REPLY CLUSTER

Identity & Access Management

Protecting organisations' identities

January 2022

Microsoft Gold Partner | Azure Expert MSP | Cloud Adoption Framework | Cloud Centre of Excellence

What is at stake?

A robust IAM system provides the means for close control of user access, drastically reducing the risk of external and internal data security breaches.

Risk creeps in incrementally

- With no central IAM system, project teams have to add IAM functionalities to the newly created systems on ad hoc basis. When developing or implementing new applications, project schedules and costs tend to be tight; thus, the team focuses on the functionalities needed to meet their core business goals. Security is often “left until later” or relegated to second place in the rush to get things done. The more data sources there are, the higher the risk involved in their secure storage and maintenance.

- Risk are not limited in the application architecture. Strictly controlling user access in a multi-system environment is notoriously difficult. When role, group, and authorization levels are independently implemented in various systems, efficient data verification and control becomes virtually impossible. In such a situation, teams tasked with data security and protection have no way to promptly verify all applications and systems. Meanwhile, the developers and administrators of these systems, lacking a clearly defined process, may grant access to confidential information to people who have no right to it.

- At Stake are:

  1. Reputational Loss
  2. Financial Loss
  3. Extinction Level Event

Research

- For organizations with over 1000 employees, automation in IAM is recommended.
- 80% of major data breaches are caused by weak or compromised passwords - Verizon 2019.
- >99% of threats observed required human interaction to infect user devices - 2019 Proofpoint.
- 70% of all attacks involve attempts to laterally move across the network – Carbon Black 2019.
- Privileged credentials are implicated in 80% of data breaches - Forrester 2019.
- 287 days is the average time taken to identify and contain a breach – IBM 2021.
- $4.62 million is the average total cost of a ransomware breach – IBM 2021.

