# Securing Endpoints with MITRE ATT&CK: From Theory to Practice

MITRE ATT&CK has become the go-to knowledge base for understanding how attackers operate since 2013. The framework's 12 tactical categories map out attack stages from original access to final impact. Security teams can spot and block threats at multiple points before any damage occurs.

This piece shows how companies can utilize MITRE ATT&CK's framework to boost their EDR. You'll find practical strategies for mapping EDR to Mitre ATT&CK, key tactics for complete endpoint security, and ways Fidelis Endpoint® helps build a strong security foundation.

## Understanding MITRE ATT&CK Framework for Endpoint Protection

MITRE ATT&CK framework is the life-blood of modern endpoint security strategies. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) has become a globally available knowledge base that documents ground cyber adversary behaviors.

The framework started as a research project in 2013 and has grown into a vital resource for cybersecurity professionals. MITRE ATT&CK stands out from theoretical security models because it draws from actual attack patterns, which makes it practical for defending against current threats. The framework's detailed structure sets it apart. Tactics show attackers' main goals like gaining initial access or stealing att&ck data.

### MITRE ATT&CK comes with three specialized matrices:

- Enterprise Matrix: Covers Windows, macOS, Linux, and other enterprise operating systems
- Mobile Matrix: Addresses iOS and Android platforms
- ICS Matrix: Focuses on industrial control systems

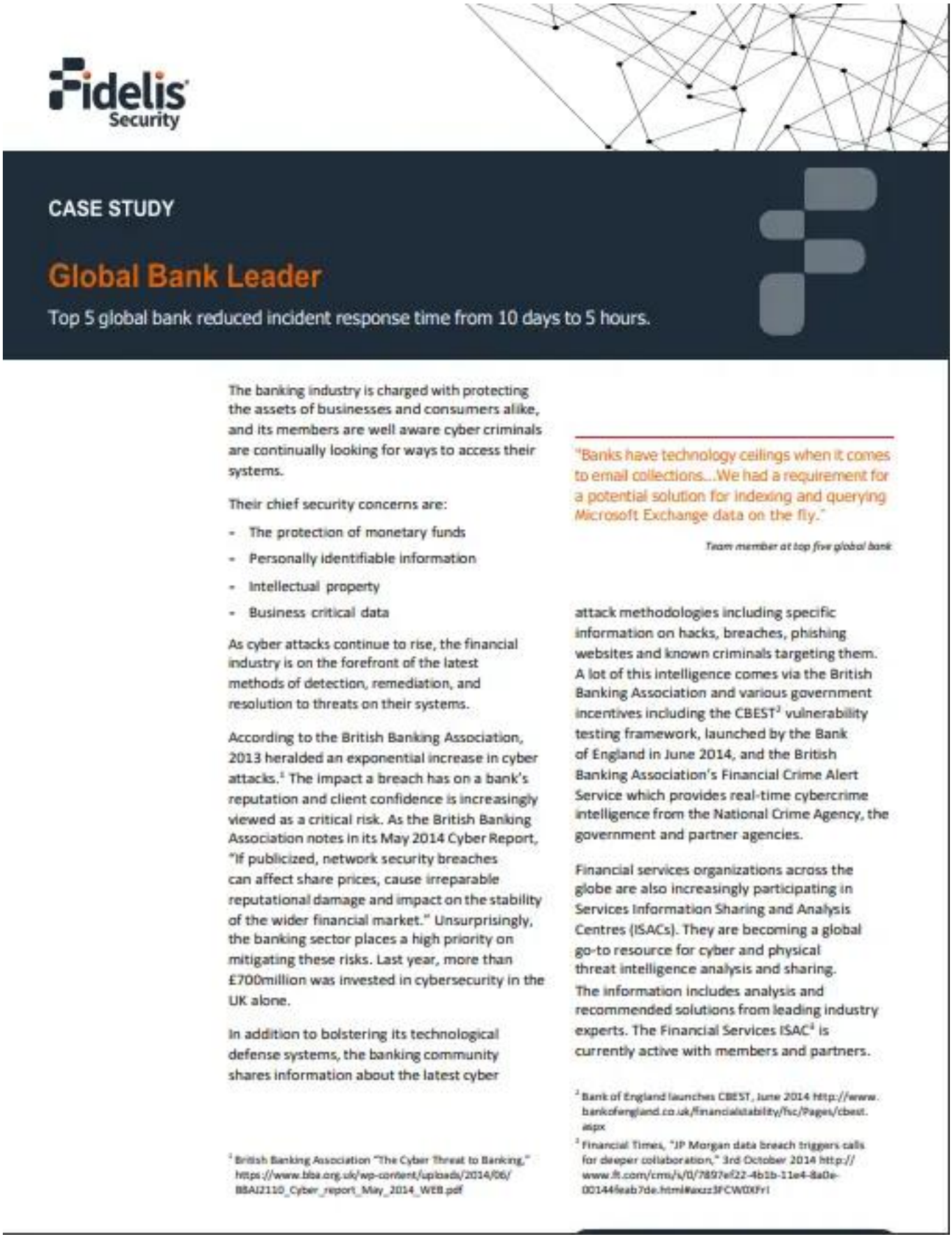
The framework's power comes from connecting attackers and defenders. Security professionals now have a common language that makes shared communication about threats easier and team collaboration smooth. On top of that, it helps companies find critical security gaps and focus their efforts on the most important threats.

