DOSANJH USA

AI and Cybersecurity

CIOs & CISOs Win Big!

AI: HOW TO WIN

Policy-Driven Security for GenAI CoPilots

Table of Contents

Strategy 2
Execution 3
Audience 4
OMNI CoPilot Suite 5
    CHAT CoPilot 5
    VOICE CoPilot 5
    VIDEO CoPilot 5
GenAI Platform 6
  Models 6
  Policies 7
    Global Inference: Policy Module 7
    Large Language Model: Policy Module 7
    Cybersecurity & GRC: Policy Module 7
    Observability: Metrics 7
Success Plan 8

AI: How To Win

Safeguard Data with Policy-Driven Security Controls for GenAI CoPilots

In today's competitive landscape, success hinges on a winning strategy and flawless execution. This principle holds true for AI-powered solutions, products, and services. Organizations that effectively implement AI will witness record growth, while those who lag behind risk falling out of the market entirely. At Dosanjh USA (DUSA), we understand the challenges CIOs and CISOs face when integrating GenAI CoPilots with cybersecurity along with governance, risk, and compliance (GRC) policies. The following guidance will help them navigate this critical process.

The question to the CIOs and CISOs is …"*Are You Ready to Win*?"

Strategy

To achieve success, organizations must move beyond a one-size-fits-all approach. Instead, they need to tailor their strategies to each departments specific business goals and desired outcomes. This demands a shift in focus for IT leadership. CIOs and CISOs must broaden their focus beyond current data workflows and extend to new eco-systems. These extend from front-office initiatives and back-office operations to third- and fourth-party data. This extended perspective ensures the selection of an optimal AI strategy that integrates into existing systems. Failure to do so will lead to hastily cobbled-together tools which can negatively impact functionality, performance and security. To address this, following strategic guidance is provided as illustrated in Figure 1:

Figure 1: Winning Strategy

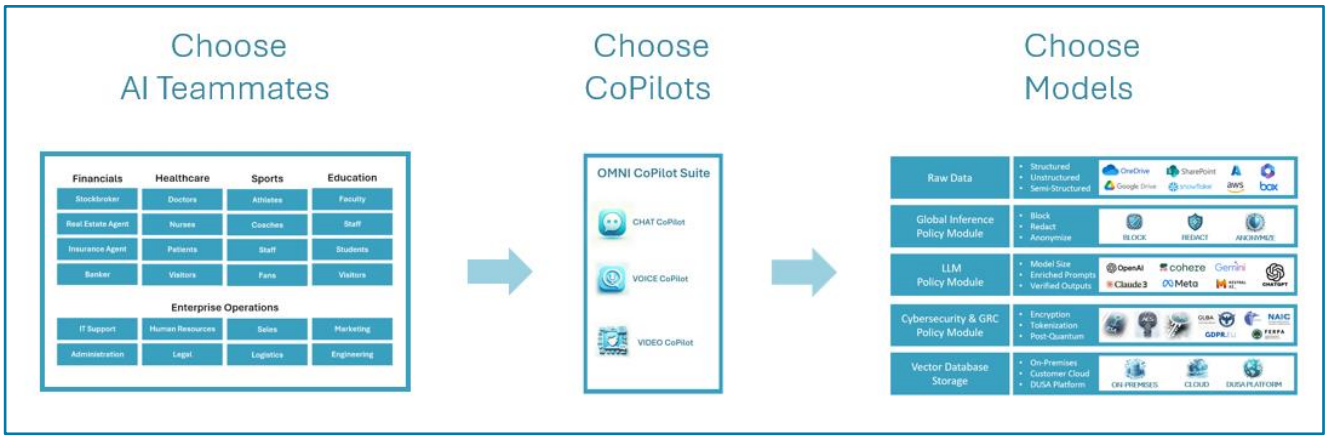
Execution

A successful AI implementation hinges on a coordinated strategy across business, technology, and operations. The Business Brief, guided by the CEO's priorities, defines the organization's goals for AI. The Technology Brief then assesses current capabilities and identifies the gap to achieve the future state. Finally, the Operations Brief ensures the organization can scale and adapt to meet market demands as AI is integrated.

As an example, communication between customers, partners, and employees can leverage AI-derived conversational chat interfaces as illustrated in Figure 2. Here, GenAI CoPilots can streamline interactions through an autonomous AI workflow. This translates to a more efficient system that handles orchestrated and automated processes.

