veza®

EBOOK

Intelligent Access

Strategies for achieving least privilege
in the modern enterprise

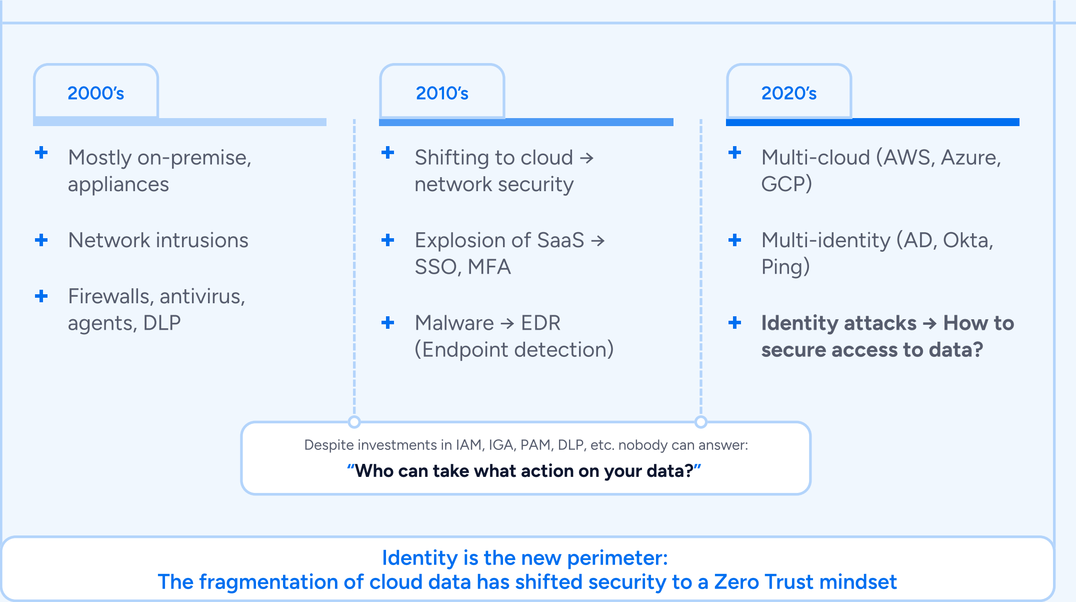
Coauthored by **Jason Chan** & **Tarun Thakur**

Foreword

Tarun Thakur • Co-Founder & CEO, Veza

Identity is a foundational technology for running and securing a business. Every system, application, and new business initiative is dependent on identity and, thus, identity platforms. Given how critical identity access management and governance are to business success, I deeply believe cybersecurity teams must prioritize identity as the foundation of an enduring cybersecurity strategy.

The landscape of identity management is undergoing a profound transformation, however, reshaping the way organizations approach managing identity. This transformation is rooted in the state of the modern threat landscape. In spite of all the cybersecurity innovations and controls currently in place (like network security, endpoint protection, SSO, and MFA) breaches, hacks, and attacks continue to make headlines every week. Breaches like those that impacted Okta, Microsoft, MGM, CloudFlare, Bank of America, and Colonial Pipeline brought to the forefront how brittle modern security infrastructure is – especially in the area of identity security. Most organizations are under-equipped for the litany of identity risks we see today.



2000's

- Mostly on-premise, appliances
- Network intrusions
- Firewalls, antivirus, agents, DLP

2010's

- Shifting to cloud → network security
- Explosion of SaaS → SSO, MFA
- Malware → EDR (Endpoint detection)

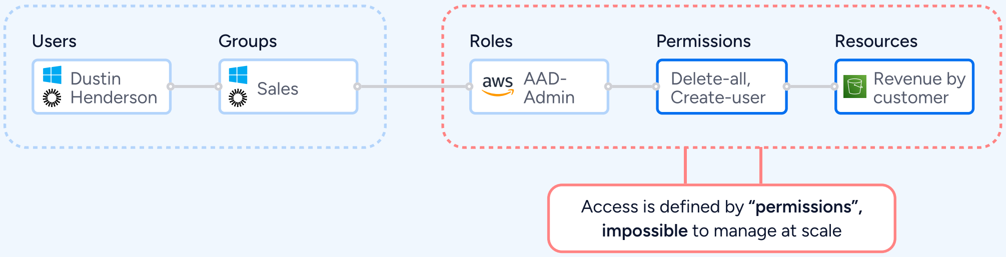
2020's

- Multi-cloud (AWS, Azure, GCP)
- Multi-identity (AD, Okta, Ping)
- **Identity attacks → How to secure access to data?**

Despite investments in IAM, IGA, PAM, DLP, etc. nobody can answer:
"Who can take what action on your data?"

