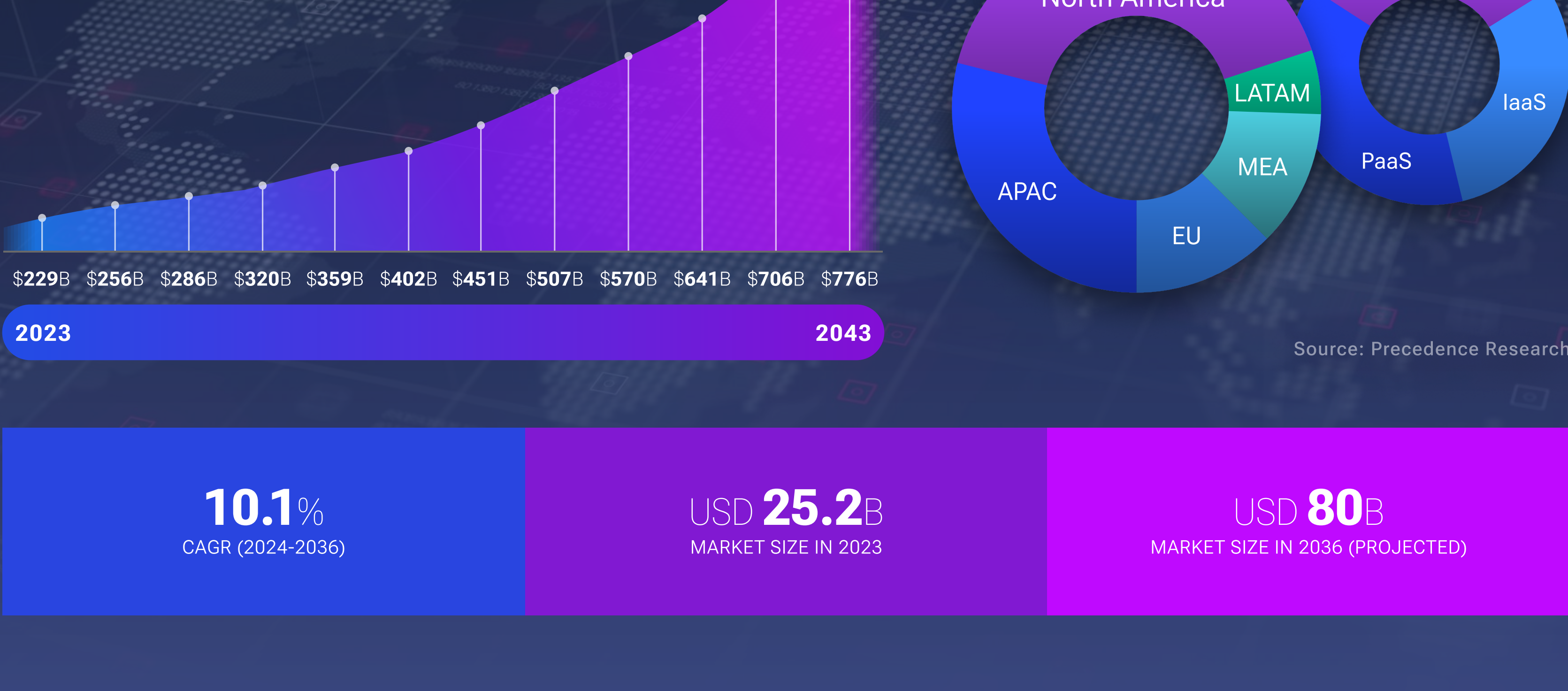
