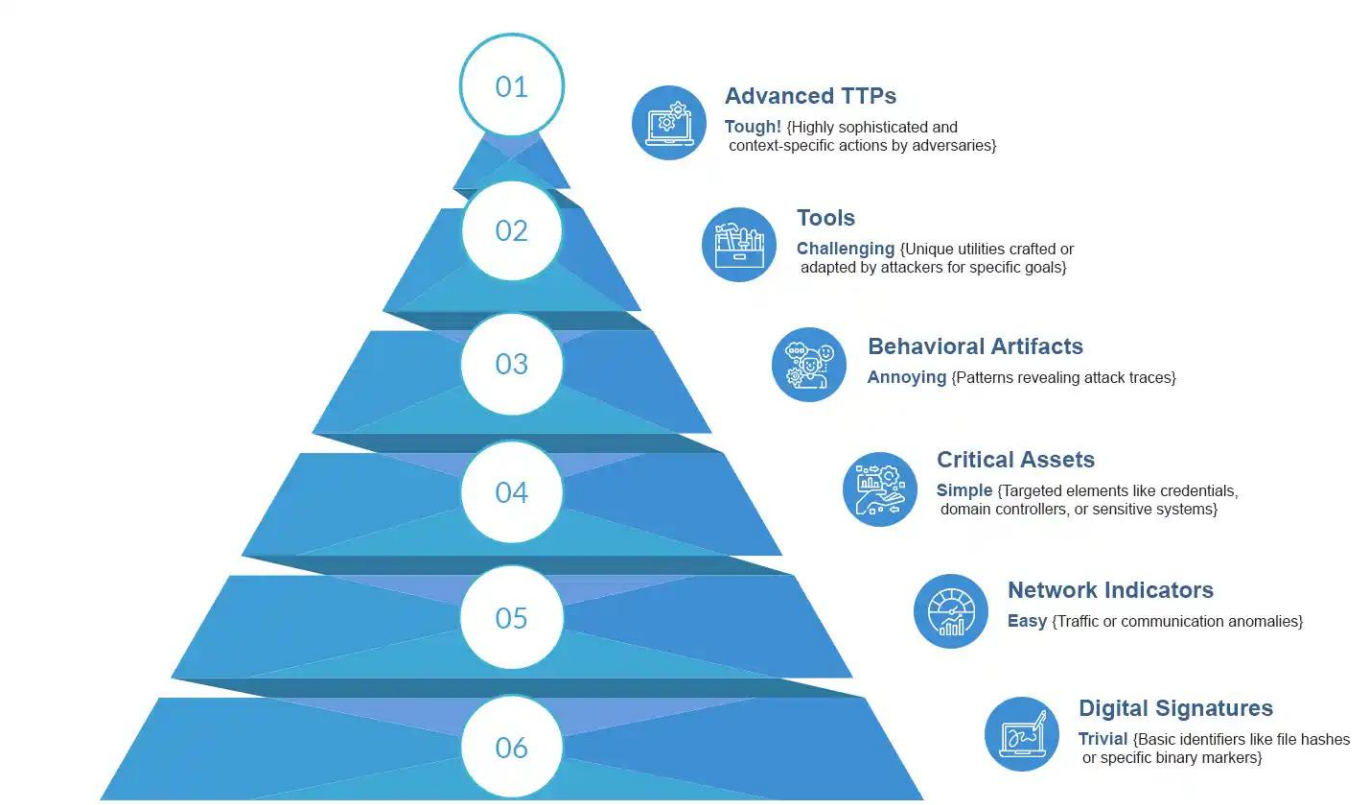
Applying MITRE ATT&CK framework to your Active Directory

Active Directory is a cornerstone of IT systems, handling user authentication, permissions, and access to resources. Its importance makes it a main target for attackers trying to get unauthorized access, escalate privileges, or cause disruptions. The MITRE ATT&CK framework, a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs), serves as a valuable tool to identify, prevent, and respond to such threats in your AD environment.

