ORT

Building an
Identity Security Program

First Edition

A BLUEPRINT FOR CISOS

Building an identity security program?
Find out where to begin and how to mature it.

FOREWORD

MATT CAULFIELD

Founder and CEO, Oort

Welcome to Oort'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! We've gathered some of the best minds in the biz to provide practical guidance and a glimpse of what a successful program can look like.

From Identity Threat Detection and Response (ITDR) to Privileged Access Management (PAM) and Single Sign-On (SSO), 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 made this guide as practical as possible. It includes recommendations for Key Performance Indicators (KPIs), free tools, and checklists to help you start building and maturing your identity security program.

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.

Please note that we have omitted Customer Identity Access Management (CIAM), which is a different set of requirements and a level of complexity beyond this paper and falls out of a typical identity security program. Similarly, if you're looking for an IAM guide, this is not it. This guide specifically looks for the most important components of both identity and security.

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

CONTENTS

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 brings together some of the best minds in the field to provide practical guidance on aligning goals, building a capability, 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.

> “By 2026, 90% of organizations will be using some type of embedded identity threat detection and response function from access management tools as their primary way to mitigate identity attacks”
>
> **Gartner: Magic Quadrant for Access Management, Nov 2022**

Project Navigator

Interested in gaining context for a specific topic? Click on the relevant links to “fast-forward”.

Glossary

A-Z of Identity Security

AD TDR	Active Directory Threat Detection and Response
CCPA	California Consumer Privacy Act
CIEM	Cloud Infrastructure Entitlement Management
GDPR	General Data Protection Regulation
IAM	Identity Access and Management
IdP	Identity Provider
IGA	Identity Governance and Administration
IOC	Indicator of Compromise
ISPM	Identity Security Posture Management
ITDR	Identity Threat Detection and Response
JIT	Just-in-Time access
KPI	Key Performance Indicators
MFA	Multi-Factor Authentication
TTP	Tactics, Techniques and Procedures
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SOAR	Security Orchestration and Response
SoD	Segregation of Duties
SOX	Sarbanes–Oxley Act
SSO	Single Sign-On
SWA	Secure Web Authentication
PAM	Privileged Access Management
PIM	Privileged Identity Management
ZTNA	Zero Trust Network Access

CHAPTER N.1

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 precisely mean by that?

The traditional approach to cyber security 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.

> Organizations have spent considerable effort improving IAM capabilities, but much of it has been focused on technology to improve user authentication, which actually increases the attack surface for a foundational part of the cybersecurity infrastructure.
>
> **Gartner, Top Security and Risk Management Trends for 2022, March 2022**

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 a large number of identity tools, predominantly cloud-based, that have been implemented by IT and IAM teams.

Often, these platforms are a significant blindspot for security teams. According to the Identity Defined Security Alliance, only 53% of security professionals have ownership of workforce IAM.

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%).

To address this divide, organizations need a joint identity incident response plan, shared documented access policies, and reports proving policies enforcements. 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.

> Identity people are now at the point of no return where you're going to have to learn more about cybersecurity. Cybersecurity people, conversely, now need to understand the notion of joiner, mover, and leaver and pick up some IAM knowledge. The bad actors don't work in silos, so we cannot work in silos on the good side.
>
> **David Mahdi, Chief Identity Officer, Transmit Security**

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 user names, 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.

The Role of Identity in Existing Security Frameworks

Identity already plays an important role in many security frameworks and is critical to any zero trust strategy. They fall into six areas: identity inventory, MFA, Access Control, IAM Hygiene, Log Collection, and Session Management.

We've mapped the CIS Critical Security Controls (CIS Controls) and the NIST Cybersecurity Framework to these six areas.

	CIS CSC	NIST CSF
Identity Inventory	**CIS CSC 5.5** Establish and Maintain an Inventory of Service Accounts	**NIST CSF PR.AC-1** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
	CIS CSC 5.6 Centralize Account Management	
	CIS CSC 6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems	
Multi-Factor Authentication	**CIS CSC 6.3** Require MFA for Externally-Exposed Applications	**NIST CSF PR.AC-7** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
	CIS CSC 6.4 Require MFA for Remote Network Access	
	CIS CSC 6.5 Require MFA for Administrative Access	

	CIS CSC	NIST CSF
Access Control	**CIS CSC 6.1** Establish an Access Granting Process	**NIST CSF PR.AC-3** Remote access is managed
	CIS CSC 6.2 Establish an Access Revoking Process	**NIST CSF PR.AC-4** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
	CIS CSC 6.7 Centralize Access Control	**NIST CSF PR.IP-11** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
	CIS CSC 6.8 Define and Maintain Role-Based Access Control	
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
Inactive Accounts and Hygiene Issues	**CIS CSC 5.3** Disable Dormant Accounts	
	CIS CSC 4.7 Manage Default Accounts on Enterprise Assets and Software	
Session Management	**CIS CSC 4.3** Configure Automatic Session Locking on Enterprise Assets	

