Enterprise Strategy Group | Getting to the bigger truth.™

ESG Research
Executive Summary

The Expanding Role and Importance of Application Delivery Controllers (ADCs)

By Jon Oltsik, Senior Principal Analyst, and Colm Keegan, Senior Analyst

February 2015

This ESG Research Executive Summary was commissioned by Radware and is distributed under license from ESG.

Contents

Introduction

The Enterprise Strategy Group and Radware recently conducted a collaborative research project that focused on the current utilization and future strategies of application delivery controllers (ADCs). The data presented in this ESG white paper is based upon a survey of 243 IT professionals working at enterprise organizations (i.e., those with more than 1,000 employees) based in North America. The ESG research reveals that the role of ADCs has expanded well beyond the historical perception of hardware-based load balancers. Organizations are deploying ADCs as virtual appliances at an increasing rate and taking advantage of ADC functionality from the network through the application layer. What's most interesting, however, is that ADCs are becoming a critical component of a defense-in-depth security strategy as enterprises fine-tune security policy and enforcement to align with their sensitive business applications.

ADCs Are More Pervasive Than Ever

Mention ADCs to IT professionals and many will think of massive hardware appliances deployed in data centers at large organizations. This perception may be historically accurate, but recent ESG research indicates that ADCs have become far more ubiquitous. For example:

