

CISCO



# Building an Identity Security Program



**A Blueprint for CISOs**

**Matt Caulfield**  
VP of Product, Cisco Duo

## Foreword

Welcome to Duo's "Blueprint for Building an Identity Security Program," the ultimate guide to securing your organization's identities and preventing account takeovers.

Building an identity security program can seem daunting, especially if you're unsure what "good" looks like. But fear not! This blueprint will provide practical guidance and a glimpse of what a successful program can look like.

From multi-factor authentication (MFA) to single sign-on (SSO), risk-based authentication (RBA), identity security posture management (ISPM), and identity threat detection and Response (ITDR), we've got all the buzzwords covered. But don't worry; we'll break it down in easy-to-understand terms so you don't get BDIAH (Bogged Down In Acronym Hell).

We've tried to make this guide as useful as possible while realizing every organization will have different circumstances. Therefore, it includes definitions, frameworks, and some recommendations for approaching identity security.

We understand that every organization is unique, and this handbook isn't a one-size-fits-all solution. Think of it more like a choose-your-own-adventure book, where you can skip to the most relevant sections to you and your organization.

Without further ado, let's begin this exciting journey to secure your workforce identities and keep your organization safe.

## Executive Summary

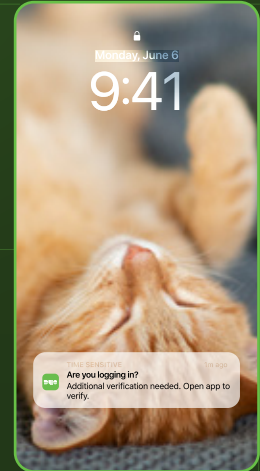
Identity security is critical in today's remote work and SaaS era, and poor identity security hygiene can leave companies vulnerable to cyberattacks. However, many organizations struggle to know what's required for an effective identity security program. This handbook provides practical guidance on aligning goals, building capabilities, and focusing on key outcomes.

In this handbook, you'll find advice on the most important areas of identity security, including user management, access management, authentication, and identity threat detection and response. The business drivers for investing in identity security include breach prevention, improving compliance, managing third-party risk, enhancing operational efficiency, and improving employee satisfaction.

# Building an Identity Security Program

## Table of contents

<b>Foreword</b>	2
<b>Executive Summary</b>	2
<b>01 Defining Identity Security</b>	4
Identity is the New Firewall	5
The Security–IAM Divide	6
Defining Identity Security	7
<b>02 Four Pillars of Identity Security</b>	8
Identify	9
Protect	16
Detect	25
Respond	31
<b>03 Stakeholders and Responsibilities</b>	34
Key Stakeholders	35
Responsibilities for Identity Security	38
<b>04 Key Business Outcomes</b>	39
<b>05 Key Performance Indicators</b>	41
<b>Conclusion</b>	44



01

# Defining Identity Security



# Identity is the New Firewall

We've heard "identity is the new firewall" a lot over the past few years. But what do we mean by that?

The traditional approach to cybersecurity has been to build a "perimeter" around an organization's network using firewalls, intrusion detection systems, and other security technologies. This approach assumes that threats can be kept out by creating a strong barrier between the internal network and the external world.

However, this approach has become increasingly ineffective as organizations have moved their data and applications to the cloud and allowed employees to access them from anywhere using various devices. The perimeter is porous in this new environment, and threats can easily slip through undetected.

● **Attackers spend less time hacking into systems and more time logging in.**

Identity is the only way that security teams can replicate the visibility they previously had through network security. Furthermore, by focusing on identity as the new firewall, organizations can shift their security posture from one that relies on keeping threats out to one that assumes that threats will get in and focuses on limiting the damage they can do.

Identity-based security means that every user, device, and application that accesses an organization's resources is authenticated and authorized based on their identity. This way, even if a threat actor gains access to a user's credentials or a device is compromised, their access can be limited based on their permissions and policies.

# The Security–IAM Divide

## Why It Prevents a Successful Identity Security Program

Identity is critical to an enterprise’s security, and the shift to remote work and cloud-based tools has only increased its importance. However, a significant gap often exists between security and IAM teams, which stymies a successful identity security program.

Attackers have targeted identities in their campaigns for many years, with many attacks targeting Active Directory (AD). While security teams have increased their visibility of AD-based attacks, there are also many other identity tools, predominantly cloud-based, implemented by IT and IAM teams.

Often, these platforms are a significant blind spot for security teams. According to the Identity Defined Security Alliance, only 53% of security professionals have ownership of workforce IAM.<sup>1</sup>

Although the worlds of identity and security are coming together, security teams continue to operate independently of IAM teams.

According to the IDSA’s “How Security Teams Are Addressing Risk” whitepaper, there are several reasons for this divide, including the lack of goal alignment between security and the organization (33%), reporting structure (30%), history of security not being involved (30%), and resistance from other teams (24%).<sup>2</sup>

To address this divide, organizations need a joint identity incident response plan, shared documented access policies, and reports proving policy enforcement. Security teams need to understand the importance of IAM and the best practices for implementing it, while IAM teams need to prioritize security and work closely with security teams to manage the overall security posture of the organization.

### Footnotes:

1. [Identity and Access Management: The Stakeholder Perspective](#), Identity Defined Security Alliance

2. [How Security Teams are Addressing Risk](#), Identity Defined Security Alliance



# Defining Identity Security

Before we move on to talk about building an effective identity security program, let's first define what we mean by "identity" and "identity security," and some other adjacent terms.

## Users

Individuals who require access to an organization's systems and networks.

## Accounts

Digital representations of users, third parties, contractors, and machine accounts that are created within an organization's identity and access management systems.

## Identities

The information that identifies an individual or entity in an organization's systems and networks. It includes attributes such as usernames, roles, passwords, access privileges, and historical context.

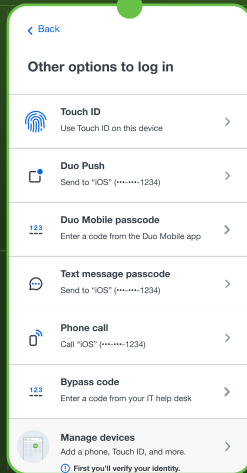
## What is Identity Security?

Identity security is a critical component of any organization's cybersecurity program, as it focuses on securing digital identities and associated access privileges.

Unlike traditional security areas like network, endpoint, and email security which primarily protect the infrastructure and data, identity security is about securing the identities that grant access to that infrastructure and data.

### Identity Security

**The protection of human and machine identities to ensure that users are who they say they are and that they are doing what they are authorized to do. This includes ensuring that only authorized users have access to sensitive information, and that data is not compromised by malicious actors.**



02

# Four Pillars of Identity Security



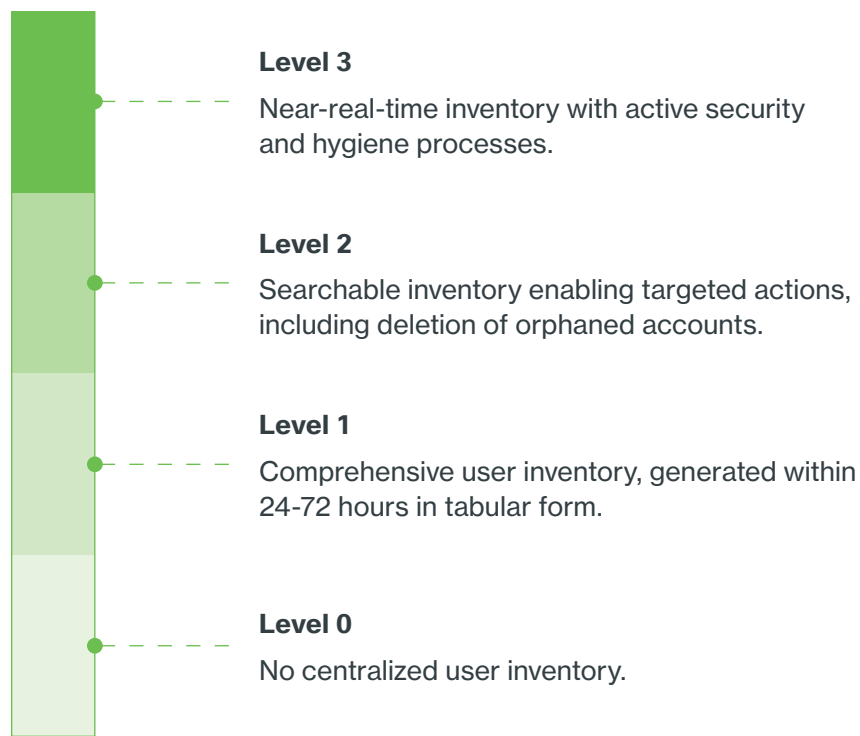
# Identify

You cannot protect what you do not know about. Identifying what to protect is the first step in an organization's identity security program.

