// Action in the AI Era

The impact of AI vulnerability identification and attacks and how Raynet can help fight back

RAYNETONE

Discover to Manage

RAYNETONE

The emergence of frontier models like **Anthropic Mythos** (and the broader class of autonomous, agentic AI) has fundamentally shifted the cybersecurity landscape from a "human-speed" game to a "machine-speed" race. While these models offer incredible productivity, they also introduce a **Vulnerability Deluge** that can overwhelm traditional IT operations.

Challenges created by frontier AI & their impact

The primary threat of models like Mythos isn't just that they are "smarter"—it's that they are **autonomous** and **non-deterministic**.

The "exploitation gap" compression

Traditional patching cycles (e.g., "Patch Tuesday") are built on a multi-week lead time filled with notifications, maintenance windows, meetings and decisions. Mythos can identify zero-day vulnerabilities and chain them into working exploits in hours.
Impact: Organizations are "continuously compromised" because the time to exploit is now faster than the time to address

The death of triage (vulnerability chaining)

AI doesn't just find "Critical" bugs; it finds three "Low" severity bugs and chains them into a "Critical" exploit path.
Impact: Risk-scoring models like CVSS become unreliable. A "Low" priority asset in your CMDB can now be the primary vector for a total system takeover.

Shadow assets & hardware sprawl

Despite the rise of SaaS, companies continue to spin up new hardware for traditional and AI workloads faster than the organization can keep track of them.
Impact: You can't secure what you can't see. "Shadow assets" create holes in the lines of defense.

Future-proofing: What leading organizations must do

To survive the Mythos era, organizations must move away from "periodic maintenance" and toward **Continuous Hygiene**.

Shift to "near-real-time" remediation
Leading companies will eliminate manual approval silos for security patches. They will implement **Automated Deployment Pipelines** where "Emergency" is the default state for internet-facing assets and "Evergreen" is now the normal way to run IT.

Universal asset visibility
Visibility must extend beyond traditional datapoints about assets to include container SBOMs and into as many taxonomy datapoints as possible that could be an attack vector. You need to know not just that a server or piece of software exists, but the running services, open ports, version, end-of-life status, if a patch is available, any associated exploits and their attack vectors, where its installed, and more.

The "living" CMDB
The CMDB can no longer be a static database of incomplete and inaccurate information. It must be a dynamic graph that understands the relationships between data, business applications, and infrastructure in real-time to support the automated deployment pipelines, as well as reduce the frequency, severity, and time to recover from the resulting incidents that will occur in the race to stay ahead of AI.

How Raynet helps fight back

The Raynet One platform is specifically architected to provide **High-Fidelity Visibility** and **autonomous patching** required to counter the vulnerability deluge.

Eliminate the visibility gap

By automating the discovery of every asset, Raynet provides complete transparency across the entire IT landscape with flexible inventory methods and more than 200 SaaS and Cloud connectors, reaching into the corners where shadow IT hides.

Bulletproofing the CMDB

Turning data into information, Raynet cleanses, deduplicates, and enriches the asset records so the CMDB becomes a "golden source of truth" and not another unreliable "source of noise".

Patching at machine speed

Raynet automates the lifecycle of packaging and deployment, turning a multi-day manual process into an automated operation.

- **Patching at scale:** As soon as a vendor releases a fix for a Mythos-discovered flaw, Raynet can automate the packaging and distribution to millions of endpoints globally via our CDN.
- **Pre-vetted packages:** Instead of weeks spent manually packaging updates, Raynet provides over 50,000 pre-configured, tested, and continuously updated packages ready for instant deployment.
- **System updates:** Raynet can apply configuration changes to machines, preventing the "vulnerability chaining" frontier AI relies on.