Companies can strengthen their Active Directory security by using the insights from the MITRE ATT&CK framework along with advanced tools like Fidelis Active Directory Intercept™. This tool can detect and mitigate attacker methods before they impact critical systems.

What is the MITRE ATT&CK Framework?



The MITRE ATT&CK framework categorizes and documents TTPs (tactics, techniques, and procedures) used by adversaries at various stages of an attack. It provides a structured approach to understanding adversarial behaviors, mapping these into a hierarchy of tactics (the “why”), techniques (the “how”), and sub-techniques.

As illustrated in the pyramid diagram, the framework highlights different attack components from easily identifiable indicators like hash values and IP addresses to more complex elements such as network artifacts, tools, and advanced TTPs.

For Active Directory, the MITRE ATT&CK framework is particularly valuable because it aligns

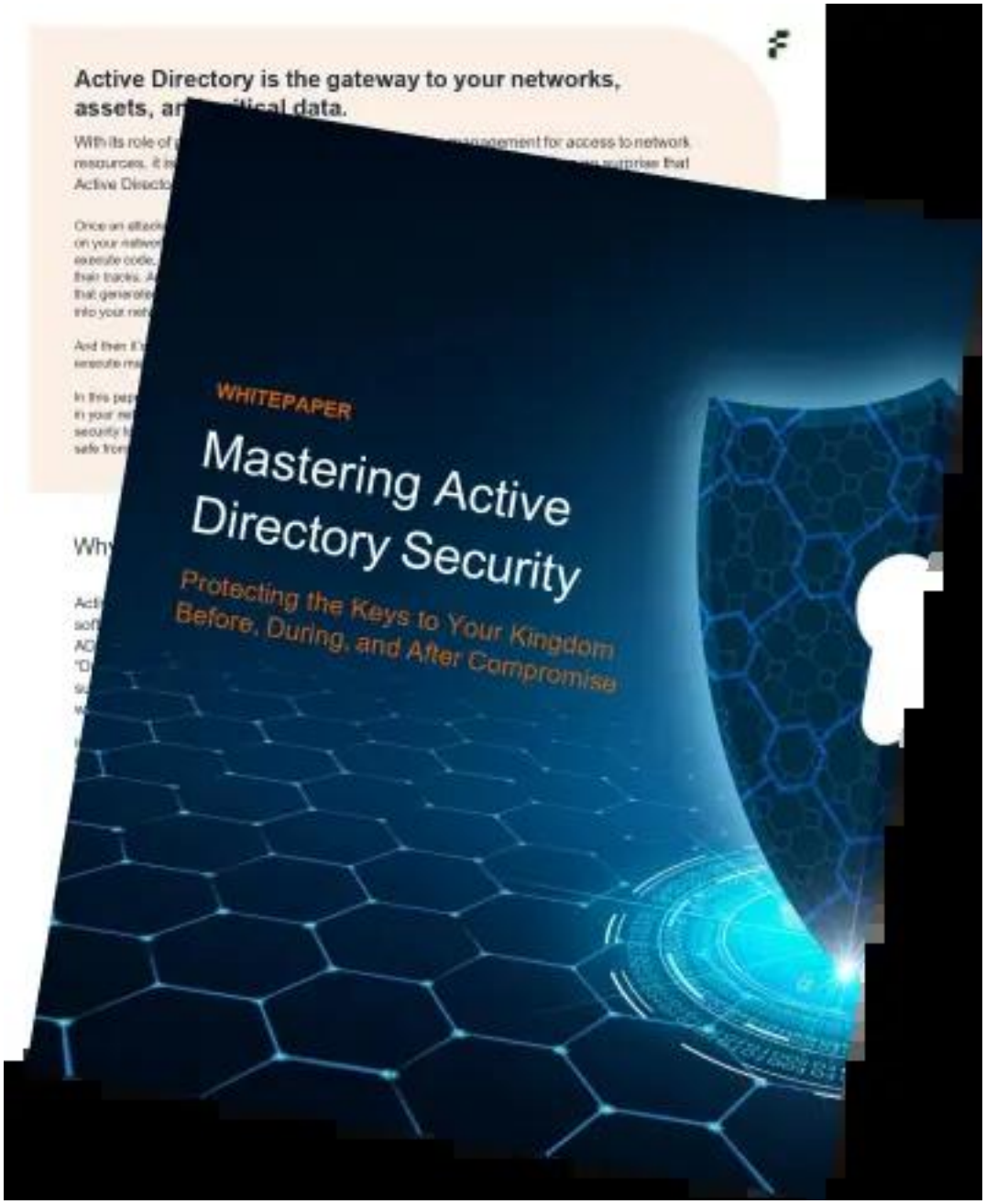
seamlessly with the ways attackers exploit identity and access systems. Security teams can leverage these insights to anticipate potential attack vectors, refine monitoring strategies, and enhance incident response efforts.