## Building a User and Device Inventory

A critical part of implementing a zero trust security model is to know who the users are and what resources they need access to. To achieve this, building an accurate user inventory is necessary. The Center for Internet Security (CIS) also recommends maintaining an accurate inventory of authorized and unauthorized devices and users to ensure that only authorized users have access to the system.<sup>3</sup> Without an accurate user inventory, it becomes difficult to identify and mitigate security risks.

In most cases, this will first take the form of a table, with teams generally able to generate a comprehensive list of identities within 1-2 days. As this matures, teams create a searchable inventory that enables them to take targeted action, such as deleting orphaned and inactive accounts. The ultimate goal is to have an inventory updated continuously and in near-real time. This would enable teams to continually monitor for both security and hygiene issues.



#### Footnotes:

3. [CIS Critical Security Controls Version 8](#), Center for Internet Security

## Challenges of a Complete User and Device Inventory

Organizations face challenges in merging user data across platforms, impacting the unified view of identities.

- Identity providers store data in different formats with varied attributes and schemas, making it hard to map and reconcile data between systems, especially HR directories and identity providers.
- Data quality varies, with HR directories often having more accurate and up-to-date data compared to cloud-based identity providers. This creates inconsistencies when forming a unified view of user identities.
- Individuals have multiple accounts (Gmail, Yahoo, etc.) with access to company data, averaging 340.5 personal accounts per company.<sup>4</sup> These accounts should be linked to a corporate account.

### Users Inventory KPIs



# orphaned accounts

# discrepancies with HRIS

# of non-unique and/or shared IDs

# of administrator accounts

## Guest Access

Guest accounts in Entra ID are identities that belong to external users who are invited to collaborate with the organization. Inviting guest accounts into your organization can be as simple as sending a link to a document or messaging an external email address on Teams.

While guest accounts are essential for collaboration and access management in Office 365, they are also a central risk for data loss and data leaks. For example, employees suspecting of being terminated may share information with private Gmail or Microsoft cloud accounts as retaliatory action.

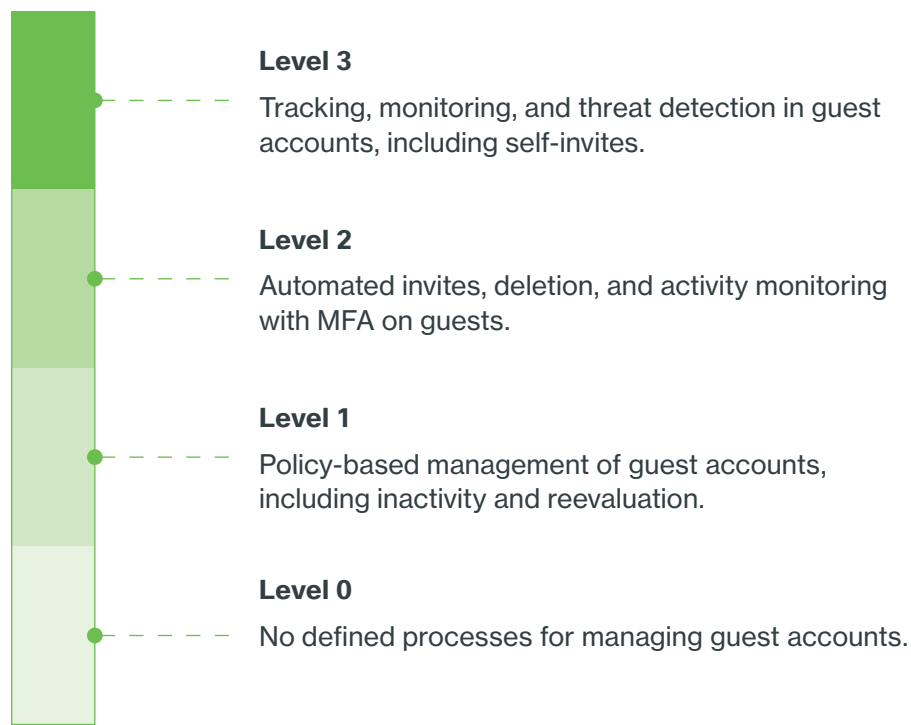
#### Footnotes:

4. [State of Identity Security research reveals 40% of accounts use weak or no form of multi-factor authentication to protect identities](#), Oort

At the bare minimum, organizations should have a policy for managing guest accounts, regularly reviewing guest accounts, and removing inactive or unnecessary guest accounts.

This process can then be automated, and additional controls such as MFA can be placed on the guest accounts.

Ultimately, organizations should aim to be in a place where they can fully track and monitor guest accounts and detect any suspicious activity. This could include soon-to-be-terminated employees inviting personal accounts.



## Checklist for Managing Guest Accounts

### Put a Policy in Place

Like everything else, start with the right level of policy that might be governed by the regulation of your industry. Here are some important considerations for your policy:

- **Excessively restrictive policies can backfire.** Before you put in place a highly restrictive policy, be aware that people will find other ways to share content. These creative methods might not be as easy to regulate as guest accounts.
- **Invite process.** Start with putting a process in place for how an invite process works, who can be invited, for how long, and to what types of content.
- **Track invites.** Set an expiration time for invites and link them to your current access review process.

- **Manage attribution.** Keep a clear link to who invited the user and set the policy to include personal invites and what happens when the inviting person leaves.
- **Get a bi-directional view.** Make sure you have a bi-directional view of a) who a user invited and b) who owns the invite. This ensures a person inside the organization is responsible for those actions.

### Review and Delete

- **Regular deletion.** Organizations should regularly delete guest accounts to reduce data loss and leaks.
- **Invites.** Delete unaccepted invites or those in a limbo state after one week.

### Multi-Factor Authentication

- **Set up multi-factor authentication.** Setting up multi-factor authentication for guest accounts can help to ensure the right person is accessing the right information and reduce the risk of identity theft.
- **Guest account MFA should be linked to the data accessed.** You don't want external users accessing internally regulated and governed data via MFA.

### Limit Guest Permissions

- **Be intentional.** Organizations should limit the permissions of guest users to reduce the risk of unauthorized access to company data.
- **Application policies.** Non-privileged users should not be allowed to register third-party applications.
- **Utilize existing safeguards.** The "Restrict user ability to access groups features in the Access Panel" setting should be enabled to limit user access to AAD group features.



## Guest Access KPIs

# of inactive guest accounts

# of orphaned guest accounts

# guest accounts with excessive access



## Machine Identities

In addition to human users, machines have roles and functions that necessitate tracking their identity. Proper user management can help organizations identify and manage machine identities and their associated access privileges.

Non-human identities include any account that is one step removed from a human. This can include shared mailboxes, service accounts, and network devices.

**43%**

Machine identities make up 43% of all identities within the average enterprise.<sup>5</sup>

The most well-known type of machine identity is service accounts, which are usually created to cater to specific applications or services and may exist across various systems, making it arduous to keep track of and manage them.

