Microsoft Defender

An overview of Microsoft Defender's capabilities and Wanstor's Managed Defender service

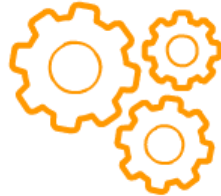# Agenda

+ Microsoft Defender: an overview

+ Key benefits of using Microsoft Defender

+ An insight into Wanstor's Managed Defender Service

wanstor

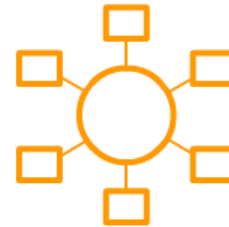# Microsoft Defender: An Overview

Microsoft 365 Defender: Unifying Enterprise Defence

Comprehensive suite for pre- and post-breach defence

Coordinates detection, prevention, investigation, and response

Covers endpoints, identities, email, and applications

Offers integrated protection against sophisticated attacks

3

wanstor

Microsoft Defender Suite

Endpoints

Cloud Apps

Cloud

Office

Identity

Defender for Endpoints
Helps enterprises protect their devices from cyber threats

Defender for Cloud Apps
Helps you monitor and protect your data in software as a service (SaaS) applications.

Defender for Cloud
A cloud-native application protection platform (CNAPP) that helps you secure your cloud-based applications from various cyber threats & vulnerabilities.

Defender for Office
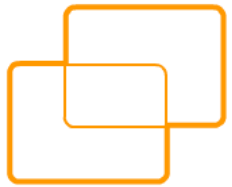Helps protect your email and collaboration tools from cyberthreats

Defender for Identity
Helps you protect your on-premises identities from advanced threats and insider attacks.

Unified Enterprise Defence
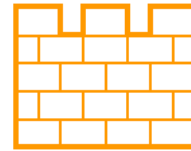
4

wanstor

Why do you need Defender for Endpoint?

Integrates with other Microsoft security solutions

Leverages power of the cloud and AI

Enables you to reduce your attack surface

Empowers you to investigate & respond to incidents

Supports various device platforms and OS

wanstor

Why do you need Defender for Cloud Apps?

Discover and control the use of SaaS apps across your organisation

Protect sensitive information in your SaaS apps

Defend against advanced attacks

Improve your security posture

Control how apps interact with each other and access your data

wanstor

Why do you need Defender for Cloud?

A development security operations (DevSecOps) solution that unifies security management at the code level across multiple-cloud and multiple-pipeline environments

A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches

A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads

wanstor

Why do I need Defender for Office?

Advanced protection

Post-breach investigation, hunting, and response capabilities

Improves your security posture

wanstor

Why do I need Defender for Identity?

It leverages the power of the cloud and artificial intelligence

It enables you to investigate and respond to incidents

It supports various identity platforms and protocols

wanstor

What is Wanstor's Service?

Consult
+ Discovery
+ Strategy
+ Metrics

Assess
+ Ensure configuration is best practice
+ Highlight industry change
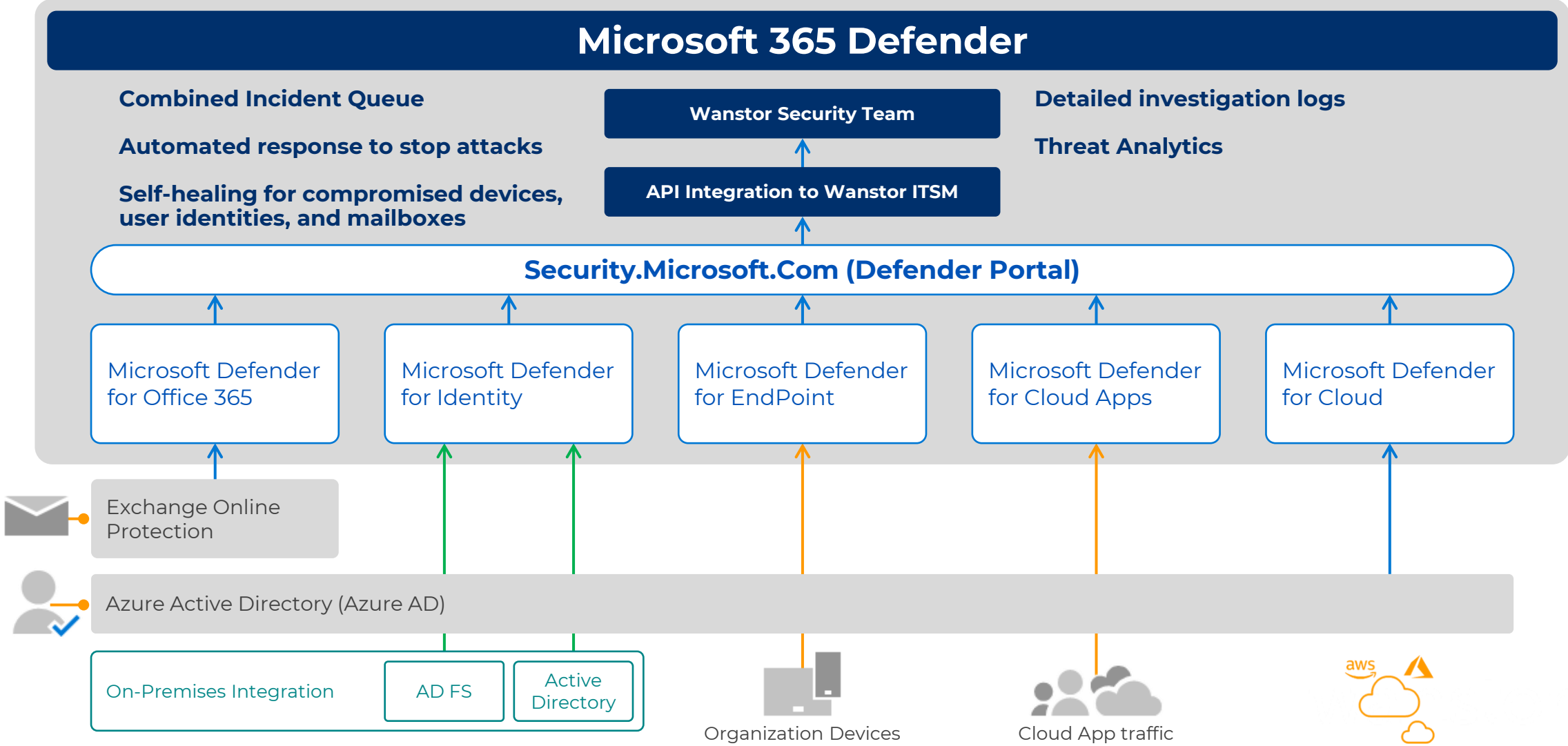+ Identify vulnerabilities

Discover
+ Highlight missing devices

Maintain
+ Lower device exposure score
+ Review CVE's
+ Ensure ASR rules are enforced
+ Ensure policies are in line with best practice

Manage
+ Monitoring
+ Support
+ Reporting
+ Optimization
+ Monthly re-occurring meetings with defender experts

wanstor

DETECT: Managed Detection and Response

Microsoft 365 Defender

Combined Incident Queue

Automated response to stop attacks

Self-healing for compromised devices, user identities, and mailboxes

Wanstor Security Team

API Integration to Wanstor ITSM

Detailed investigation logs

Threat Analytics

Security.Microsoft.Com (Defender Portal)

Microsoft Defender for Office 365	Microsoft Defender for Identity	Microsoft Defender for EndPoint	Microsoft Defender for Cloud Apps	Microsoft Defender for Cloud

Exchange Online Protection

Azure Active Directory (Azure AD)

On-Premises Integration

AD FS

Active Directory

Organization Devices

Cloud App traffic

aws

For more information, please visit www.wanstor.com or email info@wanstor.com

wanstor