Access Control Policies

Access control **is a security technique that regulates who or what can view or use resources in a computing environment**. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: **physical and logical**. Physical access control limits access to campuses, buildings, rooms, and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing, and reports to track employee access to restricted business locations and proprietary areas, such as data centres. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.

Access control systems perform identification **authentication** and **authorization** of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defence to protect access control systems.

How access control works?

These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or Internet Protocol (IP) address. Directory services and protocols, including Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

Types of access control

The main models of access control are the following:

1. **Mandatory access control (MAC).**

   This is a security model in which access rights are regulated by a central authority based on multiple levels of security. **Often used in government and military environments**, classifications are assigned to system resources and the operating system (OS) or security kernel. It grants or denies access to those resource objects based on the information security clearance of the user or device. ***For example, Security Enhanced Linux (SELinux) is an implementation of MAC on the Linux OS.***

2. **Discretionary access control (DAC).**

   This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.

3. **Role-based access control (RBAC).**

   This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.

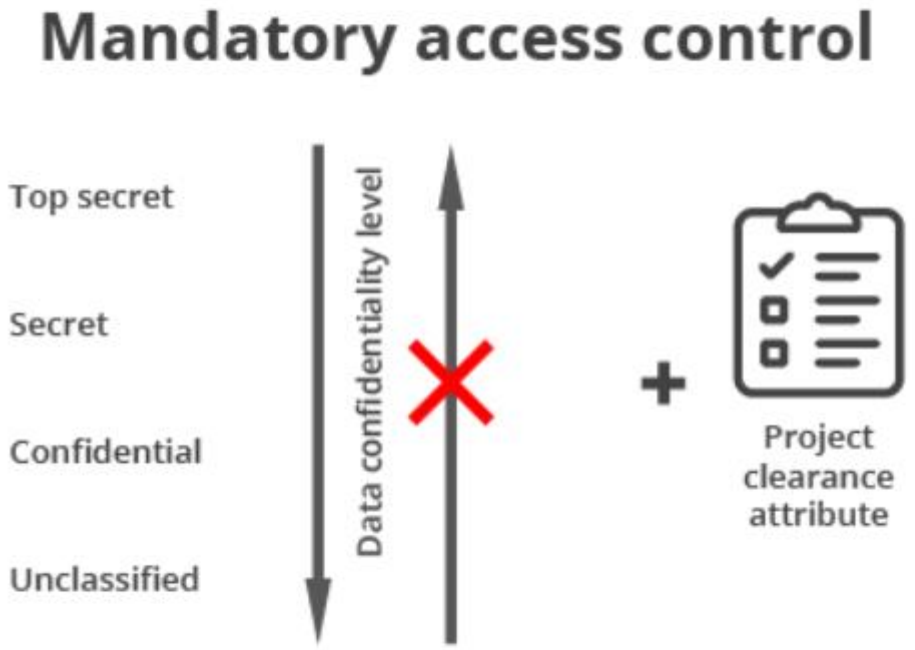
4. **Rule-based access control.**

   This is a security model in which the system administrator defines the rules that govern access to resource objects. Often, these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.

Mandatory Access Control (MAC)

Mandatory access control (MAC) is a model of access control where the operating system provides users with access based on data confidentiality and user clearance levels. In this model, access is granted on a **need-to-know** basis: users must prove a need for information before gaining access.

MAC is considered the most secure of all access control models. Access rules are manually defined by system administrators and strictly enforced by the operating system or security kernel. Regular users cannot alter security attributes even for data they have created.