The opportunity for the CIOs and CISOs … "*Choose How To Win*?"

Figure 2: Execution: Choose How To Win



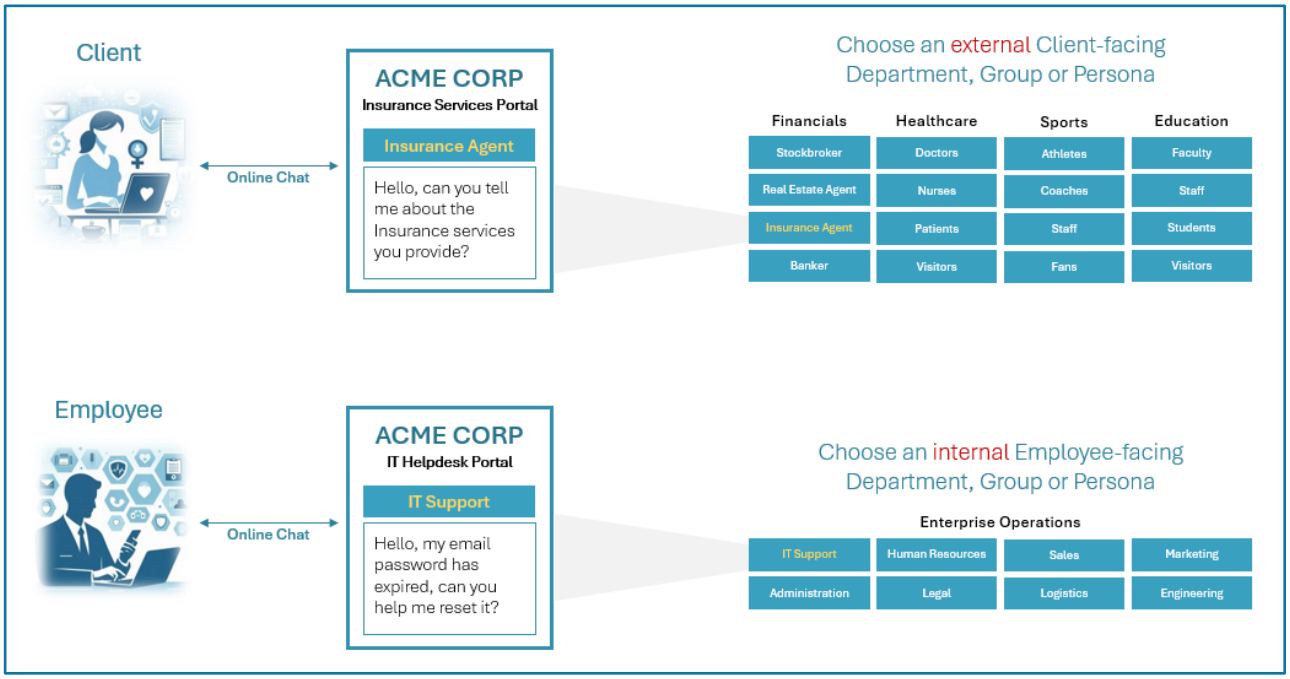
The three-step process illustrated in Figure 2 lists the important questions that need to be addressed.

1. Choose AI Teammates: (similar to a Virtual Assistant function)
    a. External: Select a function that interacts with customers and partners
    b. Internal: Select a department, group or persona that supports the External function
2. Choose CoPilots:
    a. Chat: Text based, conversational interaction from an endpoint device
    b. Voice: Dial-in via any cell/mobile enabled device for a conversational query
    c. Video: Collaborative experience with personalized communication
3. Choose Models:
    a. Large Language Models: Specialized for the AI Teammate and selected CoPilot
    b. Data Protection: Selection of both Inference and Cybersecurity GRC models

Audience

The selection for an AI Teammate is determined from the initial Readiness Assessment that defines the business drivers. These drivers will indicate the priority of communication for both internal and external audiences. For example, an Insurance industry use case for Underwriters may require multiple AI Teammates. In addition, the very same organization may require several AI Teammates for internal communication. Figure 3 depicts an example for ACME CORP with both external client and internal employee AI Teammates.

