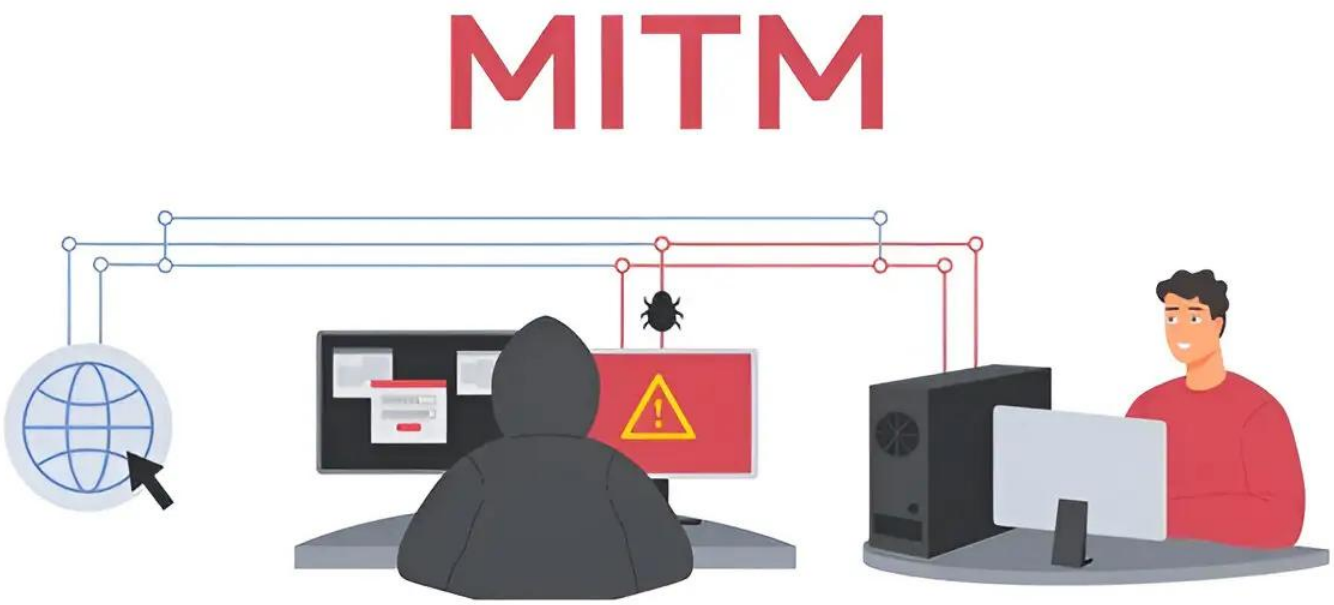
Man-in-the-Middle Attacks: DLP Solutions to the Rescue

Man-in-the-Middle (MITM) attacks continue to be one of the most dangerous cybersecurity threats. These attacks often involve intercepting data transfer between two parties, allowing the attacker to capture sensitive information. These attacks exploit vulnerabilities in communication to intercept, alter, or steal important information.

As organizations increasingly use online communication and cloud services, protecting data from being intercepted is essential. This piece investigates how MITM attacks occur, how they can be prevented, and the role of tools like Fidelis Network® DLP in defending against these threats.

What is a Man-in-the-Middle Attack?



A Man-in-the-Middle (MITM) attack is a complex threat. The attacker intercepts and secretly listens to and alters communication between two parties, without their knowledge. By doing so they access private data like login details, money transfers, and personal info without permission.

How Does a Man-in-the-Middle Attack Work?

An MITM attack works when attackers gain access to vulnerable communication channels. They secretly listen in, decode, and modify sensitive information between two individuals or devices. The attack follows a systematic approach, often involving social engineering and technical manipulation.

