IDENTITY, GOVERNANCE AND SECURITY ASSESSMENT

Protect Your Investment

This Assessment is an in-depth evaluation of the management of access and identify in your organization. We will perform a complete gap analysis of your access security in hybrid environments of **Azure** and **Office365.** Ensuring you have the right controls in place helps reduce intrusion. We will help you adopt a proper secure architecture, following best practices in terms of verification, authentication, governance and identity protection.

A Trusted Partner

Plain Concepts is an **Accredited Partner** of **National Cryptology Centre** (CCN) in Spain. Our services and methodology are certified to the highest standards. We are one of only three companies who have passed the rigorous process.

Our **methodology** makes it easy for any organization to comply with Guidelines of National Security and guarantee security on Microsoft **Azure** and **Office365.**

2 out of 5 business leaders state security controls to protect access to apps is their top priority
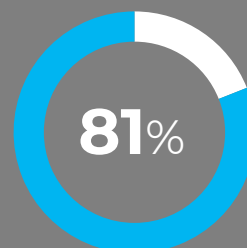
81% of breaches leverage stolen or weak passwords

About Plain Concepts

Plain Concepts, founded in 2006, has developed more than 2,400 projects. We help companies adopt new technologies deploying disruptive advances such as: Artificial Intelligence, Big Data, IoT, Virtual/Augmented Reality, Cloud Computing, Blockchain and Robotic-based services. The company has over 450 experts and is present in Spain, USA, UAE, United Kingdom, Germany, The Netherlands and Australia.

Challenges we will cover

This assessment is ideal for customers concerned about:

- **Exposure** of privileged accounts.
- Lack of **Control** accessing apps across a hybrid environment.
- Difficulties **Managing** the identity of employees, partners and customers.
- **Time** wasted managing passwords.
- Discover and control the use of **Shadow IT**.

Benefits you will find

- **Best Practices** in Office 365/Azure in terms of **Security** and **Governance.**
- Identity and Access **Lifecycle Management**.
- **Reduce the Risk** of phishing, apps and password attacks.
- **Centralized** and more efficient identity management.
- Control access based on organizational and regulatory **Policies**.
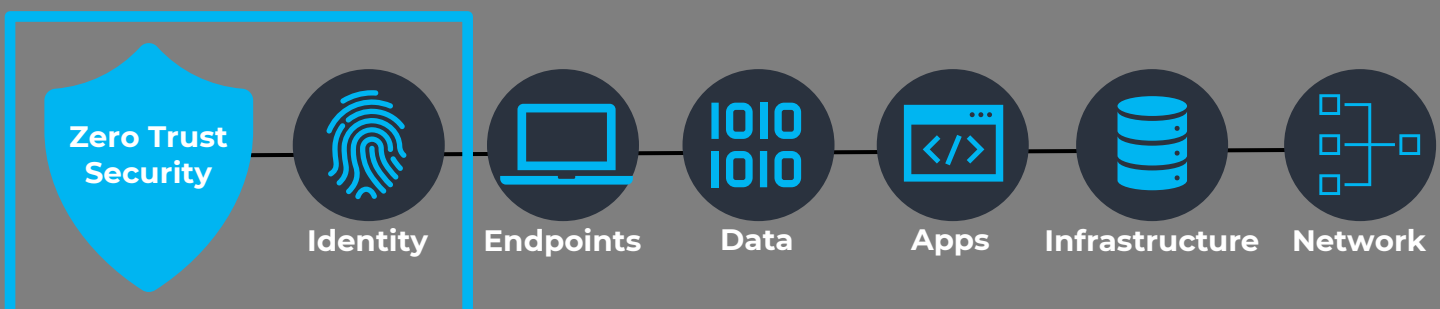
Identity **Governance** **Security** **2 Weeks**

Zero Trust Security **Identity** **Endpoints** **Data** **Apps** **Infrastructure** **Network**

Our approach in six phases

in two weeks

1 **Licensing Compliance**
The tenant's licensing will be reviewed to ensure that it is optimal and assigned correctly.

2 **Security Review**
Review of Microsoft's best practices in security of the tenant, verifying the use of MFA, Conditional Access, PIM, SSPR, Privileged Identities, external access, access reviews and Microsoft Defender.

3 **Identity Analysis**
Analysis of identity models, synchronization status, user and group configuration, ADFS, ADConnect.

4 **Governance Guidance**
Azure Active Directory Identity Governance increases users' productivity by making it easier to request access to apps, groups, and Microsoft Teams in one access package.

5 **Analysis of Tenant's Main Services**
Review of the configuration of the main services - Exchange, Sharepoint, OneDrive and Teams.

6 **Conclusions and Recommendations**
We will document our recommendations and outline timeline and steps to increase your level of early detection and reduce vulnerabilities.