Netsurion®
Powering Secure and Agile Networks

Microsoft 365 Security Monitoring Checklist

Cyber criminals actively target Microsoft 365 because of its widespread global use and privileged access to servers, data, and administrative users. IT leaders assume that Microsoft's built-in tools are sufficient to protect their 365 tenant against today's advanced persistent threats. Protecting mission-critical data is paramount, but you may lack the staff or skills to minimize your Microsoft 365 attack surface. Netsurion's Managed Threat Protection platform blocks threats, enhances visibility, and prevents attackers from exploiting your Microsoft 365 tenant.

Utilize the checklist below to ensure you are doing all you can to protect this important application.

Step 1: Basic Security Considerations

- [ ] Do you store valuable logs beyond the 7-day archive that Microsoft provides?
- [ ] Are you using Active Directory Federation Services (ADFS) instead of the safer Azure Active Directory (AAD)?
- [ ] Are you protecting sensitive data found in Microsoft OneDrive, SharePoint, and Teams?
- [ ] Can you identify any emails with malware or phishing attempts?
- [ ] Have you identified high risk privileged user accounts for increased monitoring and security?
- [ ] Do you have single console visibility across Microsoft 365 for all your infrastructure and assets?

Step 2: Threat Detection and Response

- [ ] Do you have 24/7/365 visibility and monitoring of Microsoft 365 infrastructure?
- [ ] Are you rapidly implementing all Microsoft 365 patches?
- [ ] Are you concerned about Microsoft 365 configuration gaps and human error?

Netsurion®
Powering Secure and Agile Networks

Microsoft 365 Security Monitoring Checklist

Step 2: Threat Detection and Response *(Continued)*

- [ ] Can you detect, block, or quarantine threats impacting Microsoft 365?
- [ ] If you suspect suspicious internal or external threats against your Microsoft 365 tenant, would you know where to start investigating?
- [ ] Have you implemented Microsoft 365 hardening best practices like implementing Microsoft Defender and Multi-Factor Authentication (MFA)?

Step 3: Behavior Analysis and Threat Hunting

- [ ] Are you mapping security operations to the MITRE ATT&CK framework of known threats?
- [ ] Do you proactively threat hunt to find cyber criminals already in your Microsoft 365 infrastructure?
- [ ] Can you detect suspicious behavior wherever it resides: in the cloud, on-premises, or a hybrid?
- [ ] Do you distinguish valid Microsoft PowerShell activity from suspicious ones?
- [ ] Can you perform Geo IP filtering such as undesirable countries or a user with more than one IP address?

Learn more on protecting your Microsoft 365 infrastructure https://www.netsurion.com/managed-threat-protection/microsoft-365-security