CHAPTER N.2

People, Processes, and Technology

People, Processes, & Technology

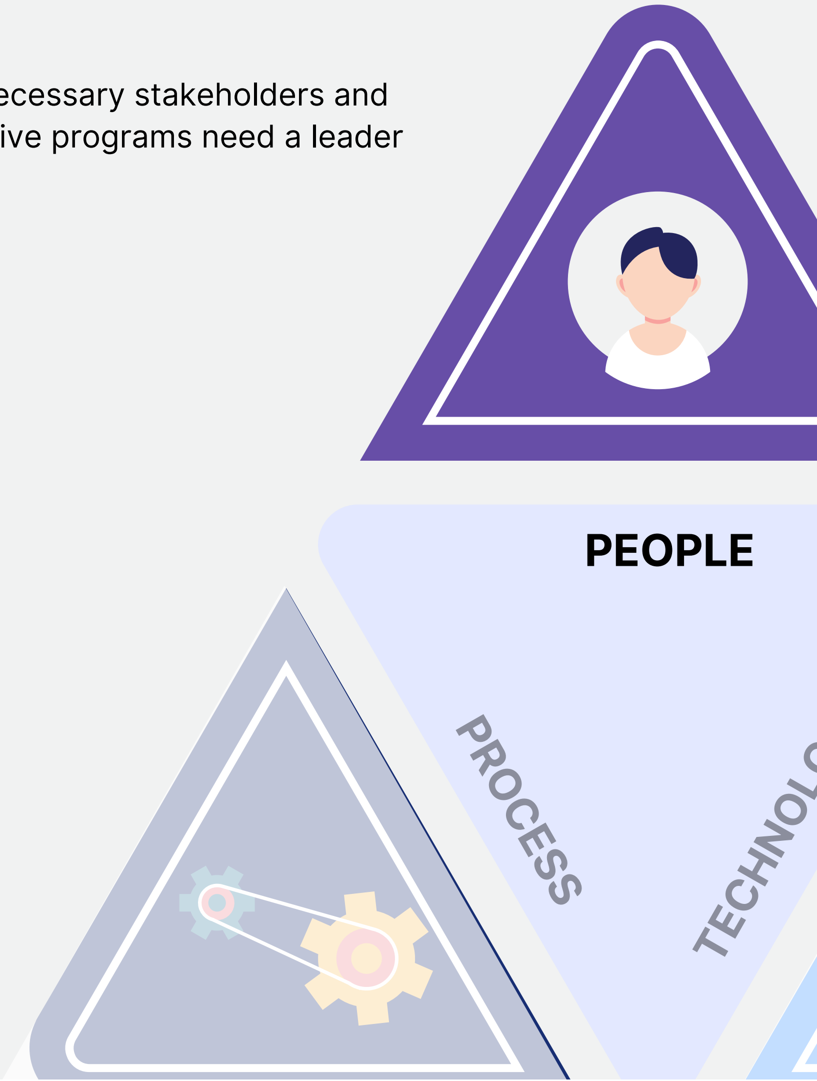
A successful identity security program must be comprised of people, processes, and technology.

People

While there has been recent talk of a “Chief Identity Officer", the driving force of identity security programs typically come from CISOs. The CISO is responsible for overseeing the identity security program and ensuring that it effectively addresses all the facets of identity security, including the people factor.

The CISO must work with various stakeholders across the organization to create a security-aware culture, provide training and education for employees, and establish clear policies and procedures for identity security. Most of all, it’s critical to bring the security and IT (or IAM) teams together.

The following section will focus on the necessary stakeholders and their responsibilities, but the most effective programs need a leader that owns and drives the initiative.



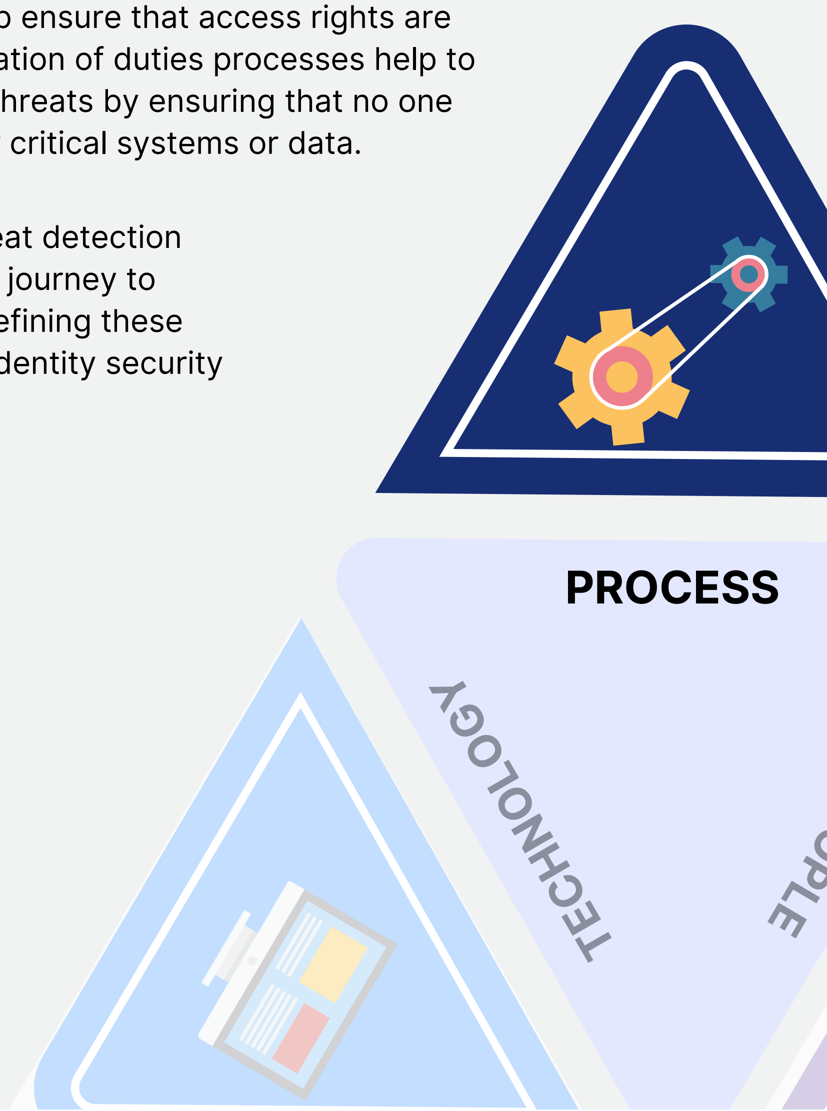
Processes

Processes are a critical facet of an identity security program because they help establish the policies and procedures that govern how an organization manages and secures identities and access. Without effective processes, an organization is more likely to make errors or oversights that could lead to security breaches or non-compliance with regulations. The security team typically defines the process, and the IT or IAM team leads the implementation.

One important aspect of processes is good hygiene, which includes routine maintenance tasks such as user access reviews, account cleanup, and ongoing monitoring. Good hygiene is critical for enabling success in future projects such as Identity Governance and Administration (IGA) and Privileged Access Management (PAM), as it helps ensure that the organization's identity data is accurate and up-to-date. It also helps to identify and mitigate risks and vulnerabilities proactively rather than reacting to them after a breach has occurred.

Other important processes in identity security include access provisioning and deprovisioning, user access reviews, and segregation of duties. Access provisioning and deprovisioning processes ensure that users have the appropriate access to systems and data they need to do their jobs, while user access reviews help ensure that access rights are reviewed and updated regularly. Segregation of duties processes help to prevent conflicts of interest and insider threats by ensuring that no one user has too much power or control over critical systems or data.