Figure 3: Audience: Choose Your AI Teammates



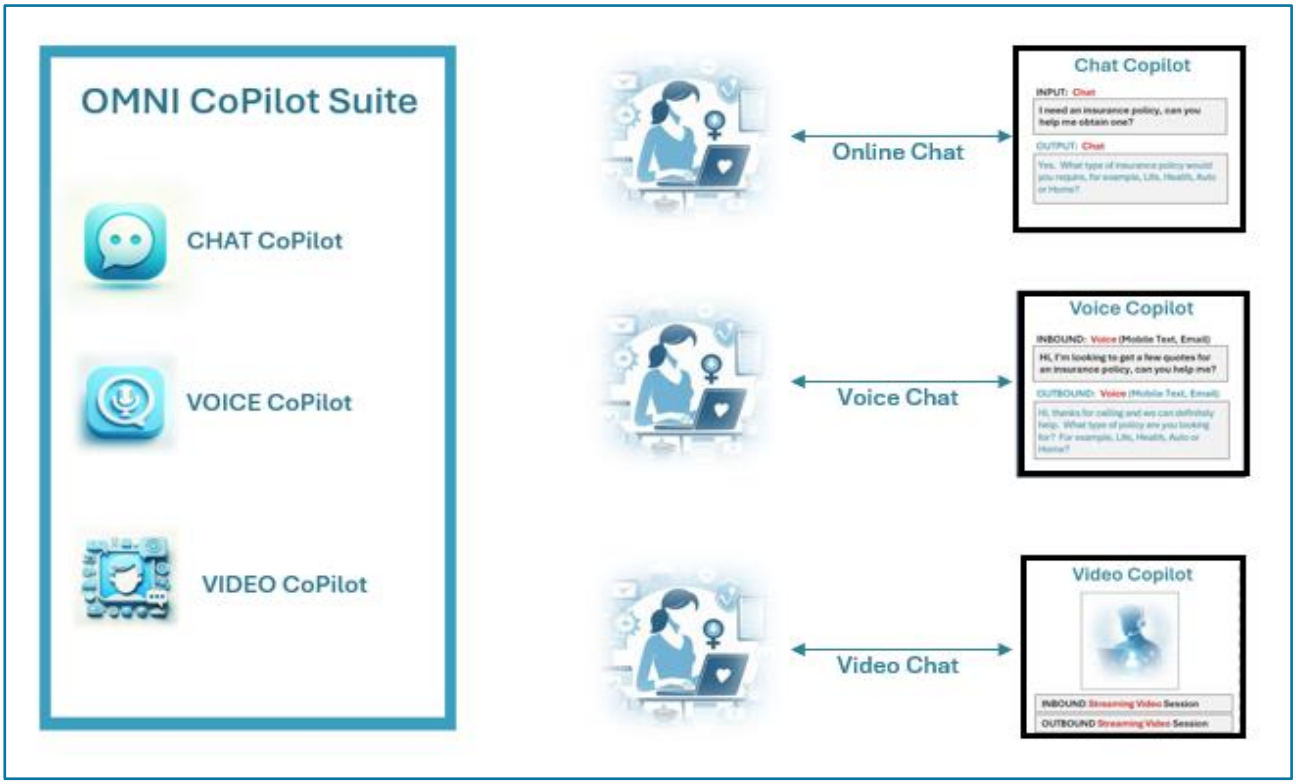
The objective for each AI Teammate is to determine the level of automated communication augmentation required for the identified use case. Figure 3 lists multiple vertical markets as an example with the Insurance Industry selected for an Insurance Agent. In addition, a large enterprise organization may have multiple lines of business under a parent organization and may require a mergers and acquisition AI Teammate.

Geography is also an important factor when addressing the internal communication requirements for multi-national organizations, specifically language translation. Colleagues are typically dispersed in different time-zones and an AI Teammate will facilitate queries when a human counterpart is not available.

OMNI CoPilot Suite

The second step in the three-step process is to select the type of functionality required for the CoPilot. The initial input from the Business Brief will dictate the type, style, tone, format, context and additional requirements for the CoPilot. Figure 4 illustrates the DUSA OMNI CoPilot Suite for Chat, Voice and Video.