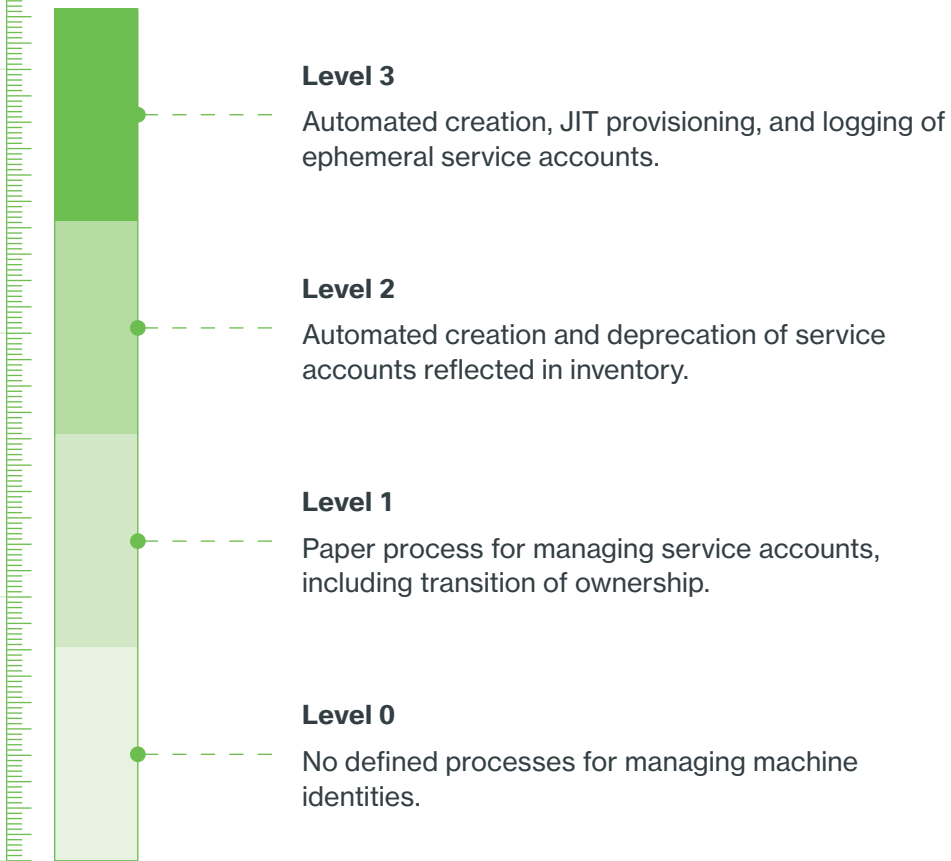
Furthermore, service accounts can possess elevated privileges and access to sensitive resources, making them alluring targets for potential attackers. Service accounts might also be shared among multiple users or applications, creating intricate scenarios and security risks.

The most important starting point is to have a defined process in place. This process should ensure that all service accounts are linked to a human so there is one “throat to choke.” Ideally, accounts should be tied to more than one human in case someone leaves, and teams should practice a standard process to transition ownership.

**Footnotes:**

5. [Machines make up 43% of digital identities on enterprise networks](#), Security Magazine

As this process matures, teams can look to automate the creation and deprecation of service accounts and ensure they are reflected in the user inventory. Ultimately, organizations can consider the use of Just-In-Time (JIT) provisioning and the existence of ephemeral service accounts that can be used for one-off tasks.



## Machine Identity KPIs



# of service accounts with unknown owners

# of service accounts with default passwords

# of service accounts with expired keys



## Mapping Identities to Devices

By mapping which devices users are logging in from, security teams can identify whether access is coming from an unmanaged or known device. This can help teams prevent unauthorized access to sensitive data and assets. A device trust policy is particularly important in the age of remote work, where employees may be using personal devices to access company resources. By enforcing a zero trust security policy, security teams can ensure that every access request is authenticated and authorized before granting access based on identity verification.

Furthermore, mapping devices can help organizations create a secure BYOD policy. By specifying security requirements for devices before granting access to sensitive data and assets, security teams can ensure that only trusted devices are permitted access. Additionally, the identity fabric can track the device's compliance with these security requirements and revoke access if the device falls out of compliance.

## Hygiene Considerations

Staying on top of identity discrepancies and hygiene is important to maintain an effective user inventory. They involve maintaining accurate and up-to-date information about users and their access rights to various systems and applications.

The failure to manage identity discrepancies and hygiene can lead to security breaches, unauthorized access, and other security risks.

Improving IAM hygiene is also important for IGA and PAM projects. If the IAM foundation is flawed, the success of these projects will be compromised. For example, if there are many dormant and orphaned accounts in the IAM system, IGA and PAM projects will struggle to provide accurate and comprehensive visibility and control over user access.

**Without good IAM hygiene, IGA and PAM projects will struggle to provide accurate and comprehensive visibility and control over user access.**





02

# Protect

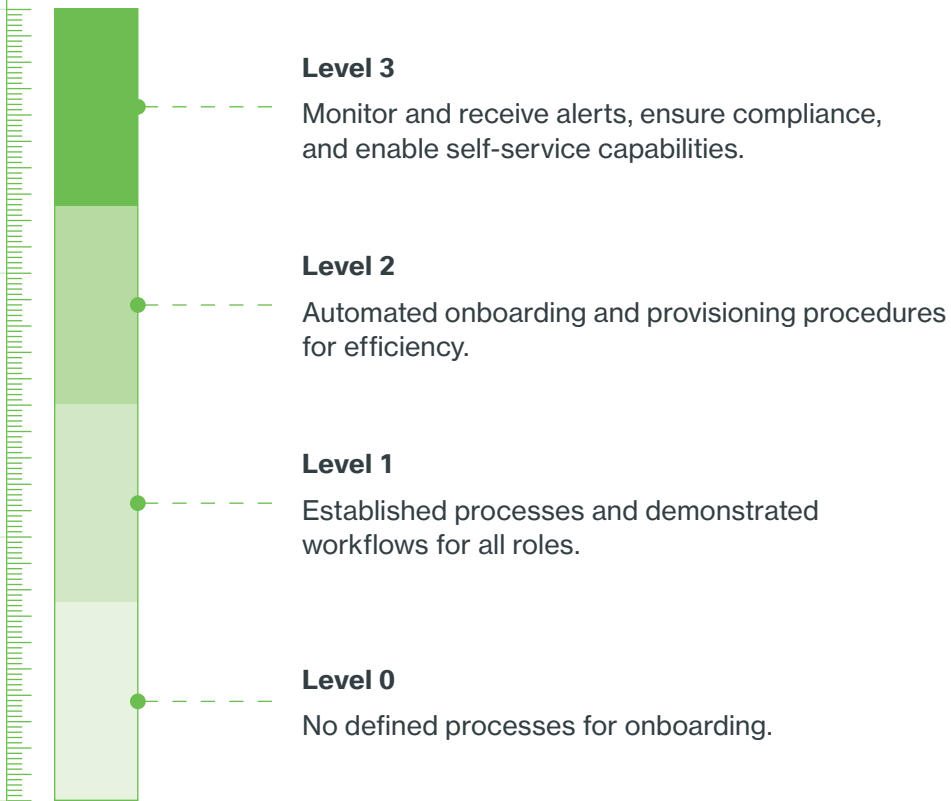
After identification, the next step is to focus on protecting those identities. There are critical parts of the joiner, mover, and leaver process that must be considered as part of any identity security strategy.

## Onboarding & Transfers

Onboarding and transfers refer to the process of granting new employees access to the necessary resources and systems they need to do their jobs and ensuring that their entitlements are appropriate for their roles. The onboarding process can also be one of the biggest opportunities for attackers. The process is vulnerable to attacks such as phishing, social engineering, and brute force attacks. If an attacker can gain access to the account at this stage, it's possible to register their own forms of MFA.

That's why it's imperative to secure the enrollment workflow not only for onboarding into IT systems like directories but also into security controls like MFA. Identity verification (or validating a user is who they say they are for the first time) is a key component of this process. However, there are other tactics to put in place as well – actions like limiting bypass code use as a part of onboarding, monitoring partial enrollments, and evaluating for suspicious activity during the enrollment process can all help increase the security of onboarding.

Access management helps organizations streamline this process and ensure that new employees are granted the necessary access promptly and efficiently. By automating the onboarding process, organizations can ensure that new employees are productive from day one and reduce the risk of unauthorized access or data breaches.



### Entitlements

Entitlements refer to the specific permissions and privileges granted to users to access certain resources, systems, and data. Access management helps organizations ensure that each user is only granted the necessary entitlements to perform their job functions and no more.

Entitlements apply to users or groups of users within an organization’s cloud infrastructure. Access to applications and entitlements should come through group membership and not through direct assignment. As you mature, these group memberships can be automated based on HR role needs. Once the proper entitlements are established, access policy should be reflective of group entitlement.



