The Technical Manager’s Guide to Zero Trust: Identity

March 09, 2023

Cybersecurity Research Analyst

Alex is a cyber security research analyst at Stratascale. His background in both research and practical security gives him a unique perspective on providing security with a risk-based approach. He focuses his expertise on emerging technologies, data-driven IT strategy, and tactical solutions to large security problems.

Submitted by Alex Banghart on 9, Mar 2023

The Technical Manager’s Guide to Zero Trust: Identity

Zero trust (ZT) rests on the six pillars of identity, data, applications, network, devices and infrastructure. All pillars contribute to success with ZT, but identity, as one of the “bookend” pillars, is one of the most critical pieces to establishing a ZT strategy. Organizations must correctly define, manage, and map identities in order to succeed with their Zero Trust programs. .

Identity management programs are evolving. With the old approach, an organization would have one siloed identity for each use (e.g. customers in CRM; applicants in HRIS; suppliers’ employees in ERP; employees in active directory; on premises machines/devices in ServiceNow; cloud services and resources in AWS). In the modern approach, the organization abandons this siloed methodology, and instead develops holistic identity personas.

These holistic identity personas merge together multiple different identities, providing organizations with a more accurate representation of how users are working and what specific data and access rights they need. An effective zero trust identity management program requires this centralized view into identity.

Technical managers responsible for ZT identity management play a crucial role in advancing their organizations’ zero trust strategies. But it’s important for them to realize that they own the identity program—how identity functions—rather than the identities themselves. To support a successful program, they will need to implement effective integration strategies between platforms, and design a system that captures the relationships between personas. ZT identity program managers will focus on the following key objectives:

- Set up an integrated identity platform.
- Eliminate multiple identity silos.
- Enable interoperability.
- Enable safe access to legacy systems.

ZT identity program managers face no easy task. But they can smooth their path to zero trust by ensuring they tackle a few critical success factors:

- Obtaining buy-in from stakeholders.
- Building a plan for the end state, while including an incremental approach.
- Conducting accurate and comprehensive data mapping.
- Taking a continuous approach to applying and removing privileges.

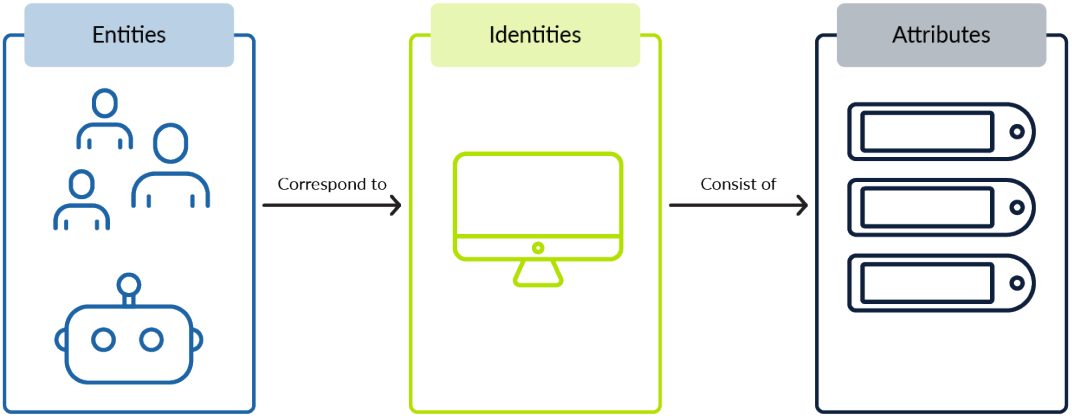
Defining Identity

Stratascale defines identity as:

> a set of identifiable attributes by which an entity (human or non human) can be distinguished from any other entity.

In other words, organizations create and manage identities—sets of containers for attributes—in order to answer the question “what entity is this, and what level of access should this entity be granted?” An entity can have multiple identities that allow them different access permissions depending on need.

The diagram below shows the relationship between entities, identities, and attributes.