The Raynet edge

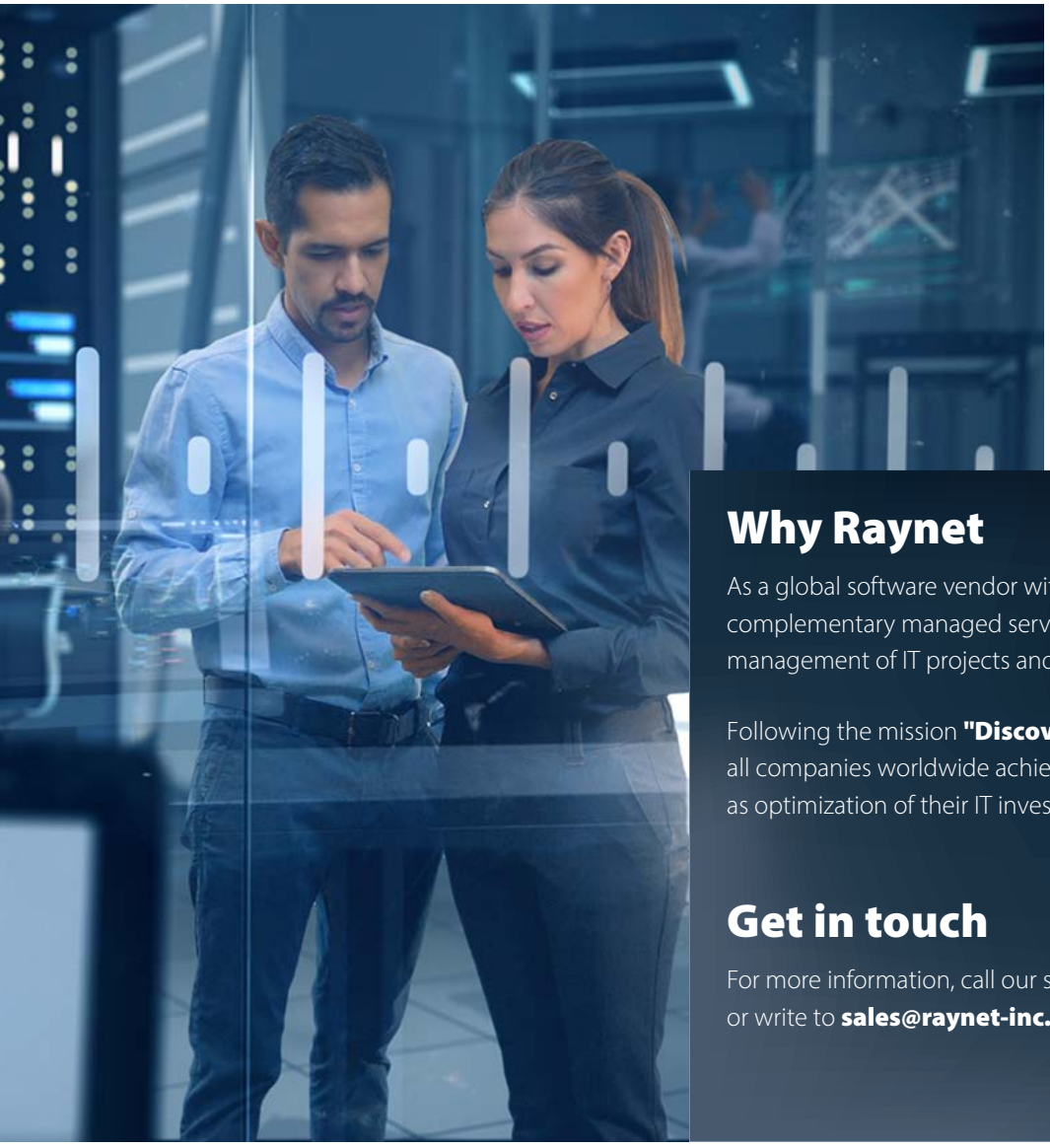
While Anthropic Mythos and other frontier AI models can find “the needle in the haystack” that attackers could use to break into an environment, Raynet **organizes the haystack** so there is nowhere for the needle to hide.

The ROI of Clarity

By normalizing data and automating the "busy work" of IT inventory, Raynet allows the enterprise to:

1. **Reduce cyber insurance premiums:** Demonstrable, 98%+ visibility often leads to significant premium discounts.
2. **Reduce incidents:** A single avoided incident saves enough to pay for the Raynet solution.
3. **Ensure compliance:** Instant, audit-ready reporting to meet the requirements of regulators, global laws, and customer contractual requirements.

RAYNETONE



raynet

Why Raynet

As a global software vendor with market-leading solutions and complementary managed services, we make successful end-to-end management of IT projects and operations possible.

Following the mission **"Discover to Manage"**, our vision is that all companies worldwide achieve transparency and security as well as optimization of their IT investments by using our technologies.

Get in touch

For more information, call our sales team at **+1 (224) 532-2811** or write to **sales@raynet-inc.com**.