Three Principles of Data Security in the AI Era

By Dan Benjamin, Sr. Director of Product Management, Palo Alto Networks

AI hype and adoption is seemingly at an all time high with nearly 70% of respondents to a recent S&P report on Global AI Trends saying they have at least one AI project in production. While the promise of AI can fundamentally reshape business operations, it has also created new risk vectors and opened the doors to nefarious individuals that most enterprises are not currently equipped to mitigate.

In the last 6 months, three reports (*S&P Global's 2023 Global Trends in AI report*, *Foundry's 2023 AI Priorities Study*, and Forrester's report *Security And Privacy Concerns Are The Biggest Barriers To Adopting Generative AI*) all had the same findings: data security is the top challenge and barrier for organizations looking to adopt and implement generative AI. The surging interest in implementing AI has directly increased the volume of data that organizations store across their cloud environments. Unsurprisingly, the more data that is stored, accessed and processed across different cloud architectures that typically also span different geographic jurisdictions, the more security and privacy risks arise.

If organizations don't have the right protections in place, they instantly become a prime target for cybercriminals which according to a Unit 42 2024 Incident Response Report are increasing the speed at which they steal data with 45% of attackers exfiltrating data in less than a day after compromise. As we enter this new "AI era" where data is the lifeblood, the organizations that understand and prioritize data security will be in pole position to safely pursue all that AI has to offer without fear of future ramifications.

Developing the Foundation for an Effective Data Security Program

An effective data security program for this new AI era can be broken down into three principles:

Securing the AI: All AI deployments – including data, pipelines, and model output – cannot be secured in isolation. Security programs need to account for the context in which AI systems are used and their impact on sensitive data exposure, effective access, and regulatory compliance.

Securing the AI model itself means identifying model risks, over permissive access and data flow violations throughout the AI pipeline.

Securing from AI: Just like most new technologies, artificial intelligence is a double-edged sword. Cyber criminals are increasingly turning to AI to generate and execute attacks at scale. Attackers are currently leveraging generative AI to create malicious software, draft convincing phishing emails and spread disinformation online via deep fakes. There's also the possibility that attackers could compromise generative AI tools and large language models themselves. This could lead to data leakage, or perhaps poisoned results from impacted tools.

Securing with AI: How can AI become an integral part of your defense strategy? Embracing the technology for defense opens possibilities for defenders to anticipate, track, and thwart cyberattacks to an unprecedented degree. AI offers a streamlined way to sift through threats and prioritize which ones are most critical, saving security analysts countless hours. AI is also particularly effective at pattern recognition, meaning threats that follow repetitive attack chains (such as ransomware) could be stopped earlier.

By focusing on these three data security disciplines, organizations can confidently explore and innovate with AI without fear that they've opened the company up to risks.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com