1. **Infiltration:** By taking advantage of an insecure and vulnerable network, such as public Wi-Fi, or by rerouting traffic using methods like DNS spoofing or ARP poisoning, the attacker secretly sneaks into the communication channel.
2. **Eavesdropping:** Once inside, the attacker monitors the communication, capturing

sensitive information like passwords, credit card numbers, or sensitive business data.
3. **Decryption or Spoofing:** If the data is encrypted, the attacker finds ways to break through—using SSL stripping, fake digital certificates, or even malware to decode it.
4. **Manipulation:** After gaining access, attackers can alter transactions, inject malicious payloads, or redirect users to phishing websites to gather more information.
5. **Data Theft or Impact:** Finally, the attacker either steals the data for their own gain or continues manipulating the communication to cause financial, reputational, or operational damages.

Types of Man-in-the-Middle Attack

MITM attacks can be grouped based on how attackers intercept and alter communication. Understanding the MITM attack types helps organizations find vulnerabilities and mitigate risks better. These attacks are also known as machine in the middle attacks, where the intercepting entity can be a bot, device, or malware.

1. Wi-Fi Eavesdropping

Attackers set up fake Wi-Fi networks that seem real to trick people into connecting. Once someone connects, the attackers can monitor and collect personal data being transmitted.

2. DNS Spoofing (Cache Poisoning)

Hackers alter DNS records to redirect people to fake websites instead of the real ones. This type of attack often targets the local area network, where DNS records can be manipulated to redirect traffic.

3. HTTPS Spoofing

Attackers make people believe they are on a secure website by using fake security certificates. This lets them intercept and decrypt sensitive information through methods like SSL hijacking.

4. Address Resolution Protocol Spoofing

Attackers send falsified ARP messages to associate their media access control (MAC) address with a legitimate IP address. This lets them intercept the data being sent between devices.

5. Email Hijacking

Attackers get unauthorized access to email accounts to intercept important messages or modify financial transactions, often capturing login credentials and targeting businesses.

6. Session Hijacking

Here hackers take over active session cookies to pretend to be users and get into accounts without needing passwords. This can lead to identity theft, where attackers use stolen session information to impersonate users.

7. VoIP Interception

Attackers aim at Voice over IP (VoIP) calls, eavesdropping on conversations or injecting malicious commands.

Each type takes advantage of different vulnerabilities, highlighting the importance of strong security measures and constant monitoring. Attackers may also exploit vulnerabilities in the user's web browser to intercept data during online transactions.

How to Detect a Man-in-the-Middle Attack?

Early detection of a MITM attack is important for reducing its effects. Here are the ways to recognize an ongoing attack:

Implementing robust endpoint security measures is crucial for early detection and prevention of MITM attacks.

1. Monitoring for Unusual Network Behavior:

- Sudden slowdowns or disruptions in the network.
- Devices connecting to unusual IP addresses or DNS servers.

2. Verifying Encryption

- Incorrect or mismatched SSL/TLS certificates.
- Alerts about unsecure websites, particularly on HTTPS connections.

3. Detecting Fake Wi-Fi Networks

- Multiple Wi-Fi networks with similar names.
- Devices automatically connect to unknown networks.

4. Unusual Communication Patterns

- Unexpected increases in data transfers or encrypted traffic.
- Unexpected redirects to different websites while browsing.

