



SECURITY OVERVIEW

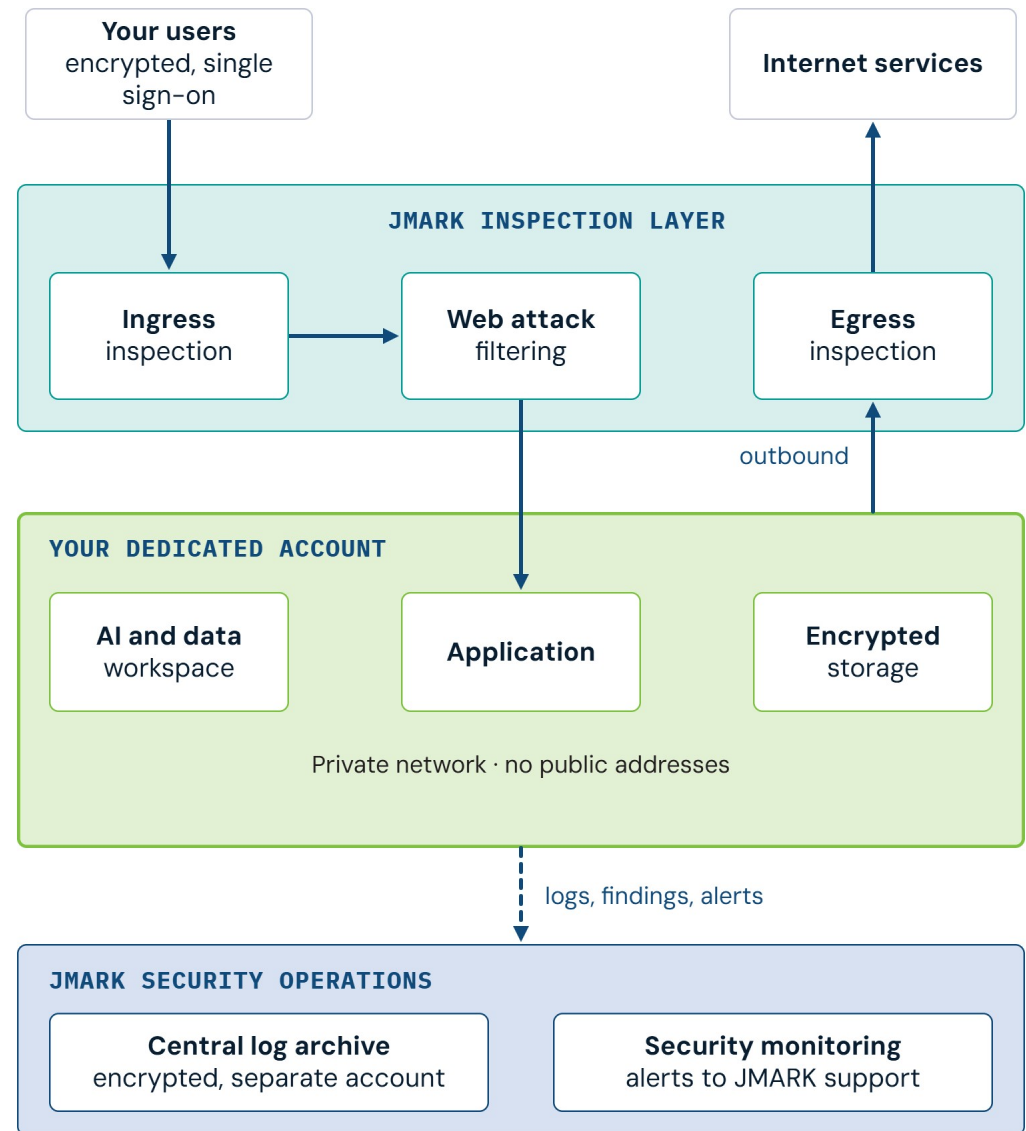
Security That Starts With Isolation

JIVE, the JMARK Intelligent Virtual Environment, brings generative AI to your organization in an environment built for you alone. Public AI services serve many customers from one shared platform. JIVE gives each client a dedicated AWS account, its own private network, and its own data workspace. Every connection in and out passes JMARK's inspection layer, and every environment is watched from separate security accounts.

Your data never shares an account with another client. That is the entire point.

Measured continuously against the CIS AWS Foundations Benchmark. JIVE software is built to the NIST Secure Software Development Framework and tested against the OWASP Top 10.

Isolation at a Glance



How We Protect Your Environment

Three controls carry the design: inspection on every path in and out, accounts isolated from one another, and oversight that never opens a path between clients.



Inspected In and Out

In. Every request enters through an inspection layer that JMARK runs in front of all client environments. A network firewall checks each connection against managed threat signatures. A web application firewall then screens each request for common attacks. A private connection carries it on to your environment, where servers have no public address.

Out. Outbound traffic passes a firewall that sees each client's traffic on its own, so every outbound connection traces back to its source.



Isolated Accounts, Controlled Access

One account per client. Your application, data workspace, and storage run in a dedicated AWS account with its own private network. Routing rules block every path between client networks.

Provisioned from code. New accounts are created from reviewed code and enrolled in central governance, which applies the same baseline automatically: audit logging, default encryption, blocked public storage, and compliance checks.

Access by identity. Staff sign in through central single sign-on with group-based assignments. Deployment access is limited to a restricted, IP-locked path, and its use is logged.



Visibility Without Exposure

Some traffic must cross account boundaries for oversight. None of it connects one client to another.

Logs. Audit and network flow records go to an encrypted log archive in a separate account.

Findings. Threat, vulnerability, and configuration findings go to a dedicated security account, which alerts JMARK support with the severity, the problem, and next steps.

Management. Administrative sessions use the cloud provider's managed channel and leave through the inspected egress path.

Your data stays in your account. Encrypted in transit and at rest. Not used to train AI models.

Questions, or a deeper security review under NDA: **844-44-JMARK** | jivesupport@JMARK.com