DOSANJH USA
AI and Cybersecurity Services

Shadow AI Prevention

Safeguard Data with Policy-Driven Security Controls for GenAI Copilots

Online Chat

Non-Secure Copilot

INPUT: Chat

Who do these Social Security Numbers belong to?
111-22-3333, 444-55-6666, 777-88-9999

OUTPUT: Chat

They belong to the following:
111-22-3333 John Doe
444-55-6666 Jane Doe
777-88-9999 Bob Roe

GenAI Copilots introduce a risk of data loss due to accidental exposure or malicious breaches. These AI-driven virtual assistants are commonly used by various departments within an organization. Although there are numerous benefits with Copilots, data protection is the primary concern of C-Suite leaders, specifically CIOs and CISOs. Issues related to data protection can hinder an organization's ability to introduce new products and services.

The narrative of data theft and exploitation has risen considerably since on-premises services were moved to the cloud. In those days, bad actors would upload sensitive data to the cloud without any approval or control methods in place. It was referred to as "Shadow IT."

Today, with the advent of Generative AI, ChatGPT, and Copilots, the data theft and exploitation are referred to as "Shadow AI."

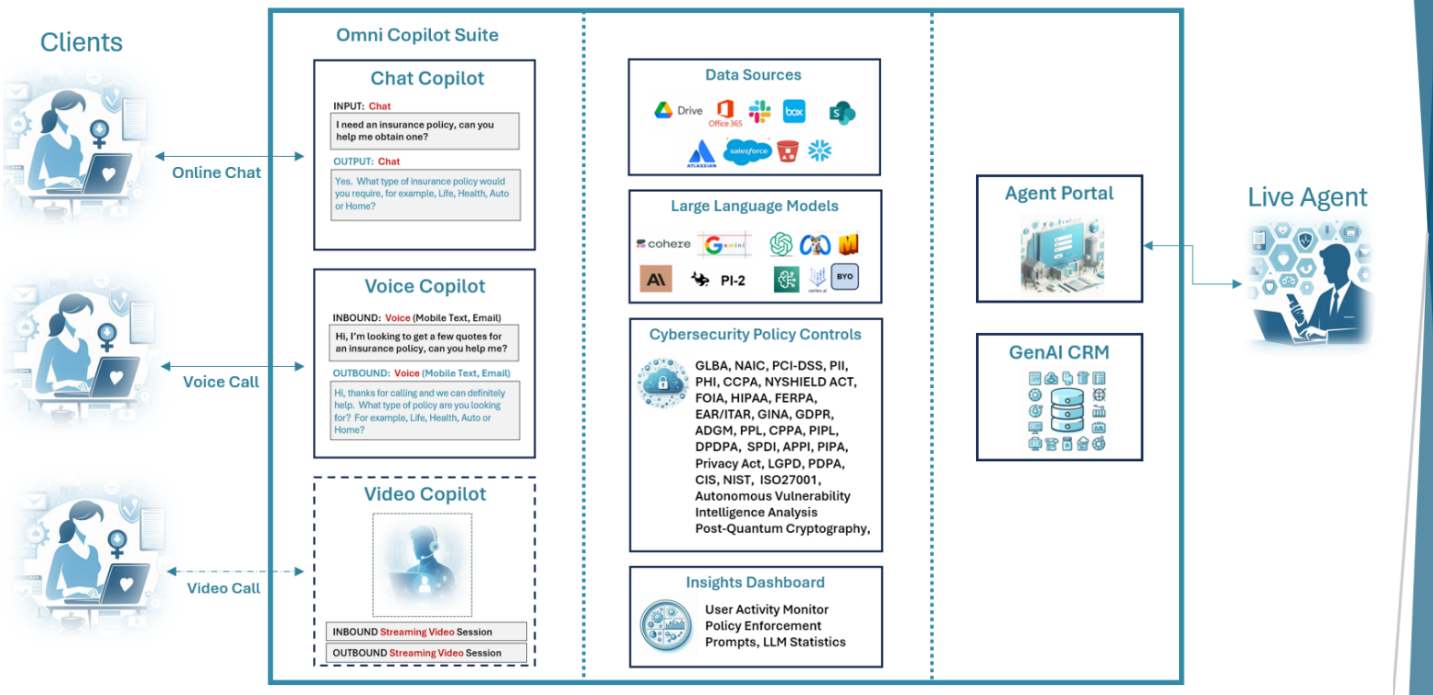
For example, rogue employees, disgruntled partners, or external adversaries can steal data and post it into a public Chatbot or Copilot and expose highly sensitive, classified information. They would have the ability to bypass any IT or InfoSec cybersecurity controls if the required protection measures are not in place. Consequently, the exposure of data may encompass sensitive elements such as intellectual property, confidential product development plans, financial records, or personal details of employees, including medical and compensation data.