With solutions like Fidelis Active Directory Intercept™, these techniques are mapped to real-time monitoring and actionable response strategies, ensuring a stronger defense against AD attacks.

Mastering Active
Directory Security: Before, During, and After Compromise

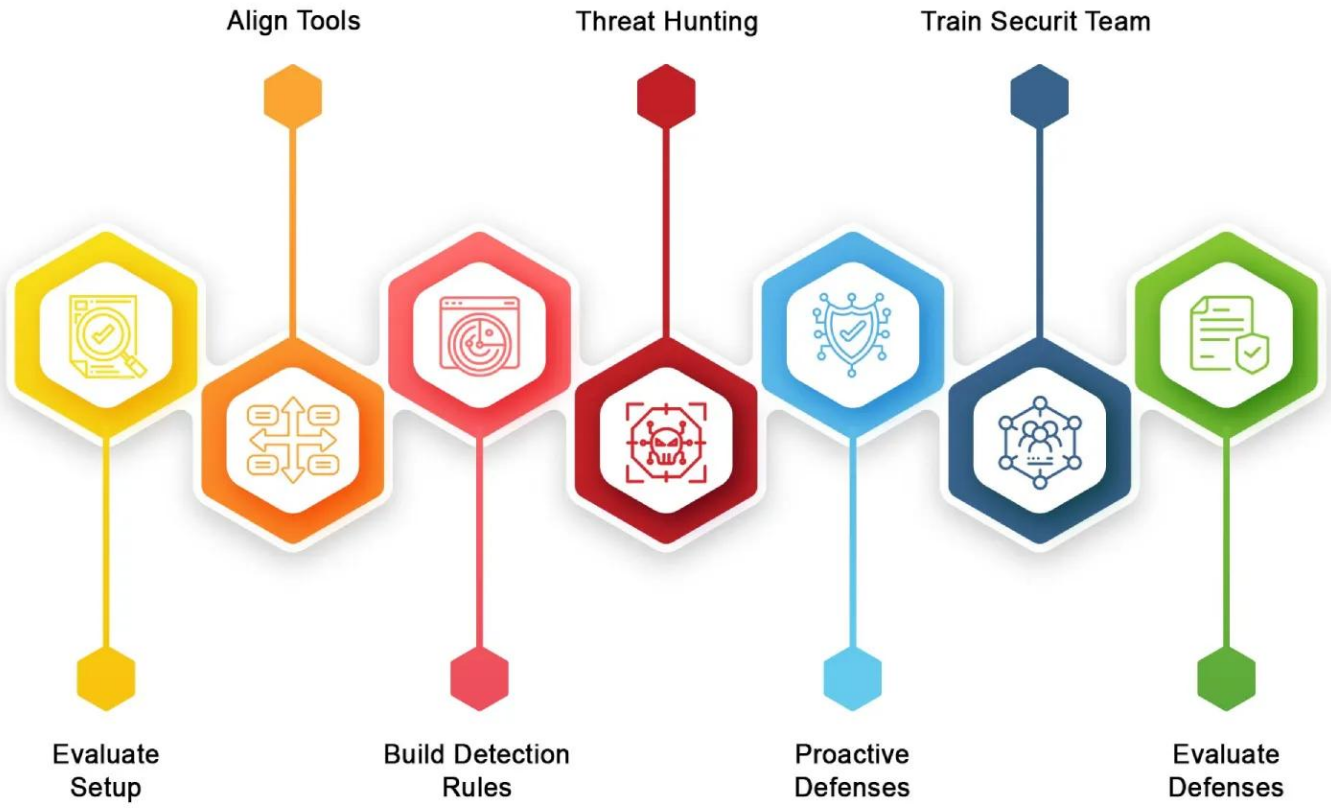
- Complete and Continuous Visibility
- Get Ahead of the Active Directory Threats
- Multi-Layered Defense