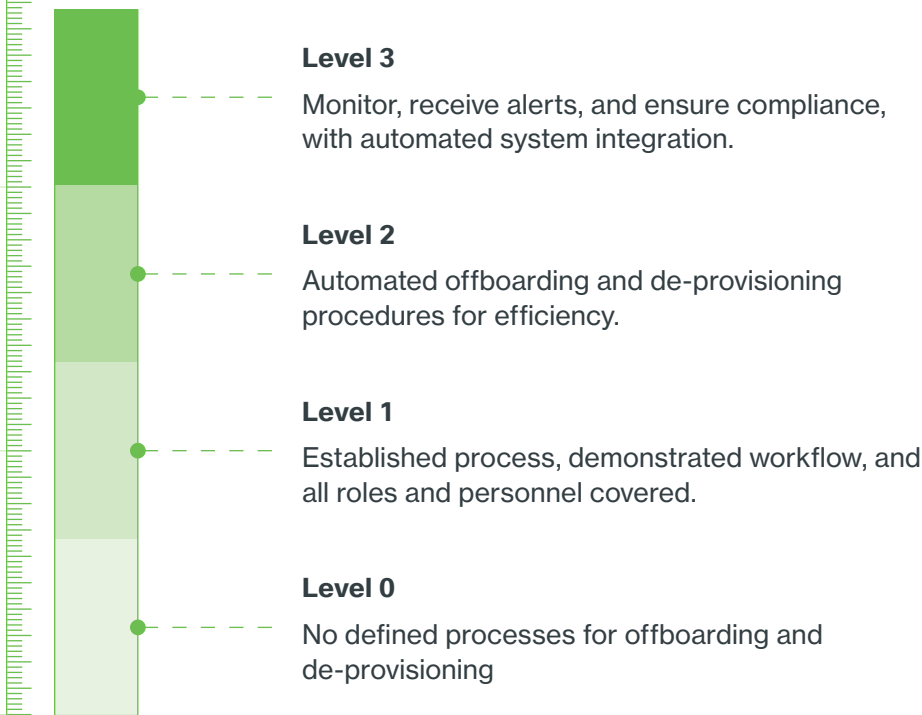
### Onboarding KPIs

# speed to onboard with new employee

# users with excessive access rights

## Off-boarding and De-provisioning

Off-boarding and de-provisioning refer to the process of removing access to resources, systems, and data when employees leave the organization or change roles. Access management helps organizations automate this process and ensure that access is revoked promptly and completely. This reduces the risk of former employees accessing sensitive data or systems after they have left the organization. By automating the off-boarding process, organizations can ensure that access is revoked promptly and reduce the risk of data breaches.



### Offboarding KPI



% accounts disabled within SLA for terminated users

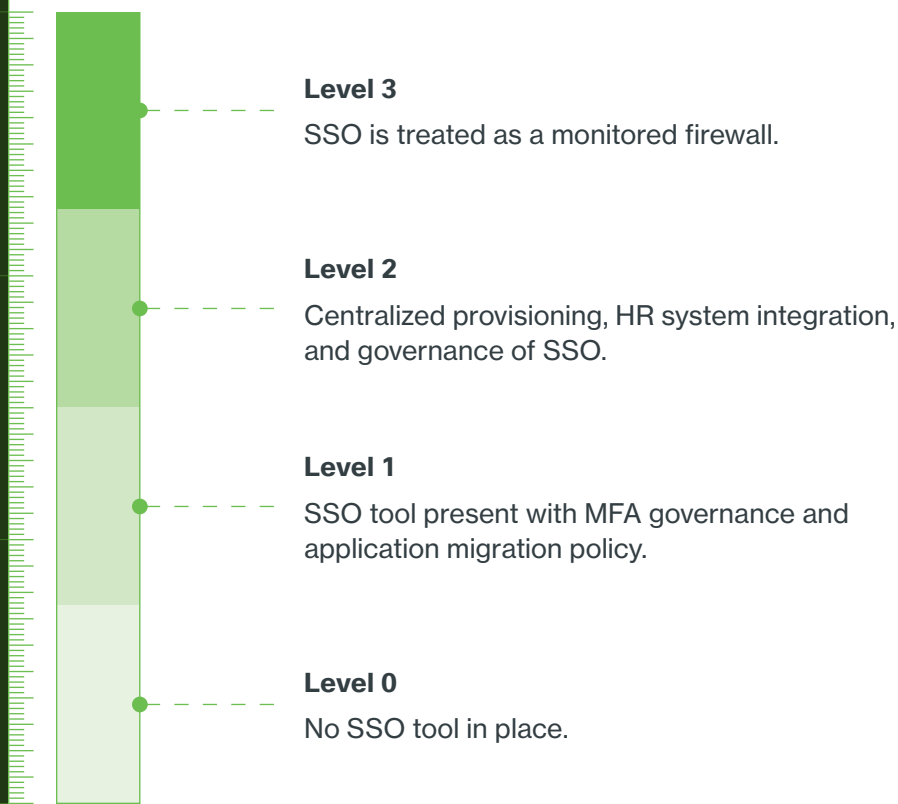
## Single Sign-On

Credential hygiene is the practice of maintaining good password management habits to protect sensitive information from cyber threats. Single sign-on (SSO) helps to solve this headache by allowing users to authenticate once and gain access to multiple systems or applications without having to provide their credentials multiple times. SSO reduces the need for users to remember multiple usernames and passwords, and it can increase productivity by reducing the time and effort required to access different systems. This can help to prevent credential stuffing and other types of password-based attacks.

SSO tools can also be used to ease the burden of onboarding and de-provisioning, which should automatically flow from an HR directory and govern everything centrally.

At the same time, as SSO becomes increasingly important, it can become a single failure point if it is not monitored properly. The most mature deployments of SSO will treat it like it is a firewall: understanding and tracking event data.

Moreover, many application providers charge extra for enabling SSO functionality; we consider this type of “SSO tax” behavior disheartening, and worthy of a stern customer support email or three.



## Session Length Requirements

More advanced SSO deployments should focus on refining session length requirements. These are rules that determine how long a user can remain authenticated before they are automatically logged out. These requirements can help to reduce the risk of unauthorized access to sensitive data or resources if a user walks away from their computer, if their device is stolen or lost, or if their session is hijacked.

Session length requirements are an essential security control in situations where multiple people use a shared computer or device, such as a kiosk or a public computer. By automatically logging out users after a period of inactivity, session length requirements can help prevent unauthorized access to sensitive data or resources.

A note should be made here though that evaluating identity data (i.e. building out the Identify step from the prior section) should also enable organizations to extend session length in trusted scenarios. If a user is accessing from the same trusted device from the same location they always do, it's possible to reduce their friction and expedite their access. Security can be an enabler – who would've thought?

**The session hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.<sup>6</sup>**

### Footnotes:

6. [Session hijacking attack](#), OWASP



## SSO KPIs

# of business apps using SSO

% password complexity rate

% of accounts with passwords updated in the last 30 days

# apps with direct access allowed



## Multi-Factor Authentication

Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more types of authentication factors to prove their identity. These factors can include something the user knows (e.g., a password), something the user has (e.g., a token), or something the user is (e.g., a fingerprint).

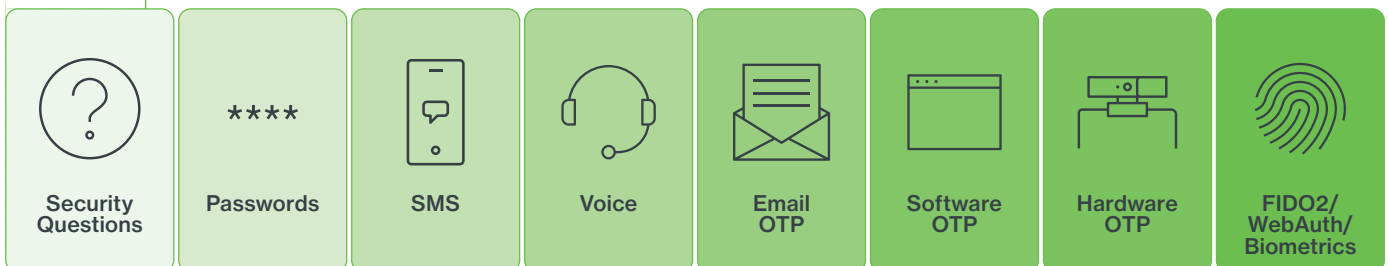
MFA provides an additional layer of security beyond a username and password. Even if an attacker manages to obtain a user's password, they still need access to the user's other authentication factors to gain access to sensitive data or resources.

**40.20%**

Of accounts have no strong forms of MFA. Oort State of Identity Security within the average enterprise.<sup>7</sup>

While many frameworks require two or more authentication factors of different types, not all factors are made equal. Unfortunately, many existing second factors like SMS and email OTP are susceptible to phishing or otherwise being bypassed. More than 40% of accounts have no strong forms of MFA enabled.