To mitigate this risk, organizations should enforce security controls, conduct periodic data assessments, and consider updated solutions. These new solutions should provide a policy-driven cybersecurity approach to data, regardless of which GenAI services are utilized. As a result, information and security leaders are in a position to meet governance, risk, and cybersecurity requirements while realizing the benefits of AI-enabled applications.

As a result, in today's organizational landscape, the implementation of GenAI Copilots is becoming a requirement across multiple departments. This includes customer-centric divisions such as Sales, Marketing, and Support, as well as core internal operations like Finance, Legal, Risk, Compliance, and IT. Each of these departments rigorously applies Information Security (InfoSec) policies that adhere to the principle of least privilege, a cornerstone of the Zero Trust security framework. However, traditional cybersecurity tools fall short in mitigating the risks associated with Shadow AI, necessitating the adoption of new capabilities. Consequently, organizations that lead with a "cybersecure policy-driven" approach are in a unique position to expedite the onboarding process for GenAI Copilots.

As an example, the DUSA platform, as illustrated in Figure 1, has advanced the integration of multiple technologies to enable both Copilots and data protection policies

Figure 1: DUSA GenAI Cybersecure Copilot Platform



Data protection begins with the Omni Copilot Suite at the forefront of the DUSA Platform which provides three modes of operation:

- **Chat** Copilot allows organizations to enable the sessions via a keyboard interface
- **Voice** Copilot answers a phone call with a conversational NLP enabled for 40+ languages
- **Video** Copilot streaming media-based functionality that is under development

The data source integration, Large Language Model (LLM) selection, cybersecurity policy controls, and insights dashboard are part of the core configuration components. Due to this data workflow configuration, additional visibility is required to identify Shadow AI-related sessions that adversely impact data processes. Emerging tools that enable autonomous vulnerability intelligence and post-quantum cryptography are now becoming required to further fortify defenses against data leakage and loss.

As Shadow AI emerges as a data protection threat, cybersecurity regulations and standards are being updated to address new controls. Figure 2 highlights regulations that influence policy decisions, and Appendix A highlights regulations and their industry or country data protection requirements.

Figure 2: Regulations and Standards

In conclusion, the integration of GenAI Copilots into organizational ecosystems presents both transformative opportunities and significant cybersecurity challenges. The evolution from Shadow IT to Shadow AI necessitates a robust, policy-driven cybersecurity framework that can adapt to the dynamic nature of AI-driven technologies. Organizations must prioritize the implementation of advanced security measures, such as autonomous vulnerability intelligence and post-quantum cryptography, to safeguard against the risks of data exposure and theft.

By embracing a cybersecure policy-driven approach and leveraging platforms like the DUSA GenAI Cybersecure Copilot Platform, organizations can harness the full potential of AI while ensuring compliance with evolving regulations and protecting their most valuable assets. The future of corporate data governance hinges on the ability to balance innovation with security, ensuring that GenAI Copilots serve as a force for progress rather than a vector for exploitation.

Contact DUSA to engage in an assessment to understand the data protection requirements for cybersecure GenAI Copilots.

info@dosanjhusa.com **+1.408.430.DUSA (3872)** **www.dosanjhusa.com**

About Dosanjh USA Inc.