Source: Stratascale 2023

Identity as the Core of Zero Trust

Identity forms the core of zero trust programs for two reasons. First, identities are how organizations implement controls that grant access to the entities that are supposed to have access to data and resources, and deny access to entities which should not have access.

Second, most successful attacks begin by targeting identities: “typically the initial attack vector comes through an identity because of compromised credentials,” observed a contributor.

To be effective, therefore, a zero trust identity program must both determine the right sets of attributes for the entities and the personas, and have a plan for securing the attributes themselves.

Drivers of ZT Interest and Investment in Identity Management

Investment drivers for ZT identity include business drivers and technical drivers.

On the business side, over the past few years the impact of successful attacks has continued to increase, with severe damages including impact on revenue, impact on reputation, legal costs and damages, and regulatory fines. All while cyberinsurance, which used to be a cheap and accessible protection against such risks, has become in many cases prohibitively expensive or unattainable.

On the technology side, many organizations have realized that they no longer even have visibility—let alone control—over the exponential growth in identities driven by the rise of corporate cloud resources, shadow IT, and bring-your-own-device (BYOD).

One contributor described this technological shift in identities as moving from “a herd of cattle that they were trying to wrangle” to a “swarm of locust.” Once identities get out of control, they can start to look like the picture below:

Photo by James Wainscoat on Unsplash

The problem isn't just the number of identities—it's the fact that they are constantly changing and shifting, often with no way to gate the creation of new identities (e.g. an employee connecting with a new device, in a BYOD context).

Getting a Handle on ZT Identity: Policy Decision Points and Policy Enforcement Points

Clearly, gating the creation of new identities has become impossible in the current technology environment. But ZT identity teams can control the swarm by creating a single source of truth for identities and leveraging policy decision points (PDP) and policy enforcement points (PEP) in access decisions.

In the zero trust model, the telemetry data used in PDP and PEP become part of the "set of identifiable attributes" used to distinguish an entity. In other words, telemetry becomes part of the identity itself. The inclusion of telemetry into identity is a core component of effective zero trust controls, and constitutes a significant shift in mindset.

There isn't a one-size-fits-all approach for PDP and PEP—these will vary based on the business and technology contexts. But designing effective PDP and PEP will be important for every organization's success with ZT. ZT identity managers may consider the following telemetry signals as components of each PDP:

- What network is the entity on?

- Where is the entity’s device located?
- What biometrics (if any) has the entity provided?
- What data is the entity trying to access?
- What is the classification of both user/data?
- What is the device’s posture?
- Does the device meet our minimum-security standards?
- Should the entity have access to this data in a foreign country?
- Should we provide access to this BYOD device?

Takeaway: Identity forms the lynchpin of an effective ZT program. Implementing PDP and PEP requires incorporating telemetry into identity. When done effectively, a ZT identity program can support elements such as cloud resources and BYOD in a frictionless way, allowing security to be an enabler rather than the “office of ‘no.’”

Key Priorities for Zero Trust Identity

Tackling a ZT identity program may seem overwhelming. Stratascale SMEs identified four key priorities for ZT identity managers to focus on:

1. Integrated identity platform.
2. Elimination of multiple identity silos.
3. Interoperability.
4. Safe legacy access.

In the rest of this section, we’ll unpack each of these top priorities.

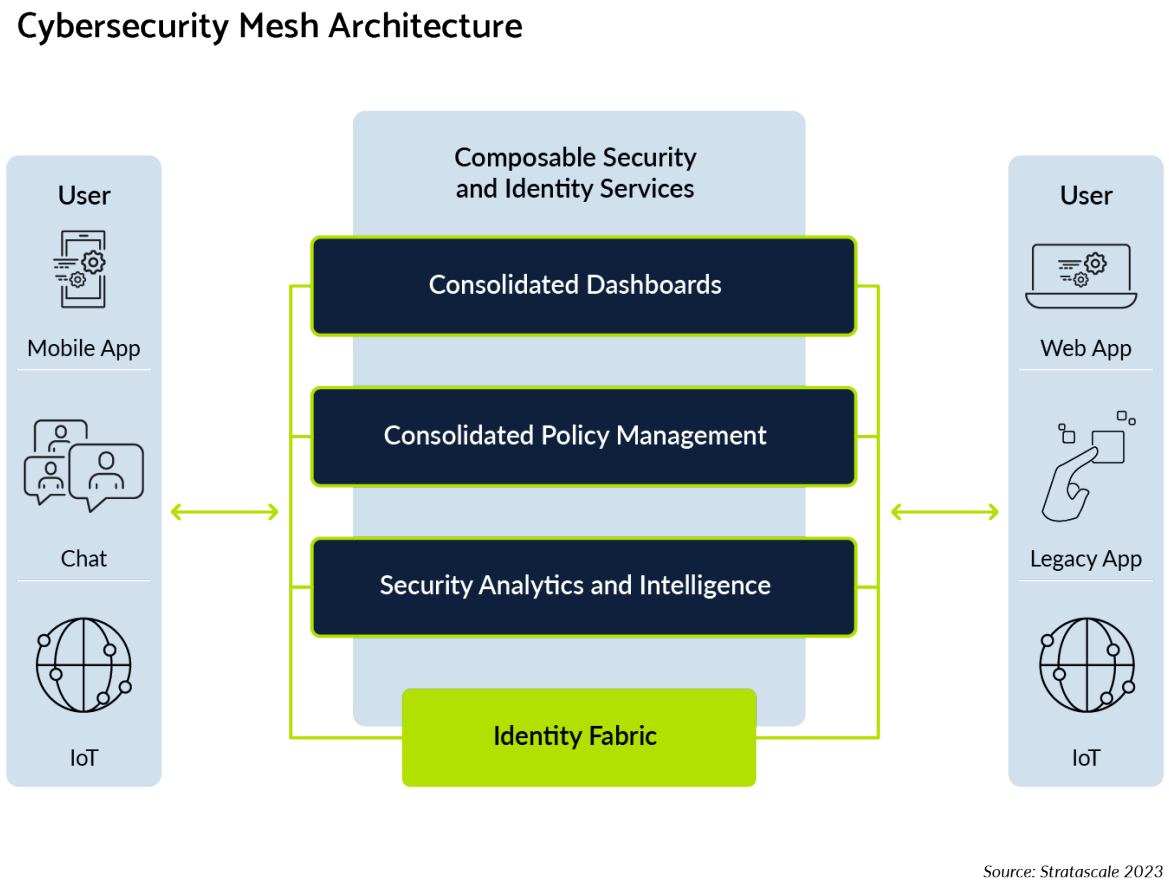
1. Integrated Identity Platform

The integrated identity platform provides central visibility into identities and allows the application of policies such as PDP and PEP to all access decisions. The identity platform must do the following:

- Service inbound access requests.
- Service outbound requests.
- Transfer information about identities to the other tools within your environment.
- Enable an identity fabric and cybersecurity mesh.
- Take queries from systems about users, and respond back with details, data, and attributes about the user.

- Consume data from a broad swatch of endpoints and systems, and the systems and signals from those settings.

ZT identity managers should avoid falling into the trap of trying to patch together different platforms to serve this purpose: a contributor mentions, “If you're IEM platform’s trying to make a decision, it can't pull in data from an MDM, an XDR platform, or anything like that. If I architected it that way, I’d be back to 15 pans. I can’t do it. It's just not feasible or truly manageable.”



Source: Stratascale 2023

2. Elimination of Multiple Identity Silos

Eliminating identity silos as a key priority for implementing a ZT Identity management plan. The more platforms attempt to integrate into your ZT infrastructure, the more challenging it will become to manage your identities effectively.

With legacy identity management platforms, companies have been able to consolidate their platforms into one central location. But with the “shift-right” to the cloud there’s been a resurgence in identity sprawl, resulting in an increased threat density for present-day architectures. As federations come from all different places, the amount of threat vectors.

