Cisco Identity Best Practices

Best Practices

A dedicated place to share best practices on identity security.

More guides coming soon!

- Identity Security Reading List
- KPIs for IAM Teams

What's Next? How to use Cisco Identity effectively

You've completed the "Getting Started" checklist - Congratulations!

This guide aims to detail how you can operationalize Cisco Identity once you have completed the initial onboarding set up steps.

Cisco Identity is unique because it is both an Identity Security Posture Management (ISPM) tool and an Identity Threat Detection and Response (ITDR) tool. To get the most of out the insights and data Cisco Identity provides, it is crucial to understand why ISPM and ITDR are equally important, and how you can leverage both types of insights to make your organization more secure.

Starting with a clean slate

The identities in your environment are under constant threat, and while bad actors may adjust or change the techniques used, they will certainly not stop trying to compromise your users' accounts. As detailed in the Identity Posture Score documentation, making sure that the identities in your environment are secure is a necessary step to protect your organization from the attacks and threats targeted at those identities.

Without strong identity security posture, not only are your identities more vulnerable to being successfully compromised, but also every attack that comes in is inherently riskier. That means you and your team will need to spend more time and resources investigating every risky event or suspected attack to ensure that the impacted identities were not actually compromised.

Identity teams are spread thin enough as is - Why spend time worrying and investigating suspicious log in attempts on an account that has not been used in 3 years when that account should have just been deleted years ago?

For this reason, we recommend starting with user clean up **before** diving head first into the threat insights available, even if your primary responsibility is focused on user investigation and threat hunting. There are a few checks that we typically recommend starting with for user clean up, and multiple ways you can make the clean up easier to manage that are described

below.

Where to start

There are several ways you can use Cisco Identity's insights to improve your organization's identity posture. To find areas for improvement, you can use the recommended actions associated with your organization's Identity Posture Score or go through the list of checks and pick a couple that stand out. We usually suggest starting with the following checks (which are also part of the posture score) since they are often quick and easy to take action on and bring immediate value:

- Never Logged In
- Inactive Guest Users
- Inactive Users
- No MFA Configured

To start, we typically recommend picking only 1 or 2 checks/posture recommendations to focus on cleaning up properly. If you pick too many checks to clean up at once, it can be difficult to make real progress.

Depending on the size of your environment, there can be a lot of users failing a given check, which can be very overwhelming and make it difficult to decide where to start. Below are a couple ways to help you can make the results of checks more manageable and actionable, and prioritize certain users who may be carry more inherent risk to your organization.

Review check settings

Before you start cleaning up users on a given check, regardless of if you are using posture score recommendations or specific checks, review that check to see if there are custom settings that can and should be modified to better align with your organization's processes, policies and risk tolerance levels. This will ensure that the users failing the check are actually relevant to take action on for your organization.

For example, by default the **Never Logged In** check will fail on users who have not successfully signed in 7 days after their account was created. However, your organization's account creation procedure is to create accounts 14 days before a user's start date. In this case, it would be critical to adjust the check's settings to better align to that procedure, otherwise there will be many users failing the check who are not actually actionable.

Creating smaller sub-groups

Each organization has different priorities and concerns, which means not all identities are created equal for every company for every check - some users may be more important to take action on, and others may be less urgent.

If you have a lot of users failing a check that you would like to clean up, we recommend utilizing the filters on the Users page to partition a given check's failing users into smaller, more manageable sub-groups so that you and your team can more easily take action.

You can do this from two places:

- Directly on the Users page - use the **Failing check** filter for the desired check, and then use additional filters or column sorting
- Via the desired Check's page
- Use the **View Users** button above the table's column headers, or in the table area if there are more than 1,000 users failing the check, to go to the Users page pre-filtered on the given check where you can add additional filters or column sorting
- Use the **Failing Users by Integration** widget on the right of the screen. Click a desired integration to go to the Users page pre-filtered on the selected integration and the given check where you can add additional filters or column sorting

For example, for the **Inactive Users** check, use the filters to display only inactive users that are internal accounts and do not have MFA configured.

