PRODUCTS AND OPERATIONS
OFFICE OF THE CHIEF TECHNOLOGY OFFICER

Data – The Intersection of Zero Trust and Artificial Intelligence

Project Fort Zero

Herb Kelsey
Project Fort Zero Lead

Table of Contents

Introduction

The global cost of cybercrime was estimated to be about $11.5 trillion in 2023.[1] As existing cybersecurity systems and practices become more obsolete, the number of cybercrimes impacting the world's sensitive data will continue to increase. In 2023, the Federal Bureau of Investigation (FBI) received 880,418 cybercrime complaints that cost $12.5 billion compared to 2019, where 467,361 complaints cost $3.5 billion.[2] As a result of the growing cost and number of cybercrimes, organizations are increasingly turning to Artificial Intelligence (AI) to modernize cybersecurity and shield themselves from cybercrime. AI allows organizations to leverage all available data to monitor, analyze, and detect cyber threats in near real-time creating an automated view with content, prediction, and knowledge.

Organizations are pivoting to AI, Machine Learning (ML), and Large Language Models (LLM) to streamline their business and enhance its value. A 2023 report by Stanford University revealed that 55% of organizations added AI into at least one business unit, compared to 20% in 2017, indicating a 175% increase in seven years.[3] The complexity of AI and its supporting architecture requires robust data policy and processes to construct the LLMs. The results are sophisticated AI models that generate significant amounts of data and encapsulate critical organizational knowledge. Artificial Intelligence models represent valuable intellectual property that if lost, stolen, or corrupted, may result in devastating consequences to organizations. AI models are highly valuable and likely targets for cybercrime. Protecting the data surrounding AI is paramount as it represents money, time, and sensitive customer information for organizations.

Artificial Intelligence provides a methodology for swift analysis of complex data required to respond to cybercrime quickly. The use of AI produces substantial amounts of data, including proprietary models and algorithms that may contain vital customer and organizational information. Artificial Intelligence is the simulation of human intelligence in machines, while ML is a subset of AI that allows AI to operate. Machine Learning focuses on teaching and enhancing the experience through AI models. Machine Learning algorithms teach AI how to respond and teach patterns observed from ML. An AI algorithm that uses deep learning techniques to process and generalize large sets of data is an LLM. Predicting future behaviors and solving problems can be done through LLMs. If organizations lose this data, it is a significant loss to their AI models, ML algorithms, business models, and customer trust.

Artificial Intelligence provides a methodology for swift analysis of complex data required to respond to cybercrime quickly.

Decision-making that leverages AI hinges on the quality of the data. The data captured must be filtered, analyzed, and compiled into ML algorithms. A remarkable amount of data is required when using AI; however, to achieve the best outcomes from the data, the data itself must be free from unauthorized alterations. The AI models become assets as the source for wisdom and training for AI, but that wisdom is only as credible as the data itself. Data creates the AI models; therefore, the authenticity of the data is critical. AI models are essential because they focus on corporate knowledge and provide it with operational capabilities. The security of the data is critical to ensure validity throughout AI and ML models.

[1] Emma Charlton, 2023 was a big year for cybercrime – here's how we make our systems safer, World Economic Forum, January 10, 2024, https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

[2] Federal Bureau of Investigation (FBI), FBI Internet Crime Report 2023, 2023, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf?trk=public_post_comment-text

[3] Stanford University, The AI Index Report: Measuring trends in AI, 2024, https://aiindex.stanford.edu/report/

In today's ever changing cyber landscape, Zero Trust exemplifies protecting the data. Through its data-centric approach Zero Trust safeguards sensitive information across diverse environments, platforms, and applications. Zero Trust reinforces data protection by ensuring only authorized personnel can access data through a core principle that no implicit trust is granted to assets or user accounts based solely on their physical or network location. Adopting Zero Trust principles requires a paradigm shift from traditional perimeter-based network security solutions and toward a microsegmented, data-centric architecture. The Identity Provider (IdP) needs to support alternative methods of multifactor authentication (MFA). Multifactor options support biometric capability and are managed using a self-service approach.