Our experts observed,

“It's not unusual for organizations to have two or three federation platforms inside their infrastructure and a lot of them are leveraging legacy Active Directory Federation Services. Still today we've talked to multiple organizations that are leveraging legacy federation tools to handle that, and they are heavy handed. They're not out of the box, they're not well patched. They have a lot of pieces of infrastructure. So moving to that central identity, modern identity platform gives them the capability to start meeting the needs of a ZT framework.”

3. Interoperability

A platform is worth nothing without the ability for authentication and authorization interoperability throughout your environment. Rather than focusing on best of breed, it becomes more useful to consider best of integration.

A contributor pointed out the importance of “understanding the limitations of the authentication and authorization within your environment as relates to your apps, and knowing how that platform **interoperates** and **integrates** across the board, at both the privileged level and the nonprivileged level at the same time, because you will have users who need privileged access to local devices and users who may need privileged access to applications.”

Our discussion on interoperability led to the key takeaway:

> We are great at giving access, we’re very bad at taking it away.

To manage identity spawl effectively and reduce the risk of outdated identities, ZT identity managers must integrate onboarding and offboarding into identity governance, which requires two-way communication between the integrated identity platform and HR systems.

ZT identity managers also need to reduce identity sprawl from SaaS applications. To remain competitive, modern-day SaaS applications now accept multiple identity providers from a single organization, enabling poor identity hygiene on the part of their enterprise customers. Getting a handle on SaaS identity sprawl by using an interoperable platform is a key step in establishing a ZT Identity program.

4. Safe Legacy Access

Many Fortune 1000 organizations have legacy applications that neither have nor will migrate to new platforms. Modern identity platforms are capable of stepping in where MFA isn't supported or isn't supported well. Identity platforms can become the decision platform for access to older applications to ensure it is done safely by using other forms of telemetry to make informed access decisions.

Zero trust identity managers must take stock of their legacy systems, and must ensure that their modern identity platform supports their authentication requirements.

Defining the path to ZT Identity

Each document in the Technical Manager's Guide to Zero Trust series incorporates a roadmap providing practical guidance to readers looking to implement ZT within their areas. The advice offered by contributors to this document addresses 4 important steps:

1. Articulate the value of shifting to ZT over perimeter-based security.
2. Get key stakeholder buy-in.
3. Map your data flows.
4. Align tools with the ZT framework.

In the rest of this section, we unpack each of these steps.

1. Articulate the value of shifting to ZT over perimeter-based security

This first step is understanding that zero trust is "not a tool" "not a technology" but rather "that paradigm shift from our security framework which used to be perimeterized security." With changes in technology environments such as remote work and SaaS, perimeter defenses such as firewalls have become obsolete. Entities and access requests can come from anywhere, so ZT controls focus on which

identity is accessing what thing, rather than trying to fortify a perimeter that surrounds ‘known good’ entities. The shift to ZT helps security evolve from the “office of no” to a service-oriented team focused on enabling the business to achieve its goals. Stratascale SMEs suggest the mantra:

> We need to be an enabler, not a roadblock.

When done right, ZT allows the security team to change that mindset from “no” to “yes but,” and to keep in mind that their true function is to “enable the business to make money,” “add value,” and “become better at what they're doing, and how they deliver customer experience, a product or whatever their value proposition may be.”

2. Get key stakeholder buy-in

In the old perimeter-based model, security controlled all the traffic by fiat. As a contributor described, “In the old days somebody might tell him to open something up, and the security guy would say something baffling about SOCKS and ports and inbound versus outbound and established connections versus, you know, outbound connections and all those fun things and baffle them with his brilliance. And they'd go, ‘oh, OK, we can't do that now.’”

Now that the perimeter is obsolete, with employees able to access SaaS applications using BYOD, ZT managers must collaborate with stakeholders to define effective controls for PDPs and PEPs. Security, application, and business leaders should ask questions such as:

- Where is the data?
- What is the context of the access?
- Why do certain people or roles have the access they do?
- How long will the entity have the access?
- Should the entity even have the access?

ZT identity managers need to interface effectively with stakeholders not only to define the controls, but also to drive the cultural shift within the business. The business must embrace the change in order for the program to be successful. One contributor advises,

“Zero trust needs to be framed in a way that it's going to be less friction on business users and it's going to enable them more. That's really the end goal of securing and protecting the business: being able to make the business more adaptable.”