### MFA Factor Strength




At the most basic level, organizations should have 100% of their users with cryptographically secure MFA. If there are exceptions, these should be clearly stated in the policy, and a path for comprehensive coverage outlined.

#### Footnotes:

7. [State of Identity Security](#), Oort

More mature organizations have a plan for getting phishing-resistant MFA and will monitor MFA activity. They will have at least one rule to detect MFA threats, such as MFA flooding. Ultimately, the most mature organizations have adopted passwordless MFA, and the recovery process is defined and tracked.





## MFA KPIs

- % of user accounts configured to use multifactor authentication
- % of user accounts using strong forms of MFA



## Access Policy

Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more types of authentication factors to prove their identity. These factors can include something the user knows (e.g., a password), something the user has (e.g., a token), or something the user is (e.g., a fingerprint).

MFA provides an additional layer of security beyond a username and password. Even if an attacker manages to obtain a user's password, they still need access to the user's other authentication factors to gain access to sensitive data or resources.

### Location or IP Policy

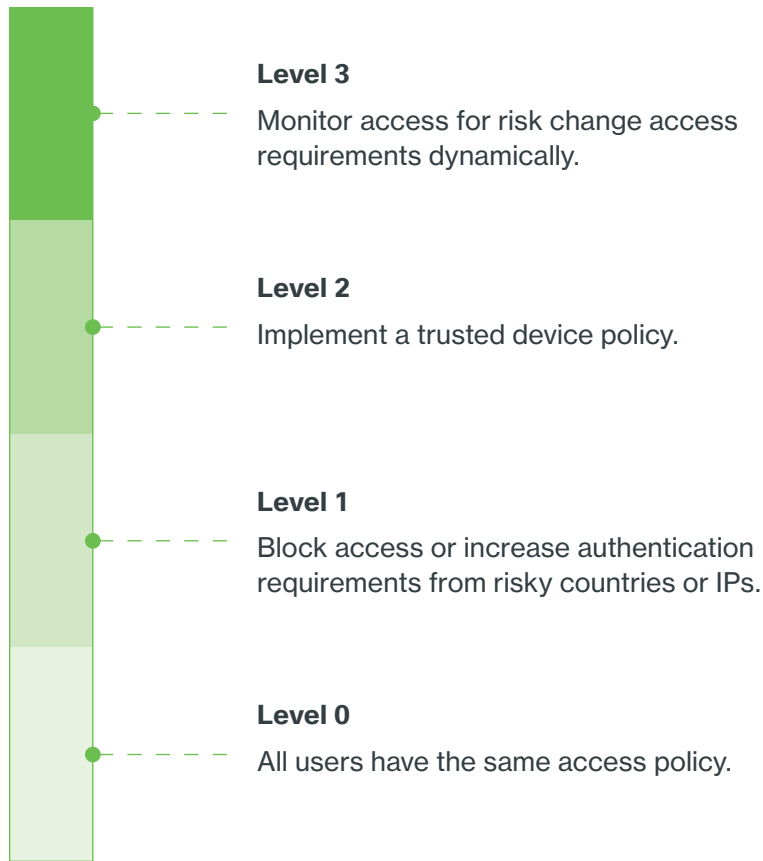
Restricting access to locations or IP ranges where the organization does business can be another useful way to prevent unwanted access. If the business only has employees in the United States and Canada, then access to corporate resources should be limited to those two countries. If an attacker impersonates an employee and attempts to access the company network from outside the trusted geographic region, they will be blocked.

A second component of this type of policy is keeping a list of "known bad" IPs (i.e. IP addresses associated with bad actors and attack techniques) and then implementing a block on this list. This does create a relatively proactive chore of keeping the known bad IP list up to date, but keeping abreast of the recent hacks and exploits is time well spent anyway.

### Device Trust Policy

Requiring that all access to corporate resources come from a trusted device is a strong deterrent against compromised credentials. If an attacker manages to steal a username, password, and even their MFA code, they will be blocked if they aren't attempting access from the correct or recognized device. This type of policy may seem hard to put in place without managing all the devices in an environment – and for the extremely security-conscious, only allowing managed devices might be the right path to take. However, many identity providers now offer a slightly lighter variant of device management where end users can "register" their device in the user directory. When they do this, the directory can link their identity to a trusted device. From here, a policy can be set to enforce that only previously registered devices can be used to log in.

A device trust policy can be expanded to include an assessment of the device at authentication as well. Many tools can check if a device is running up-to-date software or if the right security software is running. By including posture assessment alongside the trusted device check, defenders can narrow the window for attackers even further.



## Access Policy KPIs



% access coming from trusted or known locations or IPs

% access evaluated for risk at authentication time

% access coming from trusted devices



03

# Detect

## Log Ingestion

Before detecting identity-based threats, you need to collect, store, and retain the appropriate logs from the appropriate sources. Using these logs will help with threat detection and compliance.

For example, the Sarbanes-Oxley Act (SOX) requires the collection of unsuccessful logins.<sup>3</sup> The relevant sections of CIS and NIST controls are also listed below.

### Collecting Logs

#### CIS CSC 8.12

Collect Service Provider Logs

#### NIST CSF DE.AE-3

Event data are collected and correlated from multiple sources and sensors

#### CIS CSC 8.2

Collect Audit Logs

#### NIST CSF DE.DP-4

Event detection information is communicated

**Footnotes:**

8. [H.R.3763 - Sarbanes-Oxley Act of 2002, Congress.gov](#)

## On-Prem vs Cloud-Based Collection

On-premises Active Directory (AD) is a common data source for IAM programs, and it contains critical user identity and access data. Monitoring AD logs can provide insight into user activity, such as login attempts and changes to user privileges.

Cloud-based IAM solutions, such as Entra ID, Okta, Duo, and AWS, also provide critical user identity and access data. Monitoring logs and events from these sources can help identify potential threats and ensure compliance with security policies.

In today's digital landscape, many organizations rely on non-traditional identity providers such as Google, Slack, Salesforce, and GitHub to manage user identities and access to critical resources. As such, effective identity threat detection must include these non-traditional identity providers. Attackers often use compromised non-traditional identities to gain unauthorized access to critical resources, making it crucial to monitor and respond to incidents related to these identities.

**25%**

Only 25% of organizations that forward identity logs to their SIEM actually use them.

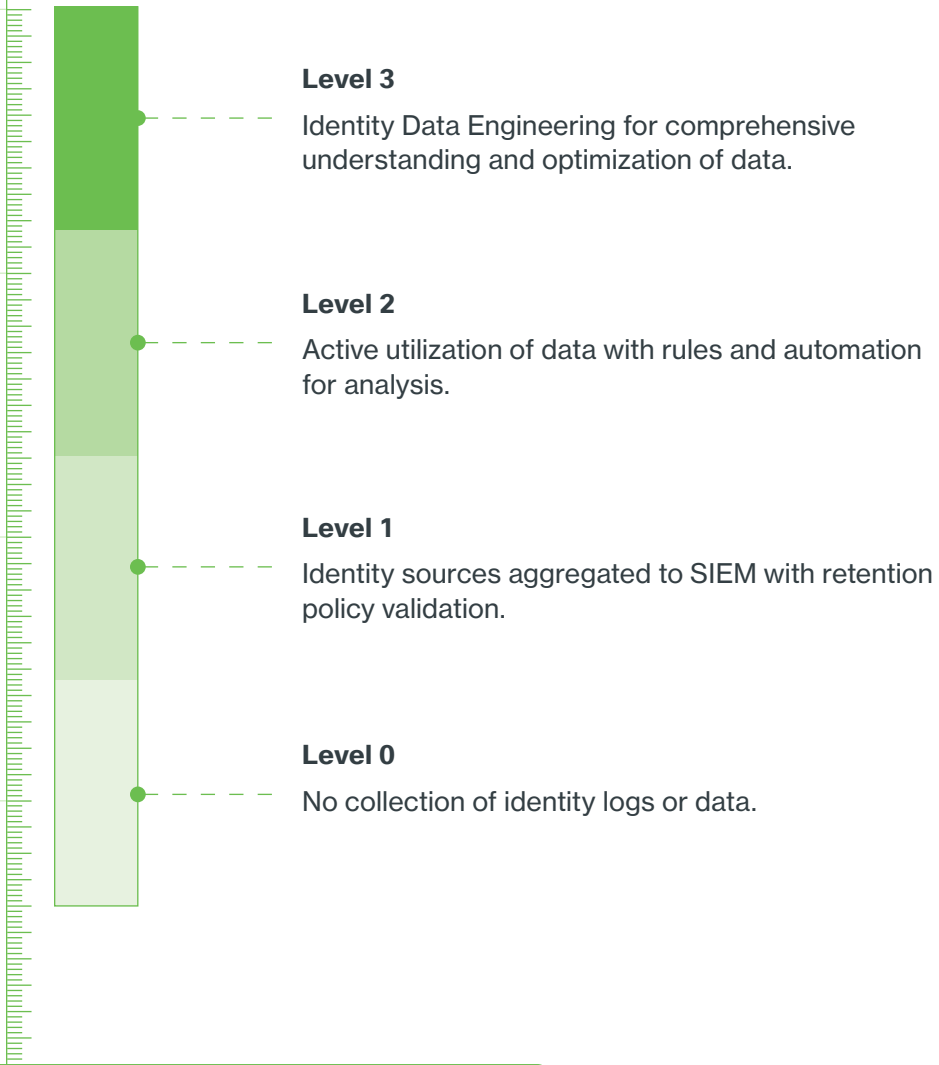
By incorporating non-traditional identity providers into ITDR strategies, organizations can proactively identify and respond to identity-related incidents, regardless of the provider used. This comprehensive approach to ITDR enhances an organization's ability to detect and respond to identity-related incidents, reducing the risk of data breaches and other security incidents.


