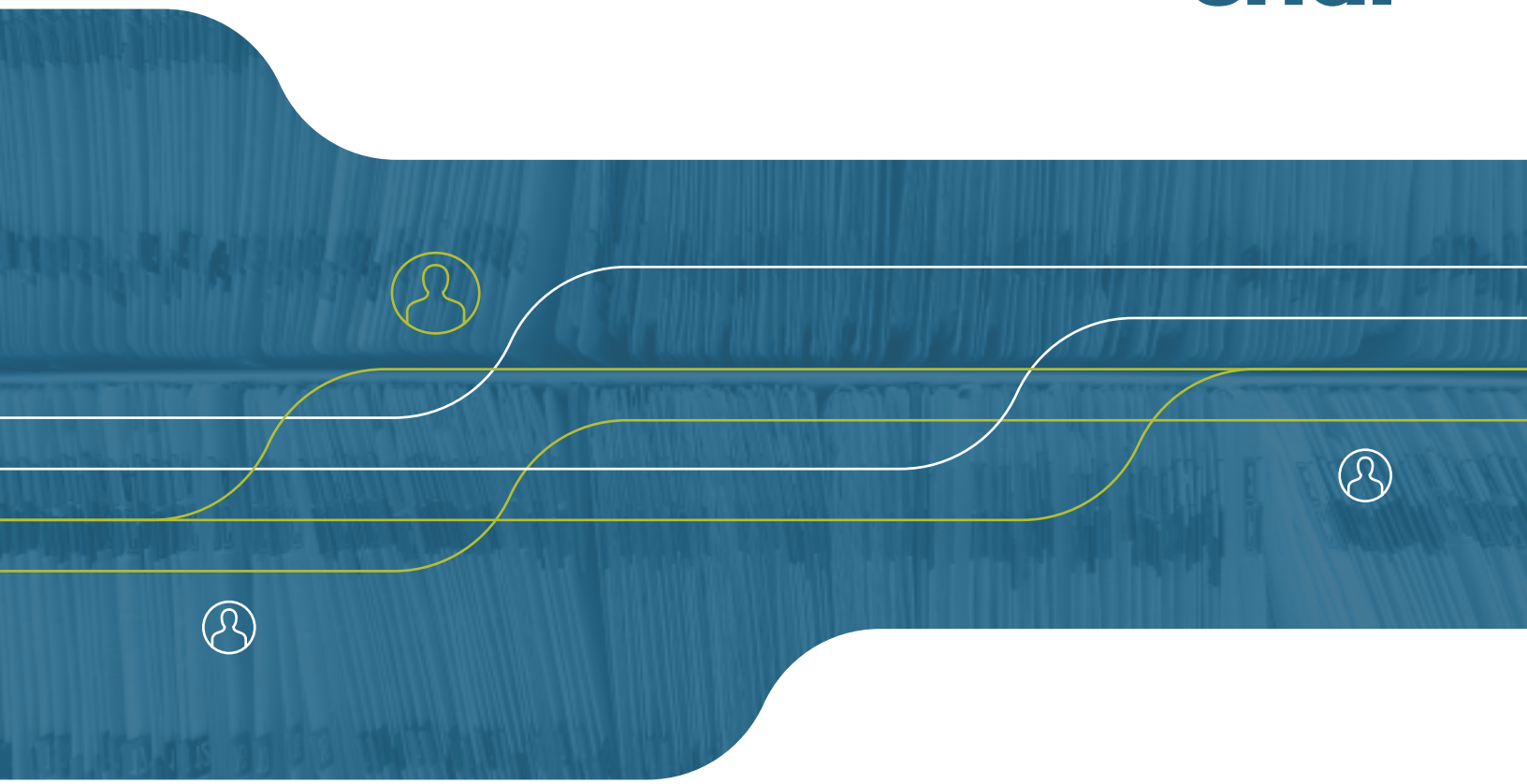
shai



Aging Accounts in Active Directory

CASE STUDY

Aging Active Directory accounts are not only a drain on your organization's resources, they are also a security vulnerability. Checking and correcting these accounts takes time and effort. Shai™ can automatically eliminate old accounts using the very same business rules you already have in place.

Navigate

If you could design your system perfectly, you would always have one user for every one Active Directory account. This can be hard to achieve in any setting, but especially in environments where a user may go from active duty to reserve, to guard, or contractor status, and back again at a later date. For these reasons, it is common for many dormant Active Directory accounts to exist and represent a security issue.

Collaborate

To understand all the checks and confirmations of finding and removing dormant accounts, NCI mapped out the step-by-step process a dedicated person would currently take to eliminate an old account. This workflow includes setting timelines for actions, informing an affected user, contacting an administrator for a final determination, and lastly eliminating the dormant account from the Active Directory.

As a highly repetitive administrative process, eliminating dormant Active Directory accounts is an ideal application for Shai™. Using the workflow previously outlined, Shai™ was trained and set up to follow the organization's business rules to identify dormant accounts which had not been accessed in 25, 30, and 45 days.

Now, Shai™ notifies any affected users that their accounts are at risk of being terminated due to inactivity. However, since a final human sign off was an important step for the customer, Shai™ alerts a system administrator and waits for final guidance before any accounts are removed. Once the administrator reviews and determines the accounts can be safely removed, Shai™ acts on their instruction and reports back on her actions.

Innovate

During the workflow scoping process, NCI determined that it took nearly 40 hours per week of a person's time to complete the dormant account process for the customer, in just a single location. Now that Shai™ is up and running as a digital colleague, she easily performs tasks related to Active Directory account aging in less than 15 minutes a week.

With this one example, NCI was able to prove and showcase the effectiveness Shai™ can have on aging Active Directory accounts, removing the need for human oversight and freeing up personnel resources. In addition to the efficiency gains, Shai™ created tangible cost savings and a more secure IT environment..

- No new tools, system replacement, APIs, or software required
- Designed to house and safeguard sensitive information
- Adheres to FedRAMP, NIST 800, HIPAA, and the HITECH Act
- Diligently works 24/7, 365 days a year