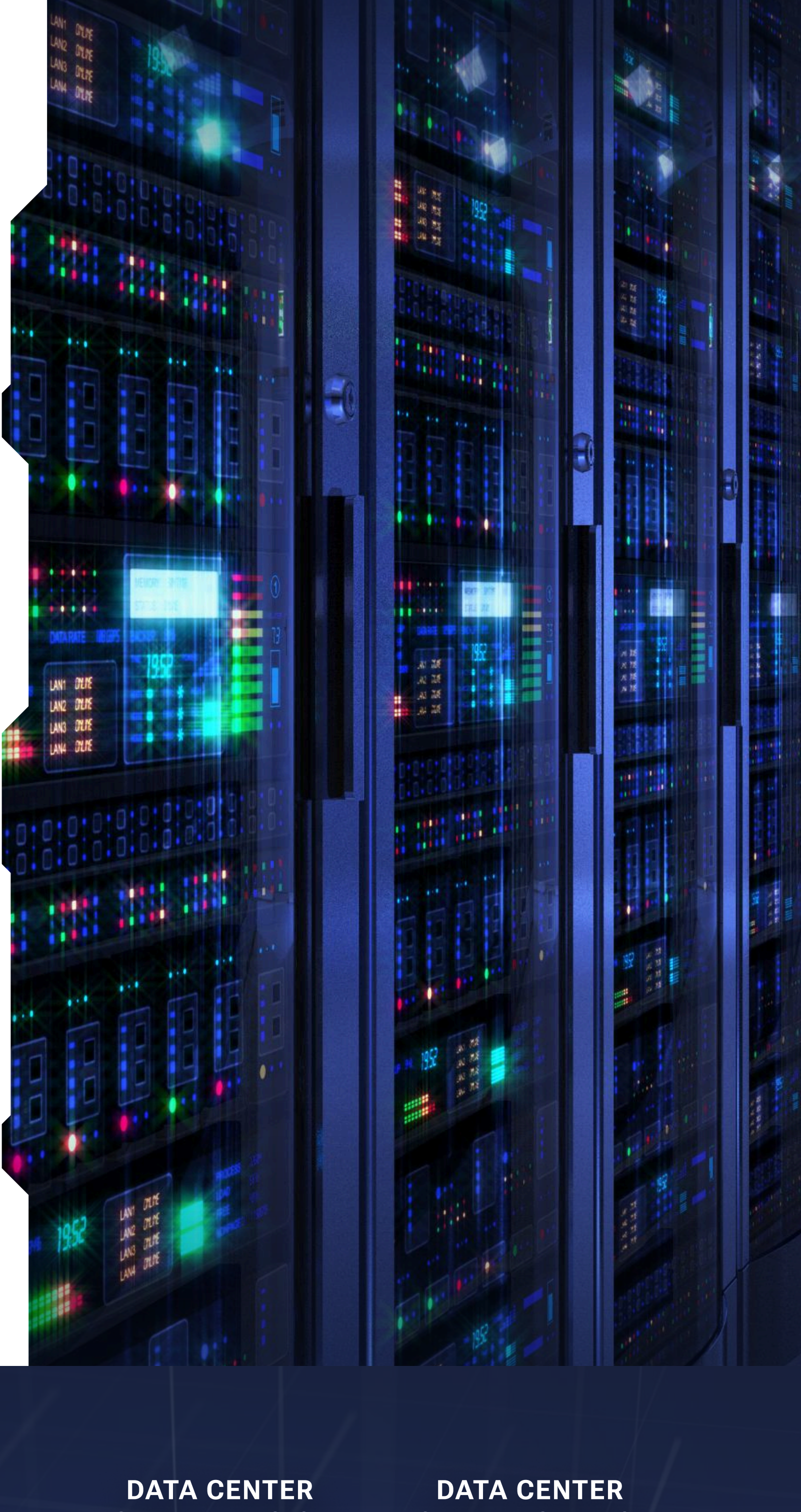