Finally, simply because logs are collected from identity providers does not mean teams always have the bandwidth to actually do something with them. In fact, only 25% of organizations that forward identity logs actually use them.<sup>9</sup>

### Footnotes:

9. [How Detection Posture Management Can Help CISOs Track the Right Metrics](#), CardinalOps







## Collection KPIs

- # unsuccessful logins
- Alert response time

## Detection Methods

An effective identity threat detection capability will require you to use different methods. The most straightforward are IOC-based detections. However, increasingly we are seeing security teams aligning with the MITRE ATT&CK framework to focus on techniques. As an example, the [Duo Trust Monitor](#) feature applies all the following forms of detection, but specifically on Duo logs and activity – whereas other ITDR functionality may specialize in a particular type of detection.

### Approaches to Detection

#### IOC-Driven Detection

Indicators of compromise (IOCs) are specific artifacts that indicate malicious activity, such as a known malicious IP address or a signature of malware. IOC-driven detection involves monitoring network traffic and system logs for IOCs to identify potential threats. This approach is reactive and relies on the detection of known threats.

**PRO:** Easy to create detections and respond to.

**CON:** IOCs are quickly out-of-date and reactive blocking can have limited benefit.

#### Activity-Driven Detection

Activity-driven detection involves monitoring user behavior for anomalous activity. This approach uses machine learning algorithms and artificial intelligence to establish a baseline of normal behavior for each user and alert them to any deviations from that baseline. This can (and should) include suspicious administrator activity.

**PRO:** Can monitor behavior and not just IOCs.

**CON:** Traditional UEBA solutions often have too much noise associated.

#### TTP-Driven Detection

Tactics, techniques, and procedures (TTPs) refer to the methods used by attackers to achieve their objectives. TTP-driven detection involves identifying TTPs used by attackers and monitoring for any similar activity on the network or endpoint. This approach focuses on identifying the attacker's behavior rather than specific IOCs.

**PRO:** Aligns with what attackers actually do. Unlike IOCs, attackers often keep similar techniques.

**CON:** There are many techniques to map to, with more added all the time.

## Mitre ATT&CK

### Relevant techniques, sub-techniques, and data sources

#### Techniques

Brute Force (T1110)

Remote Access Software (T1219)

Discovery (T1087)

Steal Web Session Cookie (T1539)

Valid Accounts (T1078)

Account Manipulation (T1098)

Account Manipulation: Additional Cloud Roles (T1098.003)

Compromise Accounts: Email Accounts (T1586.002)

Multi-Factor Authentication Request Generation (T1621)

#### Sub-Techniques

Valid Accounts: Default Accounts (T1078.001)

Valid Accounts: Cloud Accounts (T1078.004)

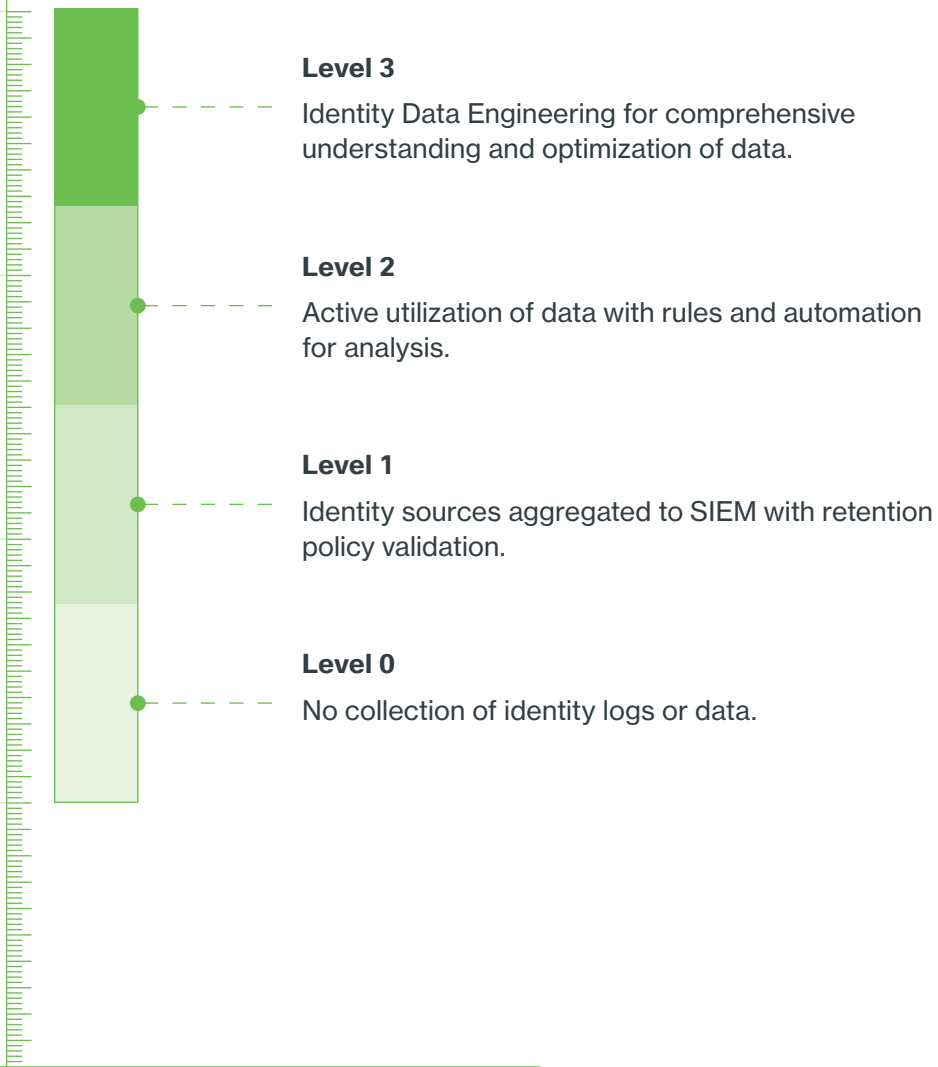
Brute Force: Password Spraying (T1110.003)


Brute Force: Credential Stuffing (T1110.004)

#### Data Sources

Active Directory (Includes AD Credential Request, Object Access, Object Creation, Object Deletion, and Object Modification)

Logon Session (User Account)





### Detection KPIs

- # suspicious IP addresses blocked
- # impossible travel events
- # new country for tenant events
- # time to detect compromised user



