USE CASE: PRIVILEGED ACCOUNT OVERSIGHT

In 2013, attackers leveraged the stolen credentials of an HVAC vendor into powerful admin accounts, resulting in the biggest retail data breach in US history. Once they were in the system, they created a new admin account - giving them access and necessary permissions to install malware, steal PII, 40 million credit card accounts of target customers, and send stolen data out of the corporate servers and into their private accounts.

If the retail company had DatAlert they would have been alerted when the new account was created, they would have been alerted when the PII data was accessed, and they would have been alerted when the account tried to exfiltrate the data.

How does Varonis help secure privileged accounts?

Varonis can automatically detect all administrative and service accounts, even unknown or newly created ones – without any manual intervention, so that there's automated, constant oversight across platforms on your most powerful accounts.

Our threat models watch file and email activity for all users to understand what's normal – and what's not – for admins as individuals and admins as a group: so even if an admin account has the right credentials, we'll know if it starts behaving out of the norm.

If an admin starts accessing atypical mailboxes, for example, DatAlert will catch that type of activity and let you know that it's time to investigate. If there's a gradual increase in lockout events of an admin – not just a sudden spike - DatAlert will compare their lockout events over time to her behavioral profile and trigger an alert if there's an increase.

Relevant DatAlert Threat Models

- Abnormal admin behavior: accumulative increase in lockouts for individual admin accounts
- Abnormal admin behavior: accumulative increase in lockouts for all admin accounts
- Abnormal admin behavior: access to atypical mailboxes
- Membership changes: admin groups