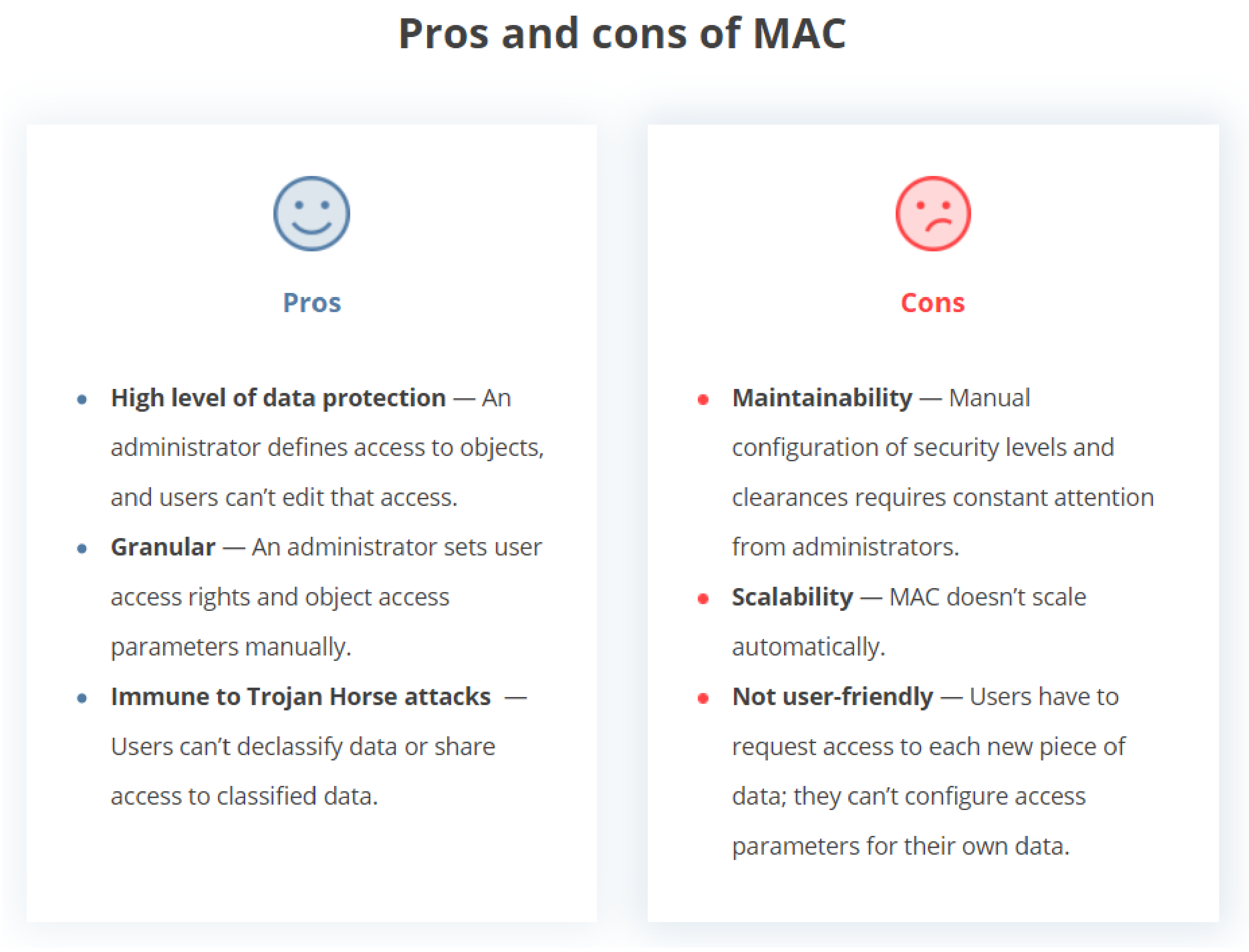


With MAC, the process of gaining access looks like this:

- The administrator configures access policies and defines security attributes: confidentiality levels, clearances for accessing different projects and types of resources.
- The administrator assigns each subject (user or resource that accesses data) and object (file, database, port, etc.) a set of attributes.
- When a subject attempt to access an object, the operating system examines the subject's security attributes and decides whether access can be granted.

For example, let's consider data that has the **"top secret"** confidentiality level and **"engineering project"** label. It's available to a set of users that have "top secret" clearance and authorization to access engineering documents. Such users can also access information that requires a lower level of clearance. But employees with lower levels of clearance will not have access to information that requires a higher level of clearance

MAC brings lots of benefits to a cybersecurity system. But it has several disadvantages to consider.



Pros and cons of MAC

Pros

- **High level of data protection** — An administrator defines access to objects, and users can't edit that access.
- **Granular** — An administrator sets user access rights and object access parameters manually.
- **Immune to Trojan Horse attacks** — Users can't declassify data or share access to classified data.