Quantum-Resilient Software Solutions Offer Data Centers Strategic Advantage

Data Centers are no longer just the backbone of the internet—they are the foundation of our digital world. Entrokey Labs is securing that foundation.

The 2020s have seen a roar of data centers being constructed around the world. This stems from the AI revolution and the digital-first economy. Since 2020 the data center industry has doubled in size. Now, with the rapidly expanding digital economy and AI revolution, we are braced for the next data center boom. We can expect another doubling in seven years.



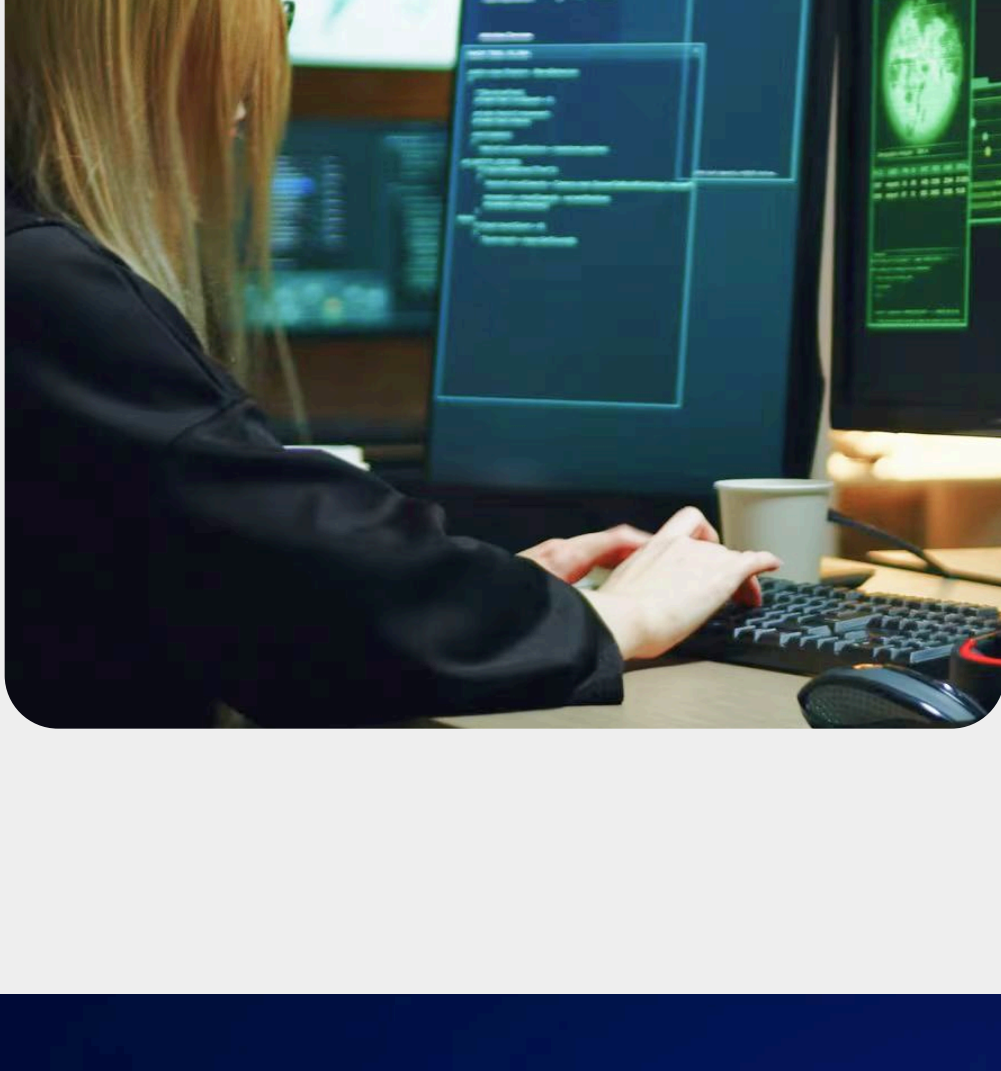
Strategic Data Centers: The Key to Competitive Edge

With a huge amount of supply coming online over the next few years, data center builders and operators will build and enhance facilities that give competitive advantages to existing and prospective customers in attracting tier-1 customers to their sites.

Cybersecurity, energy capacity, and location are the foundations of strategic advantage. For cybersecurity, data centers that lead the post-quantum readiness charge will uniquely attract a plethora of large enterprises and government clients.

