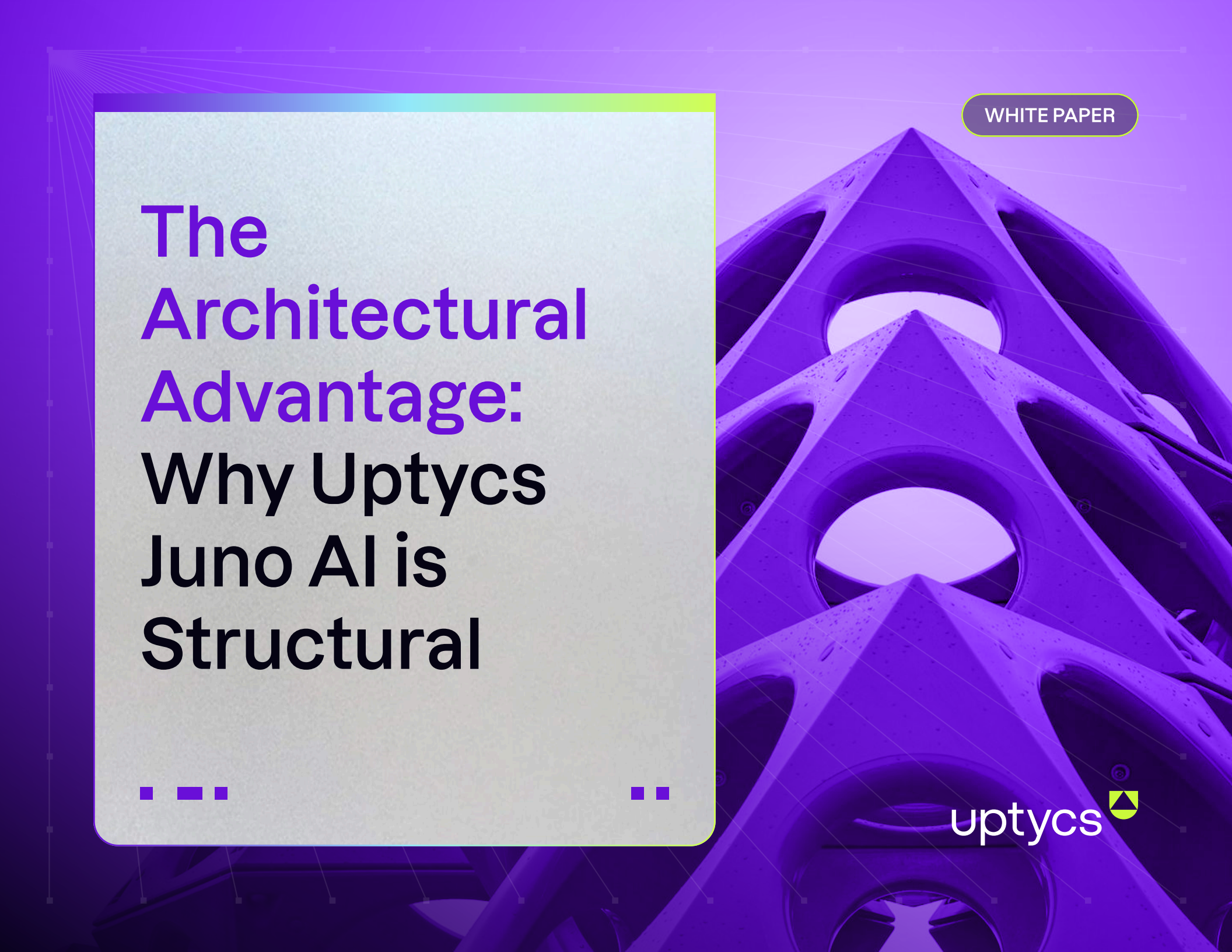
WHITE PAPER

The Architectural Advantage: Why Uptycs Juno AI is Structural



uptycs

Table of Contents

Executive Summary 01

I. The Core Innovation: The Unified Ontology 02

II. The Mechanism: "Surgical Sips" vs. Data Dumps 02

III. Why It Is "Verifiable" (The Glass Box) 03

IV. The "Moat": Why Competitors Cannot Replicate This 03

V. Real-World Impact: Minutes vs. Hours 04

