

Microsoft 365

Protection against cyberattacks



⚠️ **Challenge:**

- **Detect and prevent cyberattacks**, mitigating risks
- Protect IT infrastructure (including user credentials) from targeted hacker attacks, that are aimed to gain profit.
- **Ensure business continuity**, avoid financial and reputational losses.

👍 **Solution:**

- Enables timely **detection of suspicious activities** in corporate infrastructure
- **Protects user credentials**, and avoid PCs launching malicious software.
- Minimizes risks by **isolating the infected PC**
- Intelligence tools **detect the threat source** to prevent the spread of viruses.

Benefits:

- Lowered risks of business process disruption
- Decreased financial losses due to targeted attacks
- Reduced reputational risks
- Mitigation of consequences of successful attacks

Scenarios

- No user behavior monitoring
- No proper antivirus solution
- Lack of procedures to respond to security violations
- Lack of tools that ensure secure storage of user account data and provide protection from targeted attempts of theft?
- Not available monitoring system that detects abnormal processes during application

Solution capabilities

- Detection of suspicious user activities and attempts to compromise access rights
- Revealing the attacks like pass-the-hash, pass-the ticket, etc.
- Detection of abnormal application launches, attempts to encrypt files
- Control on installation and use of third-party software
- Virtualized storage of user credentials to prevent their theft

Tech and products

- Advanced Threat Analytics
- Windows Defender Advanced Threat Protection
- Windows Defender Antivirus
- Windows AppLocker
- Windows Conditional Access
- Windows Credential Guard,
- Windows Device Guard
- O365 Security score