To quickly access the same combination of filters later on, save your filter to your Cisco Identity tenant. These filters are available to anyone with access to your tenant.

Downloading results

If you need to share a list of users with other members of your team who may not have access to Cisco Identity, you can download the results from the Users page into a .csv. On the right side of the page, next to the Search bar is a button with a D**ownload** icon which will export the list of users (up to 2,000 users), as well as any applied filters, column additions and column sorting that was done in the platform.

You can also download the list of failing users from a given check using the **Download** button above the table of failing users, which will include the information from the table, as well as the check failure explainability. If there are more than 1,000 users failing a check, you cannot download from this view. You must go to the Users page, using the **View Users** button in the middle of the table, and download there. If needed, use the filters to get to a group of 2,000 users or less so that you can download everyone

Working with the recommended checks

Below are some tips and tricks for making the clean up process more manageable for the specific checks listed above; however, these tips can apply to many other checks, so getting familiar with the features mentioned below can be useful when cleaning up other checks.

Never Logged In

The **Never Logged In** check alerts on accounts that have never successfully signed in since their account was created. These accounts pose a high risk if they were to get compromised

as they are typically granted access to certain apps and information by default when the account was created. Additionally, bad actors often target these accounts as they do not have MFA registered, so they are easy to sign in to, and the bad actor can then register their own MFA method to maintain access to your system.

The default setting is 7 days after creation – Make sure to modify the check's default settings for this check to better align results with your organization's procedures.

Tips for cleaning up Never Logged In

External users failing this check are typically low risk to remove as the account has never been used and can easily be re-added to your environment if needed. These accounts pose a risk because it is often unknown exactly what permissions or data access a guest user was given. Depending on how the user was invited into your environment, you can review the **Invited By** info in the source card on the user's User 360 Overview tab.

- After filtering the Users page on the check, use the **User Type** filter and select **External**
- (If column is not visible) Select the **Columns** button on the right hand side, above the table headers and select **Created Date (UTC)** to add this data into the table as an additional column. Select the **Created Date** column header to sort the column from oldest to newest
- Delete any accounts that were created at least 1 month ago and have never successfully signed in. You can download these users via .csv if needed (see above for info). **Temporarily** exclude any users from this check if there is a reason they need to remain in the system for a period of time
- Users must be deleted directly at the identity data source (ex: Entra). However, if you have write permissions for Entra you can delete external Entra users through Cisco Identity via the **Actions** button on a given user's page

Admin or VIP users failing this check can be more complex to remove than external users, as they may involve some more investigation to understand why the account exists and is unused. However, these unused accounts pose a lot of risk because they have elevated privileges, are often granted wide access to several different corporate apps, assets and sensitive corporate information, and very rarely have MFA configured, making them an easy, and valuable, target to compromise.

- After filtering the Users page on the check, use the **User Type** filter and select **Internal**
- Find either the **Administrator of** filter and select **All** or the **Is Admin** filter and select **Yes**
- If the user has accounts in multiple sources, you can see where they are an admin in the source cards on the User 360 Overview tab
- (If column is not visible) Select the **Columns** button on the right hand side, above the table headers and select **Created Date (UTC)** to add this data into the table as an additional column. Select the **Created Date** column header to sort the column from oldest to newest
- Delete any accounts that were created at least 3 months ago and have never successfully signed in. You can download these users via .csv if needed (see above for info).

Temporarily exclude any users from this check if there is a reason they need to remain in the system for a period of time

- Users must be deleted directly at the identity data source (ex: Entra), you cannot delete internal users directly in Cisco Identity
- Once completed, repeat these steps using the **Is VIP: Yes** filter
- Note: VIP users are users with titles that are commonly used with executives

Internal users, like Admins users, can also be more complex to remove than external users. They also pose high risk to your environment because these accounts are typically provisioned with extensive access to different corporate systems and information, and very rarely have MFA configured.