Fidelis Security's Endpoint® solution incorporates MITRE ATT&CK to provide standard vocabulary and descriptions that improve threat detection and response. Our customers can map their EDR capabilities to the framework and find weak spots in their security setup.

How a Global Bank Slashed Response Time

- Achieved faster threat detection
- Reduced incident response from days to minutes
- Gained full visibility across hybrid environments

[Read the Full Case Study]



Fidelis Security

CASE STUDY

## Global Bank Leader

Top 5 global bank reduced incident response time from 10 days to 5 hours.

The banking industry is charged with protecting the assets of businesses and consumers alike, and its members are well aware cyber criminals are continually looking for ways to access their systems.

Their chief security concerns are:

- The protection of monetary funds
- Personally identifiable information
- Intellectual property
- Business critical data

As cyber attacks continue to rise, the financial industry is on the forefront of the latest methods of detection, remediation, and resolution to threats on their systems.

According to the British Banking Association, 2013 heralded an exponential increase in cyber attacks.[1] The impact a breach has on a bank's reputation and client confidence is increasingly viewed as a critical risk. As the British Banking Association notes in its May 2014 Cyber Report, "If publicized, network security breaches can affect share prices, cause irreparable reputational damage and impact on the stability of the wider financial market." Unsurprisingly, the banking sector places a high priority on mitigating these risks. Last year, more than £700million was invested in cybersecurity in the UK alone.

In addition to bolstering its technological defense systems, the banking community shares information about the latest cyber

"Banks have technology ceilings when it comes to email collections...We had a requirement for a potential solution for indexing and querying Microsoft Exchange data on the fly."

*Team member at top five global bank*

attack methodologies including specific information on hacks, breaches, phishing websites and known criminals targeting them. A lot of this intelligence comes via the British Banking Association and various government incentives including the CBEST[2] vulnerability testing framework, launched by the Bank of England in June 2014, and the British Banking Association's Financial Crime Alert Service which provides real-time cybercrime intelligence from the National Crime Agency, the government and partner agencies.

Financial services organizations across the globe are also increasingly participating in Services Information Sharing and Analysis Centres (ISACs). They are becoming a global go-to resource for cyber and physical threat intelligence analysis and sharing. The information includes analysis and recommended solutions from leading industry experts. The Financial Services ISAC[3] is currently active with members and partners.

