

Adaptive AI Defense

Preemptive, Multi-Layered Ransomware Protection for the AI Era

As enterprises rapidly adopt AI assistants and autonomous agents, a new and largely invisible attack surface has emerged. Traditional EDR, XDR, and AV tools (designed for detection after execution) are blind to machine-speed, AI-driven threats. **Morphisec Adaptive AI Defense** (powered by Automated Moving Target Defense) extends the Anti-Ransomware Assurance Suite, to stop AI-driven ransomware, rogue AI agents and autonomous attack chains before execution.

By combining deterministic runtime protection with adaptive cyber resiliency, Morphisec delivers preemptive cyber defense that neutralizes threats across the entire attack lifecycle – before, during, and after execution.

Key Capabilities



Discover and Govern AI Usage

- + Automatically identify approved and unapproved AI tools, agents, and connectors to restore **complete visibility** across endpoints and workloads.



Prevent Compromised Agents Before Execution

- + Block unauthorized AI agents or rogue automations from installing or executing, neutralizing ransomware at the earliest stage.



Runtime Behavior Enforcement

- + Monitor for behavioral drift, anomalous processes, and malicious automation activity (e.g., exfiltration or abnormal API calls) and stop them in real time.



Dynamic Attack Surface Mutation

- + Powered by AMTD, Adaptive AI Defense continuously randomizes memory and process structures so attackers and AI agents cannot predict runtime targets or persist.



AI-Guided Encryption Interception

- + Preemptively halt ransomware encryption attempts and data tampering in real time without relying on signatures or cloud scans.



Explainable AI Insights

- + Deliver transparent telemetry and root-cause context for SOC investigations and compliance reporting.

How It Works

AI-driven attacks operate at machine speed, often leveraging trusted agents and plugins already inside your environment. Traditional EDR/XDR tools analyze events after execution—Morphisec prevents them entirely.

Core Benefits

- **Pre-Execution Prevention:** Stops AI-crafted zero-days and mutating malware before they run, eliminating reaction delays.
- **Unified Visibility:** Discovers and controls shadow AI across the enterprise to reduce exposure and compliance risk.
- **Amplify Existing EDR/XDR:** Seamlessly integrates and fortifies Defender, CrowdStrike, SentinelOne, and other platforms to close post-execution gaps.
- **Reduce Analyst Fatigue:** Reduces false positives by **up to 90%** through deterministic runtime validation and AI-weighted confidence scoring.
- **Accelerate Response:** Shrinks containment and investigation time by **up to 65%** via AI-driven alert prioritization. Allowing Tier 1 Security Analysts to operate at Tier 3 skill and speed.
- **Continuous Adaptive Cyber Resilience:** Adaptive feedback loops update AMTD and AI models with every intercepted threat, **hardening defenses automatically.**

Example Use Cases

- ✓ **AI-Generated Malware Neutralization:** Prevents deep learning and autonomous malware variants by disrupting their memory targets **before execution.**
- ✓ **Shadow AI Visibility & Control:** Identifies rogue AI tools and agents installed without IT approval and enforces usage policies.
- ✓ **Zero-Day Resilience for Hybrid Workloads:** Protects cloud and on-premises assets without depending on patching cadence or signature libraries.
- ✓ **AI-Assisted Response Acceleration:** Ranks alerts by AI-driven confidence scores to reduce noise and speed incident containment.
- ✓ **Continuous Learning Defense Loop:** Every blocked event feeds back into AI models, strengthening resilience with each intercepted attack.

The Morphisec Advantage

Business Benefit	Impact
Pre-Execution Prevention	Blocks exploits and AI-driven ransomware before execution - no reaction cycles needed.
Reduced TCO and Analyst Fatigue	Achieves 90% fewer false positives and cuts SOC load by up to 30% .
Continuous Resilience	Self-optimizing defense adapts to evolving AI techniques autonomously.
Ransomware-Free Assurance	Backed by Morphisec's Ransomware-Free Guarantee , ensuring full accountability.
Cross-Platform Coverage	Protects Windows and Linux with <1% CPU impact and minimal memory footprint.

Adaptive AI Defense Architecture

Telemetry Ingestion:

Aggregates endpoint runtime, environmental, and AI-usage signals for real-time risk context.



AMTD Execution Layer:

Implements memory mutation and runtime concealment to thwart attack execution.



AI Inference Engine:

Uses machine learning to predict potential exploit paths and feed preventive directives to AMTD.



Continuous Adaptive Feedback:

Generates explainable forensic reports and continuously re-optimizes defense profiles.



Unified Multi-Layered Protection

Adaptive AI Defense is part of Morphisec's **five-layer Anti-Ransomware Assurance Suite**, providing preemptive defense **before, during, and after execution**:

- 1. Adaptive AI Defense:** Prevents AI-driven ransomware and shadow AI threats before execution.
- 2. Adaptive Exposure Management:** Identifies and reduces risk before attackers find it.
- 3. Infiltration Protection:** Stops intrusions and ransomware **at runtime**.
- 4. Impact Protection:** Prevents **encryption** and **exfiltration**.
- 5. Adaptive Recovery:** Restores operations instantly with immutable forensic evidence.

Together, these layers create a **unified ransomware defense fabric** for modern and AI-driven workloads across endpoints and clouds.

Ready to See Adaptive AI Defense in Action?

Stop AI-powered attacks before they start.

[Request a Demo](#)

About Morphisec

Morphisec is the global leader in prevention-first cyber defense and anti-ransomware protection, delivering preemptive security that stops attacks before execution.

By integrating Adaptive AI Defense into its multi-layer Assurance Suite, Morphisec empowers organizations to achieve ransomware-free resilience with minimal overhead and maximum clarity. Detection alone is outdated. Prevention is peace of mind.