Assessing the Cybersecurity of Microsoft Team Project 03

Archana Deepak Kumar,
Nicole Hessner
Team 06, CY545 - Data Privacy and Security,
Masters of Computer Science,
School of Technology & Computing,
City University of Seattle
deepakkumararchana@cityuniversity.edu
hessnernicole@cityuniversity.edu

Abstract

The focus of this cybersecurity assessment will be Microsoft, utilizing the Confidentiality, Integrity, Availability (CIA) security model. This model covers the application and infrastructure level components of an organization's network and describes the best cybersecurity practices followed by the organization, as well as a summary of the organizational functions required to manage information security risk in an enterprise environment. Microsoft follows the secure software development paradigm, integrating security at every phase of the development process starting from requirements analysis to maintenance. They also emphasize mitigation against the most prominent contemporary security threats, including malware, ransomware, social engineering, phishing, insider threats, and advanced persistent threats. Microsoft also conducts regular cybersecurity training, continuously invests in comprehensive cybersecurity solutions, and has adopted a zero-trust security strategy.

Keywords: Cybersecurity, Risk, Confidentiality, Access, Integrity

1. INTRODUCTION

Cybersecurity is a set of processes, best practices, and technology solutions that help protect critical computing and network systems from digital attacks. As the volume of digital information has increased and more people have the option to work from anywhere, bad actors have responded by developing sophisticated methods for gaining access to and exploiting personal, corporate, and government data for their own ends. Every year, the number of attacks increases, and adversaries develop new methods of evading detection. An effective cybersecurity program includes people, processes, and technology solutions that together reduce the risk of business disruption, financial loss, and reputational damage from an attack.

The three letters in the CIA model stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. The confidentiality, integrity, and availability of information is crucial to the operation of a business, and the CIA triad segments these three ideas into separate focal points. The CIA triad provides a simple, yet comprehensive, high-level checklist for the evaluation of security procedures and tools.
Microsoft uses the acronym "CIA" to represent the three pillars of cybersecurity.

1. Confidentiality: Ensuring secrets stay secret and ensuring that only authorized people can access files and accounts.

2. Integrity: Making sure that information is what it is supposed to be and that nobody has inserted, modified, or deleted information without the owner's permission or knowledge. For example, maliciously changing a number in a spreadsheet, or inserting malicious code into a packet in transit.

3. Access (Availability): Ensuring information and systems can be accessed when they are called. Examples of access issues would include a denial-of-service attack, where attackers flood a target system with network traffic to make accessing it by legitimate traffic impossible; or ransomware that encrypts the target system and prevents authorized users from using it.

2. DETAILS

The organization implements the following components to cover the various sections of the CIA model:

Application-level CIA Model Enforcement

1. Fortify Scan looks for security bugs like checking for data encryption protocols and denial of service (DOS). - Access
2. Dynamic Web Scan searches websites for cookies and cross site scripting. - Access
3. Encryption of data via protocols like PGP. – Confidentiality, Integrity, and Access
4. Role-based authorization of application access - Access
5. Authentication using Azure Active Directory login, complete with two-factor authentication. - Access
6. Component Governance (CG) scans for threats that are included in open-source libraries. - Access
7. Penetration testing is conducted by the Red Team to detect if attacks like SQL Injection or Denial of Service are possible. - Access
8. Data backups are conducted regularly to ensure data is available in the event of a server being rendered inoperable. - Access

Infrastructure-level CIA Model Enforcement

9. HTTPS protocol is enabled (on Computer Services) to encrypt network transmission of data. – Confidentiality/ Integrity
10. Ensure software and operating systems are up to date.
11. Data Encryption at rest is enabled on SQL Server and Azure Storage.– Confidentiality/ Integrity
12. Anti-Malware on Cloud Virtual Machines. – Confidentiality/ Integrity
13. Firewall is enabled on Virtual Machines and computers via services like WAF (Web Application Firewall). – Confidentiality/ Integrity
14. Microsoft Information Protection (MIP) and Microsoft Information Governance (MIG). Microsoft's XDR solution – M365 Defender – controls to strengthen the security posture around endpoints, servers, email, and hybrid AAD. – confidentiality
15. Microsoft Intune (MEM) also provides confidentiality to data with features such as Intune App Protection along with Windows Information Protection – confidentiality
16. Secret handling via Key Vault Azure Component– Confidentiality
17. Virtual Network to protect from any direct access of the network - Access
18. Microsoft 365 Defender & Defender for cloud: Antivirus and more to detect/protect against identities, endpoints, apps. This is available for phones, desktops, cloud machines – Confidentiality
19. Microsoft Sentinel (Confidentiality/Access): Enable Microsoft Sentinel, which is a scalable, cloud-native solution that provides:
20. Security information and event management (SIEM).
21. Security orchestration, automation, and response (SOAR).
22. Microsoft 365 has a plethora of encryption mechanisms such as Office Message Encryption (OME) for email, Bitlocker encryption with Intune, service encryption around Exchange Online, SharePoint Online, OneDrive for Business (ODfB) and Teams, with customer key and Microsoft managed keys – Integrity
23. Azure Storage Service Encryption helps to protect data at rest by automatically encrypting before pushing it to Azure-managed disks, Azure Blob Storage, Azure Files, or Azure Queue Storage, and it decrypts the data before retrieval. – Integrity
24. Transparent Data Encryption (TDE) helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups and transaction log files at rest without requiring changes to the application. – Integrity
25. M365 has multiple copies of data for redundancy purposes via Availability sets

and Availability zones. The internal DNS server and Azure DNS play a significant role in ensuring the data is available round the clock with minimum interruption. – Availability

3. RISK MANAGEMENT

Risk management at Microsoft is designed to anticipate new threats and provide ongoing security for the cloud systems and customers who use them. The organization assesses and manages the risks across the enterprise with the help of the ERM framework (Enterprise Risk Management). ERM enables an overall enterprise risk management process and works with management across the enterprise to identify and ensure accountability for Microsoft's most significant risks. ERM provides business units in Microsoft with common methodologies, tools, and goals for the risk management process.

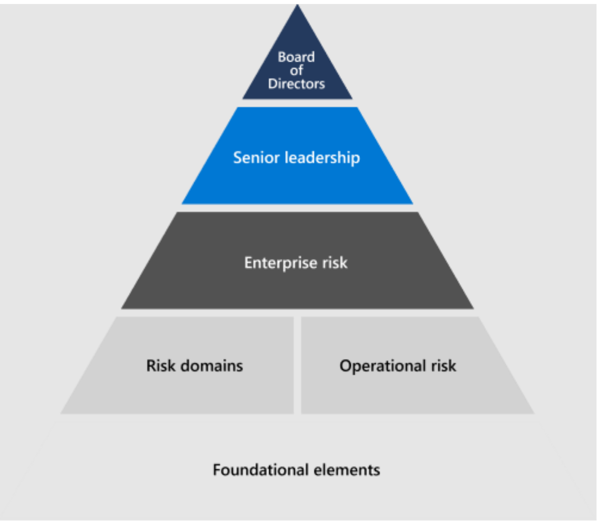


Figure 1: ERM Framework

All business units at Microsoft use these tools to conduct individual risk assessments as part of their risk management program.

The organization’s online services are regularly audited for compliance with external regulations and certifications such as ISO 27001/27002, ISO 27018 (Information Security Policies), ISO 22301, SOC 1, SOC 2, and SOC 3 (Annual Risk Assessment).

Microsoft 365 Risk Management Program
The purpose of the Microsoft 365 (M365) Risk Management program is to identify, assess, and manage risks to Microsoft 365. The Microsoft 365 Trust team is responsible for managing the Microsoft 365 Risk Management program and conducting the activities defined by the ERM program. Risk management activities fall into four phases: Identification, Assessment, Response, and Monitoring and Reporting.