5. Using Security Tools

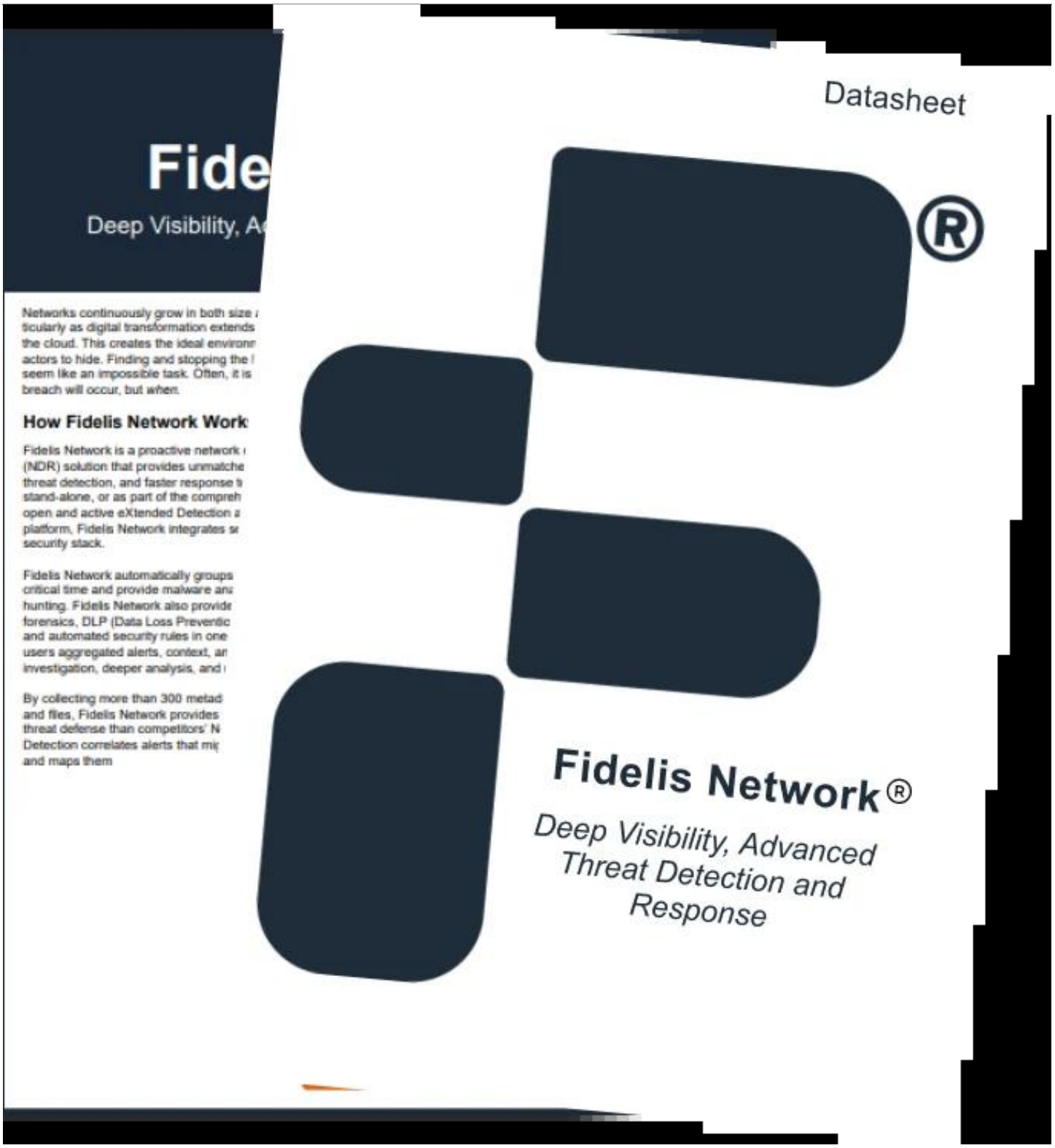
- Use advanced tools like IDS and DLP to identify any unauthorized traffic, monitor suspicious activities and respond to them to minimize the damage.

Identifying a Man-in-the-Middle attack involves advanced threat monitoring and immediate alerts, which are key features of Fidelis Network® DLP.

Fidelis Network®: Deep Visibility and Control aginst Advanced Threats

- Automated Threat Detection and Hunting Platform
- Threat Intelligence That Grows
- Accelerate Threat Response

Download Solution Brief



How to Prevent Man-in-the-Middle Attacks?

Preventing MITM attacks requires implementing security measures across networks, devices, and user behavior. Here are steps to do so:

1. Use Strong Security Protocols

- Make sure all communications happen uses strong protocols like HTTPS, SSL/TLS, and WPA3.

- Keep certificates up to date and validate their authenticity.

2. Protect Wi-Fi Networks

- Strictly don’t use public Wi-Fi for important tasks.
- Just in case you must make sure to use a VPN to keep data safe on untrusted networks.

3. Use Network Security Tools

- Set up firewalls, intrusion detection/prevention systems, and DLP solutions to monitor for unusual traffic.
- Use ARP and DNS security measures to prevent spoofing.

4. Keep Software Updated

- Regularly update operating systems, browsers, and security software to fix any gap in your security system.