- After filtering the Users page on the check, use the **User Type** filter and select **Internal**
- (If column is not visible) Select the **Columns** button on the right hand side, above the table headers and select **Created Date (UTC)** to add this data into the table as an additional column. Select the **Created Date** column header to sort the column from oldest to newest
- Delete any accounts that were created at least 3 month ago and have never successfully signed in. You can download these users via .csv if needed (see above for info). **Temporarily** exclude any users from this check if there is a reason they need to remain in the system for a period of time
- Users must be deleted directly at the identity data source (ex: Entra), you cannot delete internal users directly in Cisco Identity
- If smaller groups are still needed, add the **MFA Configured** filter and select **No** and remove these accounts from oldest to newest. Once completed, go back and remove the MFA Configured filter and follow the same account deletion process (oldest to newest)

Inactive Guest Users

The **Inactive Guest Users** check detects external/guest accounts who have successfully signed in at least one time but have not done so recently. As discussed above with the Never Logged in check, these accounts are low-risk to remove since they can be added back easily if needed, and the unknown access these users may have poses a risk to your organization, so it is important to clean up unnecessary accounts.

The default setting is 30 days of inactivity - Make sure to modify the check's default settings for this check to better align results with your organization's procedures.

Tips for cleaning up Inactive Guest Users

- Filter the Users page on the check
- Select the **Last Seen (UTC)** column header to sort the column from oldest to newest
- Note: Last Seen represents that last sign in attempt regardless of result. You can see the last successful sign in for each identity source in each source card on the User 360 Overview tab to review inactive users with more recent Last Seen dates

- Remove any users in the list, starting with the users with the oldest Last Seen date. **Temporarily** exclude any users from this check if there is a reason they need to remain in the system for a period of time

Inactive Users

The **Inactive Users** check alerts on internal accounts who have successfully signed in at least one time but have not done so recently. As discussed above with the Never Logged in check, these accounts can be more involved to remove, but pose high levels of risk because of what they have access to. These accounts can also highlight gaps in your organization's account automated or manual deprovisioning process.

The default setting is 30 days of inactivity - Make sure to modify the check's default settings for this check to better align results with your organization's procedures.

Tips for cleaning up Inactive Users

- Filter the Users page on the check. Use the **MFA Configured** filter and select **No**
- You can also use the Admin and VIP filters described in the Never Logged In check tips above to prioritize the results further
- Select the **Last Seen (UTC)** column header to sort the column from oldest to newest
- Note: Last Seen represents that last sign in attempt regardless of result. You can see the last successful sign in for each identity source in each source card on the User 360 Overview tab to review inactive users with more recent Last Seen dates
- Remove any users in the list, starting with the users with the oldest Last Seen date. **Temporarily** exclude any users from this check if there is a reason they need to remain in the system for a period of time

No MFA Configured

This check alerts on accounts that have successfully signed in at least once that have not configured any forms of MFA on their account. Accounts without MFA are much easier to compromise as they do not have a secondary authentication factor enrolled that they need to use to gain access to systems. Note: users failing the Never Logged In check are not evaluated as part of this check, even if they do not have MFA configured.

The default setting is 7 days after account creation - Make sure to modify the check's default settings for this check to better align results with your organization's procedures.

