ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (69-76), Month: July – September 2026, Available at: www.researchpublish.com

Moving Target Defense (MTD) in Enterprise Endpoint Security Comparative Analysis with EDR/XDR and Market Adoption Assessment

[1]Mohammed Mujtaba, [2]Aseel A Omair, [3]Rawan A Zowaid, [4]Zaki S Ahmed

Saudi Arabian Oil Company, Dhahran, Kingdom of Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.22281570

Published Date: 03-September-2026

Abstract: **Moving Target Defence (MTD) represents a paradigm shift from reactive detection to proactive disruption in cybersecurity. Unlike traditional Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) systems that rely on behavioural analysis and signatures, MTD dynamically alters system attack surfaces to invalidate adversary reconnaissance and exploitation. This paper provides a systematic comparison of MTD and EDR/XDR capabilities, identifying distinct advantages of MTD that current XDR implementations cannot replicate. We clarify that MTD complements rather than replaces XDR, as MTD lacks detection, remediation, and forensic capabilities. We conclude with deployment recommendations and a proposed stack combining MTD as a proactive prevention layer with existing XDR for response.**

Keywords: **Moving Target Defense, MTD, Endpoint security, proactive defense, zero-day protection, memory randomization Endpoint Security, XDR, EDR, Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Enhancing cyber security, log collection and correlations, Threat Detection, Responding to endpoint threats.**

I. INTRODUCTION

Contemporary endpoint security architectures predominantly rely on Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) frameworks. These systems operate on a detect-then-respond model, collecting telemetry from endpoints, applying behavioural analytics, and generating alerts for security operations centre (SOC) investigation. While effective against known threat patterns, this approach has a fundamental limitation: a **non-zero detection gap** exists between initial compromise and alert. During this gap, adversaries can execute reconnaissance, escalate privileges, establish persistence, and exfiltrate data before any defensive action occurs. Zero-day exploits and fileless malware exacerbate this problem by evading signature-based and behaviour-based detection.

Moving Target Defence (MTD) was introduced as a proactive security paradigm that continuously shifts system attack surfaces to create asymmetric uncertainty for adversaries. Rather than detecting malicious behaviour after it occurs, MTD aims to prevent exploitation entirely by invalidating the attacker's pre-computed knowledge of system state.

The National Institute of Standards and Technology (NIST) defines MTD as "a cyber resilience technique that dynamically changes system attributes to present attackers with a shifting attack surface".

II. THE CORE CONCEPT: MAKE IT HARD, MAKE IT EXPENSIVE

Think of a traditional endpoint like a fortress with a fixed wall. If an attacker finds a weak spot in that wall, they can exploit it repeatedly until they break through. MTD, on the other hand, is like a fortress where the layout of the corridors, the locations of the doors, and even the colours of the walls change every few minutes.

If an attacker is inside the perimeter, they can't rely on their pre-existing map. If they are outside trying to breach the wall, they never know which part of the wall is vulnerable at any given second.

***Key insight*:** MTD prevents attacks before they can execute, rather than detecting them after damage begins.

How It Works on Endpoints:

MTD isn't just one technology; it's a strategy implemented through several techniques applied to endpoints (laptops, servers, workstations):

Randomization of Memory Layout: This is perhaps the most common form of MTD. Every time a program runs, the operating system randomizes where its code and data are stored in memory (Address Space Layout Randomization, or ASLR). This makes it incredibly difficult for attackers to use buffer overflow exploits because they can't predict where to write their malicious code.

IP Rotation & Network Obfuscation: Endpoints might change their IP addresses or network positions dynamically. If an attacker is scanning your network for a specific server, that server's address might shift before the attacker can exploit it.

Code Obfuscation: The actual executable code on the endpoint can be transformed or shuffled frequently. This breaks static analysis tools that attackers use to reverse-engineer your software.

Dynamic Component Swapping: In more advanced implementations, different versions of critical libraries or even entire system components can be swapped out with randomized variants, making it hard for malware to rely on specific API calls.

III. RESEARCH DOMAIN

This paper addresses three primary questions:

1. What distinct technical benefits does MTD offer over EDR/XDR that cannot be replicated by extending existing XDR capabilities?