Finally, another important process is threat detection and response. We are still early on in the journey to creating identity threat playbooks, but defining these will be a critical step toward the overall identity security program.



Technology

Technology is an important facet of an identity security program because it provides the tools and infrastructure necessary to implement effective identity and access management processes.

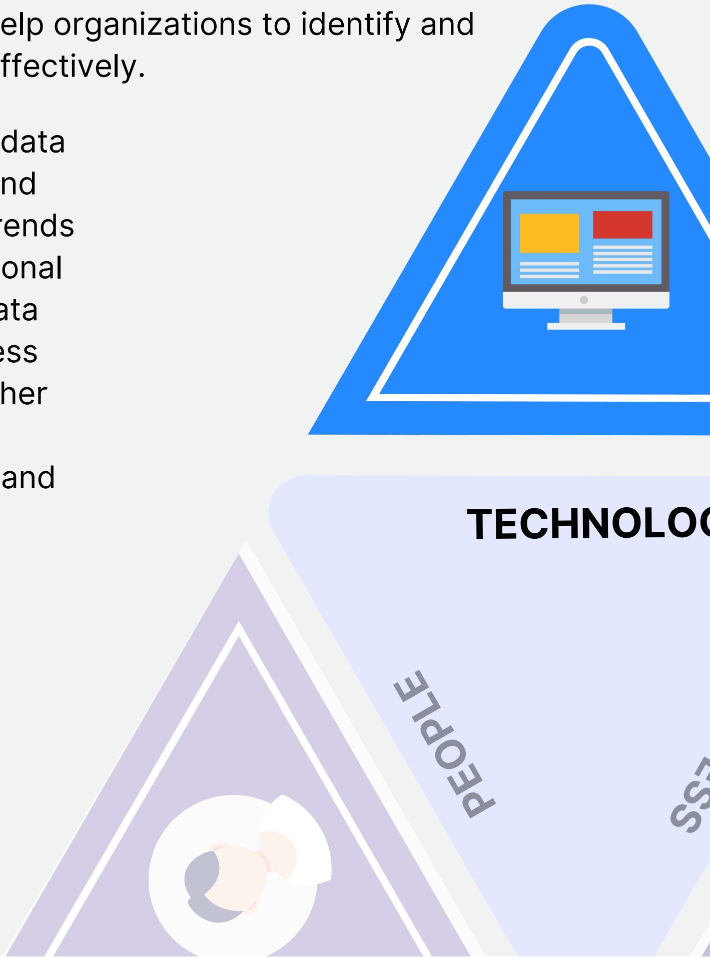
Technology can enable automation, improve accuracy, and increase efficiency in managing identities and access. There are fundamental technologies, such as Directories, Single-Sign-On (SSO), and Multi-Factor Authentication (MFA) that act as the foundation for many identity security strategies. Security leaders then turn to Identity Threat Detection and Response (ITDR), Privileged Access Management (PAM) and Identity Governance and Administration (IGA) tools to complement, improve and automate some of the processes.

Technologies often exist to support processes and are often helpful for building relationships between teams. For example, collaboration via a ticketing system will help to provide a single source of truth for investigations relating to identities.

For ease of response for security operations, consider also consuming event and incident data in a Security Information and Event Management (SIEM) or Security Orchestration, Automation, and Response (SOAR) solutions. SIEM solutions can help identify and analyze security events in real-time, while SOAR technology can help automate incident response processes.

Another technology that has grown in popularity is a security data lake. A security data lake is a centralized repository that enables the collection, storage, and analysis of security-related data from various sources, including both static entitlements and dynamic user behavior. It can help organizations to identify and respond to security incidents more quickly and effectively.

Leading organizations may also have an identity data engineering strategy, which involves collecting and analyzing identity data to identify patterns and trends that can be used to improve security and operational efficiency. This strategy can involve collecting data from various sources, including identity and access management (IAM) systems, HR systems, and other business applications. Data engineering can help organizations to better understand their identity and access risks and take more informed actions to mitigate those risks.



CHAPTER N.3

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 entitlements, 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 new 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.

R	Responsible
A	Accountable
S	Supporting
C	Consulted
I	Informed

	CISO	CIO	Security Team	IAM/IT Team	Threat Intel	IT Help Desk	Compliance Team
Identify							
Building a User Inventory	A	S	C	R			
Managing Guest Access	S	A	S	R			I
Managing Machine Identities	I	A	C	R			
Protect							
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
Detect							
Collection	A	I	R	S	S		
Detection	A	I	R	S	S		
Respond							
Response	A	I	R	S	S	S	

CHAPTER N.4

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.

QUICK TIPS

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

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.

CHAPTER N.5

Key Performance Indicators

Key Performance Indicators

Bringing all these areas together, we can develop a compelling set of Key Performance Indicators (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	Identity Capability	Example KPIs	Cybersecurity Outcomes	Business Outcomes
Identify	User Inventory	# Of non-unique and/or shared IDs # Orphan accounts	Enable zero trust journey	Breach Prevention; Employee Satisfaction; Improve Compliance
	Machine Identities	# Of service accounts with unknown owners	Reduce unauthorized access	Breach Prevention and Brand Reputation
	Guest Accounts	# Inactive guest accounts # Active guest accounts	Reduce attack surface	Breach Prevention; Third Party Risk; Improve Compliance and Reduce Audit Findings
Protect	Onboarding	# Speed to onboard new employee rate % User account creation satisfaction rate	ATO Prevention	Operational Efficiency; Breach Prevention
	De-provisioning	% Accounts disabled within SLA for terminated users % Of access removed within SLA upon employee termination	Reduce unauthorized access and data loss	Operational Efficiency; Breach (ATO) Prevention
	SSO	% Of business apps using SSO	ATO Prevention	Breach Prevention
	MFA	% Of user accounts configured to use Multifactor Authentication % Of Guest Accounts with MFA % Of user accounts using strong forms of MFA	ATO Prevention	Breach Prevention; Improve Compliance; Third Party Risk
	User Access	# Of Periodic Access Reviews completed within SLA # of access revocations	Limit access to critical data	Breach Prevention; Improve Compliance
Detect	Collection	# Unsuccessful logins (SOX)		Improve Compliance and Reduce Audit Findings
	Detection	# Of successful brute-forcing attempts # Of parallel sessions # Impossible travel events % False positive rate	Quicker detection of compromised users and insider Threats	Breach Prevention; Operational Efficiency
Respond	Response	# Average time to perform a password reset # Suspicious IP addresses blocked # Mitre ATT&CK subtechniques mitigated # Time to respond to Brute-Force # Time to respond to compromised user	Improve Mean Time to Remediation	Operational Efficiency; Improve Compliance; Breach Prevention

CHAPTER N.6

Four Pillars of Identity Security

1. IDENTIFY

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

Building a user 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. Without an accurate user inventory, it becomes difficult to identify and mitigate security risks.