Identity is the new perimeter:
The fragmentation of cloud data has shifted security to a Zero Trust mindset

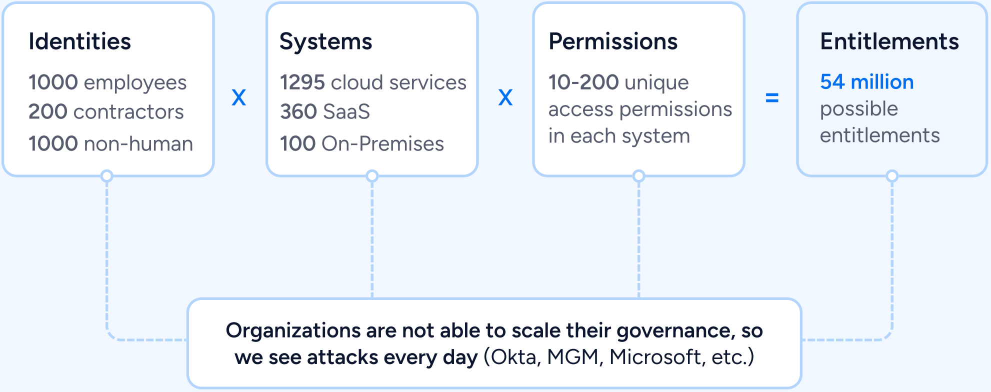
It's clear to see that "identity" is the new perimeter with the widespread adoption of zero-trust architectures. Credential and token theft, MFA workarounds, insider threats, ungoverned processes, and excessive permissions all pose a serious threat to modern-day enterprises. Furthermore, if you go beyond those risk factors, the fundamental business need of assigning and managing employee access to data (across enterprise applications, systems, data, and services) is still fraught with operational inefficiencies. This results in organizations living with an ever-growing enterprise ticket management burden, increased access debt, hampered employee productivity, and increased risk to the organization due to lack of operating identity platforms with the principle of least privilege.



Access is defined by **"permissions"**, **impossible** to manage at scale

Permissions are the "treasure map". Hackers have figured this out. Access needs to be secured.

In 2020, I co-founded Veza based on the insight that organizations are struggling to answer the question, *"who can take what action on what data,"* and, as a result, are ultimately failing to secure access to their data. This insight is paired with the intuition that identity systems are designed for "who are you?" but are incomplete when viewed as a lens for "access". "Access" is identity (user, group) **PLUS** authorization (role, permissions, resources) and this is beyond the scope of what identity systems were designed to do. Identity systems might allow connection to a system, but they do not control what you can then do in that system. We believe that these end permissions and their authorization metadata is the purest form of access and holistically controlling them is fundamental to achieving real security.



Identities
1000 employees
200 contractors
1000 non-human

X

Systems
1295 cloud services
360 SaaS
100 On-Premises

X

Permissions
10-200 unique access permissions in each system

=

Entitlements
54 million possible entitlements

Organizations are not able to scale their governance, so we see attacks every day (Okta, MGM, Microsoft, etc.)

