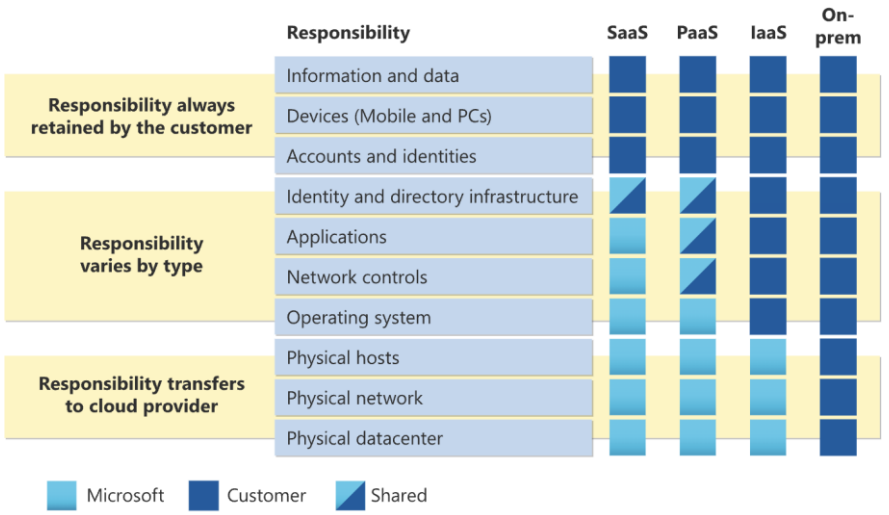
Introduction to BASE4 Azure Assesment

Market Overview

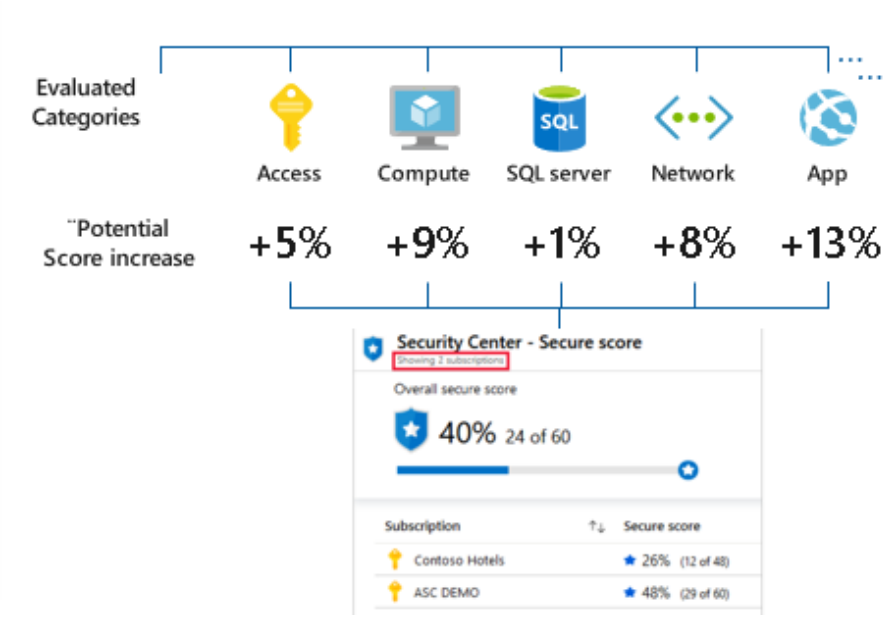
The market today relies on its cloud as the primary source of infrastructure for faster growth in a market in need of speed and flexibility. Clouds like Azure today provide the possibility of securitizing them, but they do not come by default since each company must adopt and adapt the security measures corresponding to its environment.



For this reason, at Base4 Security we offer a Cybersecurity Assessment and Hardening aimed at reducing the possible risks that the organization is facing, as well as internal bad practices.