In most cases, this will take the form of a table and teams can generate a comprehensive list of identities with 1-2 days. As this matures, teams create a searchable inventory that enable 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.

Level 3: Near-real-time inventory with active security and hygiene processes.

Level 2: Searchable inventory enabling targeted actions, including deletion of orphaned accounts.

Level 1: Comprehensive user inventory, generated within 24-72 hours in tabular form.

Level 0: No centralized user inventory.

CHALLENGES OF A COMPLETE USER 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 creating 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. These accounts should be linked to a corporate account.

> To establish a mature identity security program, it is essential to have comprehensive contextual information for every single account, while also implementing ongoing monitoring to detect identity threats and to maintain optimal hygiene.
>
> **Roman Bachurski, Senior Manager Information Security at Major League Baseball**

USER INVENTORY KPIS

- **# ORPHANED ACCOUNTS**
- **# DISCREPANCIES WITH HRIS**
- **# OF NON-UNIQUE AND/OR SHARED IDS**

Guest access

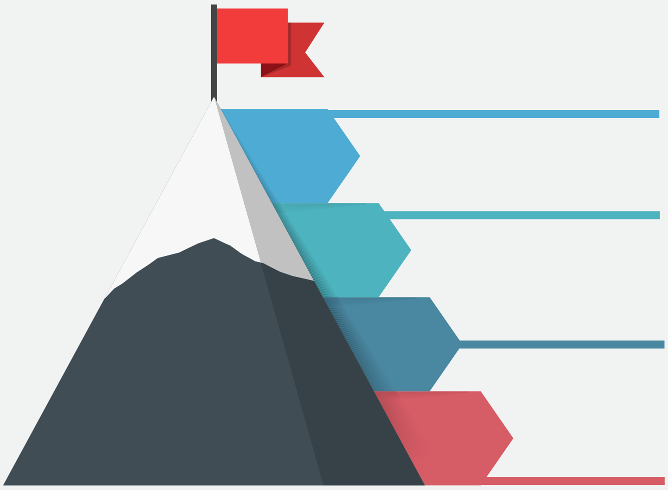
Guest accounts in Azure AD are identities that belong to external users who are invited to collaborate with the organization. Inviting guest accounts into your organization can be as simple as sending a link to a document or messaging an external email address on Teams.

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, a common practice for employees suspecting of being terminated is to share information with private Gmail or Microsoft cloud accounts.

At the bare minimum, organizations should have a policy in place for managing guest accounts. This should regularly review guest accounts and remove inactive or unnecessary guest accounts.

This process, such as the invites, deletion and monitoring, 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.



Level 3: Tracking, monitoring, and threat detection in guest accounts, including self-invites.

Level 2: Automated invites, deletion, and activity monitoring with MFA on guests.

Level 1: Policy-based management of guest accounts, including inactivity and reevaluation.

Level 0: No defined processes for managing guest accounts.

Guest access

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 work, who can be invited, for how long, and to what types of content.

- ☑ **Track Invites.** Set a time to expire 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 person that invited 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 data that internally is regulated and governed via MFA.

Limit Guest Permissions

☑ Organizations should limit the permissions of guest users to reduce the risk of unauthorized access to company data.

☑ Non-privileged users should not be allowed to register third-party applications.

☑ 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

# INACTIVE GUEST ACCOUNTS

# ORPHANED GUEST ACCOUNTS

# GUEST ACCOUNTS WITH EXCESSIVE ACCESS

Machine Identities

In addition to human users, machines,. Proper user management can help organizations identify and manage machine identities and their associated access privileges.

Non-human identities can refer to any number of accounts and is effectively any account that is one-step removed from a human. This can include shared mailboxes, service accounts, and network devices. Machine identities make up 43% of all identities within the average enterprise.

43%

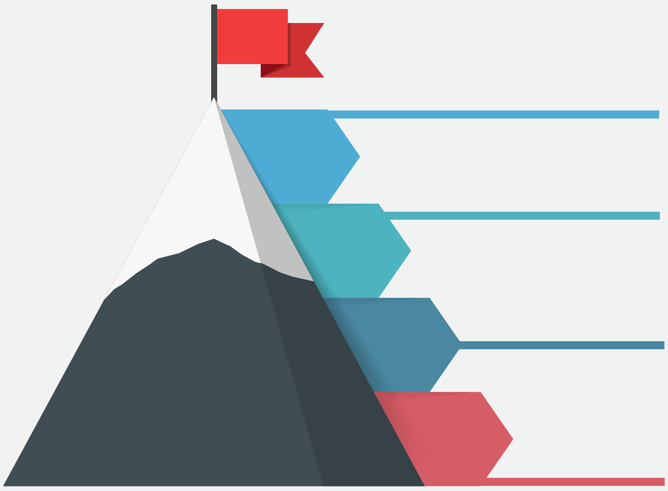
Machine identities make up 43% of all identities within the average enterprise (Sailpoint)

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 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, or have a process in place to transition ownership.

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 provisioning and the existence of ephemeral service accounts that can be used for one-off tasks.



Level 3: Automated creation, JIT provisioning, and logging of ephemeral service accounts.

Level 2: Automated creation and deprecation of service accounts reflected in inventory.

Level 1: Paper process for managing service accounts, including transition of ownership.

Level 0: No defined processes for managing machine identities.

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 unmanaged device access and prevent unauthorized access to sensitive data and assets. This 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.

> "Gaining insights into unmanaged devices and identities plays a pivotal role in designing an effective BYOD program. Understanding the landscape, minimizing noise, and obtaining comprehensive visibility enable us to accelerate and enhance our BYOD initiatives for improved security and productivity."
>
> **Lee Sullivan, Security Architect - Monster**

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.