Conclusion 04

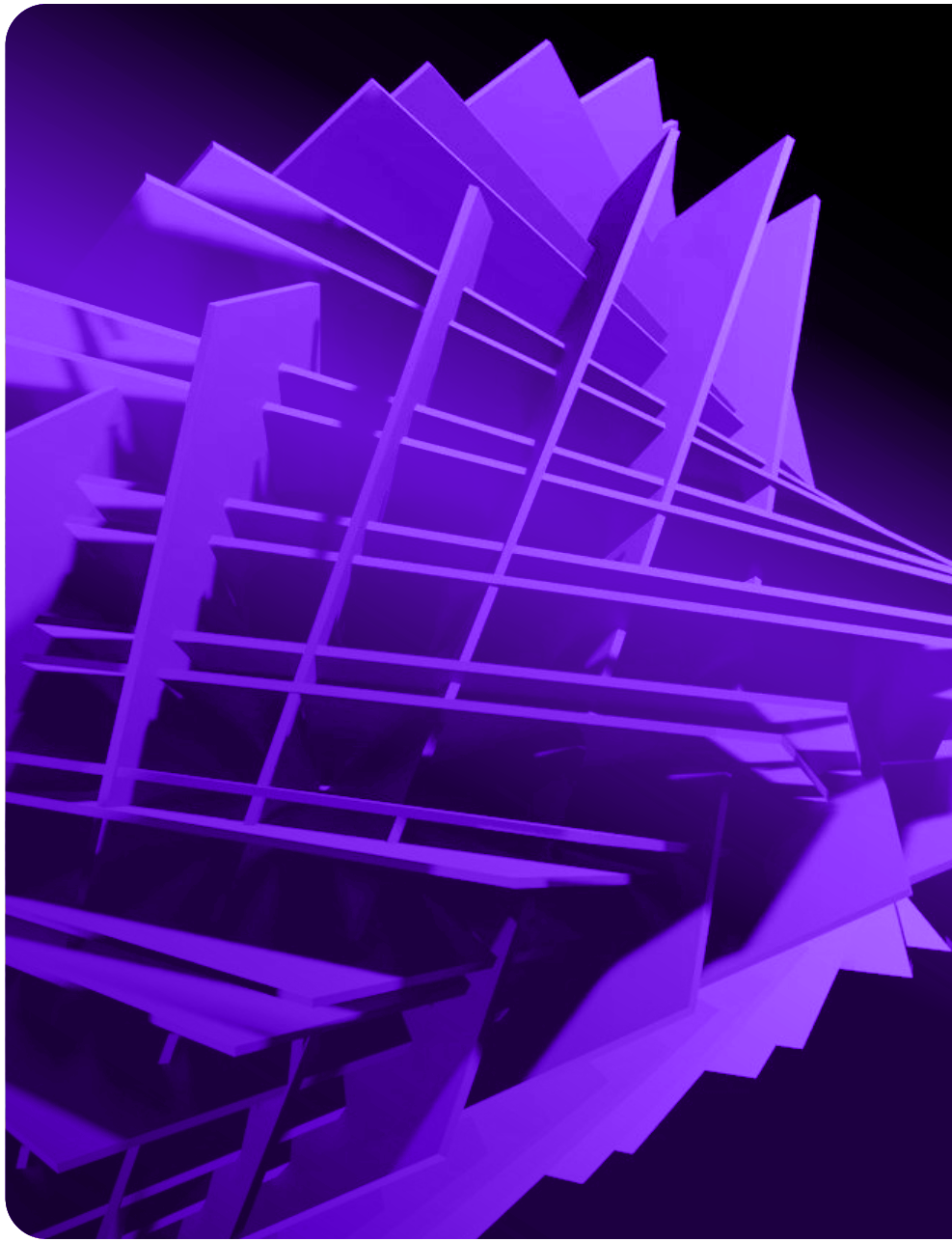
© 2026 All Rights Reserved | Uptycs | www.uptycs.com

Executive Summary

Most "AI assistants" in cybersecurity are chatbots wrapped around a search bar. They summarize alerts or offer probability-based advice, but they suffer from two fatal flaws: they guess answers (hallucinations) and they cannot show their work (opacity).

Uptycs took a different path. We built the Uptycs Juno AI Analyst. This is an agentic system that investigates rather than just chatting. This capability relies on a massive, multi-year architectural project called the Unified Multi-Cloud Ontology.

We solved the "Data Physics" problem first. We normalized petabytes of security data into a single, queryable language. Because of this foundation, Juno operates with precision, transparency, and verifiability that siloed competitors cannot match.



© 2026 All Rights Reserved

I. The Core Innovation: The Unified Ontology

Most security platforms look like "Frankenstein" architectures. They are collections of acquired tools glued together. Cloud data sits in one database, endpoint data in another, and Identity data in a third. These systems cannot "think" across boundaries because they speak different languages.

The Difference: Juno's "Universal Dictionary"

Years before the Generative AI boom, Uptycs bet on building a Unified Multi-Cloud Ontology. We built a normalized schema that maps every digital asset into a single, coherent data model. Whether it is an AWS Lambda function, a Google Cloud container, or an employee's laptop, it all lives in the same structure.

The Scale

This ontology consists of over 3,000 tables and approximately 150,000 columns of structured security data.

The Impact

This massive structure provides the "knowledge" for the Juno AI Analyst. It has a map of the entire territory, so it never has to guess where data lives.

II. The Mechanism: "Surgical Sips" vs. Data Dumps

A common failure in AI security is "Context Overload." Vendors feed an AI massive logs and ask for a summary. The AI gets overwhelmed and starts hallucinating.

Uptycs Juno AI uses an agentic architecture that mimics a human analyst taking precise steps.

Intent to SQL

When a user asks a question, such as "Show me lateral movement in AWS," Juno ignores the temptation to generate a text answer. It translates that intent into a deterministic SQL query.

Surgical Sips

Juno has the 150,000-column map. It knows exactly which specific rows to query. It takes a "surgical sip" of data and retrieves only the precise evidence needed. It avoids choking on a firehose of irrelevant logs.

Iterative Reasoning

If the first query reveals a threat, Juno autonomously formulates the next query to dig deeper. It chains evidence together the same way a human investigator would.

© 2026 All Rights Reserved | Uptycs | www.uptycs.com

III. Why It Is "Verifiable" (The Glass Box)

The industry standard is "Black Box" AI. You ask a question, and it gives you a text response. You have no way of knowing if it is true.

Uptycs Juno AI offers a "Glass Box." Juno operates by writing code (SQL) rather than just writing prose.

Transparency
You see the exact SQL query Juno generated.

Evidence
The response includes the raw telemetry rows that prove the finding.

Auditability
Every step is recorded. You verify the code rather than trusting the bot.

IV. The "Moat": Why Competitors Cannot Replicate This

Investors and analysts often ask if Google, Microsoft, or CrowdStrike can just build this.

They cannot. They are held back by Architectural Debt.

The Silo Trap
Major competitors are trapped in siloed architectures. To replicate Uptycs Juno AI, they would need to scrap their separate backends and rebuild a unified schema from scratch. That is a multi-year engineering project rather than a simple software update.

The Telemetry Gap
Verifiability requires raw data. Uptycs stores 90 days of raw telemetry and 13 months of historical data. Competitors often only store alerts or snapshots of configurations. You cannot verify a complex threat if you have thrown away the raw evidence.

The Reality
Competitors have not failed to build this due to a lack of AI talent. They fail because they lack the Unified Data Model required to feed Juno truth instead of noise.

© 2026 All Rights Reserved | Uptycs | www.uptycs.com

V. Real-World Impact: Minutes vs. Hours

The difference between "Chatbot AI" and Uptycs Juno AI comes down to speed and accuracy.

Example: Advanced Persistent Threat (APT) Detection

- **The Scenario**
  An attacker compromises a laptop, steals credentials, and pivots to AWS to steal data.

- **The Competitor Approach**
  The Endpoint tool fires an alert. The Cloud tool fires a separate alert. The Identity tool stays silent. A human analyst spends hours manually trying to correlate these CSV files.

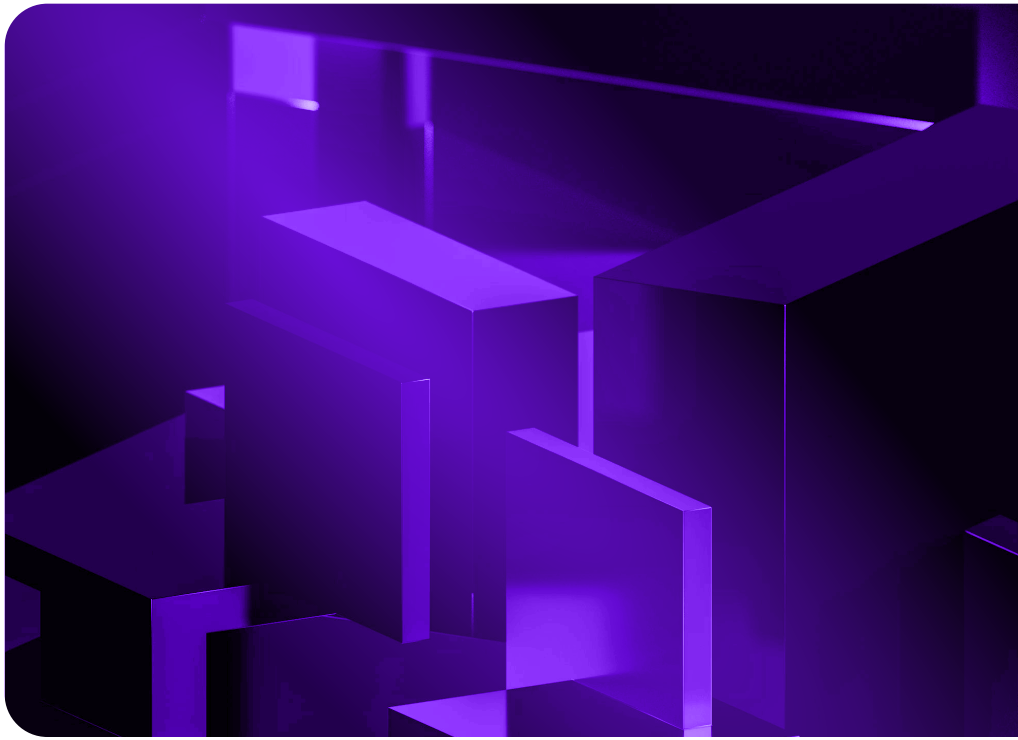
- **The Uptycs Approach**
  The analyst asks Juno to show signs of lateral movement. Juno runs a cross-platform SQL query. It correlates the laptop process, the stolen credential use, and the AWS data exfiltration in real time.

The entire attack chain is visualized and verified in minutes.

Conclusion

Uptycs has moved beyond the hype cycle. By anchoring Juno AI Analyst to a battle-tested, proprietary data ontology, Uptycs delivers the holy grail of security operations: Automation you can trust.

While the market chases chatbots, Uptycs has built the digital nervous system that makes autonomous security possible.



© 2026 All Rights Reserved

uptycs

Uptycs delivers the industry's first **Unified CNAPP** with integrated XDR, powered by Juno - the only verifiable AI Security Analyst.

Unlike traditional CNAPPs that rely on static snapshots, Uptycs unifies cloud configuration data with deep runtime telemetry across cloud, containers, and endpoints into a single Unified Ontology. Trusted by the Fortune 500, Uptycs powers Continuous Threat Exposure Management (CTEM) by normalizing telemetry into a single data lake, enabling the Juno AI Analyst to provide **"Glass Box" transparency**, turning hours of investigation into minutes of verified answers.

Learn more at uptycs.com/juno-ai

© 2026, Uptycs.