Download Whitepaper



How to Apply the MITRE ATT&CK Framework to Your AD Environment

Using the MITRE ATT&CK framework in your Active Directory environment is more than just understanding attack techniques. It consists of a systematic way to check for risks, set up defenses, and create measures to stop attackers. Here’s a detailed breakdown on how to use the MITRE ATT&CK framework in your AD security plan.



1. Evaluate Your Active Directory Setup

Before setting up defenses, you need to fully understand your Active Directory environment. This means finding important assets, assessing current security steps, and seeing where problems might be.

What to Do:

Map Out Your AD Environment: Make a detailed list of domain controllers, user accounts, group policies, and privileged accounts. Focus on old systems, service accounts, and accounts with extra permissions.

Identify Critical Dependencies: See how AD interacts with other systems and apps, especially those that use it for authentication and access.

Evaluate Current Security Measures: Assess existing configurations for password policies, access controls, and account permissions. Look for misconfigurations, like too many people

having access or outdated user accounts.

Key Deliverables:

- A detailed map of the AD environment.
- A list of important accounts, systems, and configurations that are at high risk.
- A prioritized list of vulnerabilities.

2. Align Existing Tools with MITRE ATT&CK

Many modern security tools, like Security Information and Event Management (SIEM) systems and Endpoint Detection and Response (EDR) solutions, come with built-in integrations to the MITRE ATT&CK framework. Using these tools helps you detect, analyze, and respond to AD threats.

What to Do:

Integrate MITRE ATT&CK Mappings: Pick tools that map detected events to specific ATT&CK tactics and techniques, giving you more information about the detected threats.

Enable Logging for AD Activities: Make sure logging is turned on for important AD events, like logins, modifications to accounts, group modifications, and policy updates.

Set Up Alerts for High-Risk Activities: Create alerts for actions that seem suspicious and match ATT&CK techniques, such as multiple failed login attempts, unusual requests for Kerberos tickets, or lateral movement patterns.

Key Deliverables:

- A well- optimized SIEM setup specifically for monitoring Active Directory.
- Personalized alert settings mapped to relevant ATT&CK techniques.
- Better awareness of security issues related to Active Directory.

3. Build Detection Rules

Detection rules are the basis for finding and mitigating possible attacks on your AD system. By paying attention to high-risk ATT&CK techniques, you can improve your monitoring and response actions.

What to Do:

Identify High-Priority ATT&CK Techniques: Look at techniques often used to attack AD, like stealing credentials, pass-the-hash attacks, and gaining more privileges.

Create Baselines: Establish a normal pattern for things like user logins, group policy changes, and account actions. Use these patterns as a baseline to spot anything unusual.

Make Custom Rules: Write detection rules that fit your system. For example:

- Alert when an account tries to access the AD database file (NTDS.dit).
- Flag unusual Kerberos ticket lifetimes or activity from service accounts.