2. PROTECT

After identification, the next step is to focus on protecting those identities. There are critical parts of the joiner, mover, 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 job, and ensuring that their entitlements are appropriate for their role. 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, they can register their own forms of MFA.

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.

Level 3: Monitor and receive alerts, ensure compliance, enable self-service capabilities.

Level 2: Automated onboarding and provisioning procedures for efficiency.

Level 1: Established process and demonstrate workflow for all roles.

Level 0: No defined processes for onboarding.

Onboarding & transfers

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 refer to the specific permissions and access rights that are granted 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. More advanced identity security programs include Just-in-time (JIT) access, which allows elevation of human and non-human users in real-time to provide granular privileged access to an application or system.

The role of CIEM (Cloud Infrastructure Entitlement Management) in managing entitlements is to provide visibility and control over who has access to what resources within the cloud environment. This involves monitoring and managing access privileges, such as determining who can create or modify resources, and who has the ability to view or delete them.

ONBOARDING KPIS

# SPEED TO ONBOARD 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.

> CISOs, here's a golden rule for building an identity security program: prioritize timely deprovisioning of user access. By swiftly revoking access, we neutralize risks from terminated users and fortify our defenses against unauthorized access or misuse. With clear cybersecurity practices as our shield, we safeguard both reputation and the bottom line.
>
> **Kurt Lieber, Former CISO at Wells Fargo**

Level 3: Monitor, receive alerts, ensure compliance, with automated system integration.

Level 2: Automated offboarding and deprovisioning procedures for efficiency.

Level 1: Established process, demonstrate workflow, cover all roles and personnel.

Level 0: No defined processes for offboarding and deprovisioning.

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 attacks and other types of password-based attacks.

SWA vs SAML

SWA is a simpler protocol that provides basic web-based authentication, while SAML is a more comprehensive and secure protocol that provides more advanced SSO capabilities. The choice of which protocol to use depends on the specific needs of the organization and the level of security and flexibility required for their web applications.

SSO tools can also be used to ease the burden of onboarding and deprovisioning, 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.

Level 3: SSO treated as a monitored firewall.

Level 2: Centralized provisioning, HR system integration, and governance of SSO.

Level 1: SSO tool present with MFA governance and application migration policy.

Level 0: No SSO tool in place.

Single Sign-On

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 hi-jacked.

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 to prevent unauthorized access to sensitive data or resources.

> The Session Hijacking attack consists **of the exploitation of the web session control mechanism, which is normally managed for a session token**.
>
> ***OWASP***

SSO KPIS

- **% OF BUSINESS APPS USING SSO**
- **% PASSWORD COMPLEXITY RATE**
- **% OF ACCOUNTS WITH PASSWORD UPDATED IN LAST 30 DAYS**
- **# APPS WITH DIRECT ACCESS ALLOWED**

Multi-Factor Authentication

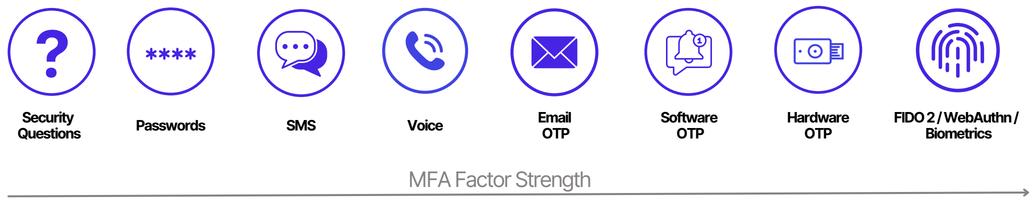
Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more types of authentication factors to prove their identity. These factors can include something the user knows (e.g., a password), something the user has (e.g., a token), or something the user is (e.g.,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

While many frameworks require "2 or more authentication factors of different types", not all factors are made equal. Unfortunately, many existing second factors are susceptible to phishing or otherwise being bypassed. In fact, more than 40% of accounts have no strong forms of MFA enabled.

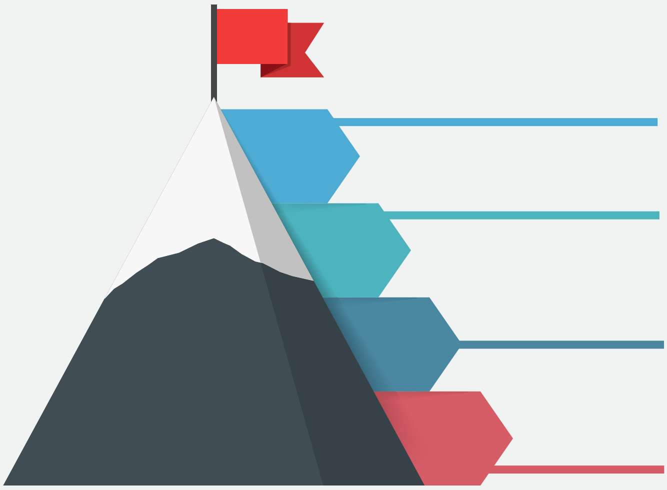


Multi-Factor Authentication

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.

More mature organizations have a plan for getting towards phishing-resistant MFA and will monitor for 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.

> “While MFA is important, it is crucial to recognize that the existing push-based, SMS-based, and TOTP-based MFA solutions must be discarded in favor of phishing-resistant MFA. Traditional MFA is no longer effective. Achieving truly unphishable 2FA is challenging, but mandatory, phishing-resistant MFA tied to what you own and who you are is essential.”
>
> **Eric Richard**
> **CISO, HubSpot**



Level 3: Passwordless MFA policy with monitored recovery process and tracking.

Level 2: Phishing-resistant MFA plan, activity monitoring, and MFA-based threat detection.

Level 1: 100% cryptographically secure MFA with clear exception policies.

Level 0: No or limited MFA adoption.

MFA KPIS

% OF USER ACCOUNTS CONFIGURED TO USE MULTIFACTOR AUTHENTICATION

% OF USER ACCOUNTS USING STRONG FORMS OF MFA

User Access

Access reviews are a process of periodically reviewing and validating users' entitlements and access to ensure that they are still necessary and appropriate. This reduces the risk of excessive access, which can occur if users are granted access to resources or systems that are no longer needed or have become obsolete.