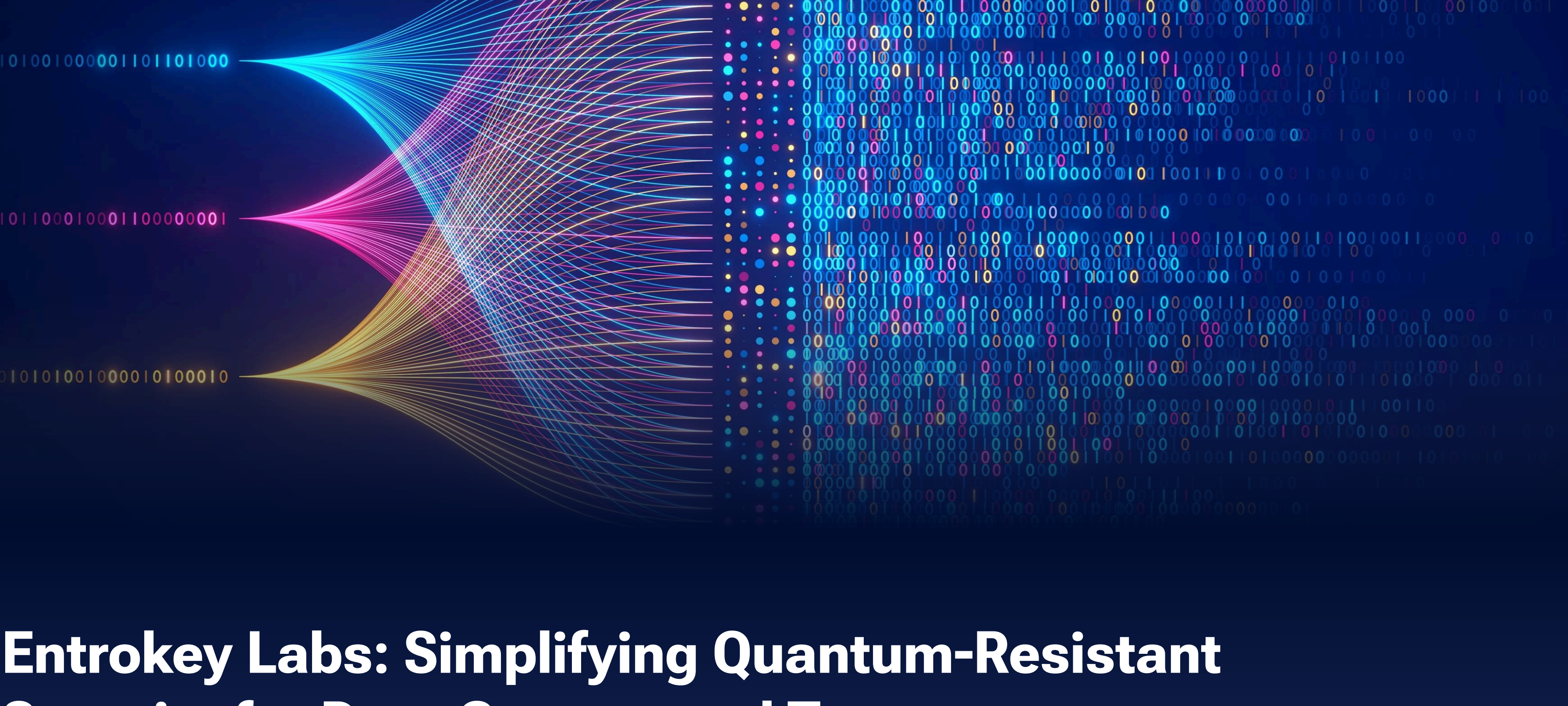


Preparing for Post-Quantum Threats: Securing Data Today Against Tomorrow's Attacks



Today, bad actors regularly engage in Hack Now, Decrypt Later (HNDL) attacks often focused on our large (regulated) enterprises, infrastructure, and government. The goal is to steal encrypted valuable data today, to decrypt it when they have enough computing power from accessible scalable quantum computers, all within 5-6 years.