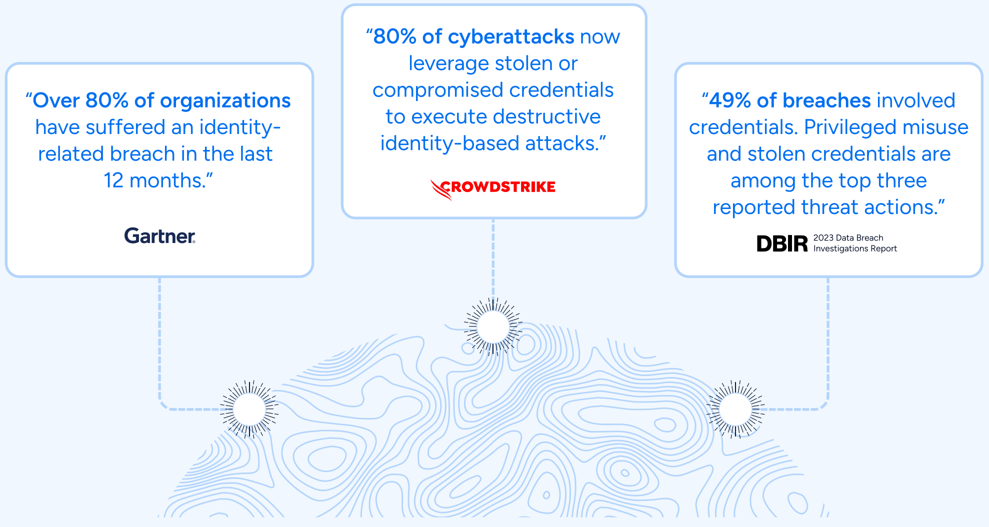
The permissions attack surface is big

With the understanding that all existing identity systems (IAM, IGA, PAM) need a revolution, my co-founders and I took stock of all the existing research and practical approaches as we were founding Veza in March 2020. This research included multiple papers and experiences from the team at Netflix (pioneers of early cloud adoption at an unprecedented scale) - as well as Security Monkey, Aardvark, RepoKid, RiskQuant, Policy Universe, ConsoleMe - and, tracing all these experiences, tools and products led us to Jason Chan! We quickly realized Jason and his team had fundamentally gone beyond the conventional IAM wisdom, and completely embraced identity in the cloud from a ground up perspective for all requirements, including:

- Least privilege access to data
- Machine identity management
- IAM Access
- Service account governance
- Just-in-time (JIT) access
- Role Analytics
- Role Recommendations
- Privilege access management
- and many more...

Jason's team's practical work and research had a deep impact on our thinking as we set out to build Veza with the north star of building the future of access control. Fast forward to 2023: Jason published an article on the modern enterprise identity platform and I finally approached him to share what we have built to gather his feedback. As we spoke and got to know each other, we recognized a deep and mutual belief that the future of identity is here. We agreed that we had a generational opportunity to bring the principle of least privilege to reality by building the modern and next-gen identity platform.

We believe that identity needs a bold second act. Conventional SSO / MFA-based approaches to identity and access management (IAM) are no longer sufficient as organizations operate in an escalating threat environment in which the perimeter has become porous.



"Over 80% of organizations have suffered an identity-related breach in the last 12 months."

Gartner

"80% of cyberattacks now leverage stolen or compromised credentials to execute destructive identity-based attacks."

CROWDSTRIKE

"49% of breaches involved credentials. Privileged misuse and stolen credentials are among the top three reported threat actions."

DBIR 2023 Data Breach Investigations Report

The identity attack surface is urgent priority

Organizations have come to realize the criticality of securing identity infrastructure. In fact, the intense focus on identity at the enterprise level has led some to call 2024 the "Year of Identity." Traditionally, every organization—from small businesses to global, multinational enterprises— has only focused on these three core areas of identity:

1. Identity Store with authentication/federation (Active Directory, Azure AD / Entra ID, Okta, Ping, Duo, etc.)
2. Identity Governance with IGA (Identity Governance and Administration)
3. Identity Privilege with PAM (Privileged Access Management)

However, enterprises are quickly adapting to invest in three new use cases to bolster identity security further:

4. Identity threat detection (ITDR) / identity defense monitoring
5. Identity security posture management (ISPM)
6. Identity for security engineering / security operations

Both the existing and emerging aforementioned use cases fall within the scope of **six critical challenges** that security teams face in today's complex digital environment.

1	2	3
Privileged Access Monitoring	Cloud Entitlement Management	Data System Access
CROWDSTRIKE	zoom	Blackstone
4	**5**	**6**
SaaS Access Security	Next-Gen IGA	Non-Human Identity Management
Expedia	INTUIT	Capital One

In the foreword of this book, we will discuss those challenges and share our vision for overcoming them. The future of identity security relies on companies having the ability to secure access at the speed of business - solving for these pressing cybersecurity challenges is the catalyst to that future world.

Privileged Access Monitoring

Organizations lack the ability to monitor apps and systems for new access that would violate policies. (e.g. local users or admins created by circumventing provisioning/SSO). Even those using traditional Privilege Access Management (PAM) tools don't have a clear picture of privileged access. That's because PAM tools are designed to focus on *documented* privileged accounts. However, as most security professionals know, it's the unexpected privileged accounts that can pose the most risk. Access creep causes a gradual, yet inevitable - and often hidden - accumulation of privileged accounts within an organization. As employees change roles and take on new projects, identities can inadvertently become "privileged" or gain escalated access without ever becoming an *official* "privileged" account, and coming under the management of a traditional PAM tool.

These blindspots are dangerous from both a security and regulatory perspective. Without clear visibility on privileged access, security teams often face regulatory repercussions, including failing audits for being deemed non-compliant. In some cases, organizations find themselves in "SOX Jail" and remain stuck there until they can prove they have handled their material identity weaknesses. These remediations take time and can be incredibly expensive, increasing operational costs while distracting security teams from potential threats.

These threats include insider threats, which can be a dangerous result of ungoverned privileged access. Although every organization would like to trust their staff, insider threats are an unfortunate reality of cybersecurity. Having a bad actor on payroll becomes even more risky when privileged access is involved; the wrong person with the right credentials can do immense damage while remaining undetected.

