rubrik

9 STEPS TO IDENTITY RESILIENCE

STEP 01 UNIFY

UNIFY VISIBILITY

TO EFFECTIVELY MANAGE A FRAGMENTED IDENTITY LANDSCAPE...

01

CENTRALIZE

Centralize your identity visibility across all your Identity Providers (IDPs), such as Active Directory, Okta, and Entra ID.

02

IMPLEMENT

Implement a single solution that gives you a unified view of all identities, permissions, and access policies, regardless of where they are managed.

03

FLEXIBILITY

Choose flexible tools that can integrate across multiple vendors without creating new dependencies.

⚠ **WHY THIS IS IMPORTANT**

This approach allows you to quickly spot and fix security gaps, ensuring consistent policies and reducing hidden vulnerabilities across your entire environment.

STEP 02 ALIGN

ALIGN IT AND SECURITY

TO EFFECTIVELY SECURE IDENTITIES, IT AND SECURITY TEAMS MUST COLLABORATE AND MAKE IDENTITY AND ACCESS MANAGEMENT (IAM) A SHARED RESPONSIBILITY.

IT TEAMS

Traditionally:

- Managed IAM for provisioning

SECURITY TEAMS

Bring critical expertise on:

- Modern threats
- Vulnerabilities
- Attack paths

⚠ WHY THIS IS IMPORTANT

By bridging these two functions and giving the CISO and security leadership a key role in shaping IAM policies and tools, organizations can align their efforts and manage identities with a comprehensive, security-first approach that keeps pace with new technologies and threats

STEP 03 PRIORITIZE

PRIORITIZE SECURITY FOR CRITICAL APPS

FOCUS YOUR SECURITY EFFORTS ON THE APPLICATIONS THAT HOLD YOUR MOST SENSITIVE DATA, SUCH AS FINANCIAL, PERSONAL, OR INTELLECTUAL PROPERTY INFORMATION.

01

IDENTIFY

Start by identifying these critical apps.

02

MAP

Map out all the associated identities, including unmanaged service accounts and API keys.

03

EVALUATE

Once you've done that, evaluate their configurations and data access to ensure that only the necessary permissions are in place.

⚠ **WHY THIS IS IMPORTANT**

This targeted approach helps reduce your risk and keeps your most important systems protected.

STEP 04 FOCUS

BROADEN FOCUS TO CRITICAL IDENTITIES

MOVE BEYOND JUST SECURING ADMIN ACCOUNTS AND IDENTIFY OTHER SENSITIVE IDENTITIES IN YOUR ENVIRONMENT, SUCH AS IT USERS WITH BROAD SYSTEM PRIVILEGES OR DATA SCIENTISTS WITH ACCESS TO CRITICAL INFORMATION.

FIRST,

map out their actual permissions and understand what they can access and do.

THEN,

directly link these identities to the sensitive data they can reach to assess how a compromise could lead to a breach.

⚠ **WHY THIS IS IMPORTANT**

Prioritizing these overlooked accounts helps close potential attack paths and limits the potential damage from a security incident.

STEP 05 DISCOVER

DISCOVER, MONITOR, AND SECURE NON-HUMAN IDENTITIES (NHIS)

01 **TAKE CONTROL**

Take control of your non-human identities, like service accounts and bots, by continuously inventorying them and enforcing the principle of least privilege.

02 **AUTOMATE**

Automate their lifecycle and credential management so that their provisioning, de-provisioning, and rotation are handled automatically and securely.

03 **MONITOR**

Finally, continuously monitor these accounts for any unusual activity and use network segmentation to contain them and limit the potential damage if one is compromised.

STEP 06 ELIMINATE

ELIMINATE STALE AND DORMANT ACCOUNTS

TO REDUCE EASY ENTRY POINTS FOR ATTACKERS, ESTABLISH CLEAR INACTIVITY POLICIES FOR ACCOUNTS. FOR EXAMPLE...

AFTER

90 DAYS OF INACTIVITY

ACCOUNTS ARE DISABLED.

