JPEK TECH: Enterprise AI Security & Infrastructure Datasheet

Revision: 2026.1 | **Classification:** Public / Prospect Information

Executive Overview

JPEK Tech provides a dual-layer security architecture designed to enable the safe adoption of Generative AI within high-compliance enterprise environments (Logistics, Finance, Healthcare). Our platform, comprising **Insight-6** and **Guardian-1**, addresses the "Shadow AI" crisis by providing total visibility and real-time data redaction.

Product 1: Insight-6 (The Discovery Engine)

The Detective: Continuous monitoring of organizational AI usage.

Technical Specifications

- **Engine:** Python-based analysis agent optimized for **AWS Graviton4 (ARM64)**.
- **Data Source:** Integration with **AWS VPC Flow Logs** and **Azure Network Watcher**.
- **Analysis Core:** Large Language Model (LLM) reasoning via **Amazon Bedrock**.
- **Reporting:** Automated SOC2-compliant risk scoring.

Key Capabilities

- **Shadow AI Detection:** Identifies unauthorized traffic to over 500+ global AI providers.
- **Departmental Attribution:** Maps AI usage to specific subnets (e.g., Finance vs. Operations).
- **Risk Categorization:** Evaluates data egress for PII, PHI, and Intellectual Property risks.

Product 2: Guardian-1 (The Active Shield)

The Enforcer: Millisecond-latency data redaction and policy enforcement.

Technical Specifications

- **Hardware Acceleration:** Powered by **NVIDIA Blackwell B200 / H100 GPU** clusters.

- **Connectivity:** Private, agentless deployment via **AWS PrivateLink** or **Azure Private Link**.
- **Throughput:** Capable of processing 1M+ tokens per second with <20ms latency.
- **Deployment:** Containerized via **Amazon ECS/EKS**.

Key Capabilities

- **Real-time Redaction:** Automatically scrubs SSNs, Credit Card numbers, and API keys before they reach the LLM.
- **Contextual Guardrails:** Prevents "Prompt Injection" and malicious system-instruction overrides.
- **Multi-Cloud Support:** Seamlessly protects Azure-based workforces using AWS-backed security logic.

Architecture & Compliance

Security Standards

- **Zero-Trust:** No data is stored or used for model training.
- **Encryption:** AES-256 at rest; TLS 1.3 in transit.
- **Governance:** Fully compatible with ISO/IEC 42001 (AI Management System).

Infrastructure Requirements

- **Deployment Model:** SaaS (Managed by JPEK) or Private Cloud (Customer VPC).
- **Network:** Requires DNS Forwarding or PAC file configuration for agentless interception.

Why JPEK Tech?

Unlike standard firewalls, JPEK understands the *semantic* content of AI prompts. We don't just block websites; we allow your employees to be productive while ensuring your "Secret Formula" stays secret.