Privileged access monitoring is critical for staying compliant, reducing risk and preventing identity threats (even from those on the inside).

Security Engineering, SecOps

Goals

Cloud access controls, privileged access, least privilege, enrich SOC, non-human machine identities, service account governance

Products	Systems
Access Search Access Intelligence	Start with key business initiatives (Zero Trust, Cloud Access, SaaS Security)

Identity & Access Management (IAM)

Goals

Next-Gen IGA, IGA enrichment, PAM for the Cloud, Identity Threat Detection, Access Intelligence

Products	Systems
Access Search Access Intelligence Access Reviews	Start with SOX applications, expand to every identity and every systems

How different teams start with Veza

Non-Human Identity Management

“Identity” is often associated with the idea of a human user, however, in today’s cloud-centric environment, this is often not the case. According to Cyberark, there are an average of **45** nonhuman identities for every ***one* human user** in the modern enterprise. This accumulates to a massive amount of nonhuman identities that are hidden in plain sight. Some drivers of this explosion of non-human identities include the following:

1. Every computer instance (including hardware, containers, and virtual machines) is a machine identity;
2. Every application built on modern data systems can map to one or more service accounts;
3. Every AI model is a service account; and
4. Every chatbot is a machine identity.

The list goes on; non-human identities are everywhere. However, identity tools are completely blind to this critical component of modern business operations. Machine identities are not included in identity systems such as Workday, Active Directory, Azure AD and Okta, resulting in a complete oversight of the non-human element. This is the Achilles heel of identity in the modern enterprise. Just as human identities can be susceptible to identity threats, non-human identities suffer from IAM misconfigurations and risky permissions that can leave doors open to attackers and make an organization’s attack surface exponentially bigger.

Data System Access

Governing unstructured data stores, cloud data lakes, and data warehouses (like Snowflake, Redshift and BigQuery) can be extremely difficult and there are not many tools available to lighten the load. Enterprises struggle to identify who has access to what table, and monitor the activity. The nature of unstructured data stores makes them inherently risky. Therefore, ensuring only the right people can read, write, create or delete the data within is critical to modern security posture. However, enterprises are stuck with archaic solutions to try to manage access for these systems: using traditional identity tools that do not provide adequate visibility or - worse yet - resorting to spreadsheets to track and manage permissions.

SaaS Access Security

One of the most important trends of the last couple of decades is the migration to the cloud. That includes not just data and workloads, but also the apps organizations use for business. The model of software as a service (SaaS) is so prevalent now that, according to Gartner, organizations maintain around 125 different SaaS apps on average.

The adoption of SaaS comes with great advantages: employees can work from anywhere without the pain of a VPN and organizations can more easily scale up or down as needed without needing to rack new servers and install software. However, SaaS access can be challenging to manage. As reported by Businesswire, 56% of all apps are considered "Shadow IT", meaning they are owned and managed outside of IT and security teams. Local accounts are also a common reality of SaaS adoption; many team members use their own applications - outside of the company tech stack - to accomplish their work. This dichotomy creates a huge problem for access: there is no source of truth for organizations to see who has access to what SaaS apps (and any sensitive data therein) across the enterprise.

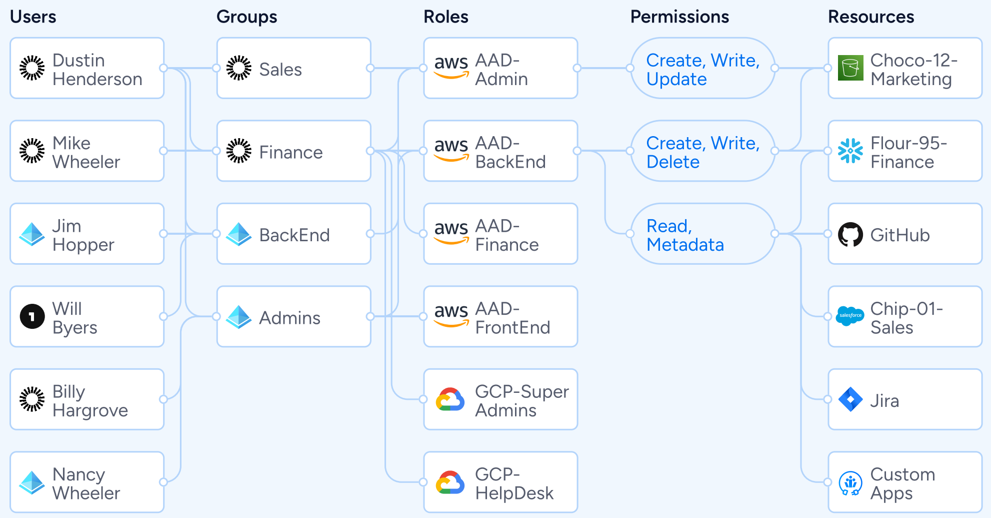
Without the ability to visualize every SaaS app and every associated identity, organizations struggle to:

1. Keep track of permissions across all SaaS applications (Salesforce, GitHub, GitLab, Box, NetSuite....), identities and accounts in real-time, and know exactly who can do what with each
2. Continuously monitor for changes in access to SaaS apps
3. Fix excess privilege, best practice violations and risky misconfigurations as they arise (e.g. lack of MFA), before they become vulnerabilities

Identity Governance and Administration (IGA)

Traditional IGA is fundamentally broken. Organizations desire to approve/reject access at the level of resources, like S3 buckets. However, traditional tools do not enable this level of granularity. Until Veza, has there been no way to effectively automate provisioning and deprovisioning across the joiner-mover-leaver employee lifecycle, and extend this governance to any system including SaaS or custom apps.

This leaves organizations relying on tedious quarterly or annual reviews to manage access. Whether done manually or through vendors like SailPoint or Okta Workflows, access reviews take countless hours to perform and often do not lead to increased security. Reviewers do not have the context they need to effectively make “grant” and “revoke” decisions during the review process and rely on arbitrary group/role names to provision. For example, they may grant “SnowflakeReadOnly” access during an access review cycle, however, security teams have no way to actually validate the permissions granted through that role are, in fact, “read only”. This leaves security teams liable to fail audits or other certifications while potentially leaving doors open to attackers.



Veza Authorization Graph

Every modern enterprise is facing at least one - if not all - of these critical challenges and security teams are desperate for a better way to govern access.

In response to these challenges, Veza has emerged as a beacon of innovation, offering the Access Control Platform to address the evolving landscape of identity threats and bring least privilege within reach at the enterprise level. By leveraging the power of authorization metadata (which we believe to be the purest form of truth of access) Veza enables businesses to visualize, understand and control who has access to what data.

The building blocks of modern enterprise identity

As seen on Bessemer Venture Partners (BVP) Atlas - read the original story on www. bvp.com/atlas/

Jason Chan • *Operative Advisor & Cybersecurity Leader*

The days of the network as a security perimeter are long past. As companies increasingly shift their data and operations to the cloud, they also have to safeguard each access point. With today's distributed workforce, that can look like devices and IP addresses from around the world, software-as-a-service (SaaS) tooling, and bring-your-own-device (BYOD) policies that make it possible to work from personal computers.

Most organizations are in some stage of digital transformation or cloud migration—by 2026, Gartner expects that 75% of organizations will adopt a digital transformation model that relies on cloud, and McKinsey estimates that cloud adoption could generate $3 trillion by 2030 across 2000 of the world's largest companies.

So, if network security is out of fashion for cloud-based enterprises, what takes its place?

As companies increasingly rely on the cloud to operate and store sensitive data, it's imperative that they build a strong identity program, to ensure the right users and devices have secure access to the right files and applications. 80% of cyber attacks today involve an identity-based technique, and these types of compromises can allow an attacker to blend into the target environment like a normal, valid user. By focusing on an identity-first security strategy, today's enterprises can better adapt and be resilient to modern attackers and techniques.

On Atlas, I'll explain the fundamentals of a modern enterprise identity program and how any founder or security leader can start building one for their business.

What is enterprise identity?

Identities represent the different touchpoints to your organization's technology—think users, devices, applications, and other systems. Enterprise identity, then, is the overall process for managing and providing these entities with access to the resources across your environment.

When considering your overall enterprise identity architecture, you'll want to build a strategy that touches on three main dimensions: the different types of identities, the identity lifecycle, and identity governance and administration.

1

Identity types: Identities can map to humans, devices, and software.

- → Human identities consist of your workforce—full-time employees and contractors—and consultants. We'll focus on human identities in this article, but many of the concepts are broadly applicable to all identity types.
- → Device identities cover machines, like laptops, servers, or mobile phones, whether physical, virtualized, or containerized.
- → Non-human and software identities cover service accounts, API keys, applications and services (often represented by certificates), and shared administrative accounts.