The first phase deals with the identification of all types of risks in the M365 environment. Phase two deals with assessing the identified risks using metrics such as likelihood, impact, and control deficiency which are used to calculate the severity of risk using risk score. The third phase deals with risk response, which classifies the risk response as one of four categories: Tolerate, Operate, Monitor, and Improve. In the fourth phase, risks are monitored and reported to relevant stakeholders.

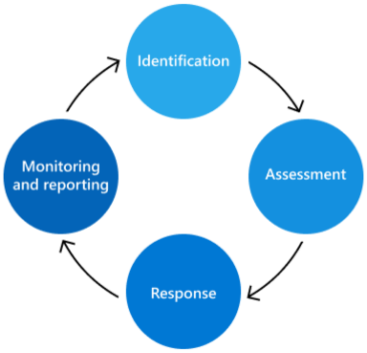


Figure 2: Risk Management Activities

4. CYBERSECURITY REFERENCE ARCHITECTURE

The Microsoft Cybersecurity Reference Architectures (MCRA) describes Microsoft’s cybersecurity capabilities, as shown in Appendix A. The diagrams describe how Microsoft’s security capabilities integrate with Microsoft platforms and third-party platforms like Microsoft 365, Microsoft Azure, 3rd party apps like ServiceNow and salesforce, and 3rd party platforms like Amazon Web Services (AWS) and Google Cloud Platform (GCP).

5. SECURITY PRINCIPLES

Microsoft Online Services teams identify critical system components and their dependencies as part of Business Continuity Management. In addition, Microsoft documents and tracks all external system connections to ensure only authorized connections are allowed in network firewall configurations.

Seven security principles lay the foundation for our framework of protecting the Microsoft 365 services from threats, detecting, and responding to any identified threats, and continuously assessing the security posture and improving services based on the results of those assessments:

1. **Data privacy**: Microsoft 365 services are designed to operate without engineers accessing customer data, unless explicitly requested and approved by the customer.

2. **Assume breach**: Personnel and services are treated as though compromise is a real possibility.

3. **Least privilege**: Access and permissions to resources are limited to only what is necessary to perform needed tasks.

4. **Breach boundaries**: Identities and infrastructure in one boundary are isolated from resources in other boundaries.
5. **Service fabric integrated security**: Security priorities and requirements are built into the design of new features and capabilities, ensuring that a strong security posture scales with each service.

6. **Automated and automatic**: Microsoft focuses on developing durable products and architectures that can intelligently and automatically enforce service security.

7. **Adaptive security**: Microsoft security capabilities adapt to, and are enhanced by, machine learning models, routine penetration testing, and automated assessments.

6. CYBER SECURITY THREATS

A cybersecurity threat is a deliberate attempt to gain access to an individual or organization's system. Bad actors continuously evolve their attack methods to evade detection and exploit new vulnerabilities, but they rely on some common methods, which can be prevented with some preparation.

Types of Cybersecurity Threats

1. **Malware:** Malware is a catchall term for any malicious software, including worms, ransomware, spyware, and viruses. It is designed to cause harm to computers or networks by altering or deleting files, extracting sensitive data like passwords and account numbers, or sending malicious emails or traffic. Malware may be installed by an attacker who gains access to the network, but often, individuals unwittingly deploy malware on their devices or company network after clicking on a bad link or downloading an infected attachment.

2. **Ransomware:** Ransomware is a form of extortion that uses malware to encrypt files, making them inaccessible. Attackers often extract data during a ransomware attack and may threaten to publish it if they do not receive payment. In exchange for a decryption key, victims must pay a ransom, typically in cryptocurrency. Not all decryption keys work, so payment does not guarantee that the files will be recovered.

3. **Social engineering**: In social engineering, attackers take advantage of people's trust to dupe them into handing over account information or downloading malware. In these attacks, bad actors masquerade as a known brand, coworker, or friend and use psychological techniques such as creating a sense of urgency to get people to do what they want.