3. Map your data flows

Organizations must have an understanding of their data flows in order to run an effective ZT identity program: the data flows underpin effective PDPs and PEPs. In the words of a contributor, “If you don’t know your device or your service, if you don’t know that inventory, it’s going to be difficult for you to protect it.”

So ZT identity managers must start with a data and application inventory in order to build out an understanding of those flows. They should consider questions such as the following:

- What entity is accessing what data?
- Does the entity need to access that data?
- Who is the data owner?
- Which entities really need access, based on roles and responsibilities?
- Does each entity need access all the time, or can just-in-time access work?

Sensible PDPs and PEPs, which assess the validity of each and every access request at the time it’s made, protect the organization from the risk posed by excessively granted privileges—for example, “role collector” employees being able to collect permanent access to a wide variety of systems as they move from job to job, each time being granted additional access privileges but never having the no-longer-needed earlier access privileges revoked.

ZT managers face a lot of work in tackling data flow mapping, but this work will pay off, because the understanding of how their data moves and how identities relate to the data will form the core of their ZT program.

Given the size and complexity of enterprise environments, the project team will likely want to leverage automated tools and/or third-party services when undertaking data flow mapping. In doing so, they should remain aware of the importance of pairing automated discovery with a sound understanding of the business context.

Only by combining data flows with a sound understanding of the entities' functions within the environment can ZT identity managers implement a central point of visibility where privileges can be handed out and taken away automatically based on roles, access requirements, and telemetry data.

As our SME points out, "if you don't know your identities, you don't know your applications, you don't know your data, you don't know how to properly define your privileges, and you can't implement that principle of least privilege model."

4. Align tools with the ZT framework

ZT identity managers should begin by articulating requirements based on the ZT framework, and then evaluate tools within that context.

As one contributor put it, "Not every tool is suited for ZT," so identity managers need to consider whether any given tool is "the right tool for a ZT framework," taking into account considerations such as "best of integration versus best of capability." Finding out that your existing tools have shortcomings might prove frustrating, but identity managers should think pragmatically. As the contributor points out, integration is crucial "because if I've got a tool but can't get the signals out of it, it does me no good."

Three ZT identity roadblocks and challenges

As one might expect with such a great change in a large enterprise, identity managers will encounter significant challenges as they pursue their ZT journey. Stratascale SMEs who contributed to this document identified three roadblocks that could impede progress for identity program managers:

1. Focusing on best of breed rather than best of integration.

In many enterprises, the traditional approach to technology acquisition was to buy best of breed. This approach worked when fine in the perimeter-based security model: each tool performed its discreet function handled by a siloed team.

But in the ZT world, integration is king. Enterprises can't buy one magic tool to do it, so they'll naturally need to rely on integration to develop a system that allows for the "one pane of glass" view necessary for the real-time visibility and actions required to investigate incidents and respond to threats. Take this example from a

Stratascale SME:

“Let’s say I have the best MDM platform, but due to the lack of integration I can't reach over and do some automation on an isolated device when I see something unusual is going on. A user may be doing something over there that I don't like, but that platform's closed. Now I've got to open a helpdesk ticket and wait for somebody else to do it. By the time somebody gets to it . . . my data is already out the door.”

To succeed with ZT, the organization needs to break down these siloes, putting automation and self-service in the place of ticket queues. Putting in place a system of controls requires the single pane of glass that can only be achieved by favoring a best of integration over a best of breed approach.

2. Turf wars over legacy systems.

In many large enterprises, programs, platforms, and processes have historically been written, managed, and maintained by small, siloed teams. In many cases, these groups have tried to appear indispensable by making their programs a type of “voodoo” and engaging in turf wars to protect their silo.

A contributing SME described a scenario he has encountered when trying to understand a legacy system: “we have to ask Mary about that program, because Mary owns that, and she’s not very cooperative. That’s her platform—she’s built and she’s run it for 13 years, so we’ll have to see if we can get her to talk to you about this. You’re being held hostage by this.”

