Protect

zcrADC

Application Delivery Controller

zcrADC improves application delivery with Layer 4/7 load balancing, high availability, SSL/TLS offload, traffic optimization, WAF, API and DoS/DDoS protection.

BUILT FOR	SMEs · Enterprise · Government · MSSPs · IT and security teams
THE OPERATING GAP	As traffic and application count grow, a single web server becomes a bottleneck and a single point of failure — without load balancing, SSL offload, and health-aware traffic routing, one server outage can take the whole application down.
PROTECTS AND INTEGRATES WITH	Web Apps · APIs · LDAP · Active Directory · RADIUS · SAML
DELIVERY OPTIONS	Cloud / SaaS · Virtual appliance · ICT hardware appliance, chosen in solution design

CORE CAPABILITIES

- Layer 4 and Layer 7 load balancing for fast, reliable, continuously available Web Applications and APIs.
- Health checks and high availability with automatic status monitoring and failover.
- SSL/TLS offload, compression, and traffic optimization to reduce workload and accelerate response time.
- WAF, API protection, and DoS/DDoS protection for Web Applications and APIs.
- Pre-authentication, SSO, and identity integration with LDAP, Active Directory, RADIUS, and SAML.
- Real-time system status and operational visibility through dashboard and monitoring.
- Enterprise management through API, automation, role-based access control, Syslog, and SNMP.

HOW zcrADC WORKS

Balance and protect application traffic, with real-time system status

zcrADC distributes traffic across Layer 4 and Layer 7, offloads SSL/TLS processing, and adds WAF and DoS/DDoS protection in front of your applications — keeping services available and fast even as traffic and server count scale.

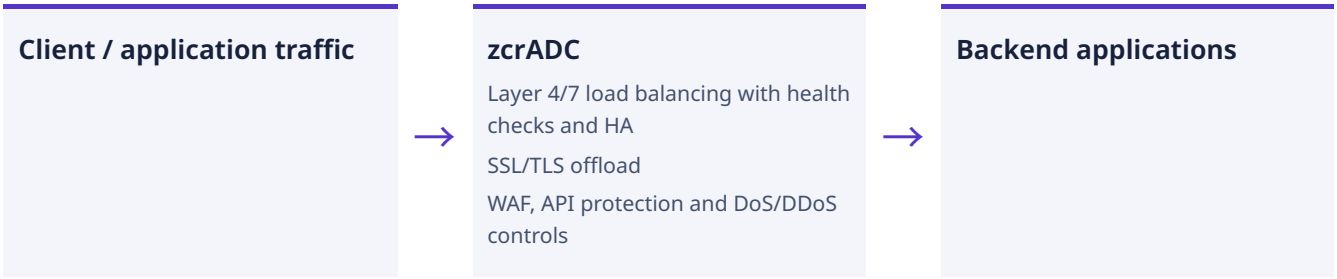
zcrADC Outcomes

- **Higher Availability** — Health checks monitor server status and fail over automatically, so traffic keeps reaching healthy servers.
- **Stronger Protection** — WAF, API protection, and DoS/DDoS protection sit in front of web applications and APIs.
- **Flexible Deployment** — Use SaaS, VM, or hardware appliance models.
- **Faster Response** — SSL/TLS offload, compression, and traffic optimization reduce server workload and speed up response time.

Make application delivery operationally visible

zcrADC gives IT and security teams a shared control plane for availability, access, and protection around important applications.

How traffic flows through zcrADC



Conceptual workflow built from the zcrADC module capabilities, not a network topology.

Key Capabilities

- SSO: Pre-authentication with LDAP, Active Directory, RADIUS, and SAML

zcrADC FAQ

How can zcrADC be deployed?

zcrADC is available as Cloud / SaaS, a virtual appliance, or an ICT hardware appliance.

Which identity systems does zcrADC work with?

Pre-authentication and SSO integrate with LDAP, Active Directory, RADIUS, and SAML.

OPERATING AND COMMERCIAL SCOPE

Cloud / SaaS	Cloud-hosted zcrADC, with no hardware to deploy.
Virtual Appliance	zcrADC as a virtual appliance on infrastructure your organization controls.
ICT Hardware Appliance	zcrADC on an on-premises ICT hardware appliance.
Pricing	Your channel partner sizes the deployment, confirms the delivery form and issues the quote.

> **The same capabilities in every delivery form**
>
> Cloud / SaaS, the virtual appliance, and the ICT hardware appliance all include the same capabilities: load balancing, SSL/TLS offload, WAF, API and DoS/DDoS protection, identity integration, and enterprise management.

Support: your channel partner provides first-line support; zcr provides product support to the partner.

Talk to a zcr.ai channel partner

Contact a zcr.ai channel partner for sizing, deployment model, and final quote.

Contact a channel partner ↗

zcr.ai/en/contact/