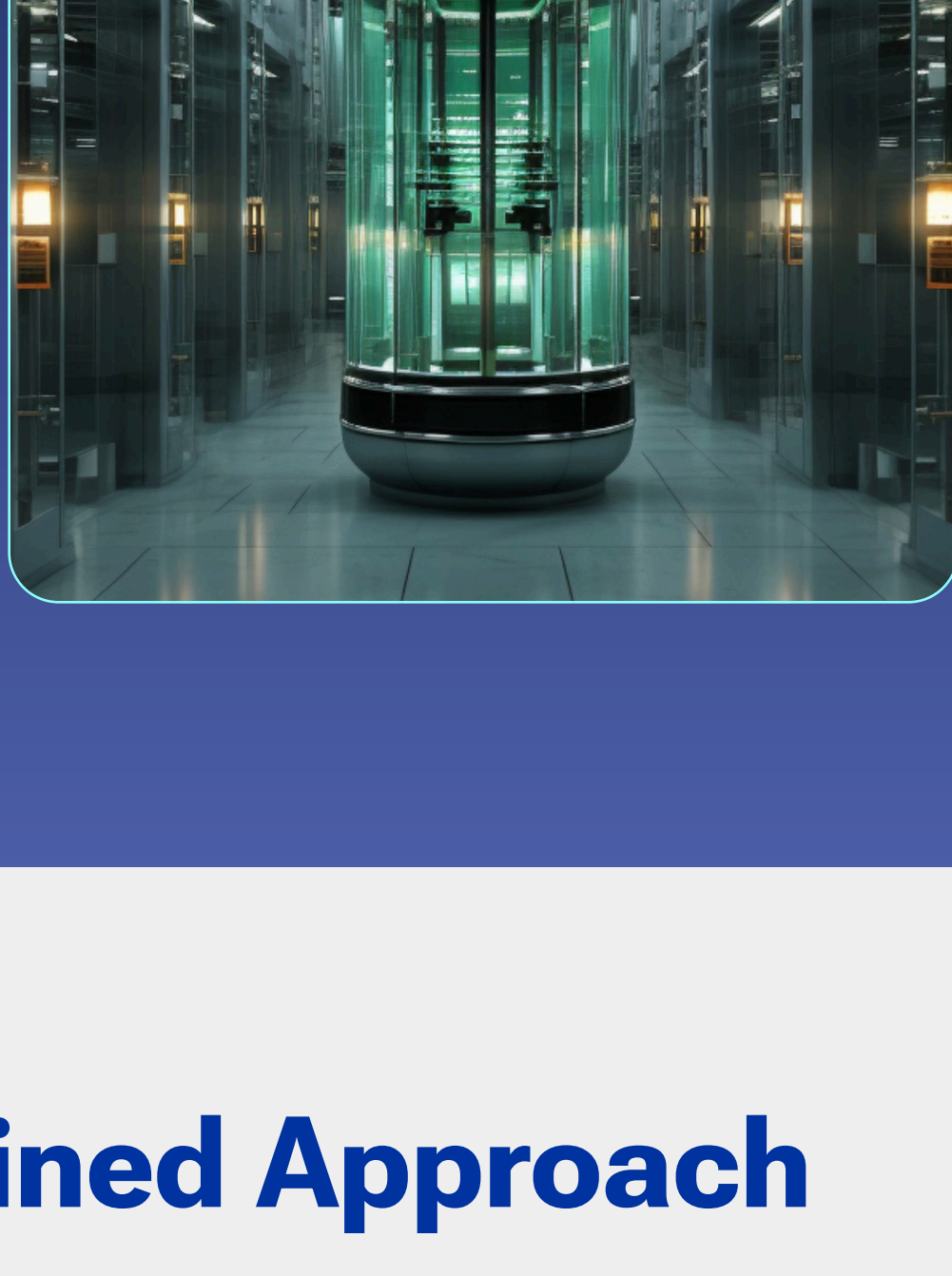
The biggest challenge is the time needed to migrate to a post-quantum cybersecurity infrastructure while ensuring whatever is in place can scale into quantum computing without impacting uptime, security certifications, and business operations. To date, the choices have been uptime impacts, new certifications, and increased latency.



Entrokey Labs: Simplifying Quantum-Resistant Security for Data Centers and Tenants

Entrokey Labs has developed the first software-only True Autonomous Random Number Generator and Quantum Key Distribution solution. It integrates with existing Hardware Security Modules (HSMs), Key Management Services (KMSs), and software infrastructure, providing quantum resistance to current "Quantum-Resistant Capable" encryption and supporting next-gen post-quantum algorithms for robust security against emerging threats.

This approach simplifies the transition to quantum-resistant security by offering a cost-effective and practical solution for data center companies. It also benefits tenants by enabling immediate resistance to Hack Now, Decrypt Later (HNDL) attacks, while strengthening long-term tenancy and business resilience.