5. Use Multi-Factor Authentication

- Add an extra layer of security for important accounts, making it harder for unauthorized users to get access.

6. Educate Employees

- Train employees and users how to spot phishing attempts and check SSL certificates.
- Encourage safe internet habits and awareness of fake networks.

Prevention is Better Than Cure

Prevention strategies should be combined with continuous monitoring to ensure that threats are identified before they can cause any damage.

Fidelis Network® DLP: A Man-in-the-Middle Attack Solution

Fidelis Network® DLP is a strong solution designed to fight against complex threats. It does more than just regular DLP tools, providing full protection for sensitive communications. It ensures secure data transfer by monitoring both encrypted and unencrypted communications.

How Fidelis Network® DLP can Help Reduce MITM Risks:

- **End-to-End Data Visibility:** It monitors both encrypted and unencrypted data to identify any unauthorized access.
- **Real-Time Anomaly Detection:** Quickly finds unusual activities over network like sudden increase in traffic, unusual increase in downloading of data, failed attempts to login, etc.
- **Automated Threat Mitigation:** Immediately stops attempts to steal data, keeping attackers from succeeding.

- **SSL/TLS Inspection:** This looks into encrypted channels to find fake certificates or SSL attacks.

By adding Fidelis Network DLP to their security system, companies can lower the chances of MITM attacks and better protect their sensitive information.

How to Remove Man-in-the-Middle Attack Threats?

We've learned how to spot and stop MITM attacks. Now, let's see how to clean up if one has already in the system, to reduce the harm. Implementing strong endpoint security measures is essential to prevent future attacks and ensure system integrity.

Steps to Remove a MITM Attack:

1. **Disconnect the Network:** Isolate the affected devices to stop further interception or data theft.
2. **Analyze Network Traffic:** Use DLP tools and network monitoring to find any unusual activity or unauthorized devices.
3. **Verify Certificates and Configurations:** Replace any compromised SSL certificates and check DNS settings for any modification.
4. **Purge Malware:** Scan systems to identify and remove any malware used during the attack.
5. **Fix Vulnerabilities:** Install necessary software updates and improve encryption protocols and patch all the gaps or loopholes.
6. **Conduct a Security Audit:** Investigate how severe the attack was, determine what data was compromised, and implement steps to stop it from happening again.

Are You Vulnerable to a MITM Attack?

- Do you connect to public Wi-Fi without using a VPN
- Is your device set to auto-connect to open networks?
- Are you using outdated browsers or apps without security updates?
- Do you visit websites without HTTPS encryption?
- Do you reuse weak or easily guessable passwords?
- Have you skipped enabling two-factor authentication (2FA) for critical accounts?
- Do you click on suspicious links or download unknown attachments?
- Are your DNS settings unprotected or not verified?
- Have you ignored installing antivirus or firewall protection?
- Do you share sensitive information over unsecured or unverified networks?

Conclusion

Man-in-the-Middle attacks remain a significant issue in cybersecurity. But they can be stopped or at least made less likely by using strong encryption and better security methods.

Fidelis Network DLP provides a complete solution for businesses to detect, prevent, and respond to MITM attacks, keeping sensitive data safe from being interception or altered.

Explore how Fidelis Security can help you!

Talk to Expert

Frequently Ask Questions

What industries are most targeted by MITM attacks?

Industries like finance, healthcare, e-commerce, and government sectors are targeted often as they handle sensitive data, making them prime targets for attackers looking to collect personal data. Businesses extensively using online channels for communication and fund transfers are especially at risk.

How does DNSSEC help prevent MITM attacks?

Domain Name System Security Extensions ensure that DNS records are verified, preventing attackers from redirecting traffic to fake websites through DNS spoofing.

Are mobile devices too vulnerable to MITM attacks?

Yes, mobile devices are actually easier to hack because many people connect them to public Wi-Fi, which isn’t very secure.

How much time do attackers need to carry out a successful MITM attack?

The time it takes can differ based on how complicated the attack is, and the vulnerabilities exploited. Some attacks can be ready to be executed in just a few minutes, while others can take a lot of preparation and effort for execution.