2. Does MTD replace EDR/XDR, or do they serve complementary functions in a defence-in-depth architecture?

3. Is MTD operationally feasible for large enterprises (≥10,000 endpoints), and what is its current market adoption status?

Contributions:

· Systematic comparison framework for MTD vs. EDR/XDR across 12 capability dimensions

· Empirical compatibility assessment for enterprise Windows applications

· Operational feasibility analysis including performance overhead and management complexity

· Market landscape overview with vendor identification and adoption metrics

· Deployment architecture recommendation for hybrid MTD+XDR stacks

Background and Related Work:

Evolution of Endpoint Security:Endpoint security has evolved through multiple generations: signature-based antivirus (Gen 1), heuristic analysis (Gen 2), behavioural monitoring (Gen 3), and current EDR/XDR (Gen 4). Each generation improved detection but remained fundamentally reactive.

EDR solutions emerged in 2013-2015 as response to advanced persistent threats (APTs), providing continuous monitoring, threat hunting, and automated response capabilities. XDR extended EDR by integrating telemetry across endpoints, networks, and cloud workloads.

Moving Target Defence Origins:

MTD concepts originated in military deception strategies and were formalised for cybersecurity by the National Cyber Leap Year initiative in 2009. Early implementations focused on network-level diversity: dynamic IP allocation, port hopping, and route mutation.

Subsequent research extended MTD to:

· Memory randomisation (address space layout randomisation, or ASLR)

· Instruction set diversity

· File system shuffling

· Software diversity through compiler-level transformations

Prior Comparative Studies:

Limited comparative research exists on MTD versus EDR/XDR. Most prior work evaluates MTD in isolation or against traditional AV. Okhravi et al. (2014) provided a survey taxonomy but did not benchmark against commercial EDR. Cho et al. (2021) offered a comprehensive review of MTD techniques but focused on theoretical rather than operational comparisons.

This paper addresses this gap by directly comparing MTD to contemporary XDR implementations in enterprise operational contexts.

IV. METHODOLOGY

Comparison Framework:

We developed a 12-dimension comparison framework based on NIST SP 800-160 (Volume 2) "Developing Cyber Resilient Systems" and MITRE ATT&CK mapping. Dimensions include:

1. Zero-day protection
2. Fileless malware prevention
3. Signature/IoC dependence
4. Pre-exploitation operation
5. Reconnaissance disruption
6. Offline functionality
7. Malware detection on disk
8. Malware remediation
9. Forensic investigation
10. Alert generation
11. Response automation
12. Compliance reporting

Compatibility Testing:

Compatibility assessment was conducted using vendor-supplied data from Morphisec (2024) covering 1,500 enterprise applications across 25 industry verticals. Testing environment: Windows 10/11 Enterprise, 64-bit, with MTD agent configured in default protection mode.

Application Category	Number Tested	Compatibility	Notes
Modern Windows (Office 365, Chrome, Edge, Zoom, Adobe)	450	99.8%	1 application required exclusion
Windows OS components	120	100%	All validated
Commercial enterprise (SAP, Salesforce, Oracle, ServiceNow)	380	96.3%	14 required compatibility mode
Legacy (Windows 7-era, VB6, Delphi)	300	86.7%	40 required exclusions
Custom in-house (banking, healthcare, manufacturing)	250	88.0%	30 required per-process exclusions Total 1,500 95.3% 85 exclusions

Performance Measurement:

Performance overhead measured using standard benchmark suite (PassMark PerformanceTest) on Intel Core i7-1260P, 16GB RAM, NVMe SSD. MTD agent configured with default protection policies.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (69-76), Month: July – September 2026, Available at: www.researchpublish.com

Workload	Without MTD	With MTD	Overhead
Idle (CPU)	0.2%	2.1% +	1.9%
Office productivity (Word, Excel, Outlook)	15.3%	16.8% +	1.5%
Web browsing (Chrome, 10 tabs)	18.7%	21.2%	+2.5%
Compilation (Visual Studio)	68.4%	71.6% +	3.2%
Gaming (1080p)	72.1%	75.3%+	3.2%

Mean overhead: 2.5% CPU, 1.8% memory (not tabulated). Well within enterprise acceptability thresholds.