[1] British Banking Association "The Cyber Threat to Banking," https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf

[2] Bank of England launches CBEST, June 2014 http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

[3] Financial Times, "JP Morgan data breach triggers calls for deeper collaboration," 3rd October 2014 http://www.ft.com/cms/s/0/7897ef22-4b1b-11e4-8a0e-00144feab7de.html#axzz3FCW0XFr1

# Why MITRE ATT&CK is Crucial for Endpoint Security

- **Threats Facing Modern Endpoints**

Endpoints are under constant attack from:

- **Ransomware** – Encrypts data, halts operations.
- **Privilege Escalation** – Gains unauthorized control.
- **Credential Dumping** – Steals passwords from memory.

- ### How Attackers Exploit Endpoints

  Attackers typically begin with phishing emails containing malicious links or files. Once inside, they:

  - Hide in plain sight (LotL attacks)
  - Exploit software vulnerabilities
  - Use social engineering to manipulate users

- ### Where Traditional EPPs Fall Short

  - Signature-based detection misses **fileless or novel attacks**
  - Too many **contextless alerts** create **alert fatigue**
  - Lack of **visibility into the full attack lifecycle**

- ### How MITRE ATT&CK Bridges These Gaps

  MITRE ATT&CK provides a **systematic approach** for identifying weaknesses and aligning defenses. Combined with Fidelis Endpoint®, it offers deeper visibility and threat detection where traditional solutions fail.

## Strategies for Mapping EDR to Mitre ATT&CK

MITRE ATT&CK implementation for endpoint protection works best with a well-laid-out plan that lines up with your organization's security goals. The framework packs a lot of depth and detail. You can tackle this by breaking it into smaller, manageable steps to secure endpoints.

- ### Mapping Your Current EDR Capabilities to ATT&CK

  Start with a review of your existing endpoint security controls against the ATT&CK matrix. Document how your current tools detect, prevent, or respond to various techniques. This process helps you create a clear picture of your EDR solution's coverage across the framework's 14 tactics and related techniques. Map out to both the Defense Evasion and Execution tactics.

- ### Identifying Critical Coverage Gaps

  Your capability mapping reveals where your endpoint detection and response solution needs more coverage. Look closely at areas where attackers targeting your industry often strike. Rate these gaps based on their possible effect and how likely they are to happen. Security teams can spot weak spots easily by comparing their controls against the framework's technique list.

- ## Prioritizing Techniques Based on Your Threat Landscape

  Each technique poses different risks to your organization. Your priorities should consider:

  - Technique prevalence in your industry sector
  - Common attack choke points
  - Organizational risk assessment outcomes
  - Infrastructure-specific vulnerabilities

- ## Improving Detection and Response of Endpoint with ATT&CK

  Build detection and response playbooks that match your priority techniques to make your EDR solution stronger. These playbooks should focus on containment steps and use threat intelligence to track new attack patterns.

- ## Incident Response and Mitigation Strategies Based on ATT&CK

  ATT&CK helps teams spot attack patterns quickly during incidents. Security analysts make better decisions faster by connecting suspicious activities to known techniques. The MITRE framework also offers specific fixes for each technique, giving clear steps for remediation.

