ACCESS CONTROL | IT'S ALL ABOUT PERMISSION

Your company's sensitive data is only as safe as those who use it. Access control defines who has permission to access company networks and resources and puts systems in place to ensure these guidelines are enforced.

Assignment

Assigning which individuals have access to what is a key component that may be influenced by factors such as job title, role and your company's data classification policy.

Authentication

Authentication is the act of verifying that individuals requesting access are who they actually say they are.

Authorization

Authorization acknowledges that while an individual may be who they say they are, he or she may not be authorized to access certain information. So it's important to factor in where permissions begin and end.

Discretionary Access Control (DAC)

In this model, one of the oldest in use, the owner of the data decides who gets access and what rules apply. It works best in small organizations where oversight is easy.

Mandatory Access Control (MAC)

Access is granted based on information clearance standards set by a central source or authority. It's often used in government.

Role-Based Access Control (RBAC)

The individual's role determines access privileges based on key security principals. This includes the 'least privilege' principal, a key concept of security, that limits privileges to the minimum required to do the job.

Attribute Based Access Control (ABAC)

In this dynamic model, attributes such as time of day and the individual's location are used to determine whether access will be granted.

Barracuda®
Your journey, secured.