Key Deliverables:

- A library of detection rules mapped to ATT&CK techniques.
- Anomaly detection models tailored for your Active Directory environment.
- A process for continuously refining detection rules.

4. Conduct Threat Hunting

Threat hunting involves actively looking for signs of harmful actions in your Active Directory (AD) environment. The MITRE ATT&CK framework provides a structured approach to guide these efforts.

What to Do:

Start with High-Impact Areas: Investigate common ways attackers get in, like stealing credentials or lateral movement, and check high-value systems like domain controllers.

Leverage Threat Information: Take advantage of ATT&CK's information to identify techniques used by active threats that target AD environments.

Check for Unusual Activities: Watch for signs of compromise, such as unusual login times, new accounts being created without reason, or attempts to access system from unknown IP addresses.

Key Deliverables:

- A guide for threat hunting that matches ATT&CK techniques.
- Regular threat hunting practice sessions.
- Detailed reports on findings and recommendations.

5. Implement Proactive Defenses

Proactive defenses are important to lower the chances of being attacked and to make it harder for attackers to succeed. These defenses should address vulnerabilities and add multiple layers of security for your AD environment.

What to Do:

Strengthen AD Configurations:

- Make sure passwords are strong.
- Disable unused accounts and legacy protocols like NTLM.
- Rotate the passwords and keys for important accounts and Kerberos regularly.

Control Access: Use the principle of least privilege.

Add Extra Security:

- Use Privileged Access Management (PAM) to protect and monitor admin accounts.
- Enable Windows Credential Guard to protect against credential theft.
- Divide your network into smaller segments to limit lateral movement.

Key Deliverables:

- A secure AD environment with reduced chances of being attacked.
- Automated protection for important accounts and systems.
- Better protection against credential-based attacks.

6. Train and Educate Your Security Team

Even the best tools and defenses won't work if the people using them aren't skilled. Training your team to understand and use the MITRE ATT&CK framework is crucial for long-term success.

What to Do:

Provide Framework Training: Hold workshops or training sessions to teach your team about MITRE ATT&CK tactics, techniques, and procedures (TTPs).

Simulate Attack Scenarios: Use exercises and tests to simulate real-world attacks on your environment. This helps your team learn how to detect and respond to threats.

Encourage Continuous Learning: Make sure your team stays updated about new ATT&CK techniques and emerging threats that target AD.

Key Deliverables:

- A security team that is well-trained and skilled in using ATT&CK-based defenses.
- Improved detection and response capabilities for AD-specific threats.
- A team culture that values continuous learning and improvement.

7. Evaluate and Evolve Your Defenses

Cyber threats are always evolving, and so should your defenses. Review your security posture regularly to make sure it can handle new and emerging attacks.

What to Do:

Conduct Regular Assessments: Use tools to find vulnerabilities and test how good your AD security controls are.

Update Detection Rules: Refine detection rules based on what you learned from incidents or

threat-hunting exercises.

Leverage ATT&CK Updates: Look at the latest updates from the ATT&CK framework and add new strategies to protect yourself.

Key Deliverables:

- A security plan that is always current and can adapt to new threats.
- Getting better at detection, prevention, and response capabilities.
- Resilience against advanced and evolving threats.

Security Checklist: Hardening
Your Active Directory with
Advanced Strategies

- Security Checklist
- Advanced Strategies for AD Security
- Multi-Layered AD Defense

Download Whitepaper

Benefits of Applying the MITRE ATT&CK Framework to AD

The MITRE ATT&CK framework is not just a guide to understand how attackers work—it's a strong tool that gives actionable insights and strategies to improve Active Directory security. When applied effectively, it enhances security in several ways. Here's a detailed exploration of the benefits:

1. Complete Understanding of Threats

The MITRE ATT&CK framework helps organizations learn about the tactics, techniques, and procedures (TTPs) attackers use.

