Ori Global Cloud

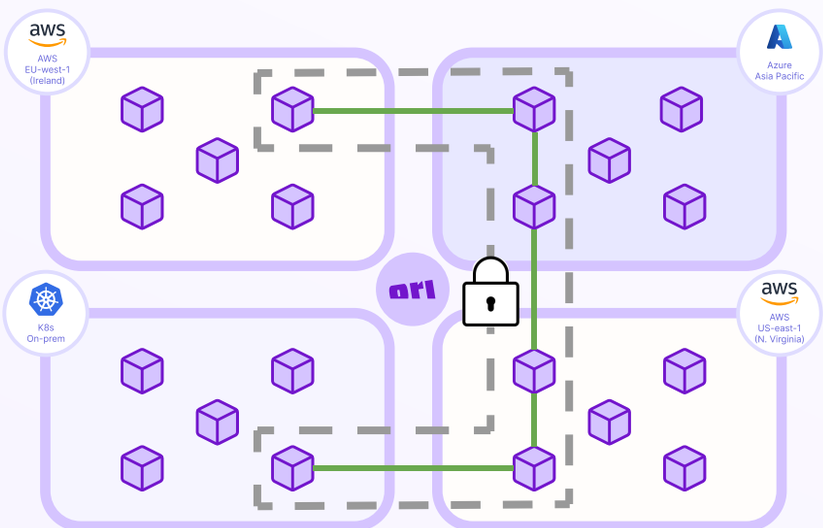
ALL YOUR APPS SECURELY CONNECTED AND DELIVERED ACROSS ALL YOUR CLOUDS

WHAT DOES SECURE-BY-DEFAULT MEAN?

The only successful way to improve the security of any system is through **"security in depth".** This means the security of any application deployment depends on a number of factors, and only by addressing each of these factors holistically can a high level of security be achieved.

Factors that need to be considered

- **TRANSMISSION SECURITY** – Preventing unwanted actors from intercepting internal communication.
- **FINE-GRAINED CONTROLS** – Preventing privilege escalation by ensuring that only those that need to communicate, can communicate.
- **SECURE CREDENTIALS** – Preventing disclosure of confidential data, such as credentials, by applying clear and effective processes for secure data handling.



TRANSMISSION SECURITY

Rather than describing each container that makes up a complex application individually in isolation, Ori makes it simple to define not only the containers, but also the required communication paths between the containers when they are deployed as part of one complete package. When a packaged application is deployed with Ori, this intercommunication information is used to deploy a **bespoke virtual private network (VPN)** between each of the containers, wherever the containers are deployed.

This VPN is **application-centric**, meaning that data that flows between the containers is encrypted such that it is only understandable to the containers of a particular deployment, and other processes on the same clusters will be unable to decrypt the data. This applies to not only other workloads deployed on the cluster, but even containers belonging to other deployments of the same application, as the cryptographic key material is unique per deployment.

The secure VPN technology allows containerised workloads deployed by Ori to become cluster-agnostic, as the communication can be allowed to flow between clusters via unsecured networks or the public Internet, in globally diverse regions, without risk of interception or reliance on a particular infrastructure technology. **This allows applications to be deployed in a multi-cluster, multi-cloud manner, without complex, brittle network security configuration.**

FINE-GRAINED DATA ACCESS-CONTROL POLICY

As part of the description of the intercommunication between workloads previously described, the user is required to specify not only which containers in their application may talk to each other, but also the exact details of that communication (*e.g.* which IP family, protocol, protocol ports are used).

This explicit description of the required communication is used by Ori to build a security policy that is applied when the application is deployed, ensuring that not only are containers only able to talk to each other, but enforcing that communication to be only what has been explicitly allowed. Effectively, with Ori, your applications communicate through a **micro-segmented network.**

This **fine-grained access-control applies a high-performance 'firewall'** between every container in the application, ensuring that not only is the expected behavior followed, but if a fault in any part of the application results in compromise, that compromise is not able to exploit other containers through unrestricted side-channels.

SIMPLE, SECURE CREDENTIAL MANAGEMENT

It is well understood that the more complex something is to do, the more likely mistakes are made. And when it comes to the handling of sensitive information such as passwords, these mistakes can be very costly.

Ori provides a clear and simple way to manage the secure handling of any confidential data required by an application when it is deployed, fully integrated with the native Kubernetes "Secrets" subsystem, without requiring the users to have deep knowledge of implementation details.

All confidential material is held securely by Ori between deployments, and the platform's role-based access control allows groups of users to manage the configuration and deployment of applications that need confidential data, while permitting a different user group to access the confidential data itself. In this way, the value of confidential information is clearly separated from the use of the confidential data, avoiding the accidental manipulation or disclosure of the data.

BE A SECURITY HERO IN A MULTICLOUD WORLD.
SECURE AND DELIVER EXTRAORDINARY DIGITAL EXPERIENCES.