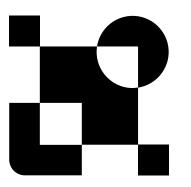
almond

WORKSTATION SECURITY WINDOWS

Workstation disk encryption with Microsoft BitLocker



WHAT IS BITLOCKER?

BitLocker is a data protection **solution integrated into Windows operating system**. This tool aims to ensure the confidentiality of data and reduce the risk in case of loss or theft of workstations.

WHAT DOES BITLOCKER PROVIDE?

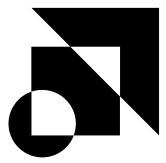
BitLocker provides **physical access protection to information** stored locally on workstation hard drives by providing the following security features:

- → **Encryption** of the hard disk.
- → Protection of access to the disk either by PIN code, or by a cryptographic key integrated into the workstation (TPM), or by external cryptographic key such as a USB key or smart card.
- → Locking of the startup sequence in case of a modification detected on the hardware or on the BIOS.
- → Centralized management of security requirements and policies for the entire computer fleet.

WHY IS BITLOCKER AN OPPORTUNITY?

If you don't have a workstation encryption solution yet, or if your current encryption solution is not satisfactory:

- → BitLocker is **integrated** into the Windows system for free.
- Deployment and management of the tool is done on the existing AD infrastructure.



WE CAN SUPPORT YOU.

Almond's Infrastructure Security team has **complete expertise** in the service chain offered by Microsoft, from the workstation to the Azure Cloud, as well as in AD and Azure AD security issues.

Mastering BitLocker projects is part of our **catalog of skills** and we will be able to **adapt to your context** so that you can use the tool's features in an **optimized and secure way**.



WORKSTATION SECURITY WINDOWS

Workstation disk encryption with Microsoft BitLocker

WHAT ARE THE BITLOCKER INTEGRATION METHODS?







| ON-PR | IN THE CLOUD | |
|---|---|--|
| Deployment and control by local policy | Deployment and control by dedicated solution | Deployment and control by Intune policy |
| → Deploying encryption policies. → Enabling Encryption. → Recovery keys on AD | → Deploying encryption policies. → Enabling Encryption. → Recovery keys on an SCCM administration portal. | → Deploying encryption policies. → Enabling Encryption. → Recovery keys on Azure AD. |
| controller or portal provided. | → Compliance check with SCCM | |

WHAT SERVICES DO WE PROVIDE?

| P | ROVIDE | GOAL | |
|-------------------------------------|---|---|--|
| Functional study | Technical benchmark. | Evaluate the BitLocker solution against competing solutions with equivalent functionality. | |
| | Functionnal validation of selected solution. | Compare the services provided by Bitlocker with the client technical and organizational context requirements. | |
| Configuration readiness | Production of configuration & run supporting documentation. | Provide complete documentation for teams administering the Windows perimeter. | |
| Technical support for deployment | Technical support during pilot. | Provide technical support for the deployment waves of the BitLocker solution | |
| | Training of production teams. | Lead training sessions for production teams in groups of up to 8 people. | |