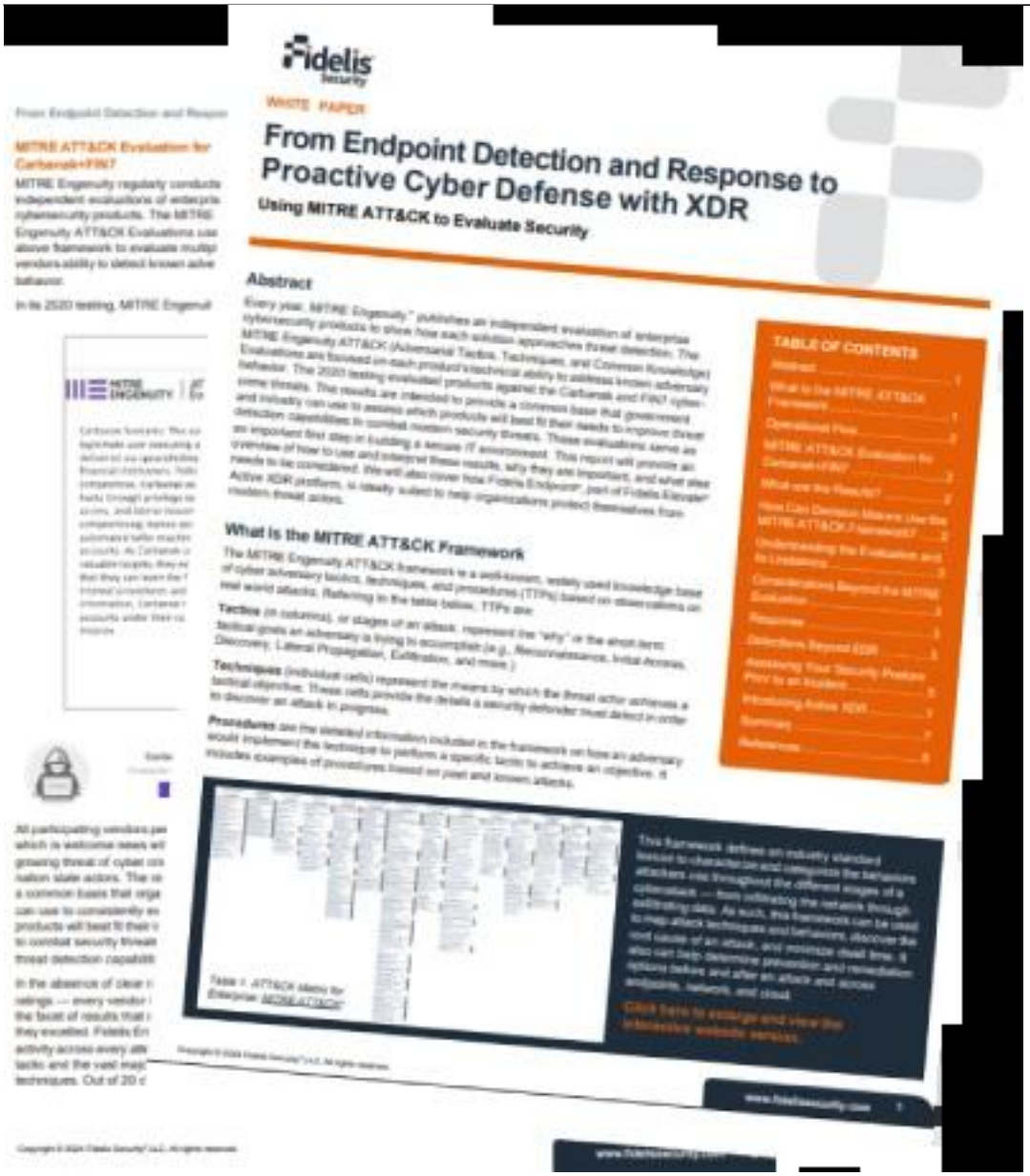
- ## Fidelis Endpoint® Integration with MITRE ATT&CK

  Fidelis Endpoint® works seamlessly with MITRE ATT&CK and provides automated playbooks for specific techniques. Our solution finds risks in places where attackers usually hide and gives you full visibility of your environment. Fidelis Endpoint® also has automated compliance reports and risk assessment features that work well with ATT&CK's organized approach.

Boost your defense with ATT&CK-aligned EDR. Learn how to:

- Map threats to ATT&CK tactics
- Real-world defense strategies
- Automate security workflows

Download the Whitepaper Now!




# Key ATT&CK Tactics for Comprehensive Endpoint Security

Security teams can disrupt attack progression by focusing on high-impact tactics:

## Initial Access & Execution: Your First Line of Defense

**TA0001 – Initial Access**:

Attackers exploit public-facing applications, spearphishing, and remote services.