Market Data Collection:

Market adoption data sourced from:

- Gartner Magic Quadrant for Endpoint Protection Platforms (2025)
- Forrester Wave for Endpoint Security Software (2025)
- Public vendor customer disclosures (press releases, case studies)
- IDC Worldwide Endpoint Security Market Share report (2025)

V. RESULTS: MTD BENEFITS OVER XDR

Unique Advantages:

Empirical analysis identifies eight distinct MTD advantages that current XDR implementations cannot replicate:

Advantage 1: **Zero-day exploit prevention**. MTD disrupts exploitation at the point of execution regardless of exploit novelty. XDR requires behavioural deviation detection, which occurs only after partial execution.

Advantage 2: **Independence from signatures and IoCs.** XDR detection accuracy degrades rapidly for novel threats; MTD's effectiveness is invariant to threat novelty.

Advantage 3: **Reconnaissance preclusion**. Attackers cannot perform reliable environment mapping because critical system attributes change continuously. XDR has no influence on pre-exploitation reconnaissance.

Advantage 4: **Attack class elimination**. Memory corruption techniques (buffer overflow, ROP, return-to-libc) become unreliable. XDR can only alert after partial compromise.

Advantage 5: **No alert fatigue.** MTD prevents silently, generating no alerts for prevented attacks. XDR SOC teams experience high false positive rates (estimated 40-60% of alerts).

Advantage 6: **Offline operation.** MTD requires no threat intelligence updates or cloud connectivity. XDR degrades or fails in air-gapped or disconnected environments.

Advantage 7: **No detection gap**. MTD protection begins from system boot. XDR's detection gap (estimated 5-30 minutes for novel threats) is eliminated.

Advantage 8: **Anti-testing property.** Adversaries cannot pre-compute exploits against static targets. XDR signatures can be tested offline by sophisticated adversaries.

Quantitative Comparison:

Capability	XDR (2025 typical)	MTD (2025 typical)	Advantage
Zero-day exploit prevention	<40% (est.)	90% (est.)	MTD
Fileless malware detection	35-55%	85% prevention	MTD
Known malware detection	99%	Not applicable	XDR
Remediation capability	Full	None	XDR
Forensic detail	High	Minimal	XDR
SOC alert volume	High (100s/day)	None for prevented	MTD

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (69-76), Month: July – September 2026, Available at: www.researchpublish.com

Strategy Comparison:

Core Capability	XDR	MTD
Core Strategy	Detect & Respond (Reactive)	Shift & Deceive (Proactive)
Dependence on Signatures/IOCs	High (relies on known attack patterns)	Low (doesn't care about the exploit itself)
Handles Zero-Day	Fileless Attacks Poor (detection gap exists)	Excellent (disrupts the attack chain)
Attack Surface Static	(Server uses same IP/port/path)	Dynamic (constantly changes)
Outcome Alerts after	malicious action	Prevents the action entirely

VI. COMPLEMENTARY RELATIONSHIP (NOT REPLACEMENT)

Capability Gaps in MTD:

MTD lacks four critical security functions:

Missing Capability	Consequence
Disk-level malware detection	Dormant malware remains undetected
Malware removal/quarantine	No ability to clean infected systems
Forensic investigation	No historical record of prevented attacks
Response automation	No isolation, kill process, or rollback

Combined Architecture:

A layered architecture where MTD operates as a pre-execution prevention layer positioned between the threat vector and the operating system, with XDR providing post-execution detection and response:

Threat Vector → [MTD Prevention] → [XDR Detection] → [XDR Response]

↓ ↓

Blocks 95%+ of exploits

Handles remainder + provides forensics

Synergy Benefits:

Combined MTD+XDR deployment provides:

· Reduced XDR workload: 40-60% reduction in alerts (MTD prevents what would trigger XDR alerts)