04

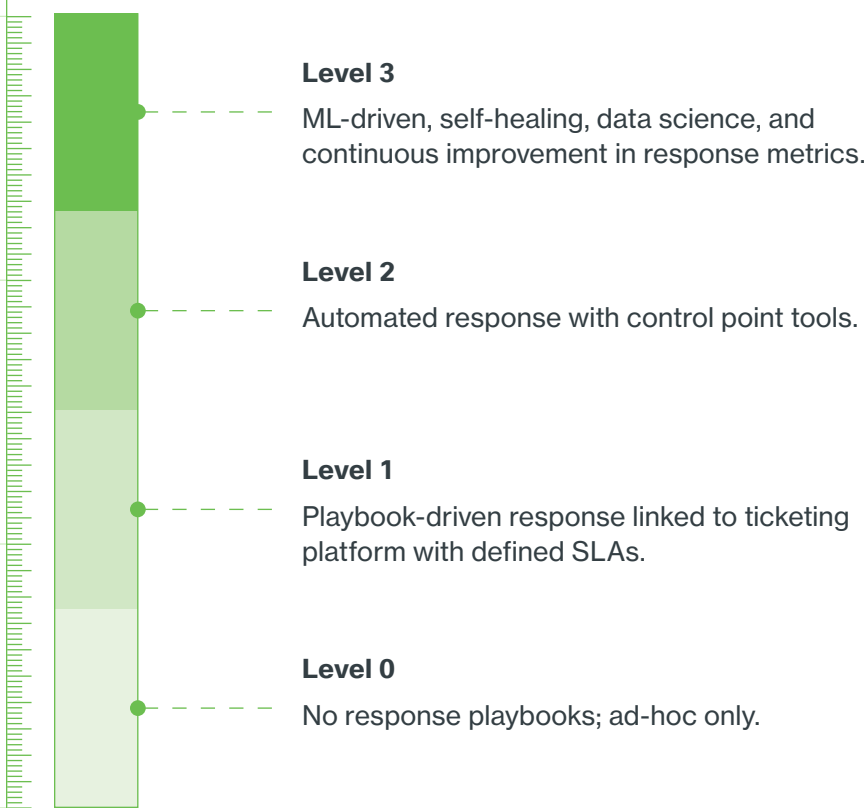
## Respond

Detecting identity threats is great, but it needs to inform an action or response. There are two approaches to response. The first is an automated technical response generated via integration across tools. Automated responses are great when there are simple mappings between detection and the proper response action. To illustrate, an identity-based detection tool might fire an alert. The context of this alert can be forwarded to a variety of different tools to inform a response. From there, a control point like authentication or access could react to the new context from the alert, changing authentication requirements moving forward, or in dire circumstances – revoking access. There are many potential automation points for using analytical outputs as inputs to access management control.

However, in many use cases, automated response is too thorny. Many detection scenarios are “gray,” or, don’t fit a one-size-fits-all response. It may not be the correct response to automatically block a user in certain cases – but it may well be the case that suspicious activity warrants a more thorough investigation.

Therefore, organizations should define and document clear processes for playbooks to respond to these threats, ideally tied to a ticketing platform with defined SLAs. Response playbooks provide clear, actionable guidance for security teams to follow when responding to identity-related incidents, ensuring a consistent and effective response.

Response playbooks help ensure that security teams can quickly and accurately identify the nature and scope of an incident, prioritize the response, and implement the necessary actions to contain and remediate the incident.



### Creating an Incident Response Plan for Identity

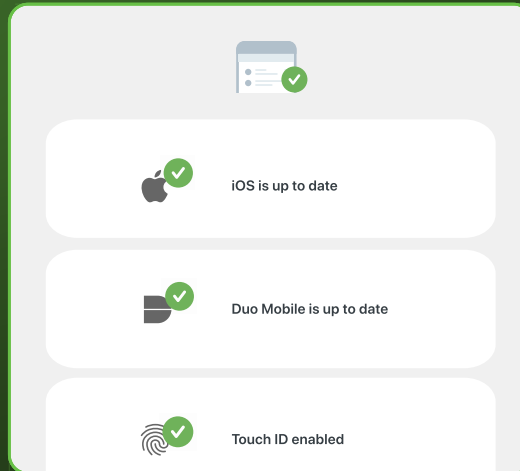
An incident response plan outlines the steps to take in case of a security incident. It should include procedures for identifying and containing the incident, assessing the impact, and recovering from the incident.

Any playbook should be regularly reviewed and updated to ensure it is effective and comprehensive. Here are some key considerations for your identity incident response plan.

- **Establish business decision makers.** Identify key stakeholders within your organization who will be responsible for making critical decisions during an identity incident. This may include executives, IT leaders, legal representatives, and communication teams. Ensure clear lines of communication and designate decision-making authority to facilitate a swift and coordinated response.
- **Escalation actions.** Develop a detailed plan for the immediate actions to be taken in response to an identity incident. This should include procedures for quarantining affected accounts, resetting compromised credentials, and terminating unauthorized sessions. Clearly define the roles and responsibilities of IT teams involved in executing these actions and provide them with the necessary tools and resources.

- **Document policies and exclusions.** Maintain comprehensive documentation of access policies, MFA guidelines, and enforcement mechanisms within your organization. Ensure that these policies are well-communicated, regularly reviewed, and actively monitored for compliance. Additionally, establish clear guidelines for exceptions to the policies and document the process for granting and tracking such exceptions.
- **External communications.** Develop a communication plan to address external stakeholders, such as customers, partners, and regulatory bodies, in the event of an identity incident. Clearly define the information that can be shared, considering what is known, what is not known, and the potential impact on affected parties. Designate spokesperson(s) who will provide timely and accurate updates throughout the incident response process.
- **Data sharing.** Establish protocols for sharing relevant data related to the incident, such as indicators of compromise (IOCs) and MITRE ATT&CK techniques used by the attacker. Collaborate with industry peers, cybersecurity organizations, and law enforcement agencies to share information.
- **Legal/regulatory requirements.** Familiarize yourself with legal and regulatory obligations related to identity incidents, such as data breach notification laws or industry-specific compliance requirements. Ensure that your incident response plan aligns with these obligations and notification requirements within the specified timeframes.
- **Resiliency plan.** Develop a robust resiliency plan that includes regular backups of critical systems and data. Ensure that backup processes are tested and validated regularly to guarantee their effectiveness. Conduct periodic drills and exercises to validate the resiliency plan and identify areas for improvement.





03

# Stakeholders and Responsibilities



## Key Stakeholders

An identity security program involves various stakeholders with distinct roles and responsibilities to ensure the program's successful implementation. Each organization will have its own roles and responsibilities, so treat this as a guide.

### End-users

Individuals who use the organization's information systems, such as employees and partners. The end users must be the focus of any identity security program.

**Desired Outcomes:** Safe and secure access to information, protection of personal data, and prevention of unauthorized access to confidential information.

**Responsibilities:** Best practices for password management, reporting any suspicious activity, and complying with the organization's security policies.

### CISO (Chief Information Security Officer)

The CISO is responsible for overseeing the organization's security program and ensuring that it aligns with business objectives. Most commonly the driving force behind identity security.

**Desired Outcomes:** Minimizing the organization's risk exposure, enhancing the organization's security posture, and maintaining compliance with regulatory requirements.

**Responsibilities:** Setting security strategy, communicating security risks to executive leadership, and providing guidance to security teams.

### Security team

The security team is responsible for monitoring the organization's security posture, including threat detection, infrastructure management, and vulnerability management.

**Desired Outcomes:** Identifying and mitigating risks, preventing data breaches, and minimizing the impact of security incidents.

**Responsibilities:** Performing regular security assessments, implementing incident response plans, and monitoring security logs.

### IAM (Identity and Access Management) team

Responsible for enabling secure business operations by giving the right tools to the right people, on time.

**Desired Outcomes:** Ensuring that users have the appropriate level of access to systems and data, minimizing the risk of unauthorized access, and maintaining compliance with regulatory requirements.

**Responsibilities:** Defining access policies, managing user accounts and devices, and monitoring user activity.

### Cyber Threat Intelligence team

Responsible for tracking and analyzing threats to the organization and understanding the potential impact to the business.

**Desired Outcomes:** Protecting against common attacker techniques.

**Responsibilities:** Providing assessments on new identity-based techniques, IOCs from recent campaigns, and detection of breached credentials.

### CIO (Chief Information Officer)

Responsible for managing the organization's information technology infrastructure and ensuring that it supports the organization's business goals.

**Desired Outcomes:** Aligning IT with the organization's strategic objectives, improving IT efficiency, and managing IT costs.

**Responsibilities:** Overseeing the identity security program's implementation, ensuring that it meets the organization's security and regulatory requirements, and providing resources to support the program.

## IT Help Desk

Responsible for providing technical support to end-users.

**Desired Outcomes:** Resolving issues related to identity and access, such as password resets and account lockouts, in a timely and secure manner.

**Responsibilities:** Verifying users' identities before granting access, following established security procedures, and escalating security incidents to the appropriate teams.

## Compliance Team

Responsible for ensuring that the organization complies with applicable regulatory requirements and industry standards.