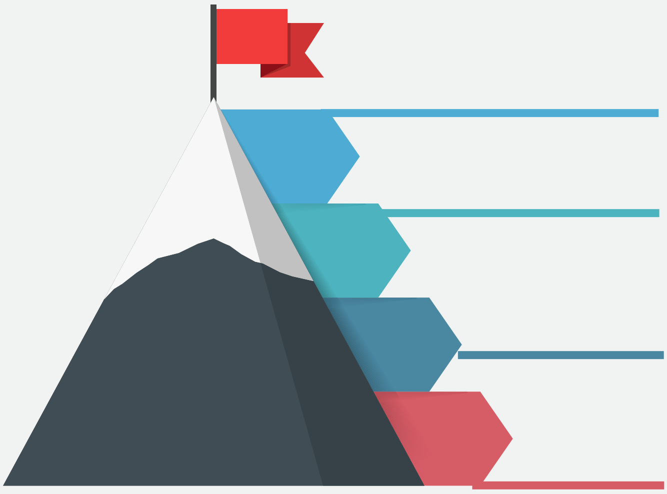
By conducting regular access reviews, organizations can identify and revoke unnecessary entitlements and reduce the risk of data breaches. Most organizations are basing this on the principle of least privilege, whereby users should only have the access they need to do their job.

At the most basic level, organizations must have reviews in place – often via a spreadsheet. This should be done for your top 20 most sensitive applications (or top 50%, whichever is higher).

As this matures, these reviews can be automated and conducted regularly. Action is taken as a result, including identifying sensitive applications and unused access.

Ultimately, organizations should strive for continuous monitoring and collection, which will enable automated actions and Just-in-Time provisioning.

Once this is in place, mature organizations may adopt Privileged Access Management controls to manage the access of privileged users.



Level 3: Continuous monitoring, data collection, and automated action for unused access. Just-in-Time provisioning and Privileged Access Management.

Level 2: Centralized automation and querying, identifying most used/sensitive and unused access.

Level 1: Excel-based access reviews for sensitive systems with owner acknowledgment.

Level 0: No user access reviews.

Segregation of Duties

Segregation of duties prevents unauthorized access to data by assigning different roles and privileges. For example, one person creates user accounts, while another grants or revokes access. This is particularly important for public companies, who must demonstrate this to adhere to SOX compliance.

Separating these roles ensures no one has complete control, preventing unauthorized access and internal fraud. For example, in software development, different individuals should write and test code to ensure security and vulnerability-free releases. This helps to reduce the risk of unauthorized access, fraud, and errors by assigning tasks to different individuals or teams.

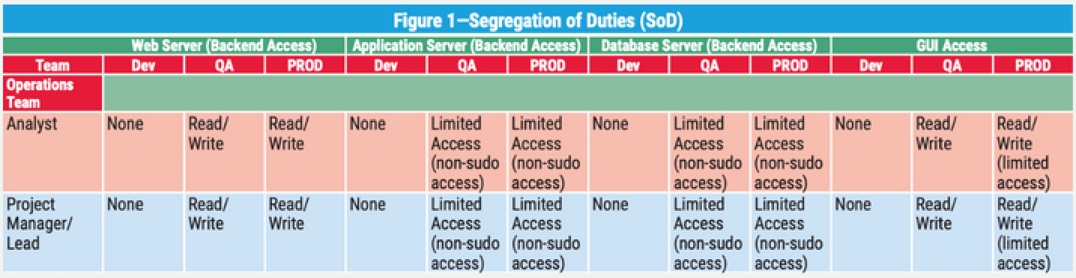


Figure 1—Segregation of Duties (SoD)

	Web Server (Backend Access)			Application Server (Backend Access)			Database Server (Backend Access)			GUI Access		
Team	Dev	QA	PROD	Dev	QA	PROD	Dev	QA	PROD	Dev	QA	PROD
Operations Team												
Analyst	None	Read/ Write	Read/ Write	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Read/ Write	Read/ Write (limited access)
Project Manager/ Lead	None	Read/ Write	Read/ Write	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Read/ Write	Read/ Write (limited access)

Example SOD Excerpt. Source: ISACA

USER ACCESS REVIEW KPIS

% USER ACCESS REVIEW COMPLETION RATE

# UNUSED APPLICATIONS

USER ACCESS VIOLATIONS

# OF PRIVILEGED ACCOUNTS WITH UNVAULTED CREDENTIALS

DETECT

Log Ingestion

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

For example, the Sarbanes-Oxley Act (SOX) requires the collection of unsuccessful logins. The relevant sections of CIS and NIST controls are also listed below. While many start off using SIEMs to analyze these logs, some higher-maturity companies are turning to security data lakes. We have provided a comparison in the following section: SIEM versus Security Data Lake.

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

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 Azure AD, 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 actually use them. CardinalOps

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 you collect logs from identity providers, it does not mean you actually do something with them. In fact, only 25% of organizations that forward identity logs actually use them.

Level 3: Identity Data Engineering for comprehensive understanding and optimization of data.

Level 2: Active utilization of data with rules and automation for analysis.

Level 1: Identity sources aggregated to SIEM with retention policy validation.

Level 0: No collection of identity logs or data

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.

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.

👍 Easy to create detections and respond to.

👎 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 on any deviations from that baseline. This can (and should) include suspicious administrator activity.

👍 Can monitor behavior and not just IOCs.

👎 Traditional EUBA 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.

👍 Aligns with what attackers actually do. Unlike IOCs, attackers often keep similar techniques.

👎 There are many techniques to map to, with more added all the time.

> Detecting session hijacking is crucial for maintaining a secure environment. Implementing strict policies in Okta for session length plays a pivotal role in reducing the window of opportunity for attackers, enhancing our defense against unauthorized access and protecting our valuable resources.
>
> **Dmitriy Sokolovskiy, CISO - Avid**

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, Ojection Deletion, and Object Modification)
Logon Session
User Account

Level 3: TTP-based detection aligned with Mitre ATT&CK, minimizing false positives.

Level 2: EUBA for anomaly detection, including impossible travel events, with reduced false positives.

Level 1: IOC-based detection with focus on brute-forcing attempts.

Level 0: No detections for identity threats.