As the SME points out, the most difficult aspect of this roadblock isn’t the technology of the legacy system, but rather the organizational culture that has encouraged teams to build such silos, and the resistance to collaboration and knowledge-sharing: “You have legacy processes tied to legacy thought patterns to legacy systems.”

ZT project teams will want to educate stakeholders, ensuring that they’re forewarned of the pain that will come with the transition, and that stakeholders understand that securing identities may mean that some people may not have access to everything all the time.

Being able to step back and change that mindset and being willing to accept the challenges along the way is critical to succeeding with ZT integration.

3. Trying to steer rather than support.

Security leaders and managers might be tempted to think that they “own” ZT, and try to steer the program based to where *they* think it should go. That’s a trap. A successful ZT Identity implementation allows security to be like “the tires on the Formula One car of the business. Allow that thing to go 100 miles an hour and take tight turns.” The business should be steering the car: security needs to define policies, define the guardrails, and allow teams to act quickly and securely protect the business. But security always needs to shape the ZT program with the aim of enabling safe and speedy progress in the direction the business is trying to go.

Photo by Patrick Robert Doyle on Unsplash

Important ZT Identity technologies and management imperatives

As part of its *Executive Guide to Zero Trust* research series, Stratascale published the report, Key Zero Trust Technologies and Management Imperatives. The ZT identity section of this report highlights the following technologies or practices that managers should understand as they plot their ZT identity strategies:

Continuous strong authentication

This category might come with a “start here!” sticker. Zero standing privileges (ZSP)/just-in-time (JIT) access represents a compelling immediate priority for CISOs pressured to show immediate progress. Moving to ZSP/JIT access from more basic privilege access management (PAM) tools aligns identity with ZT objectives by removing “admin user” privileges from the identity equation. Admin users exist only when they are needed and are temporarily created for a specific purpose. Eliminating standing admin users addresses a key source of identity-related risk.

Passwordless

The chart illustrating a sample ZT implementation plan shows Passwordless as a second-stage identity technology, with rollout targeted for many months after completion of the ZSP deployment. However, this doesn’t mean that passwordless is unimportant to zero trust success. One CISO contributing to this document is focused on passwordless because it is important to “that frictionless access culture,” “meeting users where they live,” and building identity and security on technologies, such as smartphone biometrics, which users employ in other areas of their lives.[2]

Risk-based access and authorization policies

Adaptive and conditional risk-based access policies address a critical issue in cybersecurity: what do you do to mitigate exposure in the event that a device (or user) is compromised while they are accessing a sensitive resource? Adaptive, conditional access helps to identify scenarios where this may have occurred and restricts access and authorization unless and until it is possible to re-establish trust in the user or device.

Device identities

Despite the name, device identities fit within the identity pillar rather than the device pillar. Security teams need to establish threat and posture management on devices – particularly as those devices move away from 1:1 connections with human users. Clearly, threat and posture management is important for IoT devices. But implementing device identities extends to firms that have not deployed IoT. Servers, for example, access sensitive resources as a matter of course, and these connections, too, need to be monitored as part of ZT identity.

This is a difficult area to address. One Stratascale SME observed that “everybody is horrible at device identities” and added that “most organizations aren’t anywhere near” a point where they can “get their hands around machine identities.” Although this is an important objective, if the security team can’t identify devices that are accessing resources, they can’t make good risk-based decisions on whether any given access request should be allowed or whether it represents an emerging threat within the corporate environment.

Other ZT identity considerations

Additional considerations around identity surfaced during discussions with our thought leadership group, including:

- “Moving toward a B2C infrastructure for our multi-factor authentication MFA platform.”
    - This CISO stated that as the security team opens up the MFA platform to third parties, “people in our business get very nervous. We have supply chain partners and trying to move them onto a different kind of credential store makes *them* nervous. But then you walk them through how much easier it is to register” if you apply an intelligent help function that can lead users the process. This provides a resource-efficient means of safely connecting external users to corporate assets.
        - This discussion speaks to agility gains that can be realized through implementation of better technology: in this case, identity, but the concept could apply to any other ZT pillar. In a broader context, this example argues for a need to layer in capabilities incrementally. A “big splash” might improve capabilities in one area but create issues for current or future systems in another. An important part of ZT is

the ability to align new capabilities within a comprehensive framework.