Benefits of Entrokey's Software-Defined Approach

Pushes back the threat of quantum by 10+ years

Evolves with hardware and software infrastructure

Eliminates threat vectors of hardware-dependent quantum RNGs

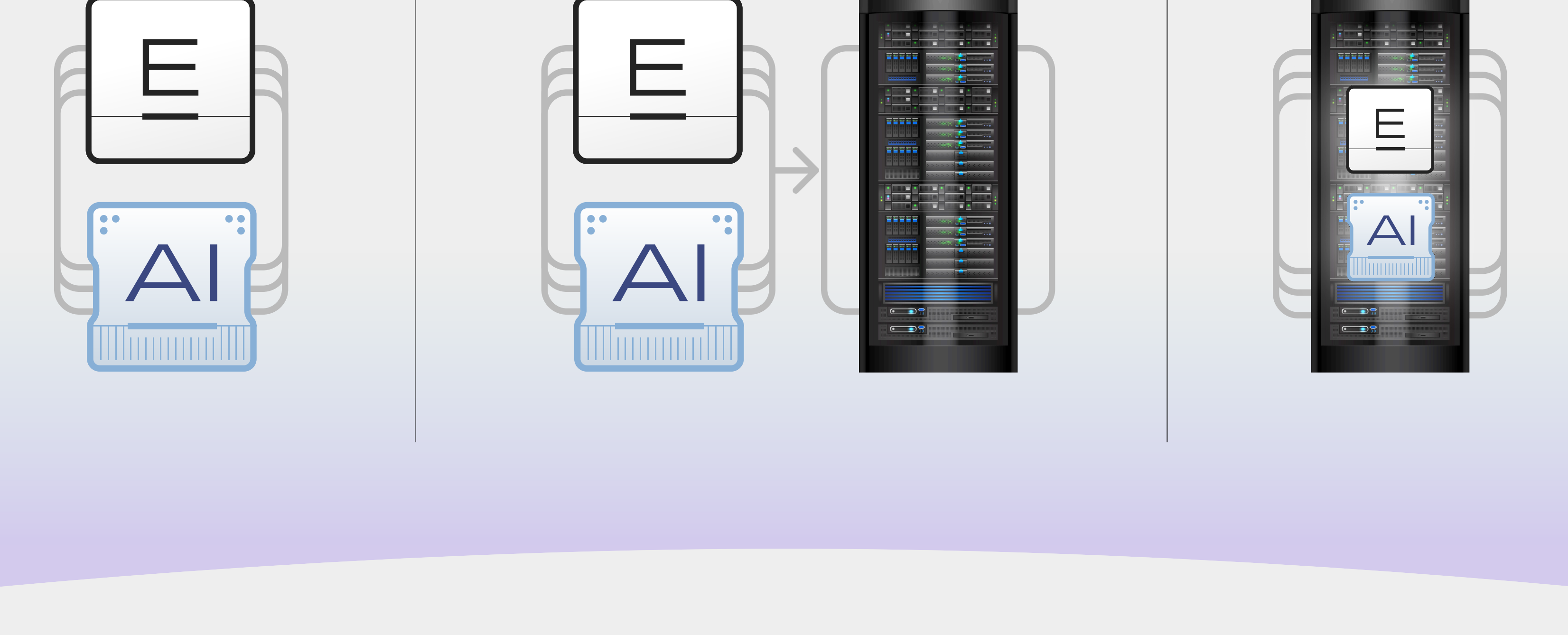
Plug-and-play, cost-effective, time-efficient to implement

