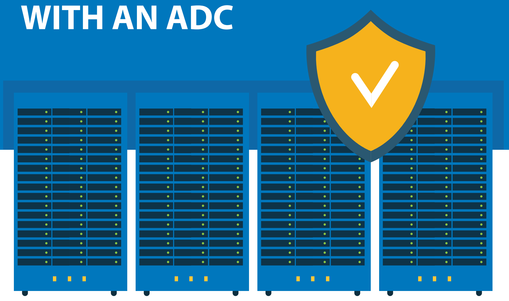
SECURING YOUR DATA CENTER WITH AN ADC



Malicious users of all types have set their sights on data center servers. **7 ways** that an ADC can help protect this vital enterprise resource.

$181,700

Avg. cost associated to an hour of data center downtime.[1]

SECURE YOUR DATA CENTER ASSETS

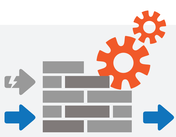
To do this, you need a high performance ADC to accelerate and optimize the performance of data center applications while simultaneously performing advanced inspection for security.

PREVENT SERVER DOWNTIME WITH INTEGRATED DDoS PROTECTION

While external DDoS prevention services are part of a sound mitigation strategy, many services cannot stop advanced application-layer DDoS attacks or detect attacks concealed in SSL traffic. In addition, organizations may want the visibility and control of an on-premise security solution which can be enabled by a robust ADC.

122.22%

increase in application layer (Layer 7) DDoS attacks[2]



WAF

A WAF complements traditional firewalls

BLOCK WEB ATTACKS WITH A WEB APPLICATION FIREWALL

Many organizations operate under a false sense of security. Unfortunately, all-purpose security products do not provide the granularity or the specialized defenses to stop advanced web attacks. To protect web applications, organizations need to deploy a Web Application Firewall.

DNS PROTECTION WITH DNS APPLICATION FIREWALL

An ADC with an integrated and powerful DNS Application Firewall can stop buffer overflow, malformed requests and Denial of Service (DoS) attacks to shield DNS servers. Additionally, an ADC can load-balance multiple DNS servers and cache DNS queries, and also provides scale, enabling DNS servers to handle heavy loads and massive attacks.

PORT 53

Most firewalls leave port 53 open, which is used for DNS queries

65%

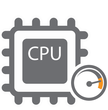
of internet traffic encrypted by end of 2016[3]

HIGH SPEED SSL DECRYPTION AND INSPECTION

Encrypted traffic makes traditional security devices blind to potential threats hidden in SSL traffic. An ADC can offload CPU intensive SSL decryption functions, enabling traditional security devices to become effective again.

PROTECT SENSITIVE DATA WITH SSL OFFLOADING

An ADC not only offloads SSL processing from web servers, it turbocharges application performance, delivering ultra-fast SSL performance and reducing web load times.



2048-bit

CPU usage generally increases 4-7 times when upgrading 1024-bit keys

Authentication Management

enables IT administrators to deploy an authentication offload solution

CENTRALIZE AND SECURE AUTHENTICATION

A robust ADC should provide an easy way for organizations to augment, streamline and consolidate authentication management. Such solutions should seamlessly integrate with authentication servers, and applications to authenticate users, support SAML for single sign-on and enforce access privileges.

[1]Source: http://www.studyweb.com/outrageous-costs-data-center-downtime
[2] Source: Akamai state of the internet report q2 2015
[3] Source: "Security must address threats from rising SSL traffic," 2013