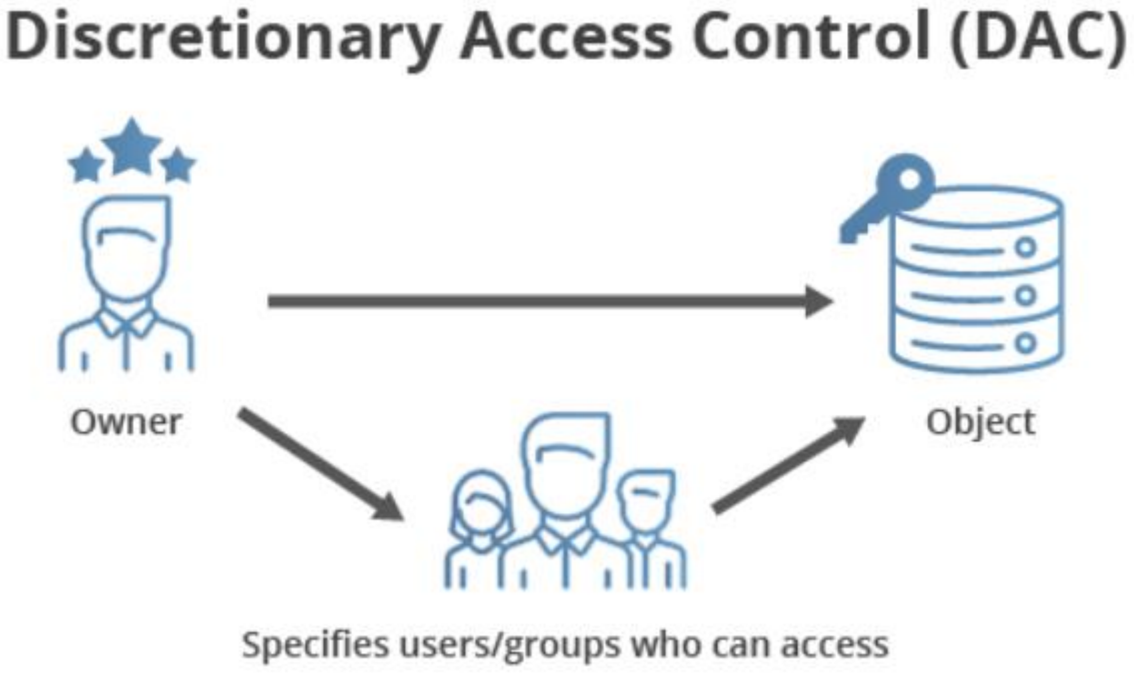
Cons

- **Maintainability** — Manual configuration of security levels and clearances requires constant attention from administrators.
- **Scalability** — MAC doesn't scale automatically.
- **Not user-friendly** — Users have to request access to each new piece of data; they can't configure access parameters for their own data.

Discretionary Access Control (DAC)

Discretionary access control (DAC) is an identity-based access control model that provides users a certain amount of control over their data. Data owners (or any users authorized to control data) can define access permissions for specific users or groups of users.

