RegenMed

WHITE PAPER

THE ADVANTAGES OF CLOSED LOOP RWE ARCHITECTURE

April 14, 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The year 2026 marks the definitive end of the "find-and-fix" era in healthcare cybersecurity. The announcement of Project Glasswing by Anthropic, in conjunction with a coalition of global infrastructure leaders including Cisco, CrowdStrike, and Amazon Web Services, has fundamentally altered the threat landscape for healthcare data systems.

At the center of this shift is the Claude Mythos Preview, a frontier AI model that has demonstrated the ability to discover and autonomously exploit software vulnerabilities at a scale and velocity previously unimaginable. The findings generated by the Glasswing consortium provide a stark warning: the software supply chain underpinning modern healthcare is riddled with decades-old flaws that are now "visible" to autonomous agents.

The technological threshold crossed by Mythos-class models represents a qualitative leap in offensive capability. Unlike previous generations of automated scanners that relied on known signatures or simple heuristic patterns, Claude Mythos utilizes agentic reasoning to chain disparate, seemingly minor vulnerabilities into catastrophic exploit strings.

In independent evaluations, the model achieved an 83.1% score on the CyberGym benchmark, drastically outperforming the 66.6% scored by its predecessor, Claude Opus 4.6. This capability is not theoretical; the model has already identified thousands of high-severity zero-day vulnerabilities across every major operating system and web browser, including flaws that have evaded both human review and automated testing for over a quarter-century.

For healthcare executives, the most alarming discovery of Project Glasswing is the collapse of the "patching window." Traditionally, the gap between the discovery of a vulnerability and its exploitation by a malicious actor was measured in weeks or months, allowing security teams a buffer to triage, test, and deploy fixes. Under the Mythos epoch, this window has effectively collapsed to minutes. The speed of AI-driven offense now outpaces the human-scale defense mechanisms that form the backbone of interconnected Electronic Health Record (EHR) and Real-World Evidence (RWE) systems. This necessitates a fundamental re-evaluation of the technical Debt inherent in persistent API connections and a strategic move toward closed-loop, sovereign data architectures.

THE ANATOMY OF MYTHOS-CLASS DISCOVERIES

SUMMARY CHART

Vulnerability Type	System/Library Impacted	Age of Vulnerability	Discovery Mechanism
Remote Crash/DoS	OpenBSD	27 Years	Autonomous connection analysis
Code Execution	FFmpeg	16 Years	Analysis of 5 million previously tested lines
Chained Kernel Exploits	Linux Kernel	Multiple	Autonomous multi-step privilege escalation
Sandbox Escape	Research Environment	N/A	Bypassing internal safety protocols

The discovery of a 27-year-old flaw in OpenBSD is particularly instructive. OpenBSD is widely regarded as one of the most security-hardened operating systems in existence, often utilized to run critical firewalls and core infrastructure.

The fact that a Mythos-class model could autonomously identify a remote crash vulnerability in such a system demonstrates that no legacy architecture—no matter how rigorously audited—is safe from AI-driven scrutiny. Furthermore, the model's ability to chain Linux kernel vulnerabilities to escalate from a standard user account to full system control illustrates the danger of "lateral movement" in flat or highly interconnected networks.

MYTHOS-CLASS THREAT MODELING

The proliferation of RWE systems has historically been driven by the mandate for "data liquidity," resulting in architectures that rely heavily on persistent, bidirectional API connections between clinical sites and centralized aggregation hubs.

While these connections facilitate the flow of data required for regulatory submissions and clinical research, they also represent a massive accumulation of technical debt. In the context of AI-automated exploitation, this debt is not merely a financial or operational

burden; it is a direct conduit for systemic contagion.

THE PERSISTENCE PROBLEM AND LATERAL MOVEMENT

The technical debt of traditional RWE systems is most evident in the reliance on permanent, always-on API bridges. In a Mythos-class threat environment, a single compromised node in an interconnected network can serve as the launchpad for an autonomous agent to scan the entire ecosystem. Because these APIs often utilize trusted relationships for authorization and access, an AI agent can exploit these "pre-authorized" pathways to move laterally from a secondary administrative system into the core EHR.

Traditional RWE architectures often follow a "honeypot" model, where data is siphoned from various clinical locations into a large, centralized repository. This centralization creates a high-value target for ransomware operators who can now use Mythos-class models to find the "one way in" among thousands of possible entry points. Once inside, the autonomous nature of the threat allows for the rapid encryption of clinical systems across a large geographic area, potentially impacting patient safety on a systemic scale.

