

KI meets NIS-2:
Wie wir uns
gegen
Cyberangriffe
wappnen können



Was sagt ChatGPT zu den Maßnahmen von NIS-2? #1

SS

How can a company ensure compliance with the NIS-2 directive through specific actions?



To ensure compliance with the NIS-2 (Network and Information Systems) directive, a company can take several specific actions. Here are some key steps to consider:

1. **Understand the NIS-2 Directive:** Familiarize yourself with the requirements and provisions of the NIS-2 directive. Understand the scope of the directive and how it applies to your organization.
2. **Conduct a Risk Assessment:** Identify and assess the potential risks to your network and information systems. Evaluate vulnerabilities, threats, and potential impacts on critical services. This assessment will help you understand your organization's specific compliance needs.
3. **Develop a Security Strategy:** Based on the risk assessment, develop a comprehensive security strategy tailored to your organization's needs. This strategy should include preventive and reactive measures to mitigate risks and protect your network and information systems.
4. **Implement Technical and Organizational Measures:** Implement appropriate technical and organizational measures to enhance the security of your network and information systems. This may include measures such as access controls, encryption, incident response plans, regular system updates and patching, and employee training.
5. **Designate a Competent Authority:** Identify a competent authority within your organization responsible for overseeing compliance with the NIS-2 directive. This authority should have the necessary expertise and resources to manage and enforce compliance effectively.

Was sagt ChatGPT zu den Maßnahmen von NIS-2? #2

6. **Report Incidents:** Establish a process for reporting and responding to security incidents. Implement mechanisms to detect, manage, and report incidents promptly to the relevant authorities as required by the directive.
7. **Cooperate with Authorities and Other Operators:** Develop relationships and channels of communication with relevant authorities, other operators, and digital service providers. Collaborate with them to share information, best practices, and insights on cybersecurity and incident response.
8. **Maintain Documentation:** Keep records and documentation of your compliance efforts, risk assessments, security measures, incident responses, and any other relevant information. This documentation will demonstrate your commitment to compliance and serve as evidence of your due diligence.
9. **Regularly Review and Update:** Ensure that your compliance measures and security practices are regularly reviewed and updated. Stay informed about changes in the regulatory landscape and adapt your practices accordingly.
10. **Conduct Audits and Testing:** Regularly conduct audits and testing of your security measures to identify any weaknesses or areas for improvement. This can include vulnerability assessments, penetration testing, and tabletop exercises to simulate incident response scenarios.

Remember, the NIS-2 directive may have specific requirements and guidelines that vary depending on the country or region. It's crucial to consult the directive itself and seek legal advice to ensure accurate and up-to-date compliance.



Andreas Wach

Partner Solution Architect
XDR & SIEM with SOC
andreas.wach@microsoft.com




**Große Entfernungen
überwinden**



Was wird dich zum Ziel
bringen?



A low-angle, upward-looking shot of a large commercial airplane, likely a Boeing 747, flying against a bright blue sky. The sun is positioned directly behind the aircraft, creating a strong lens flare and illuminating the scene. The aircraft's four engines and its distinctive hump are visible. The text "Technologie ist nur ein Teil der Geschichte" is overlaid on the right side of the image.

Technologie ist nur
ein Teil der
Geschichte

Alles beginnt mit einem Plan!

... und zu wissen,
was wann wie
zu tun ist!



1. Understand the NIS-2 Directive: Familiarize yourself with the requirements and provisions of the NIS-2 directive. Understand the scope of the directive and how it applies to your organization.

8. Maintain Documentation: Keep records and documentation of your compliance efforts, risk assessments, security measures, incident responses, and any other relevant information. This documentation will demonstrate your commitment to compliance and serve as evidence of your due diligence.

Microsoft Purview Compliance Manager

Compliance Manager

Overview Improvement actions Solutions Assessments **Regulations** Alerts Alert policies

Review the list of regulations available to your organization. you can create assessments for specific regulations to track your compliance [regulations](#)

Free regulation licenses used **1/3** Purchased regulation licenses used **0/0**

[View details](#)

8 items **EU**

Filter  Reset  Filters

Service: **Any** ▾

Role type: **Any** ▾

Overarching regulation: **Any** ▾

Created by: **Any** ▾

Activation: **Any** ▾

Regulation	Availability	Created by	Last updated date	Overarching regulation	Created date
Premium templates (8)					
EU - Directive 2006/24/EC	Premium	Microsoft	7/15/2022	EU Dir 2006/24/EC	5/23/2022
EU - ePrivacy Directive 2002 ...	Premium	Microsoft	9/28/2022	EU ePrivacy Directive	5/23/2022
Directive 2013/40/EU Of The...	Premium	Microsoft	9/28/2022	EU Directive	5/23/2022
EU Decision on the adequat...	Premium	Microsoft	9/28/2022	EU Decision on the ade...	5/23/2022
EudraLex - The Rules Govern...	Premium	Microsoft	9/28/2022	EU - EudraLex Volume ...	5/23/2022
EU GDPR	Premium	Microsoft	9/30/2022	EU GDPR	7/15/2022
European Network and Infor...	Premium	Microsoft	9/28/2022	European Network and...	5/23/2022
UK - The Offshore Petroleu...	Premium	Microsoft	9/28/2022	UK - The Offshore Petr...	5/24/2022

How do we measure success?

What does “performance” mean?

2. **Conduct a Risk Assessment:** Identify and assess the potential risks to your network information systems. Evaluate vulnerabilities, threats, and potential impacts on services. This assessment will help you understand your organization's specific compliance needs.
3. **Develop a Security Strategy:** Based on the risk assessment, develop a comprehensive security strategy tailored to your organization's needs. This strategy should include preventive and reactive measures to mitigate risks and protect your network and information systems.
4. **Implement Technical and Organizational Measures:** Implement appropriate technical and organizational measures to enhance the security of your network and information systems. This may include measures such as access controls, encryption, incident response plans, regular system updates and patching, and employee training.
9. **Regularly Review and Update:** Ensure that your compliance measures and security practices are regularly reviewed and updated. Stay informed about changes in the regulatory landscape and adapt your practices accordingly.
10. **Conduct Audits and Testing:** Regularly conduct audits and testing of your security measures to identify any weaknesses or areas for improvement. This can include



Microsoft Purview Compliance Manager

Overall compliance score

Your compliance score: 48%



12300/25206 points achieved

Your points achieved ⓘ
328/ 12,784

Microsoft managed points achieved ⓘ
11,972/ 12,422

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
App governance	0/81 points	3
Attack Simulation Training	0/9 points	1
Audit	0/65 points	11

Key improvement actions

Not completed 900 | Completed 22 | Out of scope 0

Improvement action	Impact
Enable self-service password reset	+54 points
Turn on email scanning for antivirus solution	+54 points
Enable 'Consistent MIME Handling'	+54 points
Block email application from creating child processes	+54 points
Enable 'MIME Sniffing Safety Feature'	+54 points
Block outdated ActiveX controls	+54 points
Turn on scanning of downloaded files and attachments f...	+54 points
Enable Explorer Data Execution Prevention (DEP)	+54 points
Enable 'Safe DLL Search Mode'	+54 points

[View all improvement actions](#)

Microsoft Secure Score

...for continuous posture measurement

Microsoft Secure Score

[Overview](#) [Recommended actions](#) [History](#) [Metrics & trends](#)

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

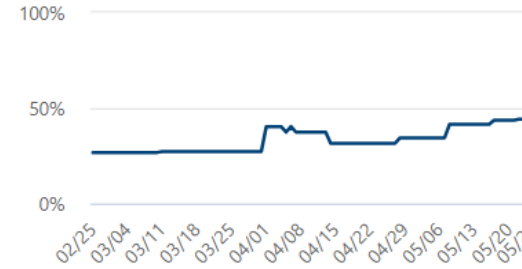
Applied filters:

Your secure score

Include ▾

Secure Score: 44.15%

107.29/243 points achieved



Breakdown points by: Category ▾

Identity 28.34%

Data 77.78%

Apps 47.98%

Points achieved Opportunity

Actions to review

Regressed ⓘ

0

To address ⓘ

35

Planned ⓘ

0

Risk accepted ⓘ

0

Recently updated ⓘ

0

Top recommended actions

Recommended action	Score impact	Status
Require multifactor authentication for administr...	+4.12%	<input type="radio"/> To address
Ensure all users can complete multifactor authen...	+3.7%	<input type="radio"/> To address
Ensure that intelligence for impersonation prote...	+3.29%	<input type="radio"/> To address
Move messages that are detected as impersonat...	+3.29%	<input type="radio"/> To address
Enable impersonated domain protection	+3.29%	<input type="radio"/> To address
Set the phishing email level threshold at 2 or hig...	+3.29%	<input type="radio"/> To address
Enable impersonated user protection	+3.29%	<input type="radio"/> To address

[View all](#)

Security Operation Center

... mit Microsoft Sentinel als SIEM/SOAR

Microsoft Sentinel | Incidents
Selected workspace: 'cybersecuritysoc'

Search

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents**
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Workspace manager (Preview)
- Data connectors
- Analytics
- Watchlist
- Automation
- Settings

Write permissions on the workspace are required to modify incidents

155 Open incidents 1 New incidents 154 Active incidents Open incidents by severity: High (6)

Search by ID, title, tags, owner or product

Severity: 2 selected Status: 2 selected

Auto-refresh incidents

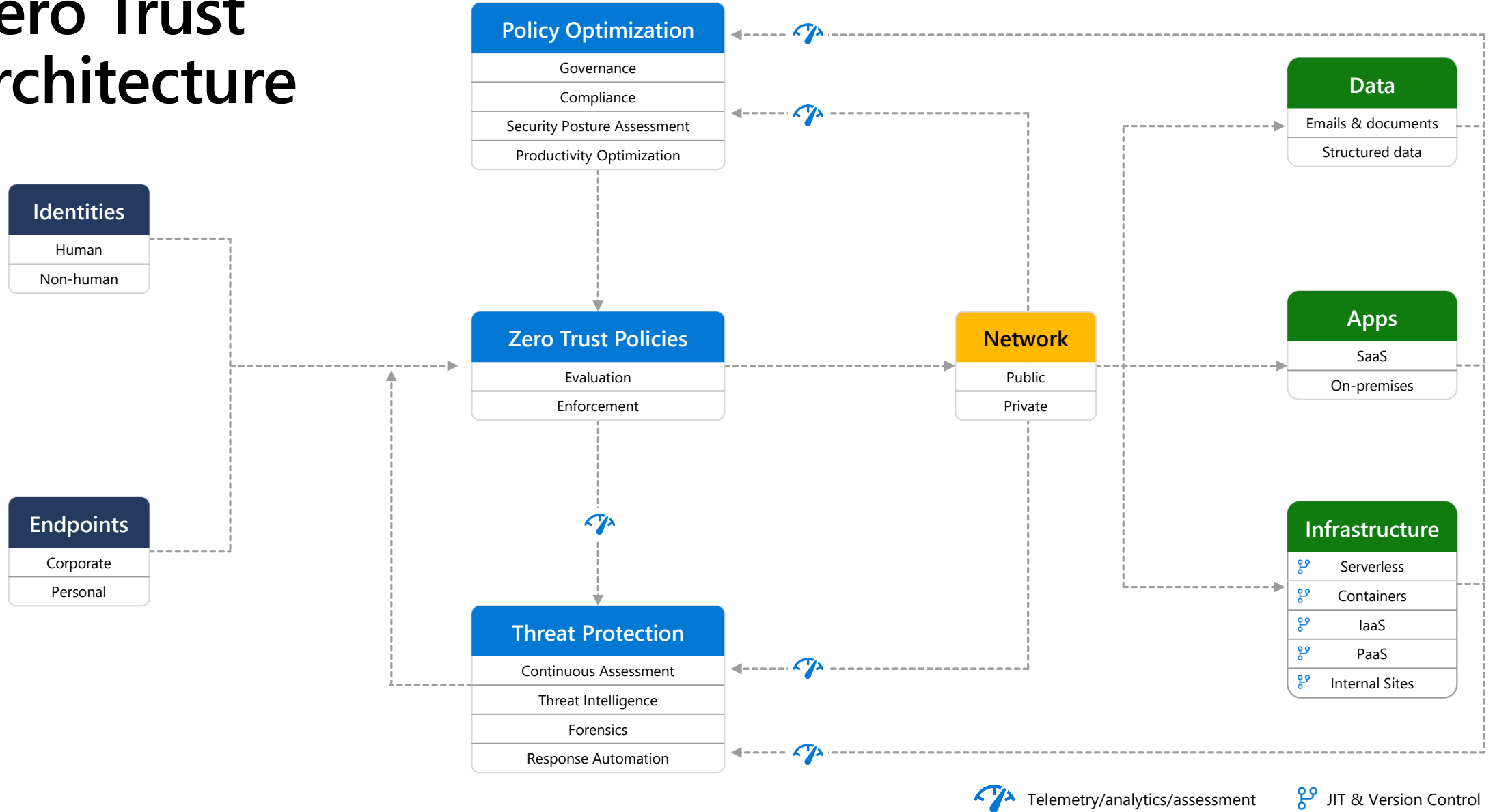
Severity	Title
Medium	Atypical travel involving one user
Medium	Initial access incident involving one user
Medium	Atypical travel
Medium	Unfamiliar sign-in properties
High	Microsoft Defender Threat Intelligence Analytics
Medium	Unfamiliar sign-in properties
Medium	Unfamiliar sign-in properties
High	SAP - (Preview) High volume of potentially sensitive data exported
Medium	Impossible travel activity
Medium	Impossible travel activity
High	TI map DestinationIP entity to CommonSecurityLog
Medium	Successful login from IP and failure from a different IP
High	A network session address 118.123.105.90 matched an IoC.
Medium	Azure portal brute-force
Medium	Atypical travel
High	SAP - (Preview) File Downloaded From a Malicious IP Address
Medium	Advanced Multistage Attack Detection

Beste Umsetzung für DICH

... die Technologie zur
Unterstützung

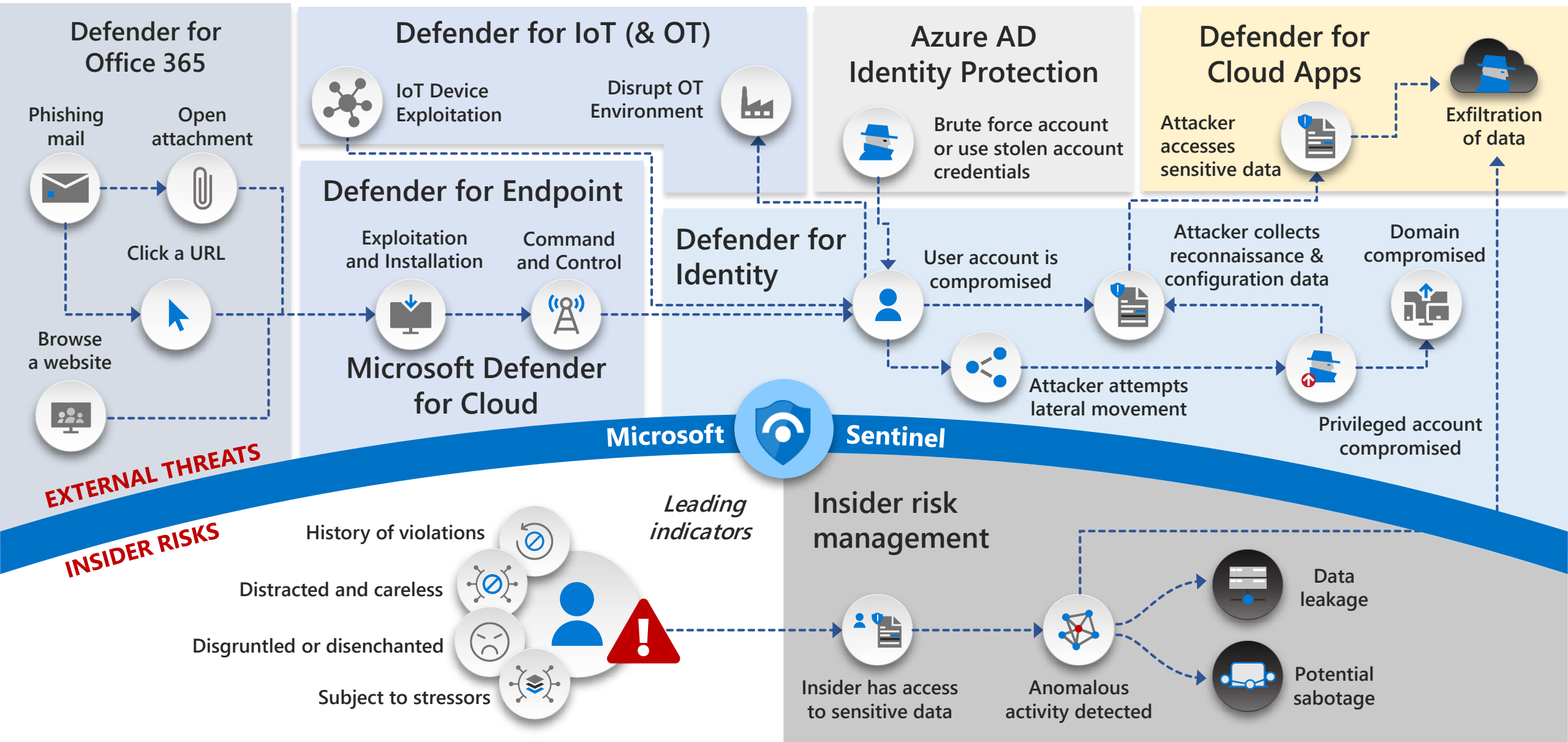


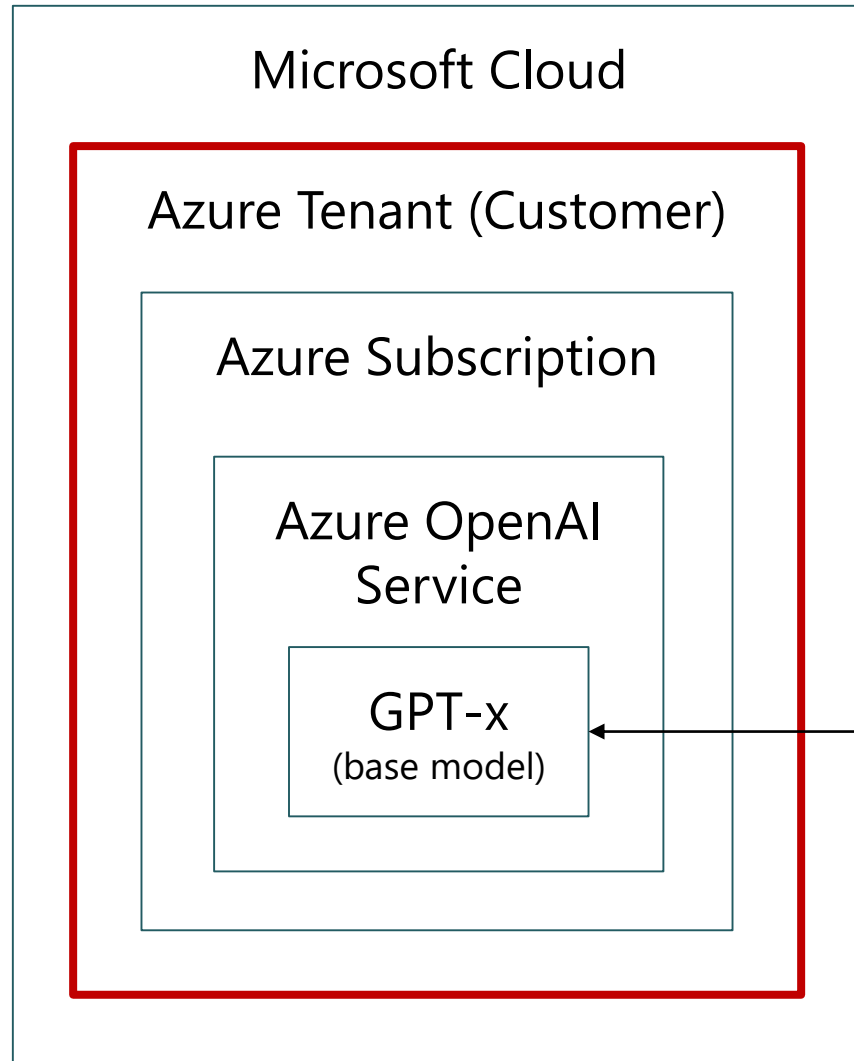
Zero Trust architecture



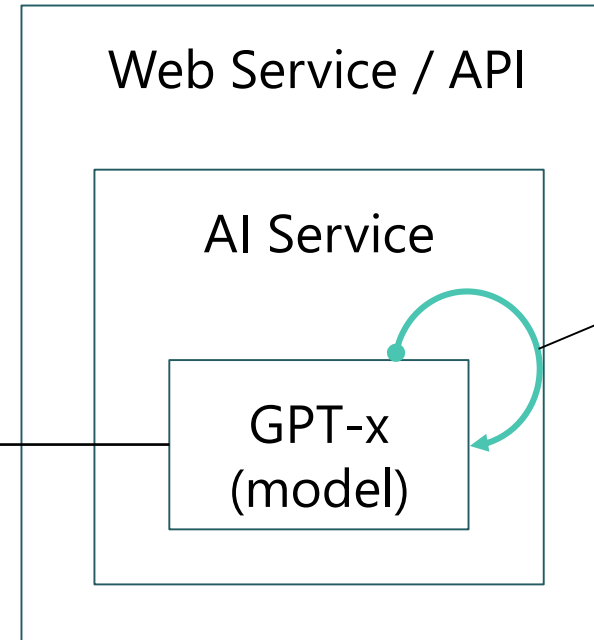
Defend across attack chains

Insider and external threats





Copy
(Instance)



Tuning
by OpenAI



Security Copilot boosting your SOC team



Security posture management

Discover whether your organization is susceptible to known vulnerabilities and exploits. Prioritize risks and address vulnerabilities with guided recommendations.



Incident response

Surface an ongoing incident, assess its scale, and get instructions to begin remediation based on proven tactics from real-world security incidents



Security reporting

Summarize any event, incident, or threat in seconds and prepare the information in a ready-to-share, customizable report for your desired audience

Wen kontaktieren?

...wenn etwas passiert ist

- 
- 6. Report Incidents: Establish a process for reporting and responding to security incidents. Implement mechanisms to detect, manage, and report incidents promptly to the relevant authorities as required by the directive.
 - 7. Cooperate with Authorities and Other Operators: Develop relationships and channels of communication with relevant authorities, other operators, and digital service providers. Collaborate with them to share information, best practices, and insights on cybersecurity and incident response.



Andreas Wach

Partner Solution Architect
XDR & SIEM with SOC
andreas.wach@microsoft.com

