Whitepaper:
Endpoint Protection with Microsoft 365 and DriveLock - an Ideal Combination.

DriveLock

The release of Microsoft 365 with the availability of Microsoft Defender for Endpoint show that Microsoft is taking security more seriously by providing a comprehensive platform for endpoint security. In addition to the virus scanner, Defender for Endpoint contains functions deeply integrated into the operating system to defend against various threats.

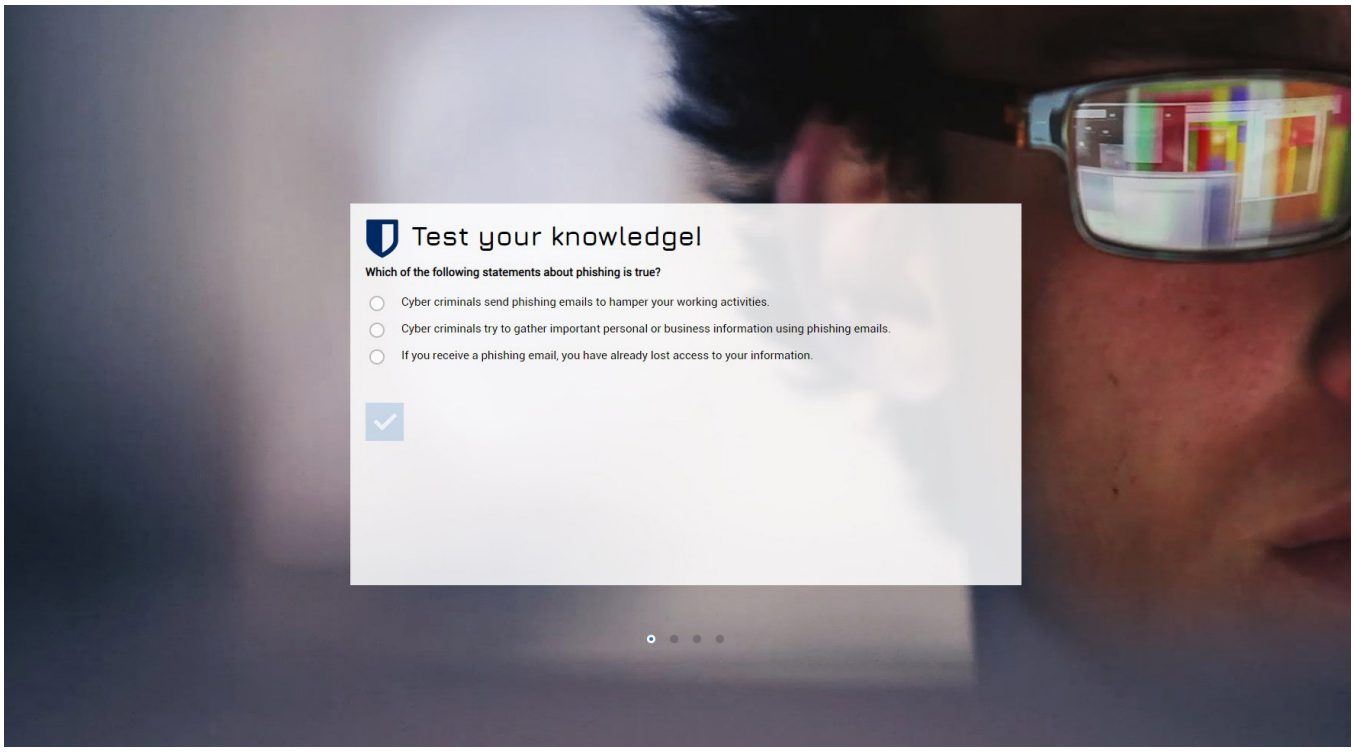
DriveLock complements this platform perfectly and does not overlap with the functionality of Defender for Endpoint, so the combination of both solutions provides unprecedented comprehensive threat protection.

Our **DriveLock Native Security** provides the ability to manage Microsoft Defender and DriveLock capabilities from one console with a level of granularity not offered elsewhere.

The „ideal combination" is best explained using the „kill chain" of an attack example:

An attacker is trying to carry out a targeted ransomware attack on a company. To do this, he has created a ransomware specially tailored to the target and sends it to the company's employees by e-mail on the one hand, and on the other, he deliberately „drops" USB sticks infected with the ransomware in the parking lot and entrance area of the company.

DriveLock already comes into play at this stage of the attack: via **DriveLock Security Awareness**, employees are regularly informed about new threats when opening their mail client and using USB sticks, and informed about how to deal with found USB sticks or mails from unknown sources, for example.



If an employee nevertheless plugs the found USB stick into his computer, **DriveLock Device Control**[1] can prevent the malware from running and Microsoft Defender can already scan the USB stick for known viruses.

