives, or your finance share? If so, you might have an attack on your hands, or an employee snooping where they shouldn't be. By monitoring and alerting on unusual access events, you can mitigate potential misuse, abuse, or threats.

CHANGES IN PRIVILEGED GROUP MEMBERSHIP

Again, AD holds the keys to the kingdom, and attackers like keys. By receiving immediate notifications on any changes to privileged groups, security can validate the changes are appropriate, and take immediate action if necessary.

OBJECT/USER/SECURITY/COMPUTER MODIFICATIONS

Changes to AD objects are part of the daily routine for IT – users are on-boarded and off-boarded, people get new computers, people change their names. However, by analyzing and creating a baseline of normal AD behavior and trends, you can spot unusual changes and potentially unauthorized access.

STATISTICS

There are some key performance indicators which will help track the health of Active Directory and highlight risky areas.

Once AD is in a healthy, known-good state, monitoring these key performance indicators ensures AD remains in the best shape possible.

By reporting and trending these metrics over time, you can make you're staying on top of Active Directory hygiene:

- Total number of AD users changes should generally reflect changes to your employee count
- Watch out for upward trends on:
    - Total number of disabled accounts
    - Total number of expired accounts
    - Total number of accounts with a password that never expires
    - Total number of deactivated accounts
    - Total number of accounts with last logon >3 month / >6 months
    - Total number of accounts that never logged on
    - Duplicate SAM accounts
    - Number of accounts for which mandatory data is missing

There are all sorts of ways to gather this data, with varying degrees of pain and technical expertise required. One of the most common is the "script and spreadsheet" method, and there are some awesome resources from Microsoft that can help writing scripts for ad-hoc queries. There are also a few neat tools on the SysInternals page that could also assist on a case-by-case basis as well. However, there are much more automated, complete off-the-shelf solutions to make management, auditing, and reporting about of AD painless.

CONCLUSION

Almost every system integrates with and authenticates Active Directory. As one of the most central, powerful tools within any organization, Active Directory requires diligent care. The four steps covered above can help every organization gain a deeper understanding of their Active Directory environment, control complexity, streamline operations, reduce the risk of mistakes, and protect itself from malicious activities. By better preventing, detecting, and recovering from issues with Active Directory and the systems that rely on it, organizations will be both more protected and more efficient.

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

Free 30-day assessment:

WITHIN HOURS OF INSTALLATION

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

WITHIN A DAY OF INSTALLATION

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

START YOUR FREE TRIAL