orange™ Cyberdefense

Managed Threat Detection [network]
for Microsoft 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 easilly move accross cloud applications and service providers within your hybrid environment.

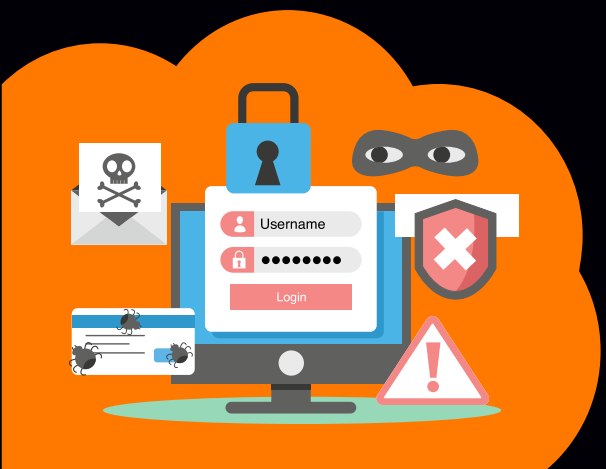
The impact can magnify quickly, with the attackers using the compromised account to inflict serious damage.

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

Protecting data where it's most vulnerable



Account Takeover

Stealing priviledged credentials enables attackers to act as malicious insider. Threat detection for Entra ID helps you to detect and stop identity misuse and accont takeover.

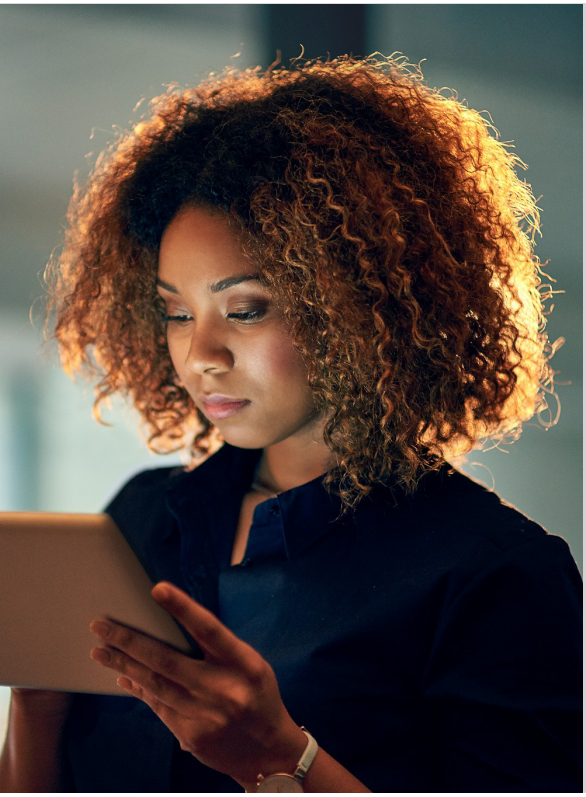
Data Breaches

Microsoft 365 is a popular target for attackers due to the wealth of vital information in contains. Detecting threats in M365 fast reduces the risk of costly data breaches.

Compliance

When storing sensitive data in Microsoft 365, complying to regulations such as GDPR is crucial. Threat detection capabilities help you to demonstrate compliance.

Find out more about Managed detection and response (MDR):
orangecyberdefense.com/global/mdr/



Benefits:

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

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

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

4. 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

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

6. Save time and money
Scales security efforts without draining resources

What to expect

Complete monitoring on accounts and identities

Early detection of unusual behaviour

Cyber resiliency against backdoor intrusion

Quick-time to value

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cyber security business unit of the Orange Group, providing managed security, managed threat detection and response services to organizations around the globe.

As the leading security services provider, we strive to build a safer digital society. Our global footprint with a European anchorage enables us to meet local
requirements and international standards, ensure data protection and privacy for our clients as well as for our employees.

We embed security into Orange Business solutions for multinationals worldwide.

Build a safer digital society

www.orangecyberdefense.com