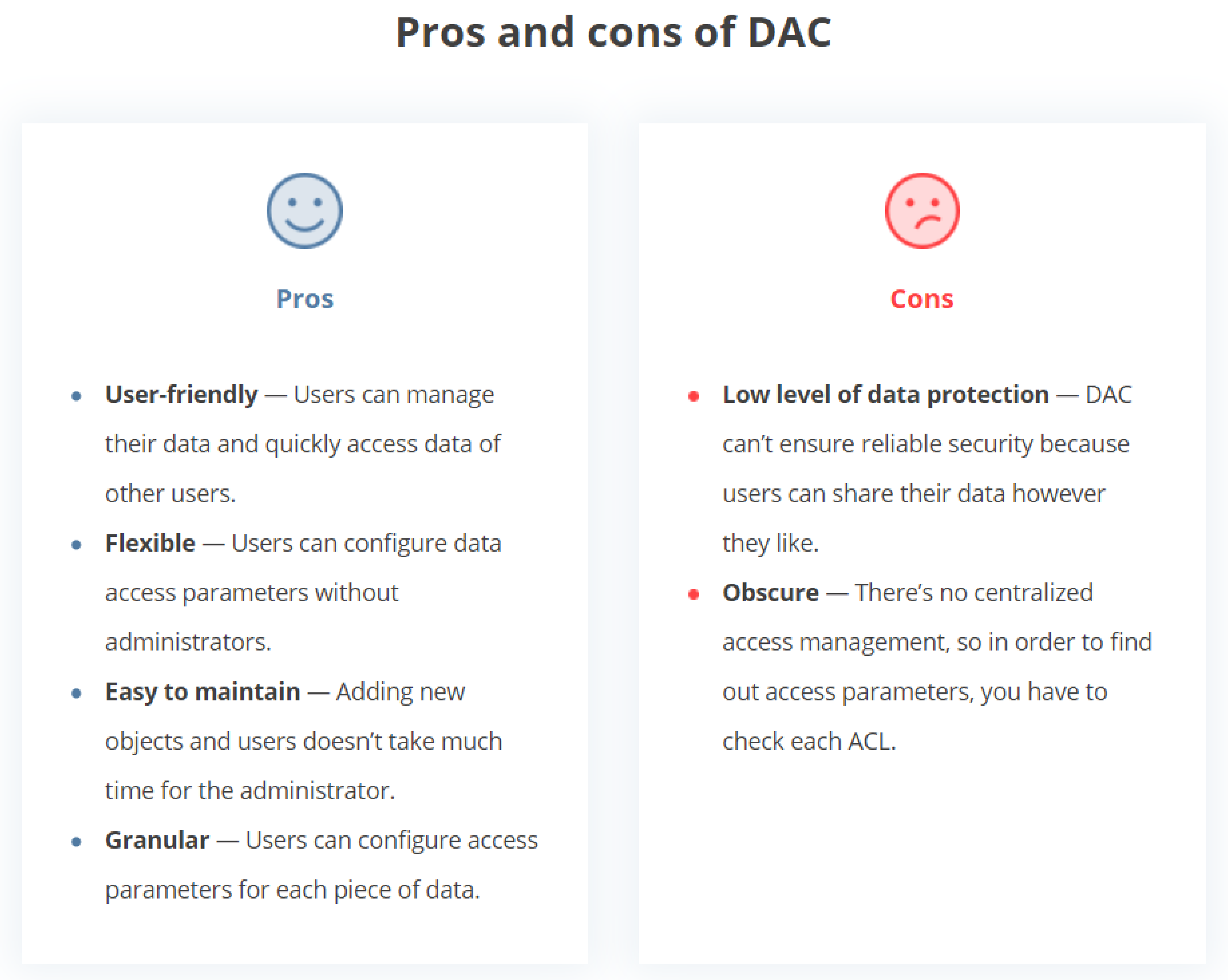
Access permissions for each piece of data are stored in an **access-control list (ACL).** This list can be generated automatically when a user grants access to somebody or can be created by an administrator. An ACL includes users and groups that might access data and levels of access they might have. An ACL can also be enforced by a system administrator. In this case, the ACL acts as a security policy, and regular users cannot edit or overrule it.


Discretionary Access Control (DAC)
Owner
Object
Specifies users/groups who can access

Gaining access in the DAC model works like this:

- User 1 creates a file and becomes its owner or obtains access rights to an existing file.
- User 2 requests access to this file.
- User 1 grants access at their own discretion. However, user 1 cannot grant access rights that exceed their own. For example, if user 1 can only read a document, they cannot allow user 2 to edit it.
- If there is no contradiction between the ACL created by an administrator and the decision made by user 1, access is granted.

Discretionary access control is quite a popular model because it allows a lot of freedom for users and does not cause administrative overhead. However, it has several considerable limitations.



