



# Cloud Security Envisioning Workshop



## Learn how to put next-generation Microsoft Security tools to work for you

Do you have a good understanding of security vulnerabilities in your multi-cloud environment including VMs, databases, Azure storage and more? Are you aware of the number of suspected authentication activities across your Azure and multi-cloud environment? In short, are you confident about the cloud security posture of your organization?

### Improve your security posture with a Cloud Security Envisioning Workshop

As the use of cloud services continues to grow, cyber risks and threats continue to evolve. Get help achieving your

Azure and multi-cloud security objectives—and identify current and real threats—by scheduling a Cloud Security Envisioning Workshop.

We can help you develop a strategic plan customized for your organization and based on the recommendations of Microsoft experts in security. You'll gain visibility into immediate threats and vulnerabilities across Azure and multi-cloud environments, plus clarity and support on how to improve your security posture for the long term.

## Engagement highlights



Review your security goals and objectives



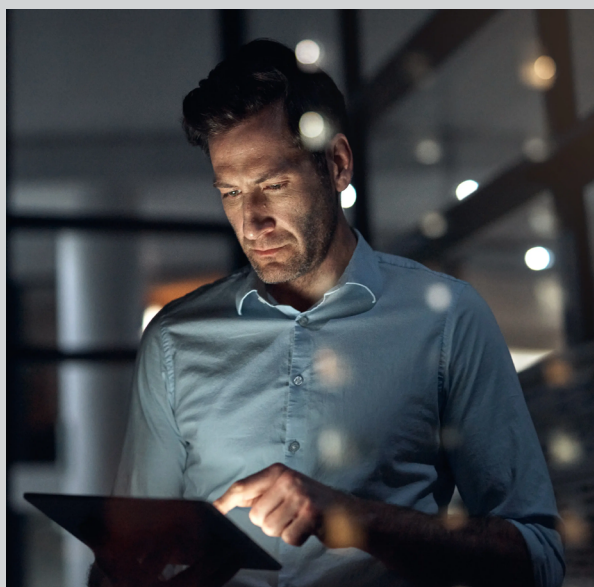
Identify real threats and discover vulnerabilities in your cloud environment



Map identified threats and vulnerabilities to specific solution recommendations



Develop joint plans and next steps



## Why you should participate

With the increasing complexity of identities, data, applications, devices, and infrastructure, it's critical to continuously assess and strengthen your organization's security posture.

By participating in this engagement, you will:

1. Uncover current and evolving security threats and identify vulnerabilities in your cloud environment
2. Collaboratively shape and document a security strategy tailored to your organization's needs
3. Gain deeper insights into how Microsoft Security tools can support your long-term security goals
4. Receive personalized, actionable guidance to help drive sustained improvements in your security journey



## What to expect

During this engagement, we'll partner with you to strengthen your organization's approach to cybersecurity. We'll help you better understand how to prioritize and mitigate potential attacks, with:

- Analysis of cybersecurity threats that are found targeting your organization.
- Actionable recommendations to help immediately mitigate the identified threats and discovered vulnerabilities.
- Visibility into vulnerabilities in your Azure and multi-cloud environments to better understand, prioritize and address vulnerabilities and misconfigurations across your organization.
- Long-term recommendations from Microsoft experts about your security strategy, with key initiatives and tactical next steps.
- Modular approach, allowing you to select three out of seven available modules aligned to your needs and requirements.

Selectable  
**Module**  
Defender for  
Servers

Selectable  
**Module**  
Defender for  
Databases

Selectable  
**Module**  
Defender for  
Storage

Selectable  
**Module**  
Defender for  
Containers

Selectable  
**Module**  
Defender for  
App service

Selectable  
**Module**  
Defender for  
AI Services

Selectable  
**Module**  
Security  
Exposure  
Management

## Who should participate

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- IT Security Architects
- IT Security Administrators
- IT Security Operations (Sec Ops)

## Why Orange Cyberdefense?

- We are a certified Microsoft Security Partner with recognized expertise across Defender, Sentinel, Entra ID, and Purview.
- Our engagements follow a proven, outcome-driven methodology designed to deliver measurable value. We align your business priorities with Microsoft's advanced security tools and demonstrate how they integrate across Microsoft 365 to provide unified protection and visibility.
- With a strong European presence and global reach, we offer trusted, enterprise-grade security services tailored to your organization.