DETECTION KPIS

- 🚫 # SUSPICIOUS IP ADDRESSES BLOCKED
- # IMPOSSIBLE TRAVEL EVENTS
- # NEW COUNTRY FOR TENANT EVENTS
- # TIME TO DETECT COMPROMISED USER

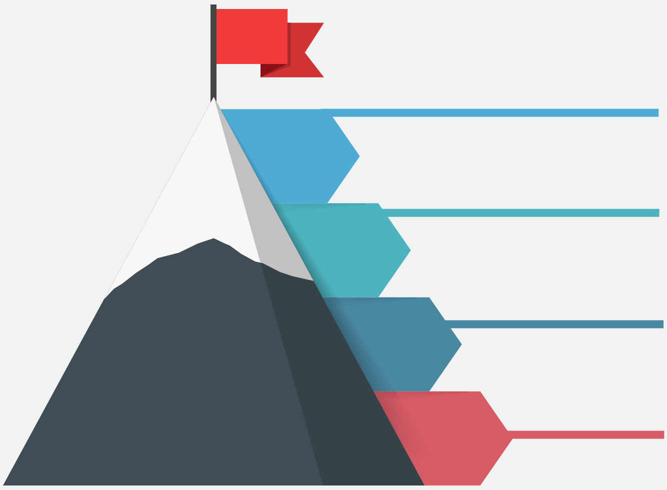
RESPONSE

Detecting identity threats is great, but it needs to inform an action or response. Organizations should define and document clear processes for playbooks to respond to these threats, ideally tied to a ticketing platform with defined SLAs.

Good response playbooks are an essential component of Identity Threat Detection and Response (ITDR) strategies. 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. Additionally, response playbooks can help reduce the response time and minimize the impact of an incident on the organization.

One way to add maturity to response playbooks is by leveraging Security Orchestration, Automation, and Response (SOAR) platforms. SOAR platforms can automate the incident response process, reducing the risk of errors and improving the speed and efficiency of the response. By integrating with ITDR tools and systems, a SOAR platform can provide additional context and insights, enabling security teams to make more informed decisions and take more effective actions.



Level 3: ML-driven, self-healing, data science, and continuous improvement in response metrics.

Level 2: Automated response with SOAR tools.

Level 1: Playbook-driven response linked to ticketing platform with defined SLAs.

Level 0: No response playbooks; ad-hoc only.

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.

This 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, multi-factor authentication (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.

> “In security investigations and incident response, rich context on identities is invaluable. The manual effort of pulling data from multiple systems, aligning it into a cohesive timeline, and extracting meaningful insights is time-consuming. Having comprehensive identity context streamlines investigations, accelerates response, and strengthens our overall security posture.
>
> **Frank Conroy, Staff Security Engineer - Collibra**”

Playbook Actions

To help you form your identity threat response playbooks, we've pulled together a list of response actions that you can take in the short and medium term. Some of these will be familiar to security teams; others less so.

Quarantine Users

When you quarantine a laptop or device, you're typically preventing it from accessing the corporate network. However, if a compromised user has already accessed a particular application or service, simply quarantining their laptop or device won't necessarily prevent them from continuing to perform malicious actions within that application or service.

Quarantining the user's account within the identity provider is a more comprehensive approach. By quarantining the account, you prevent the user from accessing any applications or services that rely on that identity. This means that even if the user tries to bypass security controls or access a specific application from a different device, they won't be able to because their identity is quarantined.

Password and MFA Reset

Password reset playbooks outline the procedures for resetting a user's password or MFA in case of a forgotten or compromised account. The playbook should include steps for verifying the user's identity and ensuring that the new password is strong and secure. Resetting the password or MFA is just one piece of the puzzle if an attacker acquires the user’s password. Some platforms will also kill the session when performing a password reset.

Kill Sessions

If a session is hijacked, it should be immediately terminated to prevent further unauthorized access. This can be done by logging the user out of all active sessions and revoking their access tokens. If the user needs to log back in, they must re-authenticate, adding an extra layer of security to the process. This ensures that only authorized users can access sensitive data or perform critical actions within your organization's applications and services.

Remove Access
If a user's account is compromised, their access should be immediately revoked. This can be done by removing their account from groups or roles that grant access to critical resources.

Rollback Changes
Identify any unauthorized privilege escalations and roll them back to their previous state. This can involve adjusting access control settings, removing unnecessary privileges, or reverting permission changes.

Confirm with User
Reach out to affected users to verify their activities. This step ensures that legitimate users are not falsely impacted while addressing security concerns.

Confirm with Manager
If you suspect anomalous behaviors, consider checking with the employee's manager to verify the activities and ascertain if it seems suspicious. For example, are they traveling for work? Are they working on a new project?

RESPONSE KPIS

- % FALSE POSITIVE RATE
- # TIME TO RESPOND TO COMPROMISED USER
- # TIME TO RESPOND TO BRUTE-FORCING EVENT

CHAPTER N.7

Outsourcing Identity Security

OUTSOURCING

Outsourcing components of an identity security program can provide numerous benefits to an organization. One option is to use managed services providers, such as BeyondID, which can help ensure that an organization's identity security program is properly maintained and monitored. Additionally, providers like Crowdstrike and Silverfort offer good visibility into AD and Azure AD, which can be invaluable for identifying potential threats.

Oort provides a layer on top of cloud IAM solutions, such as Okta, Azure AD and Duo, and provides continuous monitoring for identity threats and identity security posture management. We focus heavily on response capabilities, which enable security teams to act on the findings.

There are several key considerations that an organization should keep in mind when outsourcing components of their identity security program. The first is to look for providers that can build an ingestion pipeline that includes all relevant sources of information, such as IDP information, productivity suites, messaging tools, people information, and networking infrastructure information. Additionally, the organization should ensure that their chosen provider has a storage solution that can support both structured and semi-structured data.

Adhering to standards is also crucial, and the organization should work with providers who adhere as closely as possible to standards like SCIM. Furthermore, it's important to operationalize the outsourcing effectively by supporting lightweight automation based on tools like Slack, ServiceNow, and Jira. Finally, the organization should ensure that the data is easily accessible, including by providing digests in tickets and meeting users where they are.

Build versus Buy

SIEM Detections: The cost of building an in-house Security Information and Event Management (SIEM) system can range from $10,000 to $100,000, depending on the size of the organization and the complexity of the system. This cost includes the purchase of hardware, software, and licenses, as well as the time and expertise required to set up and configure the system.

Storage Costs: The cost of storage will depend on the size of the organization and the amount of data generated by the SIEM system. It is estimated that the cost of storage can range from $0.10 to $0.50 per gigabyte per month.

