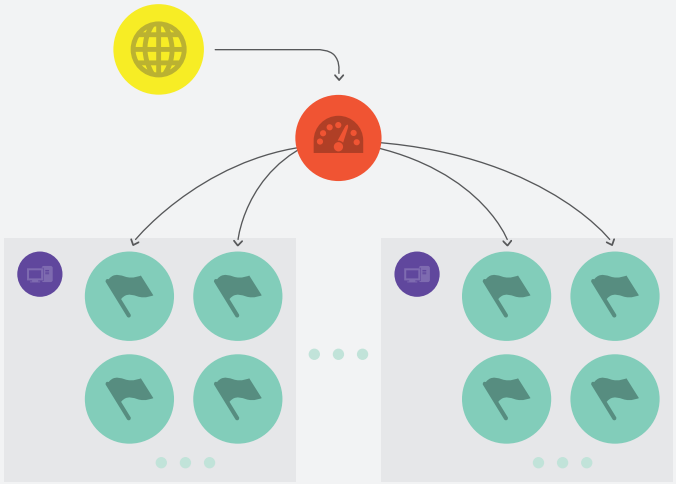
XERVO ENTERPRISE CLASS by Progress

ONE SOLUTION - IN THE CLOUD OR ON-PREMISES

Security is an important part of the Xervo™ by Progress Enterprise Class solution. Every precaution is taken to ensure installations and their data cannot be compromised. Xervo Enterprise Class uses a multi-layered network approach, strict communication restrictions and dedicated resources to provide one of the most secure environments possible.

PRIVATE NETWORK



FEATURES

No application host is exposed directly to the Internet.

The load balancer is the only entry point inside the private network. Only HTTP(s) traffic on ports 80 and 443 is allowed. All other traffic is rejected.

Firewall rules are specifically created for each server's purpose. Ports are only opened to internal endpoints that require access.

The load balancers provide DOS protection by rejecting connections that exceed abusive throughput thresholds.

Application instances are each on dedicated virtual networks and do not share or have access to resources from other instances.

DEDICATED RESOURCES

FEATURES

No resources are shared between Xervo installations. All servers are dedicated instances.

Unique SSH keys are generated for each installation. Keys created for one installation cannot be used to access resources for another.

SSH access to servers can only be done using key files. There is no password access.

Each server has SSH abuse protected that rejects connections and mitigates brute-force attacks.

INTERNET LOAD BALANCER HOST INSTANCE

* The security outlined in this document applies to managed cloud installations of Xervo. On-premises and hybrid environments will work differently depending on the specific needs of the installation.