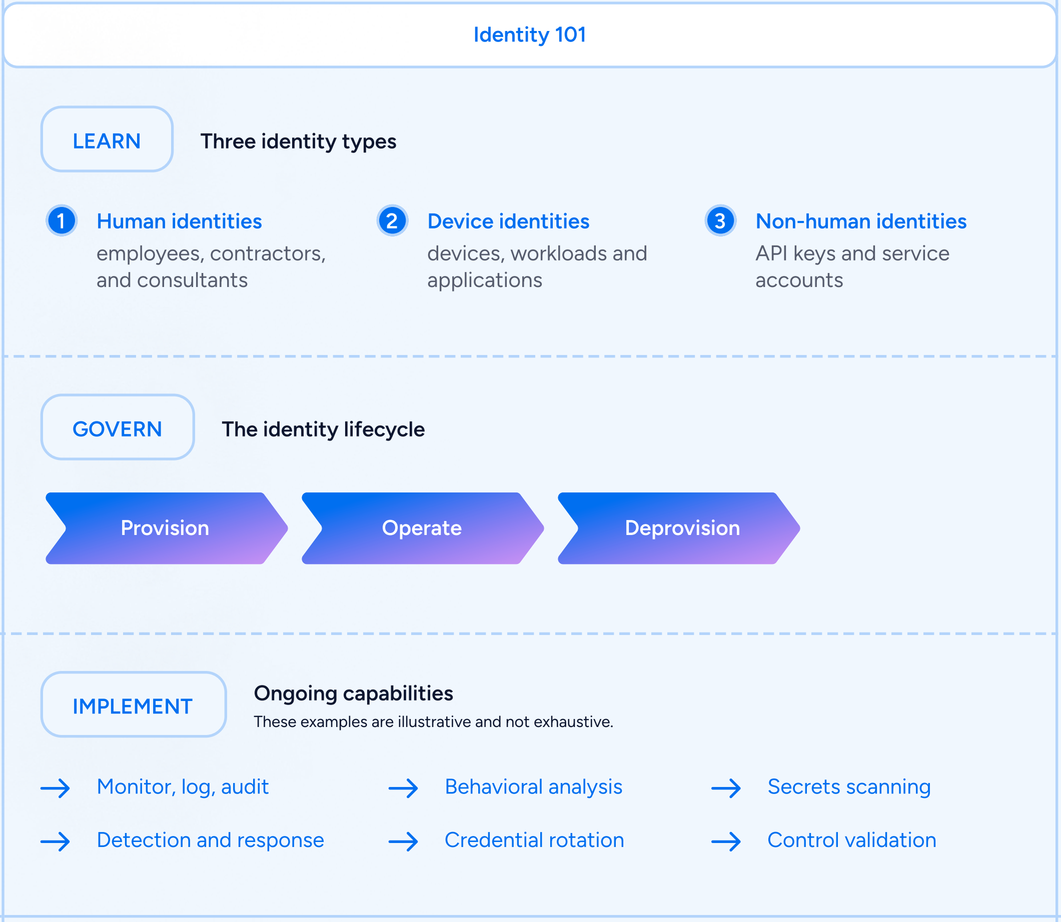
2

Identity lifecycle refers to the beginning, middle, and end of a digital identity—its creation, ongoing operation and management, and deprovisioning, which is the process of removing user, device, or software access to company data.

3

Identity governance and administration refers to the set of tools, processes, and teams managing the identity lifecycle and will reflect an organization's culture, risk tolerance, compliance, and regulatory obligations. A robust identity program is always active: for employees, from onboarding through offboarding; and for devices and software, during replacements and migrations; and for all identity types, ongoing monitoring and analytics reporting.

The interplay of these dimensions is captured in the following infographic:



Identity 101

LEARN — Three identity types

1. **Human identities** employees, contractors, and consultants
2. **Device identities** devices, workloads and applications
3. **Non-human identities** API keys and service accounts

GOVERN — The identity lifecycle

Provision → Operate → Deprovision

IMPLEMENT — Ongoing capabilities

These examples are illustrative and not exhaustive.

- → Monitor, log, audit
- → Detection and response
- → Behavioral analysis
- → Credential rotation
- → Secrets scanning
- → Control validation

Why should companies modernize their enterprise identity approach?

The old way in enterprise security was to trust all users and devices inside a network, as long as they passed an initial checkpoint or two—much like passport control, or having a ticket and ID in hand to enter a concert venue. But today's enterprises have far more than a single point of entry. As much as 98% of enterprises using public cloud services have adopted a multi-cloud strategy, meaning they already use or plan to use at least two cloud infrastructure providers. In addition to infrastructure, most enterprises use dozens or hundreds of different SaaS applications.

Cloud infrastructure and SaaS adoption lets companies innovate and implement new capabilities quickly, but it also presents a host of new security concerns that growing enterprises have to proactively address.