Infinitely scalable, zero-latency key generation and distribution

Avoids fragility and interference in hardware deployments

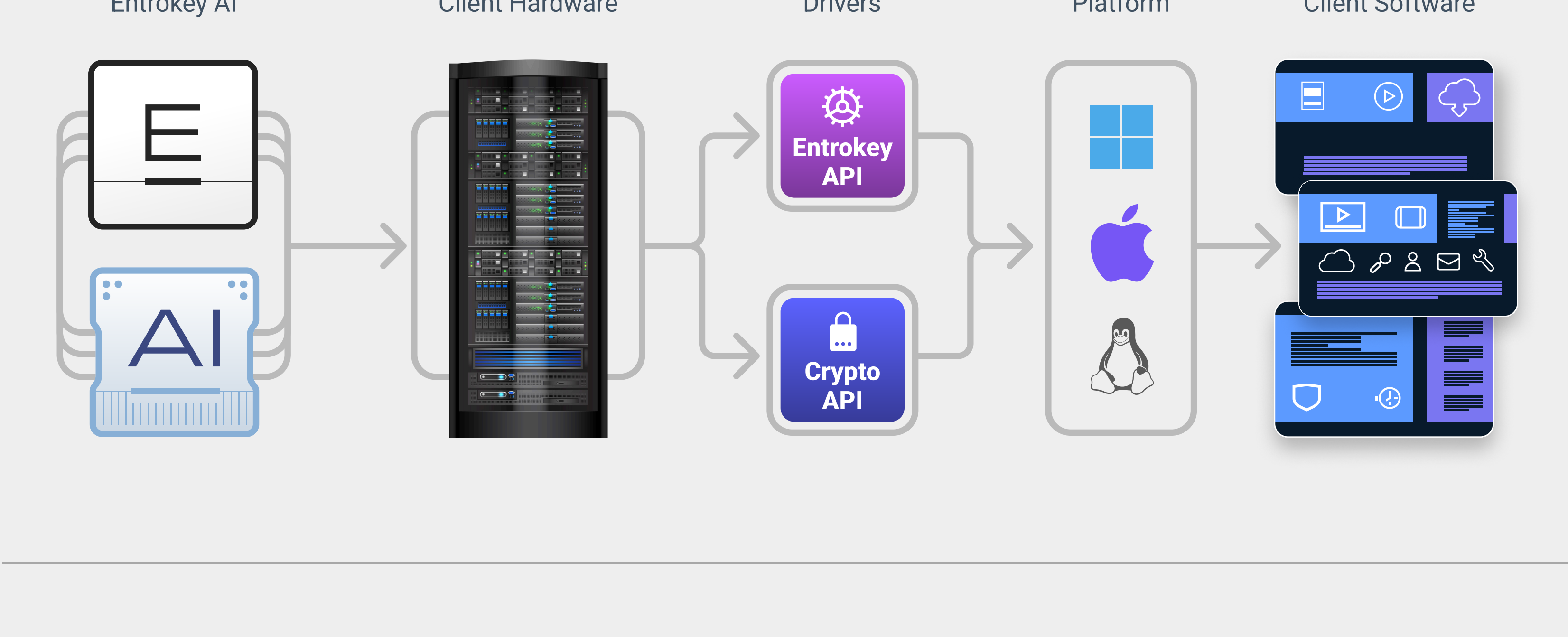
Architecture

Entrokey's AI-powered solution offers multiple deployment options to cater to various operational needs. It can be implemented in a sandbox environment for rigorous testing and validation, integrated into existing Hardware Security Module (HSM) capabilities to enhance their performance, or embedded into next-generation AI-enabled HSMs to deliver an advanced layer of protection. These flexible deployment models ensure that Entrokey can be seamlessly incorporated into existing infrastructure or serve as a cornerstone of forward-looking cybersecurity strategies.



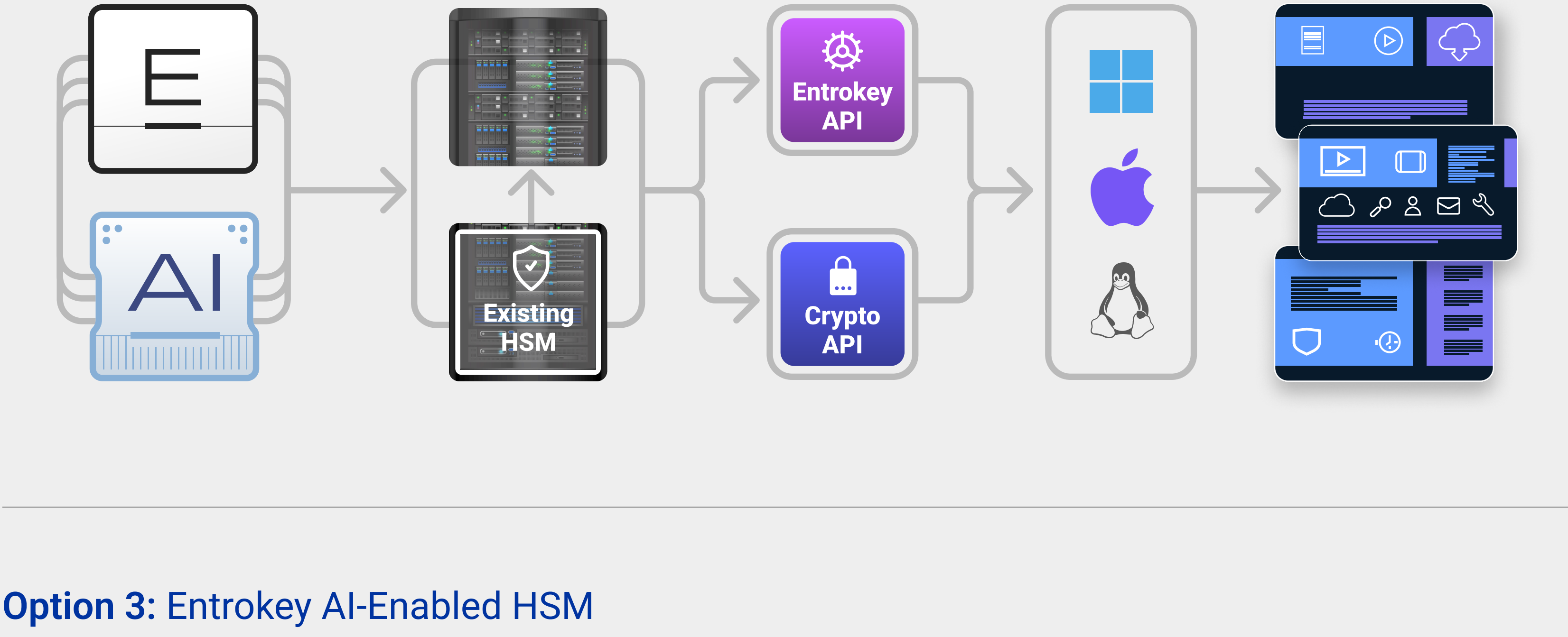
Option 1: Entrokey AI Sandbox (Testing)

EntroKey's AI software can be deployed in a standalone fashion into a customer sandbox for testing and proof of concept, where it is accessible to customer software either through Entrokey's dedicated software drivers or via major platform Crypto Application Programming Interface (API) Cryptographic Service Providers.