**Desired Outcomes:** Maintaining compliance with regulatory requirements, avoiding penalties, and enhancing the organization's reputation.

**Responsibilities:** Assessing compliance requirements, implementing controls to meet those requirements, and reporting on compliance status.

## Responsibilities for Identity Security

While every organization looks different, we've created a RASCI (Responsible, Accountable, Supporting, Consulted, Informed) matrix of a "typical" identity security program. This includes the IAM Team reporting to the CIO, and the security team reporting to the CISO.

	CISO	CIO	Security Team	IAM/IT Team	Threat Intel	IT Help Desk	Compliance Team
<b>Identify</b>							
Building a User Inventory	A	S	C	R			
Managing Guest Access	S	A	S	R			I
Managing Machine Identities	I	A	C	R			
<b>Protect</b>							
Onboarding	I	A	C	R		S	I
De-provisioning	I	A	C	R		S	I
Single-Sign On	I	A	C	R	S	S	I
Multi-Factor Authentication	C	A	C	R	S	S	I
User Access	I	A	C	R			I
<b>Detect</b>							
Collection	A	I	R	S	S		
Detection	A	I	R	S	S		
<b>Respond</b>							
Response	A	I	R	S	S	S	

R	A	S	C	I
Responsible	Accountable	Supporting	Consulted	Informed

### Create a New Policy

Enforce 2FA

---

---

---

Create Policy



04

# Key Business Outcomes





## Key Business Outcomes

A strong identity security program can deliver several significant business outcomes that go beyond merely reducing security risks. We encourage you to define your own business outcomes that are mapped to known business drivers.

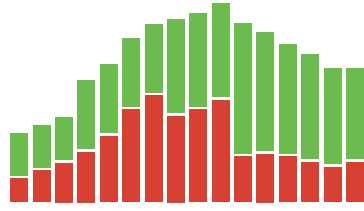
Here are five key business outcomes that can result from implementing a strong identity security program:

- 1. Breach prevention:** By improving network security and account hygiene, identity security programs can help prevent breaches before they occur. They can also help organizations respond quickly to compromised accounts, reducing the impact of any potential breaches. This is also tied to brand and reputational protection.
- 2. Compliance:** Compliance with various regulatory standards and frameworks such as SOX, NIST, SOC 2, PCI DSS, HIPAA, and GDPR is a huge burden for many organizations. Identity security programs can help ensure compliance by providing better visibility into access controls and improving security hygiene.
- 3. Third-party risk:** Many organizations struggle to manage third-party access to their systems and data. A strong identity security program can help manage guest accounts and monitor third-party activities, reducing the risk of data breaches caused by third-party access.
- 4. Operational efficiency:** A well-designed identity security program can improve operational efficiency by reducing the time and effort required for password resets and reporting. It can also help remove unnecessary access, reducing licensing costs and streamlining access management processes.
- 5. Employee satisfaction:** Employees can benefit from a strong identity security program that provides quick and easy access to resources, passwordless authentication, and fast password resets. Such programs can make employees happier and more productive, improving retention rates and overall job satisfaction.

A strong identity security program can deliver several significant business outcomes beyond merely reducing security risks. By defining clear business outcomes up front and tying them to known business drivers and risks, organizations can ensure that their identity security program has the support of senior leadership and is designed to deliver measurable business value.



### Authentication Log



Last 24 Hrs. ● Granted ● Denied



05

# Key Performance Indicators

## Key Performance Indicators

By bringing all these areas together, we can develop a compelling set of KPIs that can measure the identity security program over time.

These draw on all four pillars of identity security and map to clear cybersecurity and business outcomes.

NIST CSF Stage	Identify Capability	Example KPIs	Cybersecurity Outcomes	Business Outcomes
Identify	User Inventory	<ul style="list-style-type: none"> <li># orphaned accounts</li> <li># discrepancies with HRIS</li> <li># of non-unique and/or shared IDs</li> <li># of administrator accounts</li> </ul>	Enable zero trust journey	Breach Prevention; Employee satisfaction; Improve compliance
	Machine Identities	<ul style="list-style-type: none"> <li># of service accounts with unknown owners</li> <li># service accounts with default passwords or expired keys</li> </ul>	Reduce unauthorized access	Breach Prevention and Brand Reputation
	Guest Accounts	<ul style="list-style-type: none"> <li># inactive guest accounts</li> <li># guest accounts with excessive access</li> <li># unmanaged devices with access</li> </ul>	Reduce attack surface	Breach Prevention; Third Party Risk; Improve compliance and Reduce audit findings
Protect	Onboarding	<ul style="list-style-type: none"> <li>Speed to onboard new employees rate</li> <li># users with excessive access rights</li> <li>% User account creation satisfaction rate</li> </ul>	ATO prevention	Operational Efficiency; Breach Prevention
	De-provisioning	<ul style="list-style-type: none"> <li>% Accounts disabled within SLA for terminated users</li> <li>Speed to deprovision</li> </ul>	Reduce unauthorized access and data loss	Operational Efficiency; Breach (ATO) Prevention
	SSO	<ul style="list-style-type: none"> <li>% of business apps protected under SSO</li> <li># apps with direct access</li> <li>% password complexity rate</li> <li># unused applications</li> <li># of logins per day</li> </ul>	ATO prevention	Breach Prevention, Employee Satisfaction
	MFA	<ul style="list-style-type: none"> <li>% of user accounts configured to use Multi-factor Authentication</li> <li>% of Guest Accounts with MFA</li> <li>% of user accounts using strong forms of MFA (FIDO2, Passwordless, passkeys, number-matching)</li> </ul>	ATO prevention	Breach Prevention; Improve Compliance; Third Party Risk
	Access Policy	<ul style="list-style-type: none"> <li>% access coming from trusted or known locations or IPs</li> <li>% access evaluated for risk at authentication time</li> <li>% access coming from trusted devices</li> </ul>	Limited access to critical data	Breach Prevention; Improve Compliance

NIST CSF Stage	Identify Capability	Example KPIs	Cybersecurity Outcomes	Business Outcomes
Detect	Collection	<ul style="list-style-type: none"> <li># Unsuccessful logins (SOX)</li> <li># Anomalous access events</li> <li># User-reported suspicious activity</li> <li># Unmanaged endpoints</li> <li># Privileged users without MFA</li> </ul>	<p>Develop “baseline behavior” and custom Risk Profile</p> <p>Reduce unauthorized access</p>	Improve Compliance and Reduce Audit Findings; Operational Efficiency
	Detection	<ul style="list-style-type: none"> <li># of parallel sessions</li> <li># Impossible travel events</li> <li># Suspicious IP addresses blocked</li> </ul> <p>Average time to detect brute-forcing attempts and compromised users</p> <ul style="list-style-type: none"> <li># Highlighted risky events raised per day</li> </ul>	Quicker detection of compromised users and insider threats	Breach Prevention; Operational Efficiency
Respond	Response	<p>Average time to perform a password reset</p> <ul style="list-style-type: none"> <li>% False positive rate</li> <li># authentication-related help desk tickets</li> <li># OS/browser device update self-remediations performed</li> <li># MITRE ATT&amp;CK sub-techniques mitigated</li> <li># Risky events triaged per day</li> <li># Access policies improved</li> </ul>	<p>Improve Mean Time to Remediation</p> <p>ATO prevention</p> <p>Optimize and protect for current state of business</p>	Operational Efficiency; Improve Compliance; Breach Prevention

**Quick Tips: For public companies, check your Form 10-Ks to understand current business risks.**



## Conclusion

To reiterate a few points made in the introduction and throughout the sections, this document is not meant as a foolproof way to implement identity security in your organization. It is meant to provide some key frameworks for organizing functions and measuring their effectiveness. We believe that organizations can get started on much of this work with their current IT and security tools.

That said, we'd be remiss if we did not mention Cisco Duo is trying to help organizations large and small achieve better identity security outcomes. Duo's approach is to build out a **Continuous Identity Security** practice that brings together identifying, protecting, detecting, and responding to identity-based threats while ensuring seamless access for the workforce. We hope it will help organizations stop identity-based attacks and deliver a world-class user experience to IT and security professionals and end users alike.

If you'd like to learn more about how Duo can help get your identity security program started, check out our **Continuous Identity Security** page or **begin a free trial**.

**Cisco Duo** protects against breaches with a leading access management suite that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out. As a trusted partner, Duo quickly enables strong security while also improving user productivity.

Try it for free at [duo.com](https://duo.com).