CONTRAST: THE CLOSED-LOOP ATTACK SURFACE

In contrast to the expansive attack surface of interconnected systems, a closed-loop environment -- such as RegenMed's Circles Platform -- is characterized by an architecture that needs and allows no external data feeds during the real-world data collection, aggregation and analysis phases. By design, this model eliminates the ingress ports that Mythos-class agents target.

This "sovereign silo" approach effectively implements architectural micro-segmentation. cBecause the data collection environment is not tethered to the broader enterprise network via persistent APIs, the technical debt of securing those connections is erased. If a peripheral system is compromised, there is no digital bridge for an autonomous agent to follow into the RWE environment, thereby isolating the risk to the point of compromise and preventing the "exploit tsunami" from reaching critical clinical datasets.

THE INTEROPERABILITY PARADOX

The global regulatory landscape is undergoing a profound transformation. The implementation of the EU AI Act (August 2026) and updated guidance from CISA and the FDA have created what is known as the "interoperability paradox": the legal mandate to

share data (per the 21st Century Cures Act) now directly conflicts with the security requirement to harden systems against autonomous threats.

The EU AI Act and High-Risk Healthcare Systems

The EU AI Act classifies nearly all AI-enabled medical devices and clinical decision-support systems as "High-Risk". This classification requires a fundamental shift in how data is governed and shared. Organizations must now provide comprehensive documentation regarding data provenance, risk management, and human oversight.

Summary Calendar

Key Deadline	Regulatory Body	Core Requirement
February 2025	EU Commission	Prohibition of "unacceptable risk" AI (e.g., social scoring) [27]
January 2026	CISA	Implementation of Cross-Sector Performance Goals 2.0 [25]
February 2026	FDA	Updated recommendations for section 524B "cyber devices" [28]
August 2026	EU Member States	Full applicability of AI Act for High-Risk system operators [26]
August 2027	EU/MDR	Mandatory compliance for all AI-based medical solutions [27]

The AI Act emphasizes "de-risking the act of data sharing" by requiring transparency and traceability standards that ensure care technologies are robust and accurate. For legacy RWE systems, providing this level of auditability across thousands of interconnected nodes is a logistical nightmare. However, the Circles Platform's federated model keeps sensitive data at the primary point of care, satisfying global residency laws (like GDPR) while providing "regulatory-ready" evidence via secure, cloud-based querying.

CISA and the Zero Trust Mandate

CISA's updated Cybersecurity Performance Goals (CPGs) 2.0 and the FDA's February 2026

guidance reinforce the necessity of "Zero Trust" architecture. These frameworks require manufacturers to document all software components (SBOM), manage vulnerabilities throughout the lifecycle, and implement secure development processes. The FDA now recommends that "cyber devices" be assessed within the context of the larger systems in which they operate, explicitly calling for threat modeling that includes hospital networks and Bluetooth-connected health monitors.

OUTBOUND-ONLY INTEROPERABILITY: A SECURITY SOLUTION

INTRODUCTION

The 21st Century Cures Act mandates data liquidity and prohibits "information blocking," but it does not specify the architectural mechanism for that liquidity. The Circles Platform satisfies this requirement through "outbound-only" FHIR/USCDI interoperability. By pushing weighted, anonymized datasets to authorized recipients only when requested, the system maintains a superior security posture.

This "push" model resolves the Interoperability Paradox by providing the necessary data for research and value-based care without opening the system to the "pull" requests that Mythos-class models use to scan for vulnerabilities. It effectively decouples the *act of sharing* from the *vulnerability of access*, allowing healthcare organizations to be fully compliant with the Cures Act while remaining resilient to AI-automated exploitation.

DATA SOVEREIGNTY AND INTEGRITY: CIRCLE DATASETS AS HIGH-TRUST ASSETS

In the era of Project Glasswing, the integrity of RWE is under threat not only from external breaches but from the internal risks of "data poisoning" and unauthorized lateral movement. Circle Datasets are emerging as high-trust assets because they utilize a closed-system approach that treats data as a sovereign resource rather than a fungible commodity.