There are four main reasons why you should rethink your enterprise identity approach and make it more current:

1

To support the realities of modern technology and hybrid working environments. In today's remote-friendly workforce, it's possible to work from anywhere and any device, using SaaS applications that are nearly ubiquitous. A strong enterprise identity program supports the full spectrum of work setups, ensuring employees can access applications wherever they may be—from a company's headquarters (HQ) office, hybrid setups, or fully remote engagements. Even organizations that prefer to maintain an in-office culture will encounter identity challenges, whether it's ensuring a sick employee can work from home or that a tech support contractor can remotely access one of your user's desktops.

2

To improve the end-user experience. A modernized identity architecture makes access to your company's data not only safer but also simpler for your employees and users—any opportunity to improve in both security and user experience is a win-win for security teams and end users.

3

To safeguard from the latest security threats. Today's threats and attackers are focusing on identity, by stealing sessions, phishing for credentials, going after multi-factor authentication (MFA), SIM swapping, and attacking single sign-on (SSO). With the wrong permissions in place, attackers can create and destroy cloud environments with simple API calls, too.

4

To enable the shift toward zero trust. Through Executive Order 14028 in May 2021, President Biden directed U.S. federal agencies to adopt zero trust cybersecurity principles. And, many companies are well on their way to zero trust architectures. Zero trust principles state that no user or device should automatically be trusted since there are potential attackers inside and outside of every network. Zero trust adopters require identities to be continuously re-verified whenever resources are accessed.

What are the different stages of enterprise identity modernization?

Any investment you make in your identity program is a step forward. But given how many facets there are to enterprise identity architecture, it can be difficult to determine the right sequence of priorities. Like any other security investment, there is a logical progression to identity investment—it's important to lay the groundwork with baseline functions and capabilities, and from there, as your company matures, those programs will scale, too.

To help frame the journey, it's helpful to think about a spectrum of features that map to a maturity curve. Just like a growing plant, I recommend thinking about identity modernization in three key development phases—Seed, Sprout, and Bloom. First you'll form your identity program, then you'll help it grow, and finally you'll support its maturity. While this approach doesn't include all possible identity functions, it's intended to provide a usable model for planning and implementing an enterprise identity strategy.

We'll look at this maturity curve and implementation progression using a Seed (forming), Sprout (progressing), and Bloom (advanced) framework.

Seed
Building foundations

- Identity provisioning via HRIS
- Centralize to a single identity provider (IdP)
- Inventory your resources--SaaS apps, cloud infra, data stores, etc.

Sprout
Refining operations

- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Manage identities through privileged access management (PAM)
- Centralize access requests

Bloom
Maximize capabilities

- Continuous and conditional access
- Detection and response
- Self-service access grants
- Centralize permissions
- Passwordless experience via biometrics, passkeys

Stages of enterprise identity modernization

Seed

The main directive of the Seed phase is to build the foundations of your identity program—the elements upon which you'll build and refine. Key Seed phase activities include:

- → Integrating your HRIS with your identity infrastructure—to support automated provisioning of identities as employees and contractors are onboarded and deprovisioning when they are offboarded.
- → Centralizing your identity store to a single identity provider (IdP)—that serves as the source of truth for workforce identities. This process can begin with identifying any identity silos that will require migration.
- → Gathering context on the resources your workforce accesses—such as SaaS applications, cloud infrastructure, data stores, and custom applications. Having an inventory of resources cross-referenced by the teams that use them will be helpful as you're building out your identity program.

Sprout

Once your identity program's foundations are in place, it's time to refine your program operations, strengthen security measures, and make identity a focal point of your company's integrated security strategy. Key Sprout phase priorities include:

- Enabling ubiquitous single-sign on (SSO) across all assets. SSO simplifies your workforce's access experience and improves security by eliminating identity silos and disparate credentials.
- Enforcing multi-factor authentication (MFA). MFA provides additional protection against the risk associated with compromised credentials. Note there are varying levels of MFA strength and you can adjust as your needs and capabilities change—for instance, SMS or text message-based MFA is weaker than the FIDO2 standard, which encompasses passwordless authentication methods, like Apple Touch ID and Face ID.
- Managing shared and privileged identities through secrets management and privileged access management (PAM). Some identities have higher value and are used by multiple parties, and these functions allow you to more securely and efficiently support these types of identities and access.
- Centralizing requests and reviews for access to enterprise resources. Efficiently managing changing access needs is key to providing a positive workforce experience with security and ensuring that access isn't unnecessarily overprovisioned and that your compliance obligations are met.
- Deploying password managers to improve password hygiene across the enterprise.