Figure 4: OMNI CoPilot Suite: Choose Your CoPilot



CHAT CoPilot

- Text based interaction initiated from a kiosk, desktop, laptop, tablet or mobile device
- Ability to support hybrid interaction models based on menu/button, keyword recognition, rules or learned interactions

VOICE CoPilot

- Dial-in via any cell/mobile enabled device for a voice interaction with 24 / 7 availability
- Supports 40+ languages for a conversational interaction and switch between languages for those who are multi-lingual
- Ideal for individuals who do not have access to a keyboard device or are not physically able to navigate text based interactive devices

VIDEO CoPilot

- Personalized communication for product demonstrations, virtual tours or sharing a collaborative experience
- Enhanced customer engagement by maintaining user's attention and interest
- Training and educational purposes with interactive lessons & teaching assistants

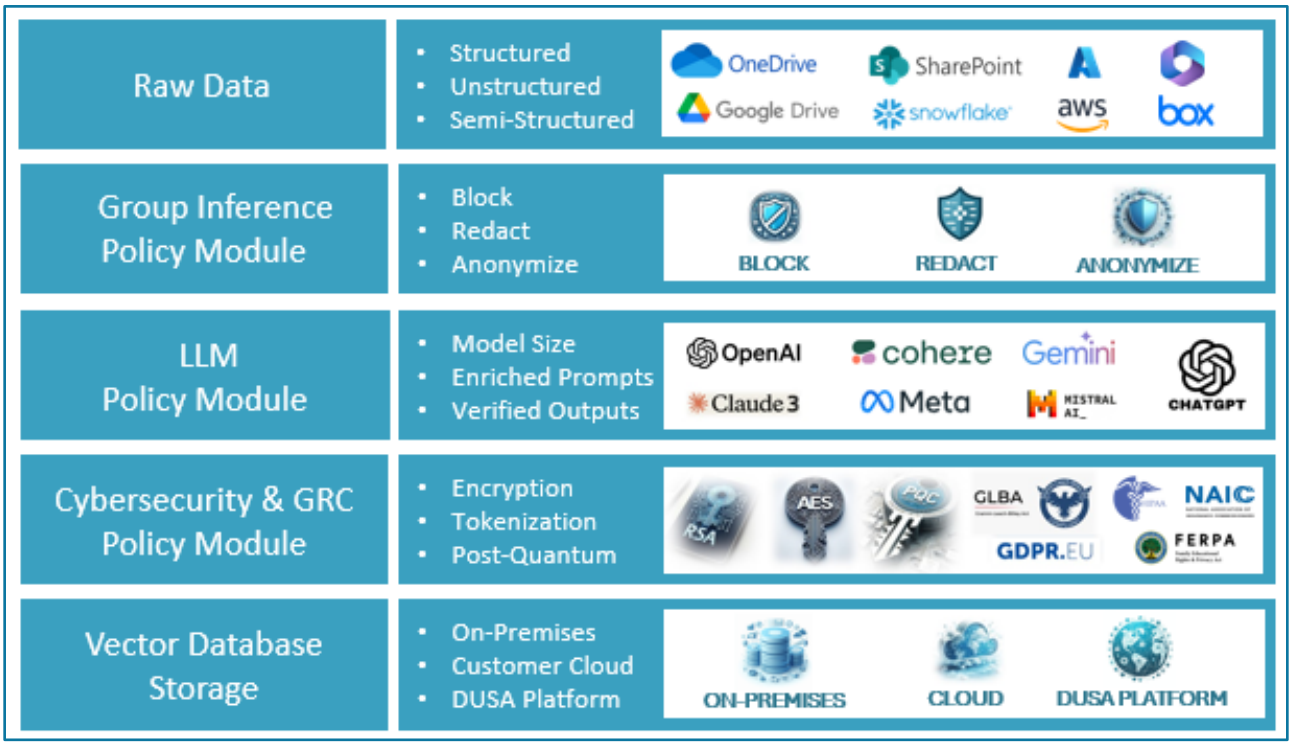
GenAI Platform

The Technology Brief plays a crucial role by guiding model and policy selection within the "no-code" DUSA GenAI Platform. These choices directly impact the processing power needed to handle high-volume prompt requests from AI Teammate Copilots.