How It Helps:

- It shows how attackers use AD at various stages of an attack, from the start to the end.
- Highlights techniques like stealing credentials or lateral movement that attackers use to compromise AD.
- By understanding specific threats, you can focus on defending against the most important and dangerous techniques.

With all this your organization becomes better at recognizing the risks to AD environment and can use resources wisely to reduce the risks.

2. Enhanced Detection Capabilities

Using ATT&CK can help you better detect and respond to unusual actions in your AD environment.

How It Helps:

- Security tools that align with ATT&CK can map alerts directly to known attack techniques, making it easier to understand and pinpoint threats.
- The framework helps you look for possible security breaches in AD, like unusual Kerberos behavior or odd login patterns.
- It encourages enablement of detailed logs for important AD activities, making it simpler to find signs of a security breach.

You can catch attacks sooner, cutting down the time attackers have to achieve their goals.

3. Better Incident Response and Remediation

When an attack happens, the MITRE ATT&CK framework helps us understand and deal with the threat in a clear way.

How It Helps:

- It connects detected suspicious actions to specific ATT&CK techniques, helping teams see how the attacker works and what they want.
- Knowing the techniques used, teams can quickly implement countermeasures to disrupt the attack.
- It provides insights into how attackers worked within the system, so you can improve your defenses and fix any security gaps.

Dealing with incidents becomes quicker, more effective, and better planned, which lowers the potential impact of breaches.

4. Proactive Defense Building

ATT&CK encourages organizations to be proactive instead of reactive, focusing on making Active Directory more secure against possible attack paths.

How It Helps:

- Use ATT&CK to mimic attacker behavior in AD, finding vulnerabilities before they can be exploited.
- Helps focus on preventive actions like disabling unused protocols, enforcing strong password policies, and protecting privileged accounts.
- The constantly changing nature of ATT&CK keeps your defenses up-to-date with new threats targeting AD.

Your AD environment becomes more resistant to attacks, with a reduced attack surface and stronger preventative measures.

5. Industry-Recognized Framework for Benchmarking

Using MITRE ATT&CK helps organizations compare their AD defenses against industry best practices and peer organizations.

How It Helps:

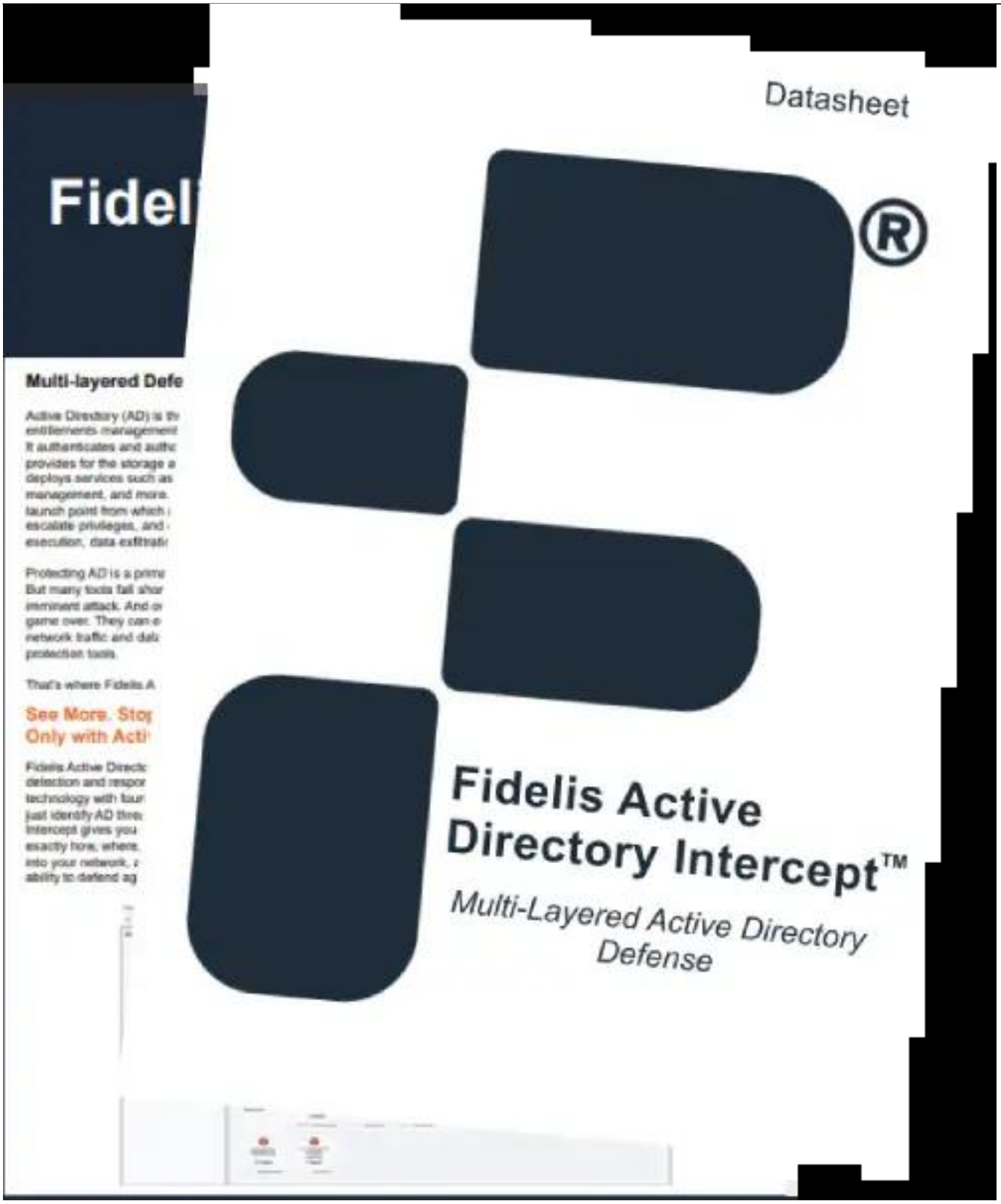
- Let’s you measure how strong your AD security strategy is using a widely recognized framework.
- Demonstrates a structured approach to securing AD, which helps with complying with rules and regulations and being ready for audit.
- Helps you see how your organization’s security measures stack up against industry standards.

You feel more confident about your security methods and demonstrate your commitment to robust AD defenses to stakeholders.

See how Fidelis see, detect, and defend against AD threats seamlessly.

- Advanced Threat Detection
- MITRE ATT&CK Alignment
- Proactive Threat Response

Download the Data Sheet



Conclusion

Using the MITRE ATT&CK framework in Active Directory environment helps organizations protect themselves from attackers by mapping real-world attack techniques to tailored defenses. When paired with advanced tools like Fidelis Active Directory Intercept™, it becomes a strong approach for keeping Active Directory deployments safe from modern cyber threats. By incorporating this framework into your Active Directory defense plan, you make sure your organization has cutting-edge tools to anticipate, detect, and neutralize attacks before they escalate.

Frequently Ask Questions

Why is the MITRE ATT&CK framework important for Active Directory security?

The MITRE ATT&CK framework is important as it offers:

- A structured way to understand how attackers operate
- Improve the ability to detect and respond
- Helps companies protect their AD systems from modern threats

How does Fidelis Active Directory Intercept™ fit with the MITRE ATT&CK framework?

Fidelis Active Directory Intercept™ maps the techniques attackers use directly to the MITRE ATT&CK strategies, helping organizations detect and respond to Active Directory threats in real time.

What are some typical MITRE ATT&CK techniques that target Active Directory?

Common techniques include:

- Credential dumping
- Lateral movement
- Golden Ticket attacks

Fidelis Active Directory Intercept™ can help find and mitigate these attacks effectively.