

Keep apps going *Yes*

Availability of applications and their servers is a key requirement for businesses today.

Key benefits

- Gain access to skilled resources and best-of-breed technology and monitoring equipment
- Helps to keep your business applications up and running, supporting overall business productivity
- Assists with minimising the costs and losses associated with application downtime
- Provides visibility of applications servers' health through advanced monitoring techniques
- Helps enhance performance of application traffic to enable better user experience
- Blocks illegal requests to help secure the application servers

Increasing use of online commerce means organisations can no longer afford or tolerate downtime of online business applications. Optus' Managed Application Delivery and Security service helps to maintain availability of critical business resources and applications to support the continued success of business operations.

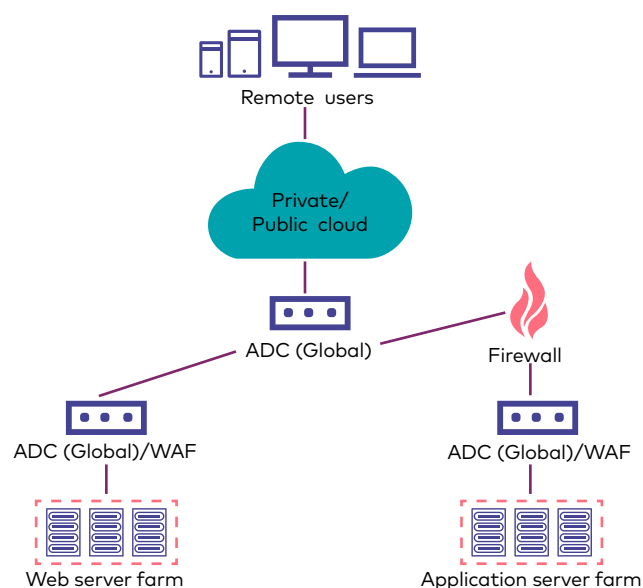
With the Optus Managed Application Delivery and Security service, best-of-breed technology for the delivery of business applications and services is managed on your behalf to maximise uptime. The service also helps to provide your organisation with improved application efficiency and convenience.

For security protection, the Application Delivery Controllers are hardened to help protect against attacks, such as Denial of Service attacks. The devices are highly capable, designed to remain in operational readiness and availability even under heavy use. Traffic is profiled and inspected against attack signatures – any detected illegal requests and protocol misuse is blocked. This helps to ensure only legitimate service requests reach the application servers.

How it works

With the Optus Managed Application Delivery and Security service:

- Application Delivery Controllers (ADCs) are implemented in the Data Centre (on the customer premise) to proxy all requests that are destined to the application servers.
- For each application a Virtual Server (VIP) is configured, which has a set of parameters to optimise the distribution and delivery of the traffic.
- Each application server is monitored by the Application Delivery Controller in regular intervals. In the event of an application server failure, the Application Delivery Controller will immediately stop passing traffic to the failed server and only distribute traffic to those that are available.
- The built-in intelligence not only maintains the reachability of the service, but also accelerates the traffic to help increase the overall performance, thereby improving user experience.



Application delivery and security functions

Depending on the solution and services chosen the following functions can be provided:

Virtual server (or VIP) management

Skilled resources manage and support issues related to the Virtual Servers; and confirm the Application Delivery Controller is serving the application on behalf of the application servers. Application traffic requests are distributed as per the agreed logic and design.

Pool management and health monitoring

Application servers are grouped into pools. Each server is monitored using the most appropriate metric to check the health of the server and its content. Upon detection of any failed servers, you are notified. The problem server is disabled/removed from the pool until the issue has been rectified.

Application Delivery Controller (Local)

ADC (Local) is meant for single site traffic load balancing and optimisations. In the simplest case, it is used to make load balancing decisions as well as off-load specific functions, such as SSL (Secure Sockets Layer), from the servers to the ADC appliance. In addition it is used to hide the backend resources from the front end users.

Application Delivery Controller (Global)

ADC (Global) is used to provide site redundancy and geographic load balancing by leveraging the worldwide Domain Name System (DNS). It integrates with the ADC (Local) product so application requests are routed to the appropriate and available resource in data centres worldwide.

Web Application Firewall (WAF)

This is a Layer 7 traffic inspection device used to help ensure security of the resources located behind it. It differs from a typical firewall in that it is inspecting and logging full http/https traffic. WAF can be deployed stand-alone or as an add-on module to an existing ADC (Local) solution.

High availability

Application Delivery Controller devices have the option of being configured in high availability mode. This configuration allows dual redundant systems to be paired into a high availability architecture with redundant systems, power and fans as well as redundant physical links.

This configuration allows the managed devices to withstand individual physical device or network link failure whilst maintaining proper network protection.

Directory integration

Integration with corporate directory services such as active directory, LDAP to provide more granular role based access control policy.

SSL offloading

To help increase confidentiality and integrity, some business applications are encrypted within SSL (Secure Socket Layer). The Application Delivery Controller can host the SSL certificate on the Virtual Server, eliminating the need for having an SSL certificate hosted on each and every application server. Administration of the SSL certificate is also centralised on the Application Delivery Controller, and managed by Optus, thereby helping to further reduce the overall complexity and cost.

Custom scripting

If you wish to have application traffic delivered in unique and special ways, the Managed Application Delivery and Security service can help meet your requirements by enabling custom scripting on the Application Delivery Controllers. Custom scripting is flexible and fully supported.

3rd Party Application Vulnerability Testing

Integrates with services, such as WhiteHat Sentinel, that perform vulnerability assessments of web applications. Vulnerability assessment services identify, classify, and report potential security holes or weaknesses in the code of your web site or specific application.

Feature availability

Optus works with industry leading vendors to provide best-of-breed technology solutions. The table below shows the service options available.

Standard features

Virtual server management

Pool management and health monitoring

Application Delivery Controller (Local)

Application Delivery Controller (Global)

Web Application Firewall

Optional features

High Availability

Directory Integration

SSL offloading

Custom scripting

3rd Party Application Vulnerability Testing

Let Optus manage your security



We want to help to reduce your exposure to security threats and incidents. Our aim is to assist you with protecting your valuable intellectual property and complying with legislative requirements.

We can help you to assess, design, implement and manage your security environment so you can move ahead with confidence knowing the confidentiality, integrity, availability and protection of your critical business data is in hand.

Through our managed services you have access to our experienced and skilled team to supplement your own resources.

Whether it is just one aspect of security such as Application and Delivery security or our whole suite of integrated security solutions, choose the peace of mind offered by Optus.