Pros and cons of DAC

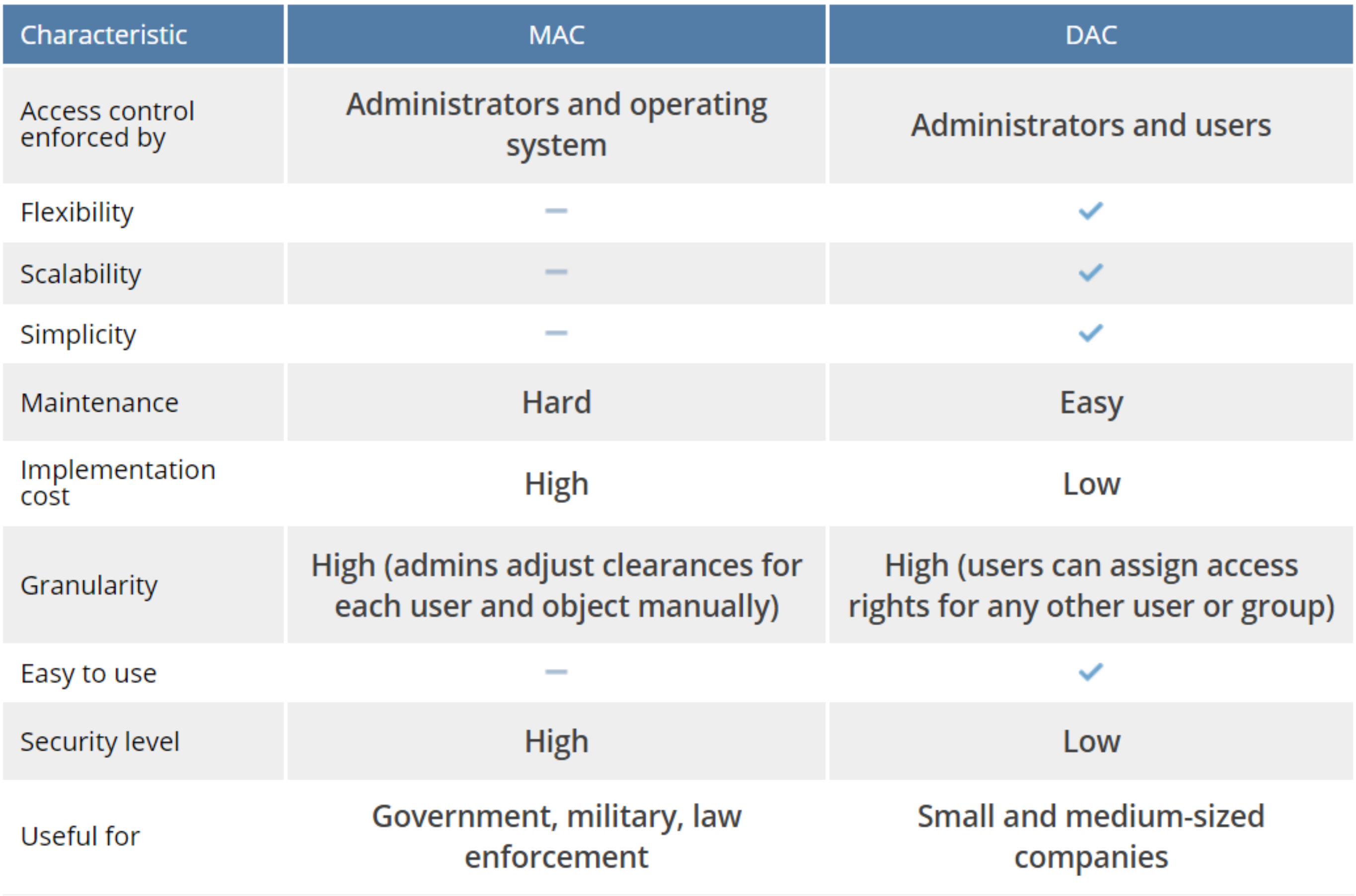
Pros

- **User-friendly** — Users can manage their data and quickly access data of other users.
- **Flexible** — Users can configure data access parameters without administrators.
- **Easy to maintain** — Adding new objects and users doesn't take much time for the administrator.
- **Granular** — Users can configure access parameters for each piece of data.

Cons

- **Low level of data protection** — DAC can't ensure reliable security because users can share their data however they like.
- **Obscure** — There's no centralized access management, so in order to find out access parameters, you have to check each ACL.

Let us review the key characteristics of these two access control models:



Characteristic	MAC	DAC
Access control enforced by	Administrators and operating system	Administrators and users
Flexibility	—	✓
Scalability	—	✓
Simplicity	—	✓
Maintenance	Hard	Easy
Implementation cost	High	Low
Granularity	High (admins adjust clearances for each user and object manually)	High (users can assign access rights for any other user or group)
Easy to use	—	✓
Security level	High	Low
Useful for	Government, military, law enforcement	Small and medium-sized companies