Microsoft Security

silent4business

MICROSOFT MICROSOFT DEFENDER FOR SERVER

Advanced protection for server workloads, with centralized detection, response, and management capabilities for hybrid and multicloud environments.

SURROUNDINGS

Increasing complexity

Servers are at the core of critical operations and are exposed to increasingly sophisticated threats, such as ransomware, unauthorized access, and targeted attacks. In hybrid and multicloud environments, the attack surface expands, requiring solutions that offer comprehensive and continuous protection.

Need for automation

Manual server security management is costly and error-prone. Defender for Server automates incident detection and response, reduces operational burden, and enables security teams to focus on strategic tasks such as advanced investigation and preventative planning.

Resilience and compliance

In addition to strengthening your security posture, Defender for Server helps you comply with international regulations (ISO, GDPR, HIPAA) through built-in audits and reporting. Its ability to minimize the impact of attacks and restore system integrity increases resilience against future threats.

FEATURES

- Protection against malware and ransomware on servers.
- Detection of vulnerabilities and insecure configurations.
- Continuous monitoring of system integrity.
- Automated incident response.
- Integration with SIEM and management tools.
- Microsoft Global Threat Intelligence.

USE CASES

1. **Critical Load Protection**: Security for servers hosting mission-critical applications.
2. **Regulatory compliance**: Auditing and reporting for standards such as ISO, GDPR, HIPAA.
3. **Attack response**: Automatic isolation of compromised servers.
4. **Centralized Management**: Consistent policies for hybrid environments.
5. **Ransomware Defense**: Blocking malicious processes and reverting changes.

KEY INTEGRATIONS AND THEIR BENEFITS

- Microsoft Sentinel: Event correlation and response automation.
- Defender for Endpoint: Advanced protection on Windows and Linux servers.
- Defender for Cloud: Security posture and recommendations for hybrid environments.
- Intune: Policy enforcement and access control.
- Defender for Identity: Protection against credential-based attacks.

Microsoft Security

silent4business

ARCHITECTURES