Tips for cleaning up No MFA Configured

Look through your Posture Score recommendations and find the recommendation that says “Require priority users to configure and utilize any MFA factor" . Select the respective Failing Users to go to the Users page, pre-filtered on this information

- Using the **Status** filter, select **Active** to identify accounts who have successfully signed in recently. Contact the end users in the list and require them to enroll a factor on their

account immediately

- Remove the **Status: Active** filter and review the users in the list. Delete any accounts that are no longer active and not needed. For unused accounts that are needed, contact the end user and require them to enroll a factor on their account immediately. Disable the account if the end user does not comply by a set timeframe
- If applicable, **temporarily** exclude any users in this list from the No MFA Configured check and leave a comment with the necessary details

If the posture score recommendation does not exist, find the recommendation that says "Require users to configure and utilize any MFA factor" . Select the respective Failing Users to go to the Users page, pre-filtered on this information

- Focus on internal users first by enabling the **User Type** filter and selecting **Internal**
- Using the **Status** filter, select **Active** to identify accounts who have successfully signed in recently
- Add the **Created Date** column to the table if needed (see Never Logged In tips above for details on how to add columns) to find the accounts that have existed the longest amount of time without MFA configured. Click on the C**reated Date** column header to sort from oldest to newest and delete any accounts that are no longer active and not needed. Contact the end users in the list and require them to enroll a factor on their account immediately
- If applicable, **temporarily** exclude any users in this list from the No MFA Configured check and leave a comment with the necessary details
- Once the **Active** users have been cleaned up, remove the **Status: Active** filter. Click on the C**reated Date** column header to sort from oldest to newest. Delete any accounts that are no longer active and not needed, starting with the oldest creation date. For unused accounts that are needed, contact the end user and require them to enroll a factor on their account immediately. Disable the account if the end user does not comply by a set timeframe. Temporarily exclude users as needed
- Deselect **Internal** from the **User Type** filter and work through the other user types based on your organization's priorities using the same techniques described above

Clean up complete - now what?

Once you have completed the clean up of a few checks we suggest doing the following:

- **Configuring your notification target on the cleaned up checks** - This allows you to take quicker action on newly failing users, preventing the number of failing users from increasing substantially over time with you noticing. Cleaning up a couple of users here and there is much easier and saves a lot of time and effort compared to going through massive clean up processes a couple times a year
- We do not recommend that you configure notification targets on these checks BEFORE you complete the clean up as it can overwhelm you more, and newly failing users may be

less critical to take immediate action on

- **Review your organization's internal policies and processes based on your findings to identify areas for improvement** - Are there any changes that can be made to onboarding or offboarding processes to ensure that unused accounts are removed automatically? Are there updates you can make to admin assignment procedures to ensure that admin accounts are not created if they are not really needed? Is there a reason that users are automatically granted access to certain resources or apps that frequently go unused - can you get rid of the resource all together or make access more 'as needed' ? Having these conversations can spark some great ideas to automate and proactively improve your organization's identity hygiene, and reduce the amount of manual clean up that needs to happen
- **Find new things to clean up -** You've cleaned up a couple checks already, now it's time to find your next area to focus on! Use the Identity Posture Score to find high priority items or go through the list of checks to see everything that is available and find issues that are particularly concerning to your organization. Review the check recommendations and then utilize the same techniques, tips and features discussed above to make the clean up as manageable as possible.

Once your organization has spent some time addressing its postural issues, you can also start looking more into the Threat Detection functionality that Cisco Identity has to offer.

Identifying and Investigating Threats

Even if your role's primary focus is investigating and responding to threats, or proactively threat hunting, we still highly recommend working with the relevant teams in your organization to follow the steps above for account clean up. This will make using Cisco Identity easier to use and more effective since you can focus on the right accounts, rather than unnecessary dormant accounts that have lingered around for too long.

Once the clean up is complete, you can leverage Cisco Identity to identify and investigate the attacks coming in on the accounts in your environment.
There is a lot of data and detections available in Cisco Identity that can easily overwhelm you and your team, which is why we recommend figuring out a plan first before diving in to the deep end.

Where to start

There are two ways you can start finding accounts to investigate

User Trust Levels

The first way to identify concerning accounts is through User Trust Levels. At a high level, each user in your organization is assigned a User Trust Level that is calculated based on the user's context, behavior and common tendencies, and failing checks. You can read this Trust Level article in our documentation for more in-depth information.

With the User Trust Level, the riskiest users are called out so that prioritization work is already done for you. Users who are assigned an Untrusted level should be investigated immediately. We also recommend investigating users with a Questionable level if time permits.

To easily find these users, you can refer to the User Trust Level widget in the Dashboard and select the desired trust level to drill into the users, or you can use the basic filters available on the Users page. From here, dive into any user to go to their User 360 Overview tab where you can find the Trust Level widget at the top of the page, which details why the user received a particular score. Read the User 360 documentation to learn more about how to utilize the widget on this page to conduct your investigation.

There is also a check called **User Trust Level Alert** that detects users who have been assigned an Untrusted level. If desired, you can also modify the check's settings to fail users who have been assigned a Questionable level. We recommend adding a notification target, such as the one created during the initial onboarding journey, to this check so that you can be proactively alerted to any new failing users and they can be investigated as quickly as possible.

Per Check

Another way you can find users to investigate is on a per check basis. For some customers, there are specific threat based detections that are particularly of interest or of concern that they want to keep a very close eye on, so they choose to use this method alone – or combine it with the User Trust Level method.

Start by reviewing the list of available checks to determine if there are any checks that are critical to your organization to be alerted about. Like with account clean up, we recommend picking only a few checks (approx 3–5) to start with so that you and your team can get comfortable with operationalizing the checks first.

For each desired check, look through the explainability of some of the failing users, when available, to understand what types of behaviors or factors lead to users failing the given check. Once you have an understanding of what causes a user to fail each check, adjust the check's settings accordingly, if needed, so that they align with your organization's risk tolerance levels, policies, tools, etc. This ensures that whenever a user does fail a check, there is a higher likelihood that it is something worth investigating. For example – you see users failing the **Users with Email Forwarding** check because they are forwarding emails internally, so you add your company's domain to the **Ignore** List on the check settings, or you see users failing the **Impossible Travel** check with corporate IP addresses, so you import an IP CIDR list with your office IPs and change the check's settings to exclude “good known IPs" .

After adjusting any necessary check settings, add a notification target, such as the one created during the initial onboarding journey, to each check so that you can be proactively alerted to any new failing users, instead of logging in daily to check if there are any new users failing the desired checks.

When you receive your first alert, practice investigating one user end to end to get a feel for how to operationalize Cisco Identity in your organization.

How to investigate

When you have identified a user for investigation, you may not know where to start to get the information needed.

Depending on how to found the user – trust levels, failed checks, or just by accident – your investigation may have a different start point such as the Trust Level explainability, check explainability, or a strange looking user's activity flow widget.

Regardless of how you start – Cisco Identity is full of information that can help you conduct your investigation, without having to jump around to different product consoles to try and compare activity logs.

When investigating we recommend using the **See in Context** buttons that are available on both a given user's Trust Level widget on the Overview tab of the User 360, or in the check explainability if it is an event based check. This takes you to the user's activity log where you can easily see the user's events, across all available systems, that happened before and after Cisco Identity flagged the user.

You may also find yourself needing more information about a user, such as their location or the device they used, to better understand if certain events are actually malicious or not, or you may want to find out if any other users may be under similar attacks from the same IP. Get familiar with all the different tabs in the User 360 and the different functionality available in each tab. Because Cisco Identity is pulling user data from multiples sources, it can provide an incredibly rich and in-depth view into an affected user with only a few clicks, making it much easier to compare events and identify concerning behavior, ultimately saving your team time and effort which is often critical in these situations.

If you do confirm that a user's account has been compromised, or highly suspect that it may have been, make sure to take the necessary steps to protect the account such as logging the user out of all sessions, resetting the user's credentials and factors, or even deprovisioning the account entirely and creating a new one. You can conduct certain remediation actions from within Cisco Identity directly as well if needed.

After an investigation

Once you have successfully investigated a user end to end and remediated the account as needed, you need to remove the user from the list of failing users so that someone else does not spend time investigating the same person.