**TA0002 – Execution**:

Malicious code is run on systems.

**Fidelis Endpoint®** uses behavioral analysis and execution monitoring to stop threats before they run.

## Persistence & Privilege Escalation: Blocking Deeper Access

**TA0003 – Persistence**:

Attackers modify system processes or startup scripts to maintain access.

**TA0004 – Privilege Escalation**:

They exploit vulnerabilities or use stolen credentials to gain admin rights.

**Fidelis Endpoint®** blocks these techniques with visibility and real-time alerts.

## Lateral Movement & Exfiltration: Halting Attack Spread

**TA0008 – Lateral Movement**:

Attackers use legitimate tools to quietly spread across systems.

**TA0010 – Exfiltration**:

Data is encrypted and sent through covert channels.

Mapping these tactics in your EDR helps detect **anomalous data movement** and contain breaches before data leaves your network.

# Operationalizing ATT&CK in Your SOC

## 1. Train Your Team on ATT&CK Methodology

Upskill your SOC with courses like:

- **ATT&CK Cyber Threat Intelligence**
- **Purple Teaming Fundamentals**
- **ATT&CK SOC Assessment Certification**

These certifications teach teams how to turn ATT&CK theory into actionable security improvements.

## 2. Incorporate ATT&CK in Incident Response Workflows

- Map adversary tactics to response plans
- Create detailed playbooks
- Accelerate decision-making during incidents

## 3. Enable ATT&CK-Based Threat Hunting

Using telemetry mapped to techniques, your analysts can hunt for compromise indicators.

**Fidelis Endpoint®** enhances this with:

- Deep endpoint telemetry
- “Tainted telemetry” linking related events for faster triage

## 4. Test Your Detection Capabilities with ATT&CK Evaluations

Use MITRE’s adversary emulation tests to:

- Simulate real-world attack chains
- Measure your tool’s performance
- Patch gaps based on test results

