USE CASE: SECURING ACTIVE DIRECTORY

A Varonis customer identified unauthorized use of a privileged service account to unlock other accounts, perform password resets, and change security group memberships.

An investigation uncovered IT admins taking shortcuts and bypassing change control policy, but it could have easily been an attacker.

How does Varonis help monitor and protect Active Directory and Group Policies?

By mapping Active Directory (AD), Varonis tells you who has the ability to make changes within AD and spots configuration problems and access control issues.

By analyzing AD activity, we alert you to unusual changes, account lockouts, password resets – the kinds of things that are indicative of privilege escalation, unauthorized changes, lateral movement, and brute-force attacks. We can also alert you when changes are made by non-administrators or outside of change control windows.

When an account is locked out, it can mean someone forgot their password, there's a configuration error, or someone is trying to break into accounts. Varonis baselines normal account lockout patterns for every individual account, groups of users (like executives), and across all accounts.

DatAlert threat models can detect sharp spikes in lockouts as well as gradual increases over time that might indicate an attacker going "low and slow."

We also track changes to Group Policy Objects (GPOs) which can affect password policies, USB access, RDP privileges, and more.

Relevant DatAlert threat models

- Abnormal admin behavior: unusual amount of lockouts across admin accounts
- Abnormal admin behavior: accumulative increase in lockouts for individual admin accounts
- Abnormal admin behavior: accumulative increase in lockouts across admin accounts
- Abnormal behavior: accumulative increase in lockouts across end-user accounts
- Abnormal behavior: accumulative increase in lockouts for individual end-user accounts
- Abnormal behavior: unusual amount of lockout across end-user accounts