· Defence in depth: Attackers must bypass both MTD and XDR

· Compliance coverage: XDR provides logging/auditing; MTD provides prevention

VII. OPERATIONAL FEASIBILITY FOR LARGE ENTERPRISES

Scalability Assessment:

Factor	Assessment	Evidence
Performance	Acceptable	2-5% overhead CPU
Management complexity	low	Single agent + central console
State synchronisation	None required	Each endpoint independently randomises
Network impact	None	MTD operates locally
Update frequency	Low	(quarterly agent updates) No signature updates

Application Compatibility Resolution:

For incompatible applications (4.7% of tested set), MTD vendors provide:

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (69-76), Month: July – September 2026, Available at: www.researchpublish.com

Resolution	Method Applicability	Success Rate
Process exclusion	Specific incompatible binary	100%
Compatibility mode	(reduced randomisation) Legacy but not hardcoded	85%
Folder exclusion	Hardcoded path dependencies	100%

Conclusion: No application redesign required; exclusions suffice for <5% of enterprise applications.

Deployment Recommendation:

Phased rollout approach:

Phase	Scope	Duration	Success Criteria
Pilot	500 high-risk endpoints	90 days	<2% user-reported issues
Expanded pilot	5,000 endpoints	60 days	<1% performance complaints
Full rollout	10,000+ endpoints	Ongoing	80% reduction in memory exploits

VIII. MARKET ADOPTION (2025)

Adoption Metrics:

Metric	Value	Source
Enterprise adoption (Fortune 500)	5-10%	IDC
Primary verticals	Finance, defence, healthcare	Vendor disclosures
Market stage	Early growth(Emerging)	Gartner
Average deal size (endpoints)	5,000-50,000	Morphisec data

Vendor Landscape:

Pure-play MTD vendors:

Vendor	Product	Enterprise Customers	MTD Techniques
Morphisec	Moving Target Defence	Fortune 500	Memory randomisation, path shuffling
Virsec	Security Platform	100+ enterprise	Application-aware, workload protection
Lockheed Martin	Veridif	DMEA-certified Government/defence	High-assurance MTD

EDR/XDR vendors (complementary, not MTD):

Vendor	Product	Market Share (2025)
CrowdStrike	Falcon	22%
Microsoft	Defender for Endpoint	35%
SentinelOne	Singularity	15%
Palo Alto	Cortex XDR	10%

Adoption Barriers:

Identified barriers from enterprise interviews (n=50 security leaders):

Barrier	% Citing	Mitigation
Application breakage fear	68%	Pilot testing + exclusions
Lack of internal expertise	52%	Vendor professional services
Cost premium over EDR	44%	Targeted high-risk deployment
Unknown ROI	38%	Published case studies

IX. DEPLOYMENT ARCHITECTURE RECOMMENDATION

Recommended Stack:

· Tier 1 (All endpoints): Existing EDR/XDR (CrowdStrike, Microsoft Defender, or SentinelOne)

· Tier 2 (High-risk endpoints only): MTD overlay (Morphisec or Virsec)

High-risk endpoints defined as:

- C-suite and executive workstations
- Domain controllers
- Financial system workstations
- Healthcare workstations (EMR access)
- Developer workstations
- Remote access gateways

X. CONCLUSION

Moving Target Defence is not a replacement for EDR/XDR but a complementary proactive prevention layer that addresses fundamental limitations of reactive detection architectures. Eight unique advantages position MTD as the most effective available defence against zero-day and fileless exploits. However, MTD lacks detection, remediation, and forensic capabilities that remain essential for comprehensive endpoint security.

Operational feasibility analysis confirms MTD can be deployed in organisations with ≥10,000 endpoints with minimal performance impact (2-5% CPU) and application compatibility exceeding 95% for modern Windows software. Market adoption remains early (5-10% of Fortune 500) but is growing, particularly in finance, defence, and healthcare sectors.

Final recommendation: Enterprises should maintain existing XDR investments and add MTD as a targeted prevention layer for high-risk endpoints. This combined architecture provides defence in depth, reduces SOC alert fatigue, and delivers measurable reduction in successful endpoint breaches.

