MORPHISEC

Data Sheet

Adaptive AI Defense

AI-Powered Preemptive Cyber Defense for the Generative Threat Era

As AI-driven threat actors use automation to evolve malware faster than humans can respond, traditional Reactive Detection and Response models fall behind. **Morphisec Adaptive AI Defense** expands its patented Automated Moving Target Defense (AMTD) technology by introducing machine-learning-driven threat prediction and self-optimizing defense mechanisms.

The result? Preemptive, predictive protection that stops AI-mutated ransomware, zero-days, and memory attacks before execution—without relying on signatures, scanning, or manual tuning.

Key Benefits

AI-Driven Threat Prediction

- Uses machine-learning telemetry to predict potential attack paths and initiate preventive AMTD adjustments.

AI-Guided Encryption Interception

- Identifies and halts malicious encryption routines in real time without relying on signatures.

Dynamic Attack Surface Mutation

- Continuously alters process and memory layouts based on AI feedback to disrupt exploit generation.

Explainable AI Insights

- Provides interpretable attack prevention reports with root-cause correlation and transparency for SOC teams.

Adaptive Risk Scoring

- Combines EPSS, CISA KEV, and organizational data to prioritize vulnerabilities and remediation actions.

Autonomous System Optimization

- Defense policies auto-update based on environmental changes—no manual tuning required.

© Morphisec Inc.

How It Works

Organizations face a new reality: **Adversarial AI outpaces human analysis.** Traditional EDRs and AI-enabled analytics depend on post-execution telemetry and pattern recognition.

Morphisec reverses the model by applying AI to **anticipate attacks before they exist**.

Core Benefits

- **Predictive Threat Intelligence:** AI models learn from live telemetry, industry threat feeds, and Morphisec Threat Labs data to forecast emerging exploit techniques.
- **Adaptive Exposure Control:** Continuously evaluates each endpoint's vulnerability context and tunes runtime mutation logic based on real-time risk scoring.
- **Self-Learning Prevention Loop:** Every blocked event enhances the AI model, creating a self-improving feedback cycle of knowledge and protection.

Example Use Cases

- ✓ **AI-Generated Malware Neutralization:** Blocks deep-reinforcement-learning malware variants before execution by mutating attack memory targets.
- ✓ **Zero-Day Resilience for Hybrid Workloads:** Protects on-premises and cloud resources without relying on patching timelines.
- ✓ **EDR Amplification:** Extends existing EDR/XDR solutions (e.g., Microsoft Defender, CrowdStrike, SentinelOne, BitDefender) by adding deterministic AI prevention.
- ✓ **Adaptive Incident Response Acceleration:** Automatically prioritizes alerts using AI-based confidence scores, reducing noise and cutting containment times by up to **65%**.
- ✓ **Continuous Learning Defense Loop:** Every attack attempt improves the AI model without requiring signatures or human retraining.

> "Morphisec prevents attacks from actually happening. It gives us an early warning sign...and that lets me make informed, intelligent decisions."
>
> Richard Rushing, CISO at Motorola

© Morphisec Inc.

The Morphisec Advantage

Business Benefit	Impact
Pre-Execution Prevention	Stops AI-crafted zero-days before they execute—eliminating the need for detection cycles.
Reduced TCO and Analyst Fatigue	Achieves **90% fewer false positives** and reduces investigation workloads by up to **30%**.
Continuous Resilience	Self-optimizing defense adapts to evolving attack techniques autonomously.
Ransomware-Free Assurance	Backed by Morphisec's **Ransomware-Free Guarantee**, ensuring full accountability.
Cross-Platform Coverage	Protects Windows and Linux environments with a minimal footprint (**<1% CPU load**).

Architecture with Adaptive AI Defense

Telemetry Ingestion:
Aggregates endpoint runtime, environmental, and threat intelligence feeds.

1.

2.

AI Inference Engine:
Applies machine-learning models to predict vulnerabilities and action probabilities.

AMTD Execution Layer:
Implements memory mutation and runtime concealment based on AI-driven directives.

3.

4.

Feedback and Audit Module:
Generates explainable prevention reports and adapts future defense profiles.

Ready to See Adaptive AI Defense in Action?

Stop AI-powered attacks before they begin.

Visit morphisec.com/demo to take the tour.

About Morphisec

Morphisec is the global leader in **prevention-first cyber defense**, protecting over **9 million endpoints worldwide** with patented **Automated Moving Target Defense (AMTD)** technology.

Our mission is to eliminate attacks before they start, ensuring ransomware-free, AI-resilient operations for customers across industries such as finance, healthcare, manufacturing, education, and technology.

© Morphisec Inc. | morphisec.com