Depending on the result of your investigation and the type of check, there are a few different triage options that can be used so that the user will no longer fail the check. Review the documentation provided to understand the different triage options available and what triage action to use in each situation. We highly recommend not excluding users from checks when

possible; however if it is needed, we recommended using a temporary exclusion so that the account can be audited and re-reviewed at a later date to determine if they should still be excluded from the given check.

As with the account clean up, we also recommend using the findings of your investigations to identify wider organizational changes that can be made to improve the organization's posture and thus, reduce the risk of each threat, and time needed investigating.

For example - you may find that you have many users failing the **A Bypass Code Was Used To Successfully Sign In** check. Rather than consistently investigating these users to revoke long standing bypass codes, work with your teams to change the issuing process for bypass codes so that there is an automated expiration date or usage count instead. If there is rampant Personal VPN usage from risky VPNs, consider implementing a corporate policy that disallows usage of VPNs on corporate devices or to access corporate assets so that you can enforce this with end users. If you consistently see threats from certain IP addresses, IP ranges, or countries, work with your networking teams to ensure these IPs are blocked.

Once you feel comfortable with the volume of alerts coming in from the checks you initially chose to focus on, pick another few checks to add notification targets to so that you can start investigating users failing those checks as well!

Conclusion

We hope this article provided you with some helpful guidance on how to start using Cisco Identity and incorporate it into your team's workflows. This just begins to scratch the surface of what is possible with Cisco Identity. The more you use the tool, the more you will find.

In the future, we plan to create new Journeys, like the Getting Started Journey that brought you here, to reflect this kind of information within Cisco Identity directly!

Identity Security Reading List

CISA/NSA

Advancing Zero Trust Maturity Throughout the User Pillar

Identity and Access Management Recommended Best Practices for Administrators

Microsoft Azure Active Directory M365 Minimum Viable Secure Configuration Baseline Draft Version 0.1

Books

Access Control and Identity Management

Authentication and Access Control

Securing the Perimeter

Identity Attack Vectors

Identity Management: A Business Perspective

Other

The Beer Drinker's Guide to SAML | Duo Security

Building an Identity Security Program | Cisco Identity

Podcasts

Identity at the Center

State of Identity

The Week in Identity

IDentity Today

The Identity Jedi

Didi and Lital Show

Decipher

✍ KPIs for IAM Teams

Identity and access management (IAM) is a critical function of any security and IT organization within an enterprise. Its primary role is to ensure that the enterprise's assets are readily and easily accessible to the authorized users within or adjacent to it.

As organizations seek to build and mature their IAM program, establishing a robust and durable set of key performance indicators (KPIs) is a critical step in ensuring that the performance and efficacy of the program can be adequately and consistently measured.

Every enterprise is organized differently, but generally speaking, IAM-related KPIs can be broken into three areas: Governance/Compliance, Operational, and Security. Naturally, these functional areas are aligned to the goals of the IAM program and the enterprise at large. Security keeps it safe from identity-related threats. Operations keeps the lights on and makes sure processes are running smoothly and efficiently. Governance/Compliance makes sure that policies and technical controls are in place, monitored, enforced, measured, and reported.

KPIs for Identity and Access Management

With these three functional areas as the organizational framework, here are some baseline key performance indicators that IAM leaders should consider focusing on and measuring. With these fundamental indicators as a starting guide, enterprise IAM leaders can develop and

curate a set of measures that are tailored to their organization's unique technology environment and business objectives.

Governance/Compliance

These KPIs measure an organization's performance against their regulatory obligations, such as Sarbanes-Oxley (SOx) or PCI DSS, or against their own audit standards.