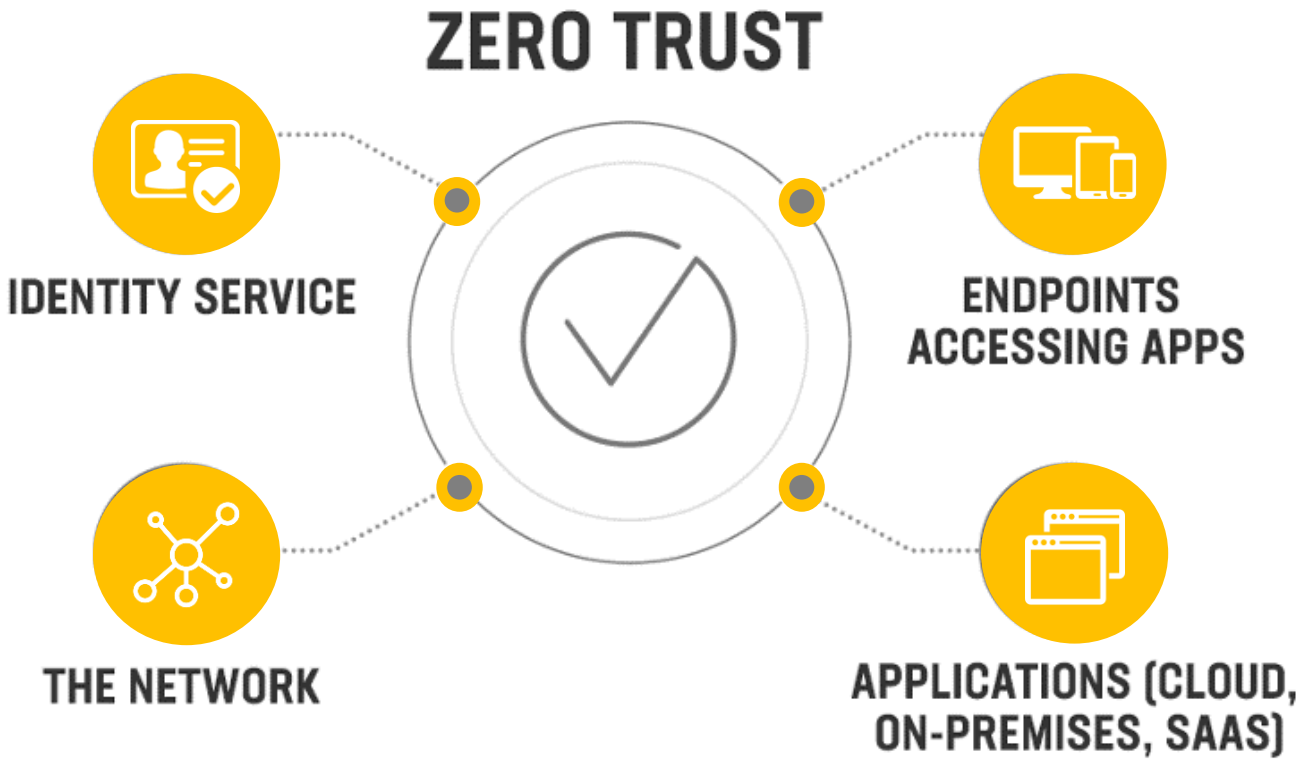
Zero Trust

The security model of the Cloud era

A Zero Trust architecture refers to a security model that treats all hosts as if they're internet-facing, and considers the entire network to be potentially compromised and hostile. This approach focuses on building strong authentication, authorization, and encryption, whilst also providing compartmentalized access and better operational agility.

Zero Trust is a relatively new security paradigm that moves away from perimeter-focused security that was dominant in the pre-cloud era. It emerged as more companies embraced cloud computing, which resulted in a shift toward treating user identity as the primary security boundary.

Organisations looking to adopt a Zero Trust architecture can incorporate Azure Active Directory (Azure AD) identity and access capabilities into an overall integrated and layered zero-trust security strategy. See Appendix B for more information on Zero Trust architecture. It should be noted that a well-planned Zero Trust architecture can also result in substantial cost saving.



Zero Trust Framework

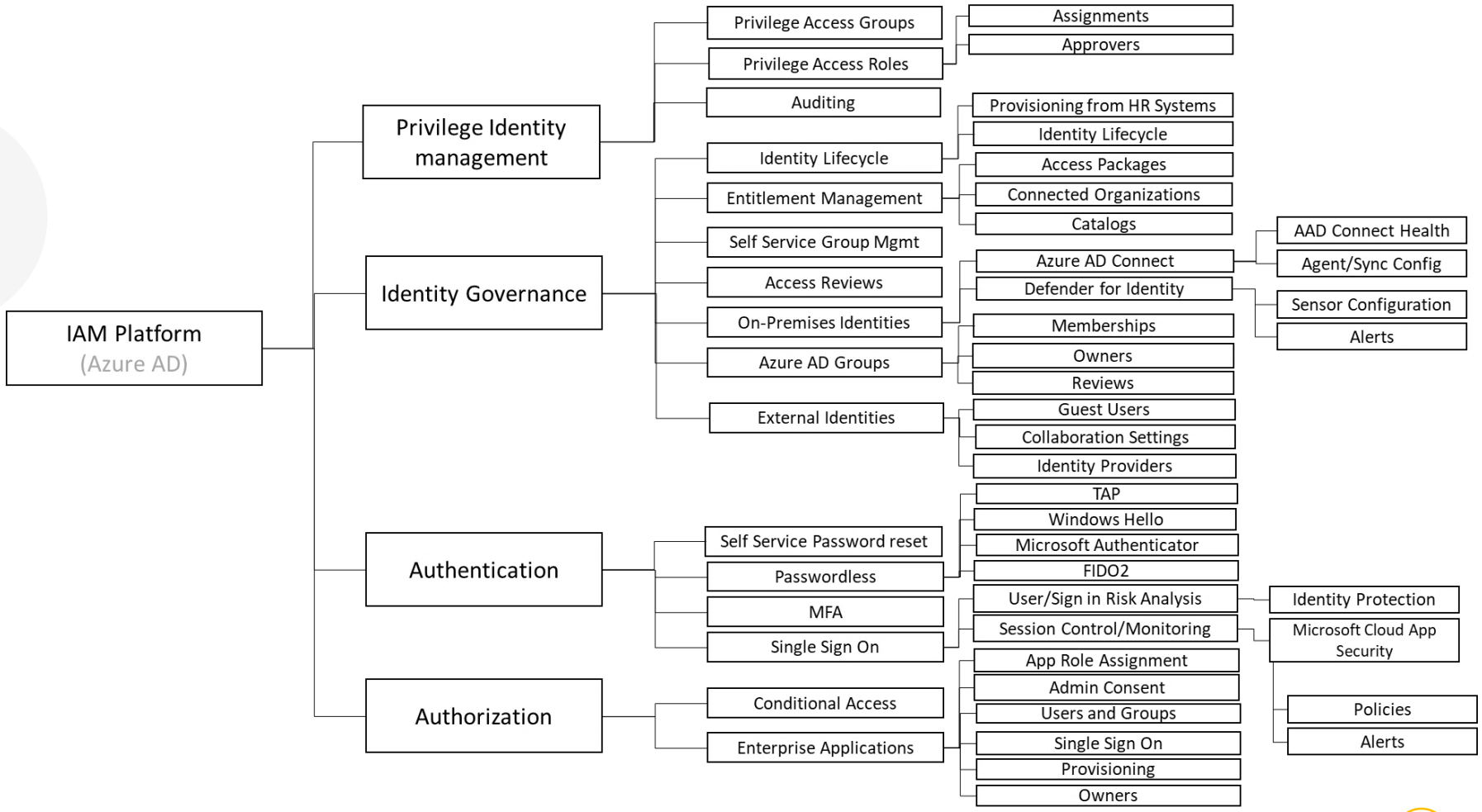
Microsoft Zero Trust Solutions for Identity & Access Management