If an employee nevertheless attempts to execute the malware, the next safety net of the product combination kicks in: **DriveLock Application Control** will block the execution in case of an attempted execution from the mail program with the help of the **Application Behavior Control**. Or, since the malware is not whitelisted in the Application Control, the execution will be prevented anyway. If the malware is already known - which, however, will only be the case with a long delay in the case of a specially prepared attack - then the malware would also be detected by Microsoft Defender Antivirus. If the malware was not sent as an attachment, but as a web link, Microsoft Defender web content filtering also goes into action and can prevent the malware from being downloaded if configured accordingly.

To completely rule out data loss, a prudent IT security department will also take appropriate measures beyond the attack described, where the products complement each other well:

- Microsoft BitLocker as native hard disk encryption under Windows is not only perfectly managed by DriveLock, but also massively upgraded in functionality by **DriveLock Pre-Boot Authentication**. For example, it is possible to enable smart card logon during the pre-boot phase or to give the user the option to log on with the known Windows username and password during the pre-boot phase. The self-service portal provided by DriveLock also massively relieves the user helpdesk in cases of forgotten password or when an additional BitLocker security check is required after hardware changes. Other features, such as network-based pre-boot authentication and extensive user self-service capabilities, round out the offering.
- **DriveLock Native Security Management**, with OS firewall rule management and local user account management, provides complementary functionality not represented in Microsoft Defender for Endpoint, but still important for comprehensive threat protection.
- **DriveLock EDR** brings all modules together and can filter and correlate events that have occurred in DriveLock or Microsoft Defender and respond to potential threats according to the configuration. Using the MITRE ATT&CK® framework, a variety of rules are pre-configured in DriveLock to combine information from Windows with DriveLock Agent intelligence to prevent attacks.

[1] Microsoft Defender for Endpoint provides a rudimentary means of device control: the device control features that have been available in Windows for years, which can be distributed via Group Policy. This effectively does not allow control of USB sticks, as there is e.g. no possibility to restrict certain files, run a virus scan before use, etc. - see below for a detailed comparison of the possibilities.

[2] Microsoft Defender for Endpoint offers a rudimentary application control capability: a more detailed comparison of the options can be found below.

Application Control Comparison

Capability	DriveLock Application Control	Windows Defender Application Control (WDAC)	Windows AppLocker
Platform support	Windows XP+	Windows 10 and 11	Windows 8+
SKU availability	All	All: 1909+ Enterprise: pre 1909	GPO: Enterprise MDM: All
Cloud management solutions	Centralised and convenient management with the DriveLock Operations Center	Intune: Limited built-in policies or custom deployment Microsoft Endpoint Manager Configuration Manager (MEMCM): Limited built-in policies or custom deployment via Software Distribution	Intune: Limited built-in policies or custom deployment Microsoft Endpoint Manager Configuration Manager (MEMCM): Limited built-in policies or custom deployment via Software Distribution
On-premise management solutions	Centralised and convenient management with the DriveLock Operations Center, Policy deployment via GPO possible	No centralised management, no reporting, Policy deployment via GPO or Powershell	No centralised management, no reporting, Policy deployment via GPO or Powershell
Management type	User interface	Powershell XML file	Powershell XML file
Per-User and Per-Group rules	Yes	No	Yes
Time- and Network-Based rules	Yes	No	No
Per-app rules	Yes	Yes	No
Managed installer (MI)	Yes	Yes	No
Reputation-based intelligence	No	Yes	No
Multiple policy support	Yes	Yes	No
Path-based rules	Yes	Yes	Yes
Hash-based rules	Yes	Yes	Yes
Codesigning certificate rules	Yes	Yes	Yes
File owner rules	Yes	No	No
Local whitelist	Yes	No	No
Automatic learning of rules	Yes	No	No
Temporary unlock	Yes	No	No
Security awareness hooks	Yes	No	No

Enforceable file types	Any	Drivers Executable files DLLs Windows installer Scripts (ps1, vbs, js) Packaged apps	Executable files DLLs Windows installer Scripts (ps1, bat, cmd, vbs, js) Packaged apps
Application Behavior Control	Yes	No	No
Tools for automated policy generation	Yes	No	No

Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/feature-availability

Device Control Comparison

Capability	DriveLock Device Control	Windows Device Control
Licensing	DriveLock Device Control	Microsoft 365 E3 for policy Microsoft 365 E5 for policy and reporting
Platform support	Windows XP+	Windows 7+
Management solutions	DriveLock Operations Center GPO	Intune Microsoft Endpoint Manager Configuration Manager(MEMCM) GPO Powershell
Management type	User interface	XML file
Per-User and Per-Group rules	Yes	No
Time- and Network-Based rules	Yes	No
Access control (Read, Write, Execute)	Yes	Yes
File filtering	Yes	No
Auditing	Yes	Limited
Temporary unlock	Yes	No
Conditional access (e.g. only after virus scan)	Yes	No
Automation on access	Yes	No
Bluetooth service management	Yes	Yes
Enforced encryption	Yes	No
Security awareness hooks	Yes	No