Response Costs: The cost of responding to security incidents can vary greatly depending on the severity of the incident and the complexity of the response. It is estimated that the cost of incident response can range from $5,000 to $50,000 per incident.

Hiring Talent: Building an in-house security program requires hiring and retaining skilled cybersecurity professionals. The cost of hiring and retaining a cybersecurity professional can range from $100,000 to $250,000 per year, depending on the level of expertise required.

SIEM versus Security Data Lake

The decision to use a SIEM versus a security data lake for identity threat detection and response will depend on the organization's specific needs, goals, and resources.

While SIEM systems have been a traditional choice for threat detection and response, security data lakes are gaining popularity due to their ability to store and analyze large amounts of data, support flexible data retention periods, and provide advanced analytics capabilities.

However, a security data lake requires additional investments in data ingestion and processing tools, and organizations must ensure they have the necessary expertise to leverage its full potential.

Ingestion costs: SIEM systems typically require significant upfront costs for hardware, licensing, and maintenance. The cost of implementing a security data lake can be more flexible as it depends on the organization's specific requirements, but it may require more significant investments in data ingestion and processing tools.

Storage costs: SIEM systems tend to store only a subset of relevant security data due to storage limitations, while a security data lake can store large volumes of data at a relatively lower cost, including both structured and unstructured data.

Data retention period: SIEM systems typically have a limited data retention period, usually measured in days to weeks, due to storage limitations. In contrast, a security data lake can provide longer retention periods, ranging from months to years, which can be helpful for forensic analysis.

Usability: SIEM systems can be complex and require significant expertise to configure, operate, and maintain. In contrast, a security data lake can be more user-friendly and may be more accessible to less technical users. Security data lakes are designed for both security analysts and data scientists, who can use advanced analytics and machine learning to detect and respond to identity threats.

APPENDIX 1

IDENTITY SECURITY MATURITY MODEL

Capabilities	Non-Existent	Defined	Automated	Optimized
Identification: User Inventory	No centralized user inventory	Comprehensive user inventory, generated within 24-72 hours in tabular form.	Searchable inventory enabling targeted actions, including deletion of orphaned accounts.	Near-real-time inventory with active security and hygiene processes
Identification: Machine Identities	No defined processes for managing guest accounts	Paper process for managing service accounts, including transition of ownership.	Automated creation and deprecation of service accounts reflected in inventory.	Automated creation, JIT provisioning, and logging of ephemeral service accounts.
Identification: Guest Accounts	No defined processes for managing machine identities	Policy-based management of guest accounts, including inactivity and reevaluation.	Automated invites, deletion, and activity monitoring with MFA on guests.	Tracking, monitoring, and threat detection in guest accounts, including self-invites.
Protection: Onboarding	No defined processes for onboarding	Establish process and demonstrate workflow for all roles.	Automate onboarding and provisioning procedures for efficiency.	Monitor and receive alerts, ensure compliance, enable self-service capabilities.
Protection: De-provisioning	No defined processes for offboarding and deprovisioning	Establish process, demonstrate workflow, cover all roles and personnel.	Automate offboarding and deprovisioning procedures for efficiency.	Monitor, receive alerts, ensure compliance, with automated system integration.
Protection: SSO	No SSO tool in place	SSO tool present with MFA governance and application migration policy.	Centralized provisioning, HR system integration, and governance of SSO.	SSO treated as a monitored firewall with impact analysis.
Protection: MFA	No or limited MFA adoption	100% cryptographically secure MFA with clear exception policies.	Phishing-resistant MFA plan, activity monitoring, and MFA-based threat detection.	Passwordless MFA policy with monitored recovery process and tracking
Protection: User Access Reviews	No user access reviews	Excel-based access reviews for sensitive systems with owner acknowledgment.	Centralized automation and querying, identifying most used/sensitive and unused access.	Continuous monitoring, data collection, and automated action for unused access. Just-in-Time provisioning.
Collection	No collection of identity logs or data	Identity sources aggregated to SIEM with retention policy validation.	Active utilization of data with rules and automation for analysis.	Identity Data Engineering for comprehensive understanding and optimization of data.
Detection	No detections for identity threats	IOC-based detection with focus on brute-forcing attempts and parallel sessions.	EUBA for anomaly detection, including impossible travel events, with reduced false positives.	TTP-based detection aligned with Mitre ATT&CK, minimizing false positives.
Response	No response playbooks; ad-hoc only	Playbook-driven response linked to ticketing platform with defined SLAs	Automated response with Security Orchestration, Automation, and Response (SOAR).	ML-driven self-healing, data science, and continuous improvement in response metrics.

APPENDIX 2

HOW IDENTITY DRIVES COMPLIANCE

	CMMC	PCI DSS	NYCR	NIST 800-63-3	GDPR	SEC	GRAMM-LEACH-BLILEY ACT	SOX	CCPA
Ensure MFA is used by all users for network/remote access	✓		✓						
Ensure MFA is used for privileged users for local access	✓								
Ensure MFA is enabled by accounts with access to any personal/customer information				✓			✓		
MFA must have two of three of something you know, you have, or you are		✓							
User access privileges to nonpublic information must be limited.			✓						
MFA to support verifier impersonation (phishing) resistance required				✓					
Protect and Secure User Data					✓				
Ensure users present a combination of two or more credentials for access verification						✓			
Monitor and audit successful and failed login activity, account and user activity, and info access								✓	
Ensure employee account information is removed					✓				✓

APPENDIX 3

IAM READING LIST FOR CURIOUS SECURITY PROS

READ

- The Beer Drinker's Guide to SAML | Duo Security
- Identity and Access Management Recommended
- Best Practices for Administrators
- Access Control and Identity Management
- Identity Management: A Business Perspective
- Authentication and Access Control
- Identity Attack Vectors
- Securing the Perimeter
- Advancing Zero Trust Maturity Throughout the User Pillar

LEARN

- Okta Essentials
- Identity and Access Management with Okta
- Azure Active Directory documentation
- Duo Admin Panel Essentials: The Hero's Journey

LISTEN

- Identity at the Center
- State of Identity
- The Week in Identity
- IDentity Today
- The Identity Jedi
- Didi and Lital Show
- Decipher

Want more insights on identity security?

Get in Touch

SPEAK TO OORT