

Managed Threat Detection [network]

for Microsoft Office 365

Detect and mitigate attacks against Office 365 and Azure AD before they cause damage

A great cloud-based productivity suite, but also lucrative for attackers

Today, Office 365 dominates the enterprise workspace with over 250 million active users each month. For many organizations, data sharing, communication and storage are based on Office 365, making it an incredibly attractive target for cybercriminals.

So it's no surprise then that Office 365 is the 2nd biggest source of incident response cases for Orange Cyberdefense (after ransomware).

The growing risk of account takeover

After compromising an account, attackers can easily move across cloud applications and service providers within your hybrid environment.

The impact can magnify quickly, with the attackers using the compromised account to inflict serious damage.

That's why it's crucial to prevent this type of potentially devastating cyber attacks.

Managed Threat Detection [network] for Office 365 helps you to maintain your Microsoft 365 security posture and hygiene.



Increased visibility into potential threats



Rapid Detection and Response

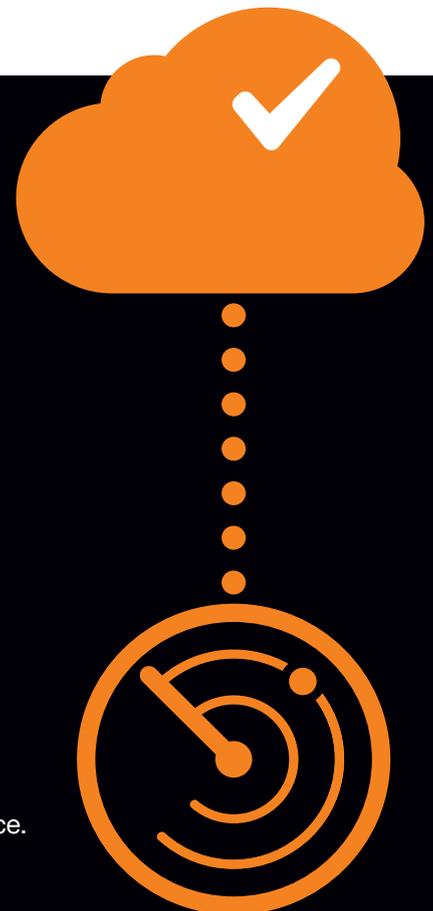


Safe and secure cloud adoption

Why Orange Cyberdefense?

Gain centralized visibility to cybersecurity risk across your Microsoft 365 ecosystems:

- **Intelligence-led approach**
Our unique threat intelligence with over 500 private and public sources goes beyond Indicators of Compromise, with aggregated data and insights from global operations, ethical hacking and digital risk monitoring teams.
- **Extended capabilities**
18 SOCs, 14 cyberSOCs to meet your demands, with 150+ analysts, delivering detection and response services 24x7x365.
- **Response coverage**
Benefit from the broadest range of response service options, including extensive experience in handling office 365 breaches. Complement your own abilities in an optimal way.
- **Future Proof**
The integration with other Orange Cyberdefense MDR capabilities allows you to extend the service based on your current and future needs.
- **Outcome-based delivery**
We provide 24x7 real-time visibility & control on the different aspects of the service.
- Orange Cyberdefense is a member of the **Microsoft Intelligent Security Association (MISA)**.



Find out more about Managed detection and response (MDR):

orange cyberdefense.com/global/mdr/



Benefits:



Complete detection visibility: In-depth analysis of your entire Office 365 ecosystem (Sharepoint, One drive, Microsoft suite...) and your Azure AD accounts



Detect unusual behavior in real time: Identify and contain compromised office 365 and Azure AD accounts as well as malicious insiders based on how they act



Increase resilience against backdoor intrusion: Monitor for zero-day-attacks based on behaviour, no use-cases, signatures or extensive rules required



AI driven solution: Automated analysis of incidents prioritizing what threats require focus right now



Quick-time to value: Easy service to implement, works with your existing security solutions.



Save time and money: Scales security efforts without draining resources

Challenges

- 24x7 CyberSOC coverage required – Office 365 is a resource prone to exploit around the clock
- Continuous management and tuning of monitoring to ensure enough context is provided for analysts without producing “alert fatigue”
- Applying global intelligence to cyber security threats

What do we do?

- Deployment of the Vectra platform
- Platform management of Vectra Cognito Detect™
- Continuous incident triage, analysis and prioritization by Security Analysts
- Managed Threat Response to isolate and lock down compromised accounts

When should you consider it?

- If you require experts to help deploy and run a sophisticated detection and response service
- If you require a provider that not only provides network detection but also log and endpoint based monitoring as well as actionable Cyber Threat Intelligence
- If you require additional Managed Threat Response capabilities 24x7.

What will you get?

- Fully Managed Platform operations
- Real-time incident analysis and alerting
- Monthly reporting
- Optional Cyber Threat Hunting
- Optional Managed Threat Response

Intelligence-led MDR: Benefits

