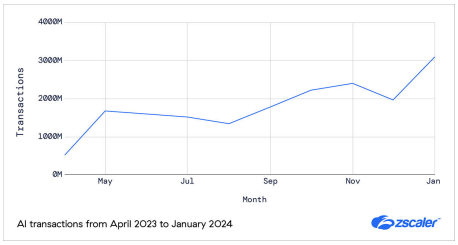
Zscaler Finds Enterprise Use of AI/ML Tools Skyrocketed Nearly 600% Over the Last Year, Putting Enterprises at Risk

March 27, 2024

ThreatLabz AI Report Reveals Enterprises Sharing 569 TB of Data to AI Tools, Stressing the Need for Better Data Security

- **Enterprise AI/ML transactions** increased from 521 million monthly in April 2023 to 3.1 billion monthly by January 2024.
- **Manufacturing generates the most AI traffic, totaling 21% of all AI transactions in the Zscaler security cloud**, followed by Finance and Insurance (20%) and Services (17%).
- **The most popular AI/ML applications for enterprises by transaction volume** are ChatGPT, Drift, OpenAI, Writer, and LivePerson.
- **The top five countries** generating the most enterprise AI transactions are the US, India, the UK, Australia, and Japan.

Zscaler 2024 AI Report



2024 AI Report

SAN JOSE, Calif., March 27, 2024 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the release of its 2024 AI Security Report, which draws on more than 18 billion AI transactions across the Zscaler Zero Trust Exchange™ cloud security platform from April 2023 to January 2024. Zscaler ThreatLabz researchers analyzed how enterprises use AI/ML tools and mapped trends across sectors and geographies, highlighting how businesses are adapting to the shifting AI landscape and managing security around the use of AI tools. Today's enterprises must secure a transformation driven by generative AI (GenAI) bidirectionally: by securely adopting GenAI tools in the enterprise with Zero Trust while leveraging it to defend against the new AI-driven threat landscape.

AI has already become a part of business as usual, as enterprises leverage and integrate new features and tools into their day-to-day workflows, multiplying the volume of transactions and data generated. The much higher volume is reflected in the nearly 600% increase in transactions as well as the 569 terabytes of enterprise data sent to AI tools that ThreatLabz analyzed between September 2023 and January 2024.

“Data is the lifeblood of every enterprise and the gold of this new era in the AI revolution,” said Deepen Desai, Chief Security Officer, Zscaler. “With the visibility provided by the Zscaler Zero Trust Exchange’s nearly 500 trillion daily signals combined with Avalor* Data Fabric, we believe Zscaler is uniquely positioned to fight AI with AI and improve Zero Trust security across the enterprise.”

AI transactions grow exponentially

From April 2023 to January 2024, ThreatLabz saw AI/ML transactions grow by nearly 600%, rising to more than 3 billion monthly across the Zero Trust Exchange platform in January. Despite the mounting security risk and increasing number of data protection incidents, enterprises are adopting AI tools in large numbers.

Manufacturers responsible for more than 20% of enterprise AI/ML transactions

Manufacturing was found to be the industry leader in AI transactions across the Zero Trust Exchange platform, driving nearly 20% of the total volume. From analyzing vast amounts of data from machinery and sensors to preemptively detect equipment failures to optimizing supply chain management, inventory, and logistics operations, AI is proving instrumental to manufacturers. The other notable verticals that comprise the top five are finance and insurance (17%), technology (14%), services sectors (13%), and retail/wholesale (5%).

ChatGPT leads the way as the most popular GenAI application

Research shows that ChatGPT accounted for more than half of all enterprise AI transactions (52%), while the OpenAI application itself ranked third (8%). Drift, the popular AI-powered chatbot, generated nearly 20% of enterprise traffic, while LivePerson and BoldChat also made the list. Writer was the favorite GenAI tool for creating written enterprise content.

The United States leads the way in enterprise AI tools usage

AI adoption trends differ globally as regulations, requirements, technology infrastructure, cultural considerations, and other factors play key roles. At 40%, the US produces the highest percentage of enterprise AI transactions globally. India was second at 16%, propelled by the country’s accelerated commitment to driving innovation.

Although the UK's share of global enterprise AI transactions is only 5.5%, it leads enterprise AI traffic in EMEA with over 20%. France (13%) and Germany (12%), as expected, follow closely behind as the second and third largest enterprise AI traffic generators in EMEA. However, the United Arab Emirates is a rapidly growing technological innovator in the region that has also emerged as a prominent AI adopter.

In the APAC region, ThreatLabz discovered a staggering increase of nearly 1.3 billion (135%) more enterprise AI transactions compared to EMEA. This surge can likely be attributed to India’s extensive usage and adoption of AI tools for conducting business across the tech sector, and it may suggest a higher concentration of tech jobs, stronger willingness to adopt new innovations, and fewer barriers to usage.

AI empowered threat actors amplify enterprise risk and security challenges

As the power of AI has advanced, it has become a double-edged sword for enterprises. While AI offers immense potential for innovation and efficiency, it also brings forth a new set of risks that organizations must grapple with–namely, risks associated with leveraging GenAI tools within the enterprise and an evolving landscape of AI-assisted threats.

The utilization of GenAI tools within enterprises introduces significant risks that can be categorized into three main areas:

1. Protection of intellectual property and non-public information: the risk of data leakage
2. AI application data privacy and security risks: including an expanded attack surface, new threat delivery vectors, and increased supply chain risk
3. Data quality concerns: the concept of "garbage in, garbage out" and the potential for data poisoning

Simultaneously, enterprises are constantly exposed to a barrage of cyberthreats, some of which are now AI-driven. The possibilities of AI-assisted threats are virtually limitless, as attackers can leverage AI to orchestrate sophisticated phishing and social engineering campaigns, develop highly evasive malware and ransomware, exploit vulnerabilities in enterprise attack surfaces, and amplify attacks' speed, scale, and diversity. To address this challenge, enterprises and cybersecurity leaders must effectively navigate the rapidly evolving AI landscape to harness its revolutionary potential while also mitigating the risks and defending against AI-powered attacks.

Enabling secure enterprise AI adoption with Zscaler

Zscaler is at the forefront of empowering enterprises to embrace the potential of AI applications while ensuring the safety of their data and maintaining an environment that’s secure against emerging channels for exfiltration. With the Zero Trust Exchange platform, Zscaler provides the comprehensive set of tools necessary for this transformative journey, encompassing four critical capabilities:

1. Full visibility into AI tool usage
2. Granular access policy creation for AI
3. Granular data security for AI applications
4. Powerful controls with browser isolation

By leveraging Zscaler’s Zero Trust security controls, enterprises can confidently embrace their AI transformation, fully harnessing the potential of generative AI while ensuring the highest level of security. They will gain the necessary tools to protect their business from AI-driven threats while benefiting from Zscaler’s fine-tuned AI policies and robust data protections.

Download the full version of the 2024 AI Security Report now to uncover even more insights about securing AI.

*See here to learn more about Zscaler’s recent acquisition of Avalor.

Methodology
Analysis of 18.09 billion AI transactions from April 2023 to January 2024 in the Zscaler security cloud, the Zero Trust Exchange.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform.

Media Relations Contact:
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/d9e83e38-6326-46a2-8223-b9d6428470d8