We use Micorosft' s Zero Trust Framework (a taxonomy of IAM technologies and practises as seen on the right) as a reference to assess the breadth of the client's existing IAM capabilities as well as the maturity of each.

Often clients utilise a broad range of Micorosft IAM solutions, (as they are part of the M365 E5 licenses), but fail to get the full benefit because the solutions are applied to a limited scope , or the required process that have not been fully developed, or the various solutions are not being used in a coherent way.

Also, typically clients still use range of legacy IAM technologies (e.g. ADFS, on Prem AD, NTLM authentication) which need to be assessed and considered as part of long-term IAM strategy

By using a structured methodology, Reply can analyse clients' estate and propose a modern, cloud-centred capabilities, aligned with best practise while leveraging existing investments.



How we add value

An indicative approach

Assess current environment

Reply has deployed **IAM solutions** across a plethora of regions & industries.

We can **rapidly assess risks, timescales and complexities.**

Agree Guiding Principles

Accelerate decision making based on **agreed principles:**

- Process follows tools
- People follow process
- Zero Trust
- Trust but verify
- …

Guiding principles to **derive increased 'multiple'** in optimised timeframes with predictable outcomes.

Select solution and agree key measures

Reply has built **strategic IAM pltaforms** for flobal organisations, in the UK , Germany and Italy.

We deploy best-of-breed teams, drawing on a **scalable cost-effective onshore / nearshore delivery model.**

Marshall resources

Our **nearshore** model optimises cultural and time zone alignment with economic advantages.

We **operate from the UK** but can source capability across Europe.

Accelerate outcomes-based deployment

All our competancies, including IAM are **results driven.**

We know what good looks like, and how to measure it.

Harnessing years of experience

Years of experience distilled into a set of ‘golden’ rules

Over +10 years of experience helping organisations establish robust IAM process and systems, we have identified a range of pitfalls, challenges and failure patterns that occur regularly across industries.

Lessons learned from these experiences have been embedded in our methodology and guide our planning.

This table illustrates common challenges alongside potential ‘solutions’.

IAM Challenge	Success Factor / Enabler
Vast scope - IAM covers a broad spectrum, from JML to Access Reviews.	**Agree scope from the outset** - Build scope from a solid foundation, then build upon it. Requirements should be dictated by regulatory obligations. Thereafter be guided by value-add and risk reduction elements. It is often not reasonable to deliver everything, at uniform levels of control. Decision making in support of the design needs to be Risk Based.
Lack of business ownership - IAM traverses organisational verticals. Acknowledge a complementary management structure is needed to support this.	**Secure senior leadership support** - To ensure support is achieved across organisation's verticals, support for IAM is required at senior management levels.
Diffusion of Responsibility - IAM traverses organisational verticals. Acknowledge a complementary management structure is needed to support this.	**Single Point of Accountability** - To prevent risks and issues getting lost between the organisation's verticals, assign a single point of accountability.
Misguided assurance - A good compliance position does not equal a good security posture.	**Smart assurance** - Identify and remove anti-patterns eg. Several layers of approvals will deliver a false sense of assurance if each level is unaware of the expectations of it. Apply a variety of "Lenses" to the solution spanning Security, Compliance, User, etc.
Talent restrictions - Many organisations lag on IAM because of a talent shortages.	**Credible partner** - Identify and partner with an organisation that provides enablement for your organisation to build internal capability (the ‘teach to fish’ model). Augmenting, and pairing with your team(s), initially leading and gradually reducing as your team(s) are enabled and grow.