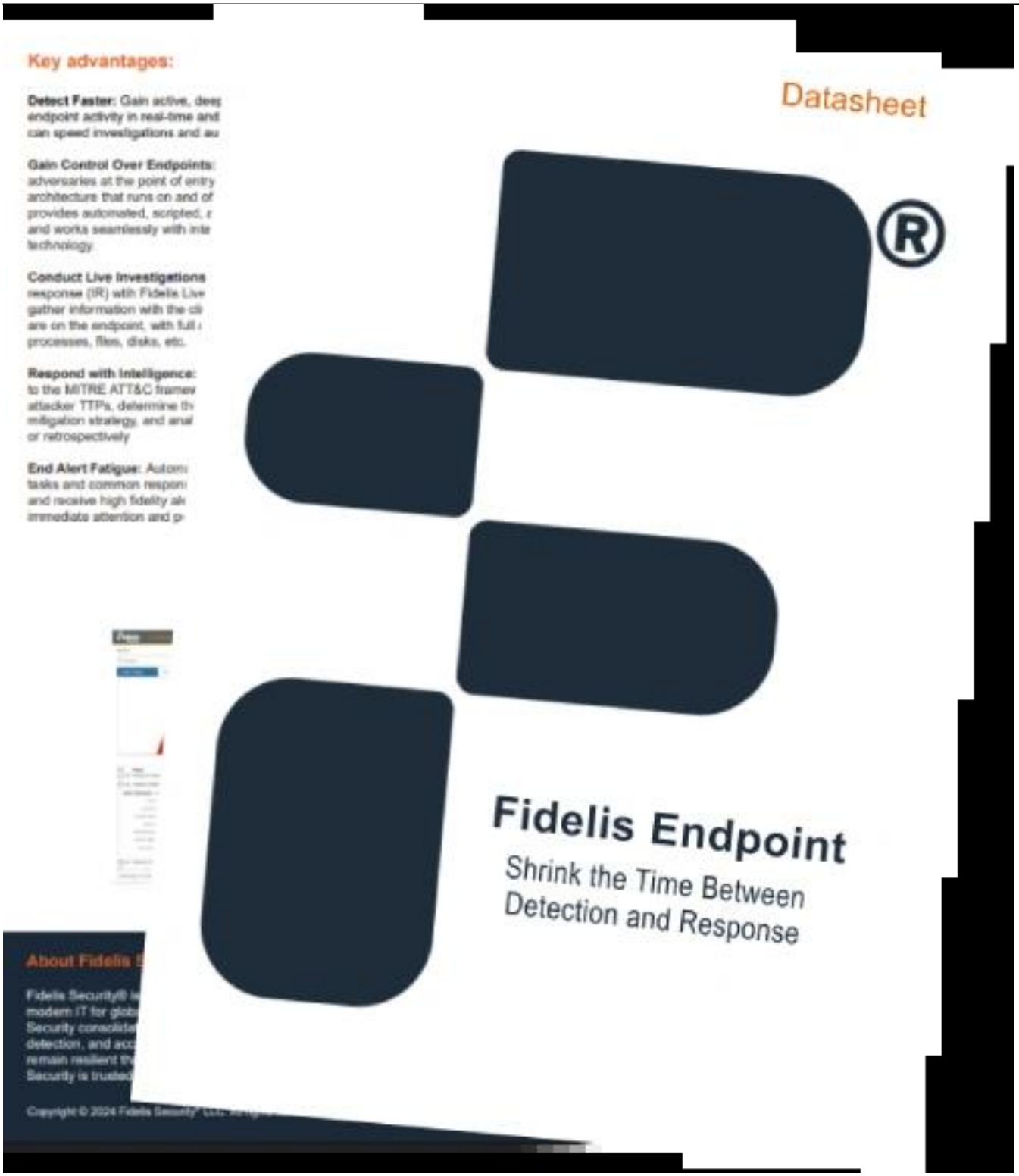
## Conclusion

In summary, mapping EDR to MITRE ATT&CK not only improves visibility but strengthens your security posture across secure endpoints. MITRE ATT&CK isn’t just a framework—it’s a powerful ally in securing your endpoints. It provides structure, clarity, and actionable intelligence that improves every part of your cybersecurity posture.

Modern EDR Built for Speed & Intelligence

- See every endpoint move
- Respond faster with automated playbooks
- Operate with MITRE-aligned precision

Download Datasheet




# Frequently Ask Questions

## What is the MITRE ATT&CK framework and why is it important?

The MITRE ATT&CK framework is a comprehensive knowledge base that catalogs real-world cyber adversary behaviors. It’s important because it provides a structured approach to understanding attack progression, helps identify critical coverage gaps, and enables more effective communication about threats across security teams.

## How does MITRE ATT&CK enhance endpoint security?

MITRE ATT&CK enhances endpoint security by providing a structured approach to understanding attack progression. It helps organizations map their current EDR capabilities, identify critical coverage gaps, and prioritize security investments based on their specific threat landscape.

## What are the key components of the MITRE ATT&CK framework?

The MITRE ATT&CK framework consists of three main components: tactics (representing the adversary’s overall goals), techniques (specific methods used to achieve these goals), and procedures (detailed descriptions of how techniques are implemented in real-world scenarios).

## How can organizations implement MITRE ATT&CK for endpoint detection and response?

Organizations can implement MITRE ATT&CK by mapping their current EDR capabilities to the framework, identifying coverage gaps, prioritizing techniques based on their threat landscape, and developing detection and response playbooks aligned with prioritized techniques. Solutions like Fidelis Endpoint® offer comprehensive integration with MITRE ATT&CK to streamline this process.

## How does MITRE ATT&CK improve incident response?

MITRE ATT&CK improves incident response by enabling security teams to quickly identify attack patterns and link suspicious activities to known techniques. This allows for faster, more informed decision-making during incidents. The framework also provides specific mitigation recommendations for each technique, offering clear guidance for remediation.