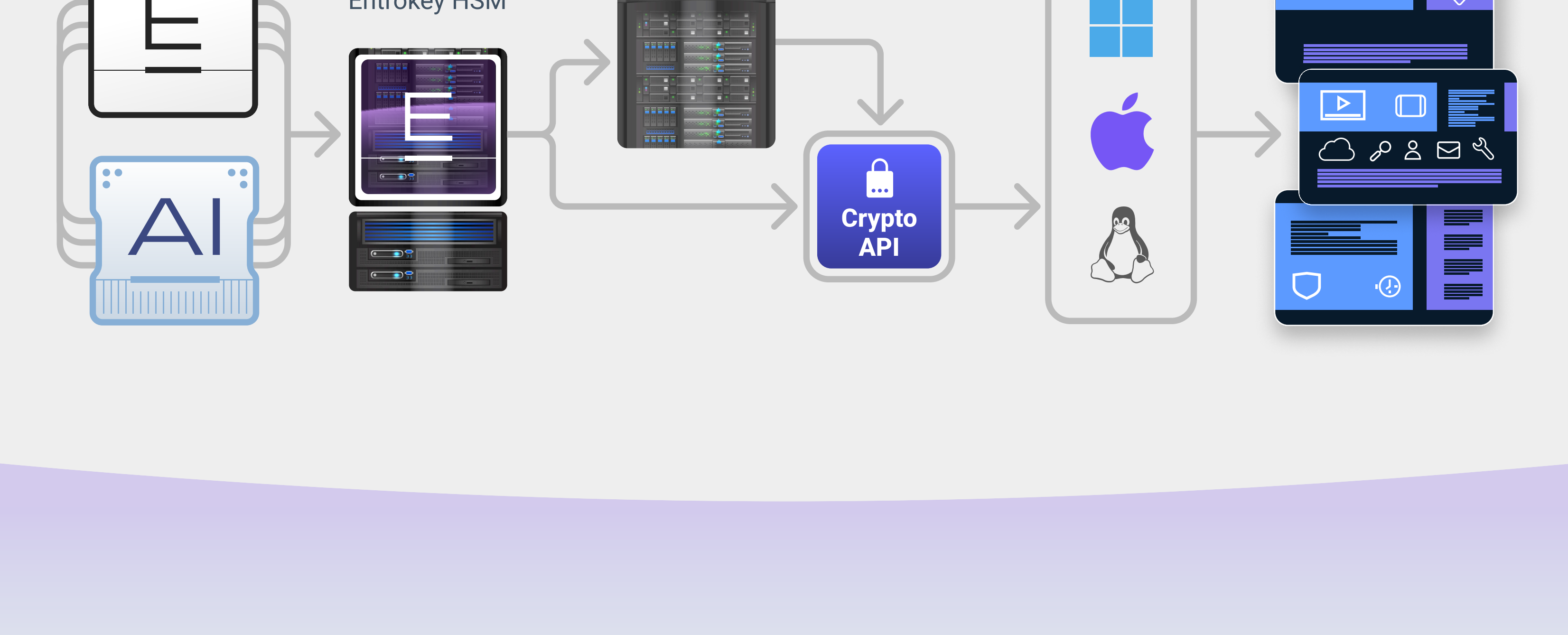
Option 2: Entrokey AI Integrated with Existing HSM

Entrokey's AI software can be deployed with existing Hardware Security Modules (HSMs) for a combined solution that leverages the strengths and performance of each. In this approach, Entrokey services can be obtained either through Entrokey's dedicated software drivers or via major platform Crypto Application Programming Interface (API) Cryptographic Service Providers.



Option 3: Entrokey AI-Enabled HSM

Entrokey's AI software can be deployed inside next-generation Hardware Security Modules (HSMs) for a fully integrated HSM using state-of-the-art technology. In this approach, Entrokey services can be obtained alongside HSM services via major platform Crypto Application Programming Interface (API) Cryptographic Service Providers, either via directly connected computers or over the customer network.



Discover more at entrokeylabs.com

Get a demo

Contact us