Preventing Data Poisoning at the Source

"Data poisoning" occurs when inconsistent, malformed, or intentionally corrupted data is introduced into a training set for clinical AI, leading to biased or dangerous medical outcomes.

Legacy big data RWE is particularly vulnerable to this, as it often relies on retrospective "cleaning" of stale EHR and claims feeds that lack longitudinal context.

Data Characteristic	Legacy "Big Data" RWE	Circle Datasets
Origin	Billing/Claims and EHR Snapshots	Rigorous Prospective Observational Protocols
Integrity Check	Retrospective cleaning/mapping	Continuous, at-source validation
Context	Often lacks long-term outcomes	Longitudinal and correlated
Vulnerability	High (Poisoning via stale data, opaque algorithms, AI weightings)	Low (Standardized capture safeguards)

Circle Datasets utilize a "Federated Healthcare Data Capture" model that enforces standardized capture and continuous validation via specific Observational Protocols. By verifying data at the moment of capture, the system transforms filtering from a manual, error-prone process into a structural safeguard. This ensures that the resulting datasets are not only statistically significant but clinically valid, providing a "biography" for every record that makes its authenticity auditable.

Eradicating Lateral Movement during Aggregation

The aggregation phase of traditional RWE is a critical vulnerability point. As data flows from various clinics into a central silo, it creates a trail that an autonomous agent can follow to move laterally through the network. Circle Datasets will prevent this by utilizing Self-Sovereign Identity (SSI) and private keys. Even when data is queried for cloud-based analysis, the raw patient records remain at the primary point of care (the local node). The query only returns the necessary mathematical "insights" rather than moving the data itself, effectively cutting the path for lateral movement.

This approach treats trust as "continuous agency" rather than a one-time permission. Physicians and patients maintain control over their data at every stage, ensuring that "rights-laden" information is protected as a human right while still enabling the aggregation of regulatory-ready evidence.

ECONOMIC AND OPERATIONAL ANALYSIS

For healthcare and IT executives, the decision to maintain legacy interconnected systems or transition to a sovereign model like Circles is increasingly driven by the new economics of cyber risk". The financial impact of integration debt and rising cybersecurity insurance premiums has reached a breaking point in 2026.

THE INTEGRATION DEBT TAX

"Integration Debt" refers to the compounding cost of maintaining, patching, and securing thousands of unique, interconnected data bridges. In 2026, healthcare technology leaders report that nearly 60% of their systems cannot adequately protect agentless medical devices that are tethered to these networks. The operational cost of managing this complexity is enormous, with managed services often required to reduce IT costs by 30% just to maintain a baseline of security.

Project Glasswing has shown that the technical debt" of legacy code -- such as the 16-year-old flaw in FFmpeg -- is easily exploitable by AI. For organizations with highly interconnected platforms, the cost of auditing every line of code across their entire infrastructure is prohibitive. The Circles Platform bypasses this debt by operating as a streamlined, sovereign model where the burdensome – and increasingly costly and dangerous -- integration with external systems is eliminated in favor of simple, standardized outbound exports.

CYBERSECURITY INSURANCE: 2026 BENCHMARKS

The cyber insurance market in 2026 has transitioned into a "buyer-friendly" phase for most industries, with pricing falling by approximately 7% in late 2025. However, the healthcare sector is a notable exception. Due to the systemic risks highlighted by the Change Healthcare breach (which cost $2.9 billion in response) and the ongoing threat of Mythos-class exploits, insurance carriers are maintaining high premiums and increasing underwriting scrutiny for healthcare firms.

Summary Chart

Insurance Metric (2026)	Healthcare Sector	General Market Trend

Premium Change	Single-digit increase	7% reduction
Segmentation Requirement	46% of carriers request proof	Standardized
Average Ransom Demand	$1.1 Million	$1.1 Million
Peak Demand/Payment	$150M Demand / $75M Paid	N/A

HIMSS 2026 research indicates that 46% of cyber insurance carriers now request segmentation controls at the time of renewal. Organizations that cannot demonstrate effective micro-segmentation or risk isolation are being penalized with higher rates or even denied coverage for "system failure". The sovereign, closed-loop model of Circles provides a direct pathway to lower insurance premiums by fundamentally reducing the systemic risk of lateral movement and large-scale data exfiltration.