Tip:

% of test controls with no control deficiencies

Tip:

SOX testing cycles with no IAM-related significant deficiencies

Tip:

# of non-unique and/or shared IDs

Tip:

% of access granted with all necessary approvals formally documented

Tip:

% of roles or entitlements compliant with Segregation of Duties (SOD) requirements

Tip:

% Accounts disabled within SLA for terminated users" or something similar

Note:

When it comes to compliance, one thing to keep in mind is that not all frameworks are prescriptive. In many cases, the controls themselves are up to the organization to define, implement, and measure against, and many unregulated organizations elect to use SOx-like controls to hold themselves to a high standard. Whatever the case may be, auditors will hold you accountable to the controls you define.

Using SOX as an example, below is a simple controls list that you can use as a baseline for compliance and measuring KPIs. Note that 'X' usually carries a value of '24', but you can use a larger or smaller time frame based on your organization's requirements and readiness,

1. Accounts for terminated users must be disabled within X hours of the user's last day of employment
2. Accounts may not be provisioned unless documented, formal management approval has been obtained
3. Access must be periodically reviewed by authorized individuals to ensure it is still appropriate

4. Accounts must be disabled within X hours if deemed inappropriate/not needed during the Periodic Access Review
5. Applications must define entitlements that, if granted, would create Segregation of Duties concerns (aka ‘toxic combinations')
6. Access may not be granted if it creates an SOD violation, unless compensating controls are implemented

Operational

These KPIs seek to measure the performance of the operational functions within the IAM program and team. Examples include:

Tip:

% of access requests fulfilled within SLA

Tip:

% of access requests fulfilled accurately

Tip:

# of Periodic Access Reviews completed within SLA

Tip:

# of access revocations completed within SLA – as a result of the Periodic Access Review

Security

These KPIs measure the security functions within the IAM program and team. Examples include:

Tip:

% of access removed within SLA upon employee termination

Tip:

% of user accounts configured to use Multifactor Authentication (MFA)

Tip:

# of privileged accounts with unvaulted credentials

Tip:

# of privileged accounts with unknown owners

Tip:

# of applications leveraging centralized directory accounts

Tip:

# of service accounts with unknown owners

Takeaways

Embrace SLAs

SLAs or “service level agreements” are policies set by an organization as a measure of time by which an action will be performed. Setting SLAs for your IAM organization is essential to holding your team accountable and to set expectations across the enterprise with regard to the delivery of IAM tasks.

Visibility is essential

Seeing who has access to what and what they’re doing with that access is paramount to IAM success. Without persistent visibility into the identities within your organization, you are quite simply flying blind. After all, you cannot effectively manage what you cannot see.

Automation is a priority

A major challenge in IAM is the fact that for every identity, there is often some logarithmic function of downstream attributes automatically associated with it. For example, one person leaving the company may actually spawn dozens of actions for the IAM organization to remove individual accounts across a multitude of applications used by that departing employee. This is where the trouble lies. While you can never have too many qualified bodies in an IAM team, you need automation to keep up with this enterprise identity sprawl.

The reality on the ground

In a perfect world, each identity on a network would have the perfect level of birthright access from day one and seamless just-in-time, just-for-now access to the specific resources they need at any given moment. If this scenario sounds familiar to you, it is likely because it is indeed the essence of the elusive “zero trust” model that so many organizations are seeking to achieve and investing so heavily in. True “zero trust” only exists in this imaginary, perfect world, and even then, it’s easiest when you start from scratch. What a luxury that would be. Nevertheless, when it comes to compliance controls, the expectation is that of perfection when the auditors come knocking, so you need efficient, repeatable processes to thrive in IAM.

The reality on the ground inside many enterprise organizations is that identity and access management is far from perfect. You are not starting from scratch; you have thousands of users who expect the availability of resources and to be able to fulfill their roles and responsibilities. Access policies, entitlements, and group memberships can vary between systems for the same user, so both wide-angle and telephoto visibility are essential to success in IAM.

Where to start

Measuring the performance of your IAM program does not need to be painful. Start with defining your controls, attach the KPIs that align with your goals, and commit your team to some SLAs. Measure these at a regular cadence and you will be well on your way to achieving IAM success by remediating vulnerabilities caused by identity blindness and sprawl.