Three-day IAM Workshop

REPLY CLUSTER

Enable your organisation to design and plan the optimal identity model

IAM technologies and practices have evolved substantially since the advent of Cloud computing. Modern authentication methods (e.g. OAuth, OpenID Connect etc.) and new security paradigms (e.g. Zero Trust Architecture) enable more secure and more flexible ways of ways of working. A modern IAM platform allows organisations to leverage some of the aforementioned innovations and would be a foundational building block of a future-ready IT estate.

Designed as a three-day engagement, the Securing Identities Workshop enables the assessment of the maturity of a customer's identity estate. By making use of Secure Score and application discovery tools, this workshop gives customers visibility into their present state and will help define clear next steps and the best ways to mitigate risks.

Evaluate & Prepare

Evaluate your estate and define the scope by gathering key information

Design & Plan

Plan the optimal identity model which considers maturity vs urgency

Envision

Re-think your approach to foundational security

Microsoft Gold Partner | Azure Expert MSP | Cloud Adoption Framework | Cloud Centre of Excellence

IAM Workshop - Overview

A structured approach based on Microsoft best on practises and a well-defined methodology

Audience

Customers
Execs, IT Security, IT Operations, Architects/Engineers

Cluster Participants
Consultants/Architects/Engineers

Workshop

Evaluate & Prepare
Pre-Engagement Activities

- Define scope, and gather information on current identity estate
- Identify executive sponsors and business stakeholders
- Pre-engagement questionnaire

Envision
Art of the Possible

- Drive intent through the engagement setup
- Secure Score for identity
- Application discovery
- AD FS Migration
- Showcase security scenarios with demo's

Design & Plan
Create a Strategy

- Develop deployment plans based on key results and recommendations
- Define next steps

IAM Success Stories

Delivering value to our clients

Global Recruitment firm

IAM Strategy

Reply are currently advising S|Three, a global recruitment firm, on their IAM strategy and roadmap, as part of a multi-million digital transformation programme. The engagement includes migration of Active Directory to Azure AD DS as well as deployment of rage of peripheral IAM technologies paving the way towards a zero trust architecture.

Public Sector & Healthcare

IAM Programme

Consolidation of directory services in preparation for future identity and access controls for new applications and central services. Started with a simple synchronisation of account data between 3 active directories and developed to a full identity management solution with end to end identity life-cycle governance for internal and external resources.

Global Retailer

Security Strategy & IAM

Reply provide security strategy and architecture services to lead the IAM project for our global retail customer whilst providing security strategy, Security Operations and BAU direction and security architecture perspective

Financial Services

IAM & MFA

Reply supported our customer to design and develop various solutions in order to be compliant to the new Payment Service Directive including the integration of Identity Access Management and Multi Factor Authentication. As a result, sales increased over 20% and the number of visits increased by more than 10%

Major UK Retailer

Identity, AD & PAM Security Architecture

Our customer embarked upon an Identity and PAM transformation programme leveraging a redesigned Active Directory structure and migration of user, device and service accounts with Employee, Customer, Supplier and privileged accounts being migrated.

Large Global FMCG

AD B2C implementation

The client required a centralised Identity Management solution for external identities. Previously relied on disparate solutions, specific to individual local markets. The work delivered involved assessing the as is estate, designing planning and implementing a unified Consumer Identity Access Management (CIAM) platform using Azure AD B2C.

A broader and more detailed set of case studies is available upon request.

The Cluster Advantage

Cluster Reply is a multi-award winning technology consultancy specialising in Azure