THE ROI OF DATA OWNERSHIP AND MONETIZATION

Beyond risk mitigation, the economic value of Circle Datasets lies in the "Longitudinal Value Formula". Unlike static, licensed datasets that lose value over time, Circle Datasets grow in value as more Cases are added and tracked over multiple years. Because Circles Platform architecture eliminates the need for retrospective data cleaning, the gross margins for monetization are significantly higher than traditional RWE models.

Summary Chart

Operational Metric	Legacy RWE Platform	RegenMed Circles
Time to Launch	Months/Years	4–6 Weeks
Subscription Cost	High (due to data licensing)	$35/mo per subscriber
Data Ownership	Contested/Unclear	85% Physician-Owned
Gross Margin	Low (squeezed by cleaning costs)	High (patented automated engine)

RegenMed's "Split-IP" model ensures that both patients and physicians have financial

motivation to maintain data continuity, transforming a series of clinical snapshots into a high-value evidence stream that is attractive to drug and device manufacturers.

CONCLUSION: A STRATEGIC BLUEPRINT FOR THE MYTHOS ERA

The evidence provided by the Project Glasswing consortium is categorical: the era of human-centered cybersecurity defense is coming to a close. As autonomous AI models like Claude Mythos proliferate, the technical debt of persistent API connections and centralized "honeypot" architectures will become a liability that no amount of patching can fully remediate.

For healthcare and IT executives, the strategic imperative is clear. The move toward sovereign, closed-loop RWE architectures like the Circles Platform is not merely a technical upgrade; it is a fundamental act of de-risking the organization's most valuable asset—its data. By adopting a federated capture model and "outbound-only" interoperability, healthcare organizations can satisfy the demands of the 21st Century Cures Act and the EU AI Act while maintaining a security posture that is resilient to the coming wave of AI-driven exploitation.

As we move toward 2030, the healthcare cybersecurity market is projected to reach $48 billion, driven by the explosion of connected clinical devices and tightening regulations. The winners in this landscape will be those who prioritize data sovereignty, integrity, and architectural simplicity over the fragile promises of universal interconnectedness. The sovereign model of Circles offers a credible, cost-efficient, and future-proof foundation for the next generation of medical evidence.

REFERENCES

Anthropic's Claude Mythos Finds Thousands of Zero-Day Flaws Across Major Systems. https://thehackernews.com/2026/04/anthropics-claude-mythos-finds.html

Project Glasswing - Anthropic. https://www.anthropic.com/project/glasswing

Anthropic says its most powerful AI cyber model is too dangerous to release publicly — so it built Project Glasswing | VentureBeat. https://venturebeat.com/technology/anthropic-says-its-most-powerful-ai-cyber-model-is-too-dangerous-to-release

Project Glasswing: Securing critical software for the AI era - Anthropic. https://www.anthropic.com/glasswing

The AI Arms Race Just Went Public: What Anthropic's Project Glasswing Means for Every Security Team - Blog. https://www.menlosecurity.com/blog/the-ai-arms-race-just-went-public-what-anthropics-project-glasswing-means-for-every-security-team

Tech giants launch AI-powered 'Project Glasswing' to identify critical software vulnerabilities. https://cyberscoop.com/project-glasswing-anthropic-ai-open-source-software-vulnerabilities/

Bug Management in the Mythos Era: 'Assume You're Unpatched'. https://www.cuinfosecurity.com/blogs/bug-management-in-mythos-era-assume-youre-unpatched-p-4091

Anthropic launches Project Glasswing, says Claude Mythos found risks in every major OS and browser. https://www.financialexpress.com/life/technology-anthropic-defines-project-glasswing-says-mythos-has-found-vulnerabilities-in-thousands-of-systems-4201201/

Anthropic's Project Glasswing addresses how AI exploits vulnerabilities - SD Times. https://sdtimes.com/open-source/glasswing-reveals-ai-exploits-vulnerabilities/

Mythos and Like AI Tools Raise Stakes for Healthcare Cyber - FraudToday. https://www.fraudtoday.io/mythos-like-ai-tools-raise-stakes-for-healthcare-cyber-a-31380

Why Claude Mythos Shifts Focus From Finding to Fixing Bugs. https://www.healthcareinfosecurity.com/blogs/claude-mythos-shifts-focus-from-finding-to-fixing-bugs-p-4088

