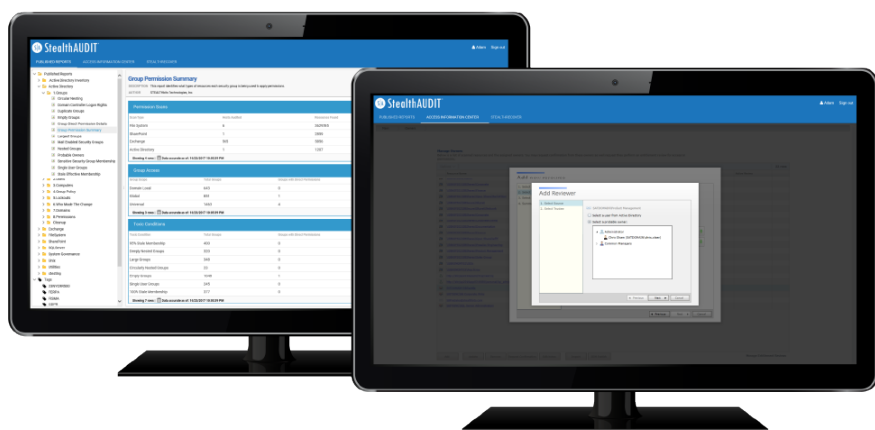# ACTIVE DIRECTORY GROUP GOVERNANCE

Automating Group Membership Management

stealthbits
NOW PART OF **netwrix**

ACTIVE DIRECTORY GROUPS

Active Directory groups are the primary way in which user access is managed in most organizations. Users requiring similar access to information are grouped together and provisioned with the access they need via permissions set at the group level. Generally, these groups are defined by the line of business to which the users of the group belong.

The problem with governing AD group membership

Despite groups being defined by the line of business, it is left up to IT to manage group membership across entire organizations. Often times, IT receives no insight from the business to determine whether group membership is up to date and correctly configured. Over time, this disconnect exacerbates the problem of users acquiring and retaining inappropriate access and presents security risks as users continue to have access to information that they should no longer be entitled to.

The challenge of enabling a group membership review program

While there are sometimes processes in place to communicate changes in group membership between the line of business and IT, they are generally manual, relying primarily on emails and spreadsheets. Requests for group membership changes and confirmation that group membership is accurate are not standardized, leading to issues with reliability and potentially compliance with audit regulations.

In many cases, there are no processes in place where the line of business responsible for a group can attest to that group's membership due to the complexity of establishing rightful ownership in the first place.

STEALTHBITS' AD GROUP GOVERNANCE SOLUTION

The solution to the problem of erroneous group membership is rooted in bridging the gap between IT and the line of business. With the Access Information Center (AIC), organizations are empowered to let the line of business manage their own groups with IT's oversight. Three main workflows exist to help organizations govern group membership:

Group owner assignment

The AIC provides AD admins the ability to assign owners to groups based on either Stealthbits' recommendation of the "probable owner" for the group or manual selection. Group owners have the opportunity to confirm or decline their assignment via automated email.

Self-service requests

Employees of an organization can sign into the AIC to request membership to the groups they require access to. These requests are routed directly to that group's owner; the best person to determine whether the requested access is justified.

Group membership reviews

To ensure that IT and the line of business are on the same page, AD admins can trigger group membership reviews that allow group owners to attest to their group's membership. If there is a problem with the group's membership, the group owner can suggest changes from within the review itself. Upon submission, IT can execute the changes.

Ad-hoc changes

Access needs change quickly, and nobody understands who should have access better than group owners. The Access Information Center lets owns see and modify the membership of their groups on-demand, empowering owners to ensure that only the right people have access to their data at all times.

Stealthbits can read and write file classification tags to enhance governance and increase the effectiveness of your encryption or data-in-motion security tools.

HOW IT WORKS

Governing Active Directory Groups properly is difficult, but with Stealthbits' Access Information Center, it's not nearly as hard as you might think:

Assign owners

Assign manually, through bulk imports, or allow the AIC to suggest the "Most Probable Owner". Once established, confirmation requests are sent to confirm selections.

Conduct group membership reviews

Administrators trigger reviews for Group Owners to attest to their group's membership. Changes are reviewed for final approval and execution.

Enable self-service membership requests

End users request membership to groups and group owners review, choosing to accept or reject requests

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits

NOW PART OF **netwrix**