Credentials

Gold Microsoft Partner | Azure Expert MSP

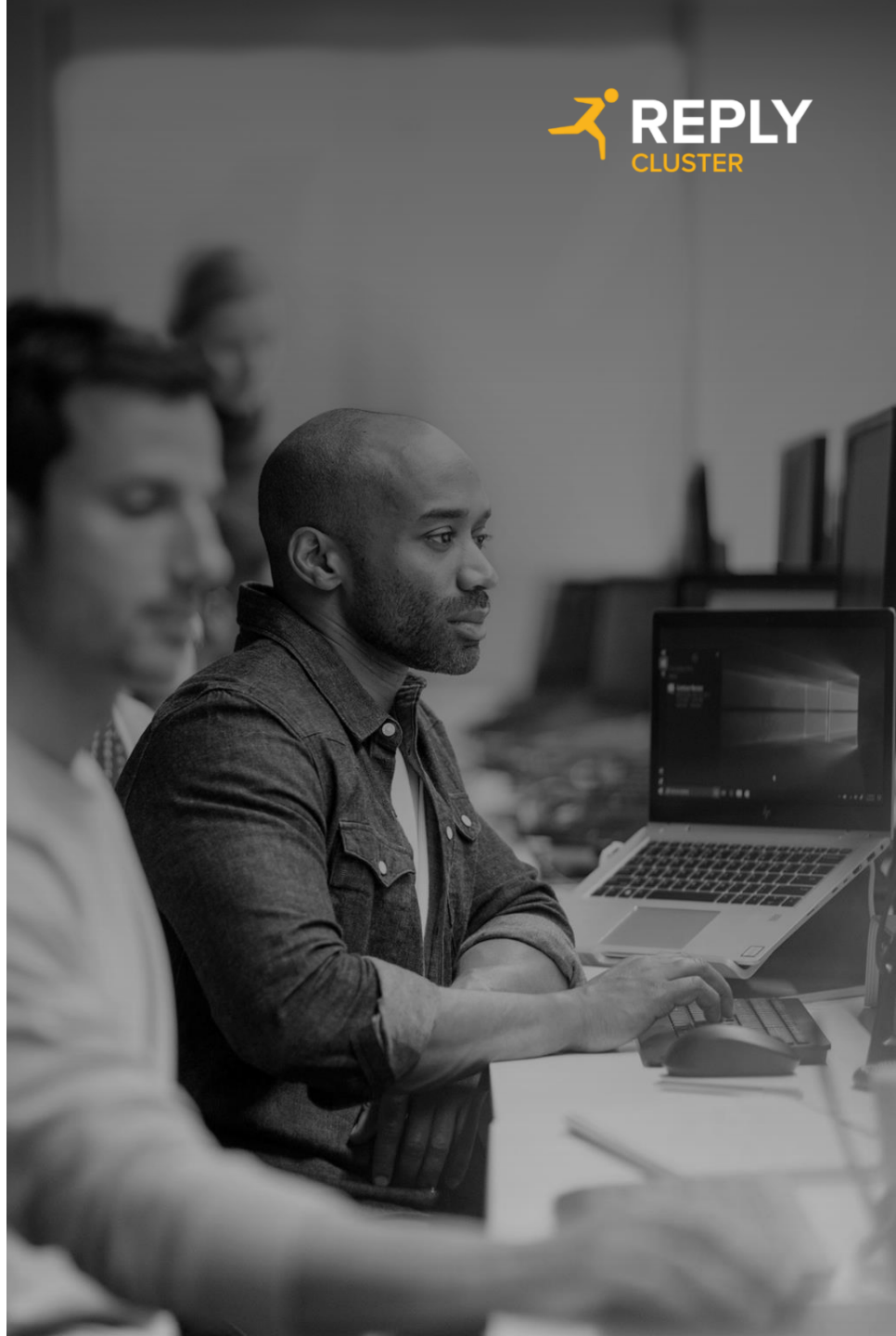
- Microsoft Gold Competencies – Gold competency is awarded to companies that have demonstrated the top level of expertise on a particular technology or service area. We hold 14 Microsoft Gold competencies, including Gold Windows and Devices, Gold Datacentre, Gold Security and Gold Cloud Platform.

- Azure Expert MSP – this accreditation assures clients that they are connecting with one of Microsoft's most capable and high-fidelity Azure Managed Service Providers. Whether you are working on mission-critical apps, entire datacentre footprints, or hybrid environments, Cluster Reply have proven their capabilities to be able to help you

Technical Expertise & Experience

Our architects and engineers have extensive experience in:

- Formulating IAM strategies and roadmaps helping organisation move towards a Zero Trust security model
- Helping clients adapt their identify solutions following acquisitions or divestments (we have designed and delivered AD migrations covering many thousands of AD objects, and leveraging tools such as Quest Migration Manager for AD and ADMT)
- Assessing and optimising large-scale and complex Active Directory (AD) environments covering multiple domains/forests, across different geographies (this is what we're currently doing for SThree)
- Designing and implementing cloud identity technologies including AAD, Azure ADDS, AAD Connect, and 3rd party IDPs (Ping, Okta etc), as well more established technologies including AD, GPOs and Certificate Authorities etc.



REPLY CLUSTER

Making the most of cloud

Contact:

Christos Myrsakis
c.myrsakis@reply.com
+44 (0) 7880921202