Claude Mythos, Anthropic AI capable of hacking any software, joins forces with Google, Apple, AWS & more; Users' personal data at risk?. https://m.economictimes.com/news/new-updates/claude-mythos-anthropic-ai-capable-of-hacking-any-software-joins-forces-with-google-apple-aws-more-users-personal-data-at-risk/articleshow/130106401.cms

Insightful AI & Tech Blog | Trends, Tips & Expert Insights - NeuraMonks. https://www.neuramonks.com/blog

HIMSS Global Health Conference & Exhibition 2026: How AI, Interoperability, and Resilience Are Redefining Healthcare Delivery - Avasant. https://avasant.com/report/himss-global-health-conference-exhibition-2026-how-ai-interoperability-and-resilience-are-redefining-healthcare-delivery/

HIMSS26: Top 5 Takeaways from Healthcare's Biggest Conference - HealthMark Group.

https://healthmark-group.com/himss26-top-5-takeaways/

Mythos announcement hit different if you work in cyber : r/cybersecurity - Reddit. https://www.reddit.com/r/cybersecurity/comments/1sibhjd/mythos_announcement_hit_different_if_you_work_in/

AI Costs Dropped 280x: Complete Implementation Guide - Orbilon Technologies. https://orbilontech.com/ai-costs-dropped-280x-guide/

HIMSS Medical Device Security Survey [2026 Key Findings] - Elisity. https://www.elisity.com/blog/himss-medical-device-security-healthcare-microsegmentation

Latest News on Real-World Evidence and Circles Use Cases .... https://www.rgnmed.com/about-us/latest

CISA Releases New Sector Specific Goals for IT and Product Design. https://www.cisa.gov/news-events/news/cisa-releases-new-sector-specific-goals-it-and-product-design

2026 Cyber + Technology State of the Market at a Glance - CRC Group. https://www.crcgroup.com/Tools-Intel/Specialty-Tools-Intel/2026-cyber-state-of-the-market-at-a-glance

EU Regulation on AI | Insight - Baker McKenzie. https://www.bakermckenzie.com/en/insight/publications/resources/product-risk-radar-articles/eu-regulation-on-ai

CISA updates cybersecurity benchmarks for critical infrastructure organizations. https://www.cybersecuritydive.com/news/cisa-cybersecurity-performance-goals-update/807766/

The EU AI Act Has Arrived - Gardner Law. https://gardner.law/news/eu-ai-act-compliance-timeline

How the AI Act will affect hospitals and patients: five key points .... https://www.tucuvi.com/blog/how-the-ai-act-will-affect-hospitals-and-patients-five-key-points-explained-by-tucuvi

Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions | FDA. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket

The EU AI Act implementation timeline: understanding the next deadline for compliance. https://www.kennedyslaw.com/en/thought-leadership/article/2026/the-eu-ai-act-implementation-timeline-understanding-the-next-deadline-for-compliance/

FDA Tightens Its Medical Device Cybersecurity Guidance - FedTech Magazine. https://fedtechmagazine.com/article/2026/03/fda-tightens-its-medical-device-cybersecurity-guidance-perfcon

Navigating FDA's Cybersecurity in Medical Devices Guidance - Exponent. https://www.exponent.com/article/navigating-fdas-cybersecurity-medical-devices-guidance

2026 Healthcare IT Trends: What Leaders Need to Prepare For. https://www.himssconference.com/2026-healthcare-it-trends-what-leaders-need-to-prepare-for/

Cyber insurance trends: What's shaping the 2026 landscape? | Nixon Peabody LLP. https://www.nixonpeabody.com/insights/videos/2026/02/09/cyber-insurance-trends-whats-shaping-the-2026-landscape

2026 Cyber Insurance Market Outlook - Gallagher. https://www.ajg.com/-/media/files/gallagher/us/news-and-insights/2025/2026-cyber-insurance-market-outlook.pdf?utm_source=slipcase&utm_medium=affiliate&utm_campaign=slipcase

HIMSS 2026: Focused on AI, cybersecurity, digital health and unified communications - Spectrum. https://www.spectrum.com/business/enterprise/insights/blog/himss-2026-healthcare-technology-and-automation-reimagined

Top Healthcare Cybersecurity Vendors for 2026 [Compared] - Elisity. https://www.elisity.com/blog/top-healthcare-cybersecurity-vendors-2026

Cyber risk: A look ahead to 2026 - WTW. https://www.wtwco.com/en-us/insights/2026/02/cyber-risk-a-look-ahead-to-2026