- Bring your own identity (BYOI)
  - BYOI can enable “differentiated access to corporate systems…segmentation that differentiates between external users supply chain partners accessing systems via BYOI – which uses externally managed identities and internal users with corporate credentials.”
    - BYOI offers security leaders two primary benefits. One is that it transfers the effort associated with identity maintenance outside the organization, reducing staff commitments. The other, stated in the quote, is that BYOI access provides an inherent basis for segmentation, allowing the security team to identify external users accessing corporate systems and assign them appropriate access and authorization.
  - Incremental, non-binary identity signals
    - One thought leadership group member urged security teams to use multiple methods to reaffirm identity on an ongoing basis. By assessing the user’s context as it changes, the argument holds that it is possible to use “non-obnoxious methods” to monitor user sessions. The goal is to capitalize on approaches that are “silent or easy to do with biometrics on device or other options to refresh.” If a session ends because the user logged out or timed out, “you can reauthorize, but you don't have to impose the same authorization method(s) – if they're just doing something read-only versus read/write or whatever it is, you could just apply complementary, potentially unintrusive methods as much as you want.”
      - This sounds amorphous, but there is a great deal of potential in this notion of regular reification of identity via non-obtrusive telemetry or other inputs, as compared with highly intrusive requests for passwords or similar means.

ZT Identity recommendations

At the end of the research discussion, contributing SMEs were asked to propose recommendations that will help Stratascale client managers succeed in establishing

ZT identity security. These recommendations include:

1. Don’t confuse identities with entities.

It’s natural for us to think of an identity as having a one-to-one relationship with a certain entity. But ZT identity managers need to remember that identities are **not** entities, but rather those sets of attributes we use to distinguish those entities (see the definition above).

When we keep this in mind, getting a true handle on identity means not just thinking about humans listed in the directory, but also keeping in mind all the identity silos, where they come from and where those attributes are. So rather than thinking about just Sarah, we should be thinking about Sarah’s AD, Sarah’s HR login. An identity isn’t just Sarah, its Sarah’s iPhone. It’s app XYZ.

2. Consider all the attributes as equal components of each identity.

A Stratascale SME described this thought process as follows: “Stop thinking of identities as individuals. Think of identities as personas of things that are accessing your data and your resources. Understand where your identities live and how they're made up, because you're pulling data from all over the place about not only your user, but also about applications and devices. So, understand where those details live and then understand that it's not just about your user as a person, it's about your identities human and non-human.”

3. Account for the distributed ownership of identity.

ZT identity managers do not own identity. Rather, they own how identity *functions* As a SME point out: “You only own the functioning of identity. Identity is owned by different pieces of the organization. The identity of the individual and the apps. Some of it's the app team, some of it's the database teams, some of it's the dev team, some of it's the business team making decisions on what that app needs to have access to, when and how and why. So, there are different owners of identities. It's not just one person. There's other players in the game that you have to consult with and be partnered with to make it effective.”

ZT Identity Metrics

As part of its ZT research program, the Stratascale team has developed the Stratascale Zero Trust Metrics in Context and Action (*Stratascale ZT-MICA*) metrics set, which provides strategic insights to executives, operational perspectives to IT and security management, and tactical data to managers responsible for ZT within each of the six pillars.

ZT Identity program management metrics within Stratascale ZT-Mica include:

- % of Admin accounts enrolled in MFA
- % of end user accounts enrolled in MFA
- % of Admin accounts enrolled in passwordless
- % of end user accounts enrolled in passwordless
- # of 3rd party users with privileged access to sensitive critical systems/applications
- # of 3rd users with privileged access to other systems/applications
- % of users accounts access review quarterly/yearly
- # of privileged accounts

Collectively, these measurements help identity program managers assess readiness and progress over time and identify and respond to areas of need before they are exploited.