AFTER

180 DAYS OF INACTIVITY

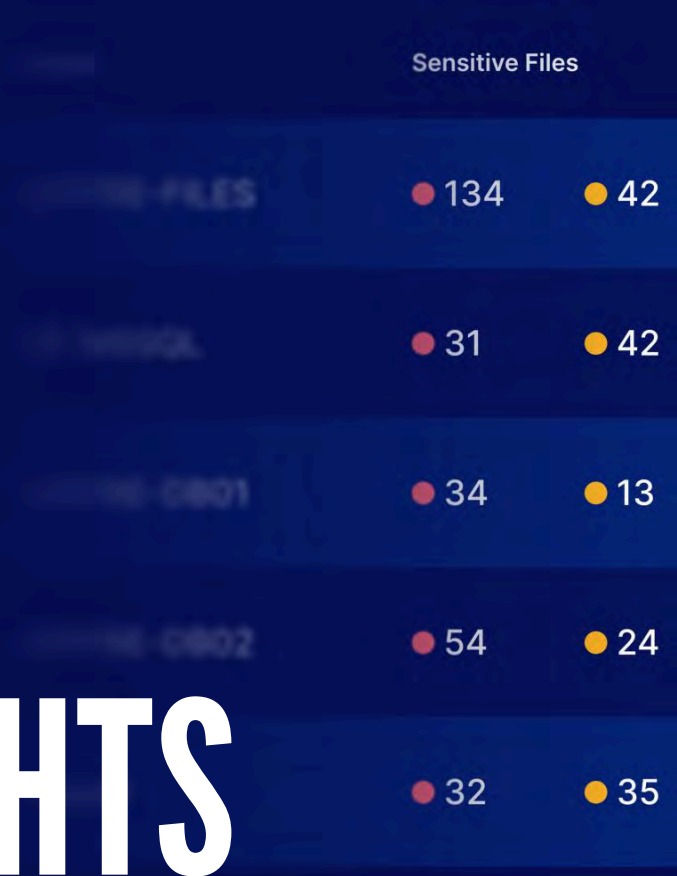
ACCOUNTS ARE DELETED.

AUTOMATE

Implement automated processes that securely bridge your HR systems and identity providers to streamline de-provisioning.

REVIEW

Regularly review user permissions, especially when they change roles, to ensure they don't retain old, unnecessary access.



STEP 07 **REMEDIATION**

MOVE BEYOND AUDITS TO ACTIONABLE INSIGHTS AND REMEDIATION

INSTEAD OF JUST IDENTIFYING SECURITY ISSUES, PRIORITIZE AND ACT ON YOUR AUDIT FINDINGS, FOCUSING ON HIGH-IMPACT IDENTITIES FIRST.

HOW TO DO IT

When an audit flags a problem, like a user lacking multi-factor authentication (MFA), start the remediation with your most sensitive accounts—not just admins.

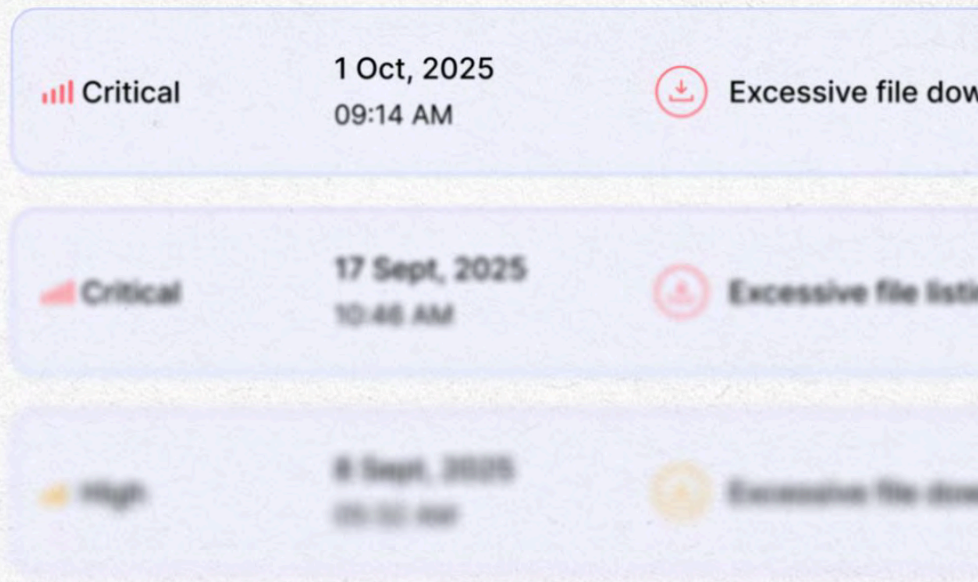
NOT FEASIBLE?

For any exceptions where MFA isn't feasible, set up robust monitoring and specific security rules to promptly detect and respond to any signs of compromise.

STEP 08 **MONITOR**

MONITOR, REMEDIATE, AND REVERT CRITICAL IDENTITY PROVIDER CHANGES

To prevent unexpected changes from creating security gaps, implement proactive alerts that notify your team immediately when a critical identity configuration is changed or unusual activity occurs.



MAKE SURE YOUR SOLUTIONS OFFER A SIMPLE, ONE-CLICK WAY TO REVERT UNAUTHORIZED OR UNWANTED CHANGES.

⚠ WHY THIS IS IMPORTANT

This allows you to quickly restore your clean configurations and limit exposure to attacker activity or damaging misconfigurations.

STEP 09 RECOVERY

PLAN FOR BREACH AND RECOVERY

Prepare for a breach by choosing an identity recovery solution specifically designed to withstand attacks, ensuring it remains secure and operational even when your environment is compromised.

WHAT SHOULD IT DO?

INTEGRATE EVERYTHING

This solution should support multiple identity providers and reliably synchronize identities and configurations after an incident.

PINPOINT CHANGES

It should also be able to pinpoint exactly which identity attributes were changed, enabling you to quickly and easily remediate the issue.