> Through its data-centric approach Zero Trust safeguards sensitive information across diverse environments, platforms, and applications.

Safeguarding AI Models and Data

The AI models are only as valuable as the data they use. Quality data is essential to capitalizing on the full potential of AI. Flawed data may result in inaccurate analysis, recommendations, and actions. Artificial Intelligence requires complex data pipelines and computing resources to construct LLMs. These pipelines generate and leverage significant amounts of data. The results are critical to organizations and represent the intellectual property used to drive decisions. Keeping this data secure is essential for operations, which in turn increases the significance of ensuring AI models and their supporting data are secure. Artificial Intelligence data is used to drive business decisions, increase revenue, and train the AI models. Losing this vital data could be overwhelming. Organizations can best safeguard AI models and assets by creating and storing them in a secure network with multiple identity verifications.

In many networks today, cyber criminals can easily maneuver in an organization's system once beyond the perimeter, creating opportunities to manipulate and steal data. The U.S. Department of Defense (DoD) Zero Trust Reference Architecture (ZTRA) defines five tenets that establish a foundation to influence Zero Trust: Assume a hostile environment; presume breach; never trust, always verify; scrutinize explicitly; and apply unified analytics.[4] Focusing on the tenets, Zero Trust can take proactive measures to minimize lateral movement, analyze behavior anomalies, and apply safeguards to protect data. By assuming a breach, an advanced Zero Trust solution mitigates the cyber criminals' ability to access steal, corrupt, or modify data, ultimately reducing the impact on operations. When Zero Trust is coupled with AI, large quantities of data can be analyzed at near real-time which reduces an organization's attack surface, minimizes the need for human intervention, and automates security protocols.

> Dell is scheduled to begin assessment during the summer of 2024.

Dell Technologies Project Fort Zero (PFZ) is tackling the integration challenge and developing a greenfield advanced ZT solution. Project Fort Zero is a sovereign on-premises enterprise private cloud architected to meet all the requirements for Advanced-Level Zero Trust as identified in the U.S. DoD Zero Trust Reference Architecture (U.S. DoD ZTRA). Dell is scheduled to begin assessment during the summer of 2024 by the U.S. DoD to validate the PFZ solution against all 152 activities derived from the 45 capabilities identified in the U.S. DoD ZTRA.

[4] U.S. Department of Defense (DoD), DoD Zero Trust Reference Architecture, July 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Project Fort Zero uses AI/ML to provide conditional user access, assist in decision-making for network analytics, tag and classify data, automate encryption processes, prevent data loss, analyze behavior, and automate access policies. Robust logging of all activity is used within PFZ to iteratively teach AI/ML algorithms and continuously improve decision-making. Once implemented, AI/ML solutions will automatically update security profiles through continuous monitoring. Using existing AI/ML functionality allows users to automate workflow activities by identifying, procuring, and implementing policies.

The PFZ solution leverages self-learning capabilities alongside AI to analyze attack patterns, automate data restoration, and strengthen defenses. These capabilities improve threat detection and reduce the time required to analyze large amounts of data. PFZ uses AI/ML to enable organizations to detect, analyze, and react to unwanted activity quickly and accurately.

Conclusion

> With exponentially increasing demand for AI adoption, the need to protect the data becomes most critical.

The PFZ end-to-end solution enables an accelerated adoption of Zero Trust principles. Organizations that adopt PFZ will be best postured to defend against the most sophisticated cybercrimes. With exponentially increasing demand for AI adoption, the need to protect the data becomes most critical. Organizations must secure critical data, policies, language models, and customer behaviors to shield their business from negative consequences and ensure stability in the market. Safeguarding critical organizational elements remains important for protecting information from cyber criminals.

Current trends and global influence are driving the criticality for implementing Zero Trust and AI solutions. Organizations must shift their paradigm and modernize their cybersecurity posture to effectively combat the increase in cybercrime. AI is the future, and with an advanced Zero Trust solution organizations leveraging AI can reach their full potential.