4. **Phishing:** Phishing is a type of social engineering that uses emails, text messages, or voice mails that are from a reputable source to convince people to give up sensitive information or click on an unfamiliar link. Some phishing campaigns are sent to a vast number of people in the hope that one person will click. Other campaigns, called spear phishing, are more targeted and focus on a single person. For example, an adversary might pretend to be a job seeker to trick a recruiter into downloading an infected resume.

5. **Insider threats**: In an insider threat, people who already have access to some systems, such as employees, contractors, or customers, cause a security breach or financial loss. In some cases, this harm is unintentional, such as when an employee accidentally posts sensitive information to a personal cloud account. However, some insiders act maliciously.

6. **Advanced persistent threat**: In an advanced persistent threat, attackers gain access to systems, but remain undetected over an extended period. Adversaries research the target company's systems and steal data without triggering any defensive countermeasures.

7. CYBERSECURITY BEST PRACTICES

Microsoft follows the following cybersecurity best practices:

Adopt a Zero Trust Security Strategy

With more organizations adopting hybrid work models that give employees the flexibility to work in the office and remotely, a new security model is needed that protects people, devices, apps, and data no matter where they are located. A Zero Trust framework starts with the principle that access requests can no longer be implicitly trusted, even if it comes from inside the network. To mitigate the risk, an individual or organization must operate under the assumption that a breach has occurred and explicitly verify all access requests.

Employing least privilege access to give people access only to the resources they need and nothing more is a best practice that adds an additional layer of security. This can reduce the amount and sensitivity of data lost in event of a breach.

Conduct Regular Cybersecurity Training

Cybersecurity is not just the responsibility of security professionals. Today, people use work and personal devices interchangeably, and many cyberattacks start with a phishing email directed at an employee. Even large, well-resourced companies are falling prey to social engineering campaigns. Confronting cybercriminals requires that everyone works together to make the online world safer. Training a team includes information on how to safeguard their personal devices and help them recognize and stop attacks and conducting refreshers on this training regularly. Effectiveness of this program can be monitored with phishing simulations, in which the company's own security team sends out fake malicious emails to employees to determine how many are likely to fall prey to a real attack.

Institute Cybersecurity Processes

To reduce risk from cyberattacks, individuals and organizations should develop processes that help prevent, detect, and respond to an attack. Software and firmware should be patched and updated regularly to reduce vulnerabilities. Team members should be provided clear guidelines as to what steps to take in the event of an attack.

Cybersecurity processes do not need to be created from scratch. Guidance from existing cybersecurity standards organizations, such as the International Organization for Standardization (SOC) 2700 or the National Institute of Standards and Technology (NIST) have templates and guidelines for creating a process.

Invest in Comprehensive Solutions

Technology solutions that help address security issues improve every year. Many cybersecurity solutions use AI (Artificial Intelligence) and automation to detect and stop attacks automatically, without human intervention. Other technology helps make sense of what is going on in an environment with analytics and insights. Get a holistic view into your environment and eliminate gaps in coverage with comprehensive cybersecurity solutions that work together and with your ecosystem to safeguard your identities, endpoints, apps, and clouds.

8. MICROSOFT 365 DEFENDER

M365 Defender is a cloud-based enterprise defense suite which coordinates prevention, detection, investigation, and response across endpoints, apps, emails, and other applications.

Anatomy of a Cyber Security Attack

Appendix B contains an example illustrating an attack that is underway in which an Employee receives an email with an attachment and the employee unwittingly opens the attachment. This leads to a chain of events resulting in theft of sensitive data.

M365 Defender Architecture

Microsoft 365 Defender combines the signals from all the Defender components to provide extended detection and response (XDR) across domains. This includes a unified incident queue, automated response to stop attacks, self-healing, cross-threat hunting, and threat analytics. A diagram of the M365 Evaluation Architecture is included in Appendix C.

1. Defender for Office 365:

Defender for office 365 helps detect the phishing email and use certain rule to stop the mail entering Inbox. Exchange Online Protection (EOP) is integrated to provide end-to-end protection for incoming emails and attachments.

2. Defender for Endpoint:

Defender for Endpoint helps detect the network and device vulnerabilities that might be exploited otherwise.