Bloom

As your company matures, so does your identity program. In the Bloom phase, it's time to maximize and mature your identity investments and capabilities. When in this phase, you will leverage identity data for a variety of purposes, and your workforce's experience with your identity systems should be increasingly sophisticated and user-friendly. Key Bloom phase agenda items include:

- Supporting continuous and conditional access control to improve security and support zero trust. When a mature organization's systems makes authentication and authorization decisions, they can leverage multiple signals, including access time and location, whether the device is actively in use, and historical device activity. And if your team identifies a "yellow light" before moving ahead with authorization, you can implement capabilities such as step-up authentication or other mechanisms for demonstrating identity proof.
- Leveraging identity logs and data to support detection and response efforts, including more sophisticated use cases such as anomaly detection and behavioral analytics. These capabilities can help identify a variety of issues from compromised identities to insider threats to overprovisioned access.

- Automating and centralizing identity-related evidence and data to support audits and investigations.
- Providing automated, self-service access requests and grants to enterprise resources. You understand the systems, applications, and data your workforce needs access to and are able to provide it as needed on day one of an employee or contractor's hire, as their role changes, or as business needs require.
- Enabling least privilege and just in time (JIT) access across the environment to ensure users have only the access they need and that overprovisioned access does not contribute to security issues. Additionally, having finely tuned permissions aligned with least privilege provides the foundation for high-fidelity signals for detection and response.
- Providing a passwordless experience via passkeys, biometrics, or other means can significantly improve your user experience and provide impactful resistance against phishing and other attacks on credentials. While passkey support is not yet ubiquitous, some online services, browsers, and password managers have implemented support and the coming years are sure to see much broader compatibility.
- Centralizing permissions and entitlements by providing a single means for expressing, configuring, and granting permissions across enterprise assets, whether in the cloud or on-premise.

Focus on transitions over total transformation

Just like the Seed, Sprout, and Bloom phases, it's important to break down any cybersecurity modernization project into incremental stages—this implementation structure helps make the changes more concrete and approachable, and each individual action contributes to a long-term strategy. For example, as a founder or CISO, you might plan on first making a few tactical shifts as your organization commits to enterprise identity modernization.

These transitions could look like going from:

1. Siloed to centralized identities.
2. Username and password based authentication to MFA.
3. SMS-based MFA to stronger, phish-resistant MFA.
4. Local identities to SSO.
5. Distributed and unknown identities to maintaining an inventory.

Finally, you might consider building an identity strategy around specific workflows in your employees' lifecycles and day-to-day responsibilities. For instance, you can focus on all the identity needs around employee onboarding and offboarding, and when and how to grant access to sensitive assets.

There's no reaching enlightenment in the world of cybersecurity—there's too much risk to mitigate and change to navigate, and even the largest enterprises know that. So, while it can seem daunting to think about developing a modern, enterprise-grade identity program, remember that it's a process: it doesn't have to all happen at once.

l happen at once.

Meet the Authors

A serial entrepreneur, Tarun Thakur is a Co-Founder & CEO of Veza, the identity security company. Tarun co-founded Veza in 2020 to address one of the toughest issues in enterprise security today: who can take what action on what data. Veza has established a robust customer base consisting of Fortune 500 and global enterprises like Intuit, Blackstone, Wynn Resorts, Sallie Mae, KKR, Expedia, Crowdstrike, and many more. Veza has raised $120M+ in venture financing from leading firms such as Accel, Google Ventures, Norwest, True Ventures, and Ballistic Ventures.

Prior to Veza, Tarun was Founder/CEO of Datos IO, and has extensive B2B SaaS experience at companies including IBM Research, Symantec, Data Domain (acq. EMC), and others. Tarun graduated from Duke University with his MBA in Strategy and Marketing. Tarun holds 20+ patents in various fields of distributed systems, security, and next-gen storage and compute architecture.

Tarun Thakur
Co-Founder & CEO, Veza

Jason Chan is an operating advisor at Bessemer Venture Partners where he brings over twenty years of experience in cybersecurity and is especially passionate about large-scale systems, cloud security, and improving security in modern software development practices.

Most recently, Jason built and led the information security team at Netflix for over a decade. His team at Netflix was known for its contributions to the security community, including over 30 open-source security releases and dozens of conference presentations. He also previously led the security team at VMware and spent most of his earlier career in security consulting.

Jason enjoys coaching, mentoring, and helping folks from underrepresented groups enter and advance in the cybersecurity industry. Outside of work, he enjoys reading, running ultramarathons, and volunteering in habitat restoration, trail maintenance, and wildfire management. He received a BS from the College of Charleston and his MS from Boston University.

Jason Chan
Operating Advisor &
Cybersecurity Leader

veza®

The Identity Security Company