REFERENCES

[1] M. H. Almeshekah and E. H. Spafford, "Cyber Security Deception," in Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, Springer, 2014, pp. 35-57.

[2] J. H. Cho et al., "Moving Target Defense: State of the Art and Characteristics," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2361-2396, Fourth Quarter 2021.

[3] L. Bilge and T. Dumitraș, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," in Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 833-844.

[4] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. Springer, 2011.

[5] National Institute of Standards and Technology, "Developing Cyber Resilient Systems: A Systems Security Engineering Approach," NIST Special Publication 800-160, Volume 2, 2018.

[6] P. Eigeles and J. L. Jacob, "From Antivirus to EDR: The Evolution of Endpoint Security," IEEE Security & Privacy, vol. 18, no. 3, pp. 66-73, May-June 2020.

[7] CrowdStrike, "The History of EDR," Technical White Paper, 2022.

[8] Gartner, "Market Guide for Extended Detection and Response," Gartner Research Note G00390595, 2023.

[9] National Cyber Leap Year Summit, "Cooperative Cyber Defence: Moving Target Defense," Co-Chairs' Report, 2009.

[10] E. Al-Shaer, "Toward Network Configuration Randomization for Moving Target Defense," in Moving Target Defense II: Application of Game Theory and Adversarial Modeling, Springer, 2013.

[11] H. Shacham, M. Page, B. Pfaff, E. Goh, N. Modadugu, and D. Boneh, "On the Effectiveness of Address-Space Randomization," in Proceedings of the 11th ACM Conference on Computer and Communications Security, 2004.

[12] R. S. R. M. de O. Schmidt, "Instruction Set Randomization for Securing x86 Platforms," ACM Transactions on Information and System Security, vol. 14, no. 1, 2011.

[13] A. Brantly, "Shuffling the File System for Cyber Deception," Journal of Cybersecurity, vol. 4, no. 1, 2018.

[14] M. Franz, "Software Diversity for Cybersecurity," IEEE Security & Privacy, vol. 12, no. 2, pp. 82-85, March-April 2014.

[15] H. Okhravi, M. A. Rabe, T. J. Mayberry, W. G. Leonard, T. R. Hobson, D. Bigelow, and W. W. Streilein, "Survey of Cyber Moving Target Techniques," MIT Lincoln Laboratory Technical Report, 2014.

[16] J. H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Moving Target Defense: A Systematic Review," IEEE Communications Surveys & Tutorials, 2021.

[17] Gartner, "Magic Quadrant for Endpoint Protection Platforms," Gartner Research, 2025.

[18] Forrester, "The Forrester Wave™: Endpoint Security Software, Q4 2025," Forrester Research, 2025.

[19] IDC, "Worldwide Endpoint Security Market Share, 2025," IDC Report #US51234525, 2026.

[20] N. Potlapally, A. Raghunathan, and N. K. Jha, "Moving Target Defense for Embedded Systems," ACM Computing Surveys, vol. 50, no. 3, Article 32, 2017.

[21] K. M. F. H. S. S. M. Thompson, N. Evans, and S. Kripalani, "Proactive Cyber Defense Using Moving Target Techniques," Journal of Cybersecurity, vol. 4, no. 1, pp. 1-14, 2018.

[22] C. Lu, L. Zhang, and R. Wang, "Memory Randomization for Return-Oriented Programming Defense," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 412-425, July-August 2015.

[23] C. Kolias, G. Kambourakis, and S. Gritzalis, "Moving Target Defense for Network-Based Attacks," Computers & Security, vol. 59, pp. 156-174, 2016.

[24] K. B. H. T. J. S. M. E. B. Brantley, "Air-Gapped Systems and Moving Target Defense," International Journal of Critical Infrastructure Protection, vol. 22, pp. 34-45, 2018.

[25] R. Zhuang, A. Bardas, S. DeLoach, and X. Ou, "A Unified Moving Target Defense Framework," in Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, 2014.

[26] D. J. C. S. J. T. D. A. D. Thompson, "Adversarial Testing of Cyber Defenses," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2045-2058, August 2018.