Models

The following guidance in Figure 5 illustrates the sequence that the GenAI Platform processes the AI-driven workflow:

Figure 5: GenAI Platform: Choose Your Models

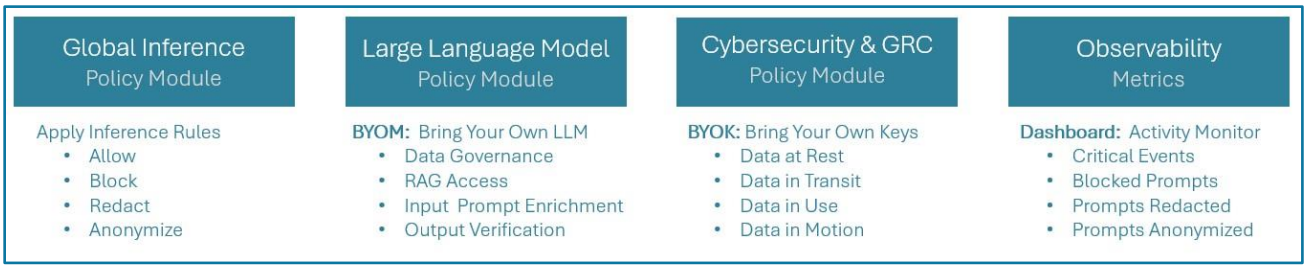


1. Connect to internal or external data sources and integrate semantic search for Retrieval Augmented Generation (RAG)
2. Align with the InfoSec Policy guidelines to configure the Group Inference controls for sensitive data, PII, PHI, Intellectual Property, Source Code etc.
3. Enable the communication requirements utilizing a single LLM or chaining LLMs together with policy-driven access to the dataset
4. Import data protection keys (AES/RSA Encryption, Tokenization or Post-Quantum Cryptography) to protect data in use, at rest, in transit and in motion
5. Select your existing data storage environment, Public/Private/Hybrid Cloud/Datacenter on-premises or DUSA GenAI Platform

Policies

An organizations Information Security Policy provides the standards required to securely introduce GenAI Copilots. Policy-Driven in this example defines the required controls within each Policy Module as identified in Figure 6:

Figure 6: GenAI Platform: Choose Your Policies



Global Inference: Policy Module

Data classification rules dictate the levels of control for sensitive or non-sensitive data before forwarding it to the LLM (Large Language Model) Policy Module.

Large Language Model: Policy Module

The option of BYOM (Bring Your Own Model) or utilizing an organizations pre-selected LLMs provides the method of how input prompts and output verification i.e., factualization, hallucinations are determined.

Cybersecurity & GRC: Policy Module

Identity and data controls are at the forefront of this policy module. An organization can leverage their existing investment in Key Management Systems, Hardware Security Modules and Identity Providers to ensure data is managed according to InfoSec policies.

Observability: Metrics

The Operations Brief plays a key role in setting alert and notification thresholds. A dedicated GenAI Copilot dashboard provides real-time insights, highlighting blocked, redacted, and anonymized prompts. Additionally, it tracks user behavior, identifying top users, prompt volume, and average prompt size. This data empowers organizations to optimize token allocation and manage processing costs effectively.

Success Plan

This paper tackles the critical question of how to achieve success with GenAI Copilots. It outlines a winning strategy with actionable steps and example metrics to securely scale an enterprise, business or organization. The secret for success for CIOs and CISOs? Deploying AI tools with robust cybersecurity policies (Figure 7). This ensures a smooth implementation and unlocks the full potential of GenAI Copilots for CEOs, CIOs and CISOs.

Figure 7: GenAI Platform Success Plan Checklist

CEO Business Value Checklist	Status
Enhanced Customer Experience	✓
Cost Efficiency	✓
Innovation	✓
Market Differentiation	✓
Competitive Advantage	✓
Strengthened Brand Identity	✓
Real-Time Collaboration	✓
Better Decision-Making	✓
Improved Productivity	✓
Scalability	✓
24 / 7 Availability	✓
Enhanced Security	✓
Employee Development	✓
Business Budget Allocation	✓

CIO & CISO Checklist	Status
Business Readiness Assessment	✓
Infrastructure Readiness	✓
AI Strategy	✓
AI Teammates Internal & External	✓
Copilots Chat, Voice, Video	✓
User Access	✓
Permissions & Authorizations	✓
Secure Data Access	✓
Inference Policy Methods	✓
Large Language Model Identification	✓
Cybersecurity & Governance, Risk, Compliance	✓
Vector Database, Hosted on Public/Private/Hybrid Cloud	✓
Observability and Reporting	✓
Technology Budget Allocation	✓

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