Dosanjh USA Inc. (DUSA) headquartered in Silicon Valley, provides information technology services for medium and large enterprises. DUSA enables production ready cybersecure AI Copilots with a data protection policy-driven approach. Additional services include assessments for AI, data, cybersecurity, post-quantum cryptography, multi-cloud and workflow automation. DUSA also offers virtual CxO services to empower enterprises with leadership and direction. Learn more at www.dosanjhusa.com

APPENDIX A: REGULATIONS AND STANDARDS

- **GLBA** Gramm-Leach-Bliley Act is a U.S. federal law that requires financial institutions to protect consumers' personal financial information through stringent privacy and data security measures.
- **NAIC** National Association of Insurance Commissioners is a U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from all 50 states aimed at harmonizing and enhancing the effectiveness of state insurance regulations.
- **PCI-DSS** Payment Card Industry Data Security Standard is a set of security standards designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.
- **PII** Personally Identifiable Information refers to any data that can be used to identify a specific individual, such as names, addresses, social security numbers, and biometric records.
- **PHI** Protected Health Information refers to any information in a medical record that can be used to identify an individual and that was created, used, or disclosed in the course of providing health care services, such as diagnoses, treatment information, and medical histories.
- **CCPA** California Consumer Privacy Act is a state law that grants California residents new rights regarding their personal data, including the right to know, delete, and opt-out of the sale of their information, and imposes data protection responsibilities on businesses.
- **NY Shield Act,** officially known as the Stop Hacks and Improve Electronic Data Security Act, is a New York state law aimed at strengthening data security and breach notification requirements for businesses handling private information of New York residents.
- **FOIA** The Freedom of Information Act is a United States federal law that grants public access to government agency records, allowing individuals to request information from federal agencies unless it falls under one of the nine exemptions outlined in the Act.
- **HIPAA** Health Insurance Portability and Accountability Act is a United States law that protects the privacy and security of individuals' medical information.
- **FERPA** Family Educational Rights and Privacy Act is a federal law in the United States that protects the privacy of student education records.
- **EAR/ITAR** January 2022, the EAR (Export Administration Regulations) and ITAR (International Traffic in Arms Regulations) are regularly updated by the U.S. Department of Commerce and the U.S. Department of State, respectively, to adapt to changing international security concerns.
- **GINA** Genetic Information Nondiscrimination Act is a United States federal law that prohibits discrimination in employment and health insurance based on genetic information.
- **GDPR** General Data Protection Regulation is a European Union regulation that governs the processing and protection of personal data within the EU and the European Economic Area.
- **ADGM** Abu Dhabi Global Market data protection framework; regulations and guidelines designed to safeguard personal data processed within the Abu Dhabi Global Market, ensuring compliance with international data protection standards and enhancing trust in the handling of personal information.

- **CPPA** Consumer Privacy Protection Act in Canada aims to enhance privacy protection by introducing stricter consent rules, data mobility, and stronger rights for minors and their guardians.
- **PPL** Israel's top data protection act is the Protection of Privacy Law, enacted in 1981. It's the main legislation governing data privacy and grants individuals' rights over their personal information.
- **PIPL** Personal Information Protection Law in China is a comprehensive legislation designed to regulate the processing of personal information and ensure data privacy and security within the country.
- **DPDPA** Digital Personal Data Protection Act, India 2023 (DPDPA). It's the first comprehensive data privacy law in the country, establishing rules on how personal information is handled.
- **SPDI** Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, Enacted in India, these rules require insurance companies to have a comprehensive framework for data, cloud, mobile, and cybersecurity.
- **APPI** Act on the Protection of Personal Information is Japan's federal data protection law, overseen by the Personal Information Protection Commission (PPC). It regulates the handling of PI by individuals and organizations, emphasizing consent for sensitive data and security measures.
- **PIPA** Personal Information Protection Act in South Korea, which regulates the processing of personal information and ensures individuals' privacy rights are protected through various provisions and obligations placed on data controllers and processors.
- **Privacy Act of Australia** The primary data protection law in Australia is the Privacy Act 1988, which regulates the handling of personal information by Australian government agencies and businesses.
- **LGPD** Lei Geral de Proteção de Dados is Brazil's comprehensive data protection law that regulates the processing of personal data and establishes rules for its collection, use, storage, and sharing, ensuring individuals' privacy rights are protected.
- **PDPA** Personal Data Protection Act in Argentina is a law that governs the processing of personal data, ensuring individuals' privacy rights are respected and providing guidelines for data handling by organizations.
- **CIS** Center for Internet Security is a non-profit organization providing cybersecurity solutions and best practices to organizations worldwide.
- **NIST** (National Institute of Standards and Technology) is a U.S. federal agency that develops and promotes standards, guidelines, and technology to enhance cybersecurity and innovation across various industries.
- **ISO 27001** is an international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within the context of the organization's overall business risks.
- **PQC** Post-quantum cryptography designs new encryption methods to stay secure even against the potential threat of powerful quantum computers.