Glasswing.ai Launches the Industry's First Network-based AI Firewall

SAN DIEGO, CALIFORNIA, UNITED STATES, March 7, 2024 /EINPresswire.com/ -- Glasswing.ai announced it has launched the industry's first network-based AI firewall. Glasswing AI firewall provides guardrails for enterprises protection. When an Enterprise opens their NGFW to allow AI communication, Glasswing provides fine-grained control of all usage of AI solutions. Glasswing can block unauthorized use of AI solutions or redirect traffic to an approved AI solution.

Glasswing's AI Firewall provides fine-grained control over AI usage within an enterprise (logos trademark of their respective owners)
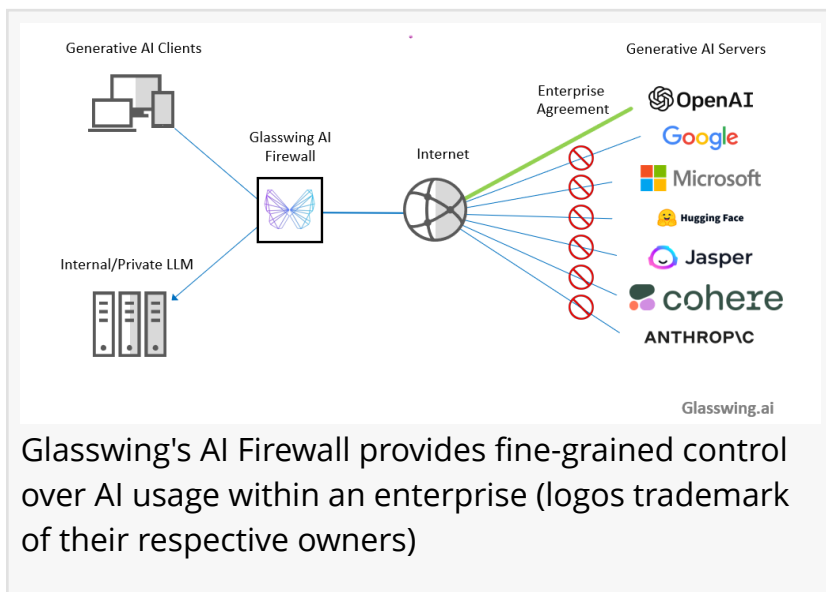
Many enterprises will adopt a specific AI solution based upon the use case. For example, an enterprise will choose one AI company for the "software development assistant" use case. A separate AI company may be approved for Content Generation, Image generation, or voice generation. Glasswing can enforce these policies and redirect connections to an approved AI vendor.

> With the Glasswing.ai AI firewall an enterprise can has a view of every AI system being used. By enforcing AI usage policies organizations eliminate the risking accidental data disclosure."
>
> *Brett Helm, CEO and Co-Founder of Glasswing.ai*

The platform also enables companies to understand and control the magnitude of their usage of AI platforms. With Glasswing's solution, enterprises can harness the power of AI platforms while ensuring that company confidential data is not leaked to these platforms.

Glasswing's AI firewall monitors and controls all usage of AI tools, including those used without enterprise license, to show which AI platforms are being used across the entire organization. The AI firewall can be used as a standalone solution or installed as a "firewall behind a firewall", much like Next Generation Firewalls (NGFWs) were originally positioned. The solution is available now.

Generative AI solutions have exploded in popularity. There are now over 2400 AI companies including industry leaders OpenAI ([ChatGPT](#)), Google ([Google Bard](#)), and Microsoft (Bing AI). These solutions can improve efficiency, reduce errors, and improve an organization's operations. There is, however, a dark side as these tools create a risk of confidential data being exposed.

Samsung is one of many companies who have banned the use of generative AI tools from company devices and from personal devices connected to company networks. Samsung mandated this after data was leaked to ChatGPT in three separate incidents.

Generative AI tools promise to be an offensive tool for companies to achieve greater efficiency, increase productivity, or create better products and technology. Today, we introduced a defensive tool to protect companies from using non-approved AI connections, losing IP, trade secrets, and confidential data.

"For the first time an enterprise can have a comprehensive view of every AI system being used by company employees and control what AI system is used for specific purposes," said Brett Helm, CEO, Chairman and Co-founder of Glasswing.ai. "By enforcing AI usage policies, the Glasswing AI Firewall allows organizations to adopt AI without risking accidental data disclosure."

A network-based AI firewall can be used with a customer's NGFW to make AI fine granular decisions. Available as a network appliance or virtual machine image, the solution can be installed inline behind a traditional firewall to block requests that don't comply with company policies. The solution can also be installed alongside a traditional firewall or network router via a span port or transparent traffic ingestion. With this configuration, the solution acts as a visibility and discovery tool, providing detailed reporting on usage of AI tools.

Utilization of a network-based AI firewall provides several benefits over browser-based plugins, the only other solution currently available:
• The solution is easy to install and centrally managed
• The solution provides a single point data collection for AI usage audit and privacy compliance enforcement
• No changes are required to user endpoints
• The solution manages all access to AI tools, including access from any browser or via APIs for cloud-based connections or on prem solutions.
• Protection for non-browser-based applications
• Supports both cloud and legacy on prem environments

Glasswing.ai was founded by industry veterans including Brett Helm, former Intel executive and CEO of DB Networks, Coradiant, and iPivot Inc., Eric Varsanyi, former CTO at DB Networks, Coradiant, Intel, and BSDi, and Steve Schnetzler co-founder IPivot Inc.

Brett Helm
Dragonfly Cyber

+1 515-707-4179
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/694204072