Secure Score

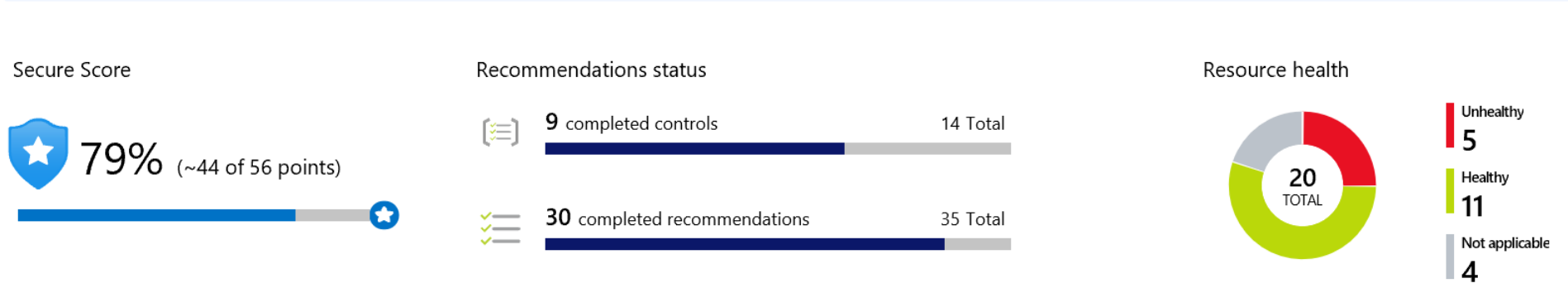
The service will be based on the improvement of the Azure Secure Score. Secure Score helps you understand the current security situation and efficiently and effectively improve your security posture. Security Center continuously evaluates all resources and aggregates all findings into a single score: the higher the score, the lower the level of risk identified. Secure Score is displayed as a percentage value, and Security Checks: Each check is a logical group of related security recommendations.



Assesment Service

The Assesment on the Azure environment has the goal of giving the CISO's a clear vision of it's risks and a recomendation plan to remediate them in a short term and without a lot of investment.

It has a duration between 120 and 200 hours and will give a Techincal and Strategic report on the foundings of the service as well as a Remediation Plan, all based in the Secure Score average.



Assesment Service

- It will include the following subjects:

Infra	Storage	Red	Security	BD	App
Virtual Machine Containers AKS	Storage account Disks	Virtual Networks Load Balancer Application Gateway DNS	IAM Defender flor Cloud KeyVault Diagnostic Settings	Azure SQL	Functions Azure Devops App Service

Assesment Deliverables

Deliverables Audit:

- Safety Improvement Plan
- Executive and Technical Report of risks and vulnerabilities found
- Creation of a Security Improvement Plan based on the survey carried out for Azure and the increase of the Security ScoreCard within the cloud.
- Identification of activities for short, medium and long term segregated by criticality

Neccesary Information

Needed information:

1. How many Microsoft Azure accounts/subscriptions do you have?
2. How many resources and what services do they use in each of those accounts?
3. Do you use ADFS, SAML or another centralized identity server authentication system? or do they use Azure AD itself?
4. What zones do you use?
5. Cloud resources; Are they integrated with on-premise servers in the company's internal network? If so, please describe all the integrations, so that no false positives are raised in the audit (example: an AKS server with on-premise worker nodes).
6. Is a full audit of the entire environment (Azure plus internal resources) or just cloud-native services required?
7. How many users are there using the cloud?
8. How many workgroups are there using the cloud?
9. . How many environments are there in operation within the cloud? Example; Dev, QA/Homologation, Production, Testing, etc.
10. From which devices can the cloud be accessed? Do you have restriction policies or is it free for users to access it as they wish with their users?

Requirements

- Requirements:
- A user created in Azure AD with the role of "Global Reader" that will allow everything to be read but not to make changes and with "Security Reader".
- A list of all the resources that need to be audited (in csv or excel format). To do this, you can perform the following procedure: ○
  - You must go to the Azure portal; https://portal.azure.com ○ Then proceed to go to the “All Resources” section available through search on the top bar. ○ Make a selection under “Export to CSV”.