3. Defender for Identity:

Defender for Identity helps detect sudden account changes like privilege escalation or high-risk lateral movement.

4. Defender for Cloud Apps:
Defender for cloud apps notices anomalous behavior like impossible travel, credential access, and unusual download, file shares and report these to security team.

5. Azure AD identity protection:
Azure AD Identity Protection evaluates risk data from billions of sign-in attempts and uses this data to evaluate the risk of each sign-in to your environment. This data is used by Azure AD to allow or prevent account access, depending on how Conditional Access policies are configured.

6. Evaluation process for M365 Defender cyber security:
Following steps are involved in the evaluation process for M365 Defender cyber security:

- Create the Evaluation Environment
- Enable Defender for Identity
- Enable Defender for Office 365
- Enable Defender for Endpoint
- Enable Microsoft Defender for cloud apps
- Investigate and Respond to threats
- Promote the trial to production

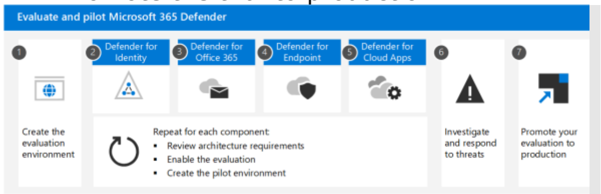

Evaluate and pilot Microsoft 365 Defender
1
2 Defender for Identity
3 Defender for Office 365
4 Defender for Endpoint
5 Defender for Cloud Apps
6
7
Create the evaluation environment
Repeat for each component:
Review architecture requirements
Enable the evaluation
Create the pilot environment
Investigate and respond to threats
Promote your evaluation to production

Figure 5: m365-defender-eval-process

9. FUTURE WORK

For future work, the team would like to assess cloud security in Microsoft through MS Azure Cloud Services. This assessment will provide customers with a comprehensive look at their cybersecurity infrastructure, including current software deployment and usage, and deliver key insights to help them establish the right processes for cyber-risk reduction in the cloud.

10. CONCLUSION

This paper concludes with assessing the cyber security at Microsoft using CIA triad. It assesses the risk management and cyber security best practices followed in the organization. It also assesses the different cyber security threats and identity access management through M365 Defender. Based on the information we were able to obtain, it appears that Microsoft has a comprehensive security plan in accordance with the Confidentiality, Integrity, and Availability (Access) model.

11. REFERENCES

Vacca, J. R. (2017). *Computer and Information Security Handbook* (3rd ed.). Morgan Kaufmann.

T. (n.d.-b). *Microsoft security documentation - Security documentation*. Microsoft Docs.

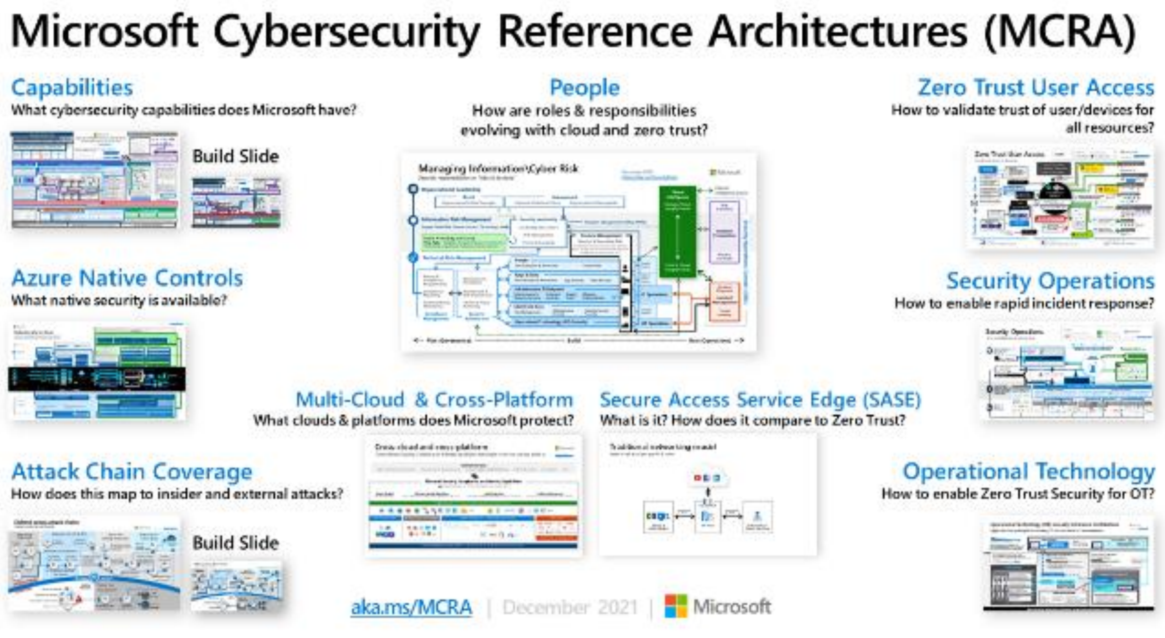
What is the CIA Triad and Why is it important? (n.d.). Fortinet.

CIA Triad – The Mother of Data Security. (n.d.). United States.

T. (2022, January 3). *Microsoft Services in Cybersecurity*. Microsoft Docs.

M. (n.d.-a). Microsoft 365 Defender documentation. Microsoft Docs

Appendix A
Microsoft Cybersecurity Reference Architectures (MCRA)



Microsoft Cybersecurity Reference Architectures (MCRA)

Capabilities
What cybersecurity capabilities does Microsoft have?

Build Slide

People
How are roles & responsibilities evolving with cloud and zero trust?

Managing Information/Cyber Risk

Zero Trust User Access
How to validate trust of user/devices for all resources?

Azure Native Controls
What native security is available?

Security Operations
How to enable rapid incident response?

Multi-Cloud & Cross-Platform
What clouds & platforms does Microsoft protect?

Secure Access Service Edge (SASE)
What is it? How does it compare to Zero Trust?

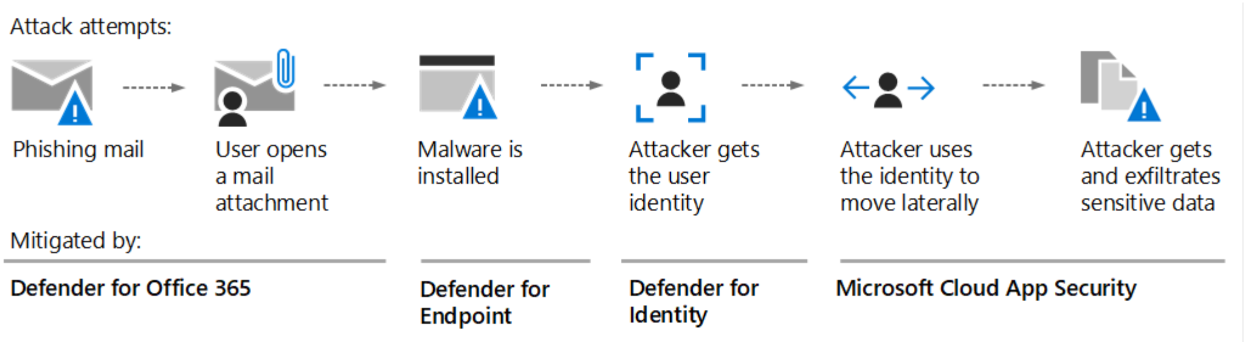
Attack Chain Coverage
How does this map to insider and external attacks?

Build Slide

Operational Technology
How to enable Zero Trust Security for OT?

aka.ms/MCRA | December 2021 | Microsoft

Appendix B
M365 Defender Evaluation Threat Chain



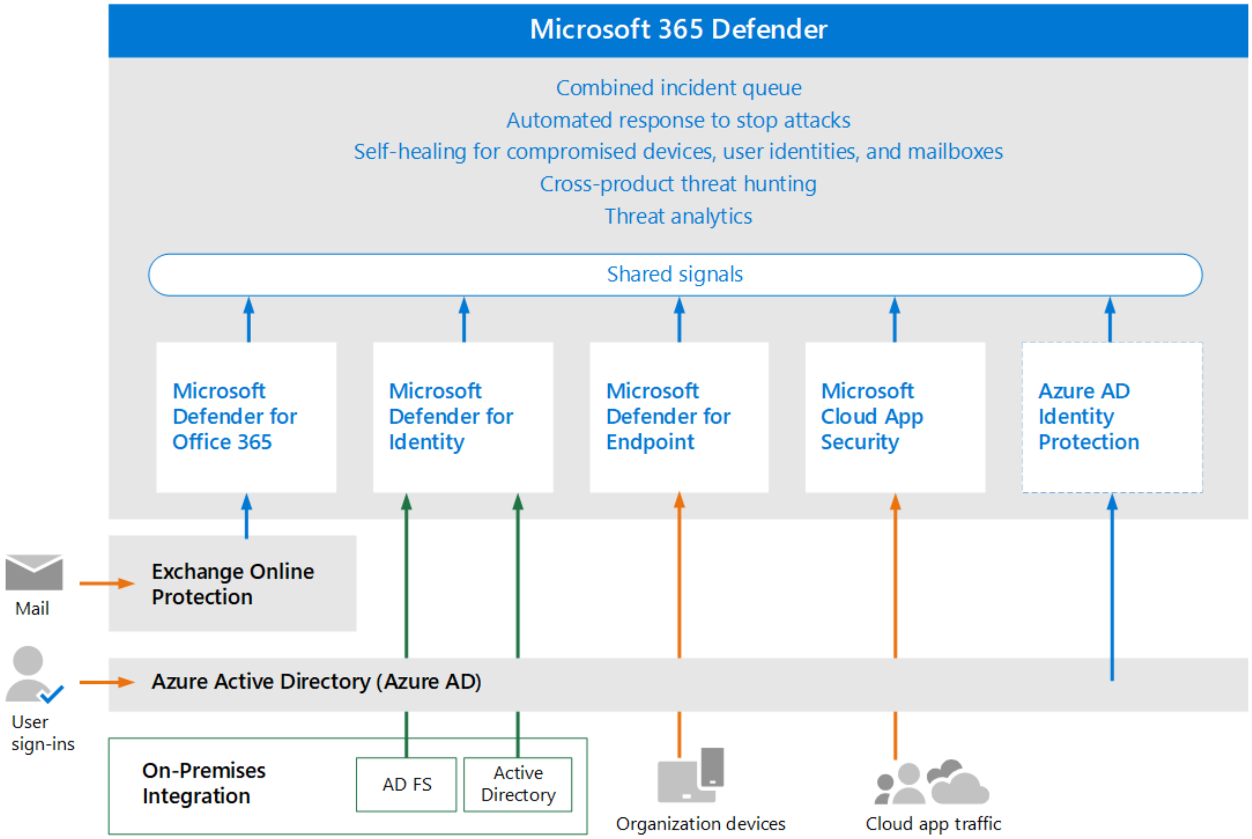
Attack attempts:

Phishing mail → User opens a mail attachment → Malware is installed → Attacker gets the user identity → Attacker uses the identity to move laterally → Attacker gets and exfiltrates sensitive data

Mitigated by:

Defender for Office 365 | **Defender for Endpoint** | **Defender for Identity** | **Microsoft Cloud App Security**

Appendix C


Microsoft 365 Defender
Combined incident queue
Automated response to stop attacks
Self-healing for compromised devices, user identities, and mailboxes
Cross-product threat hunting
Threat analytics
Shared signals
Microsoft Defender for Office 365
Microsoft Defender for Identity
Microsoft Defender for Endpoint
Microsoft Cloud App Security
Azure AD Identity Protection
Mail
Exchange Online Protection
User sign-ins
Azure Active Directory (Azure AD)
On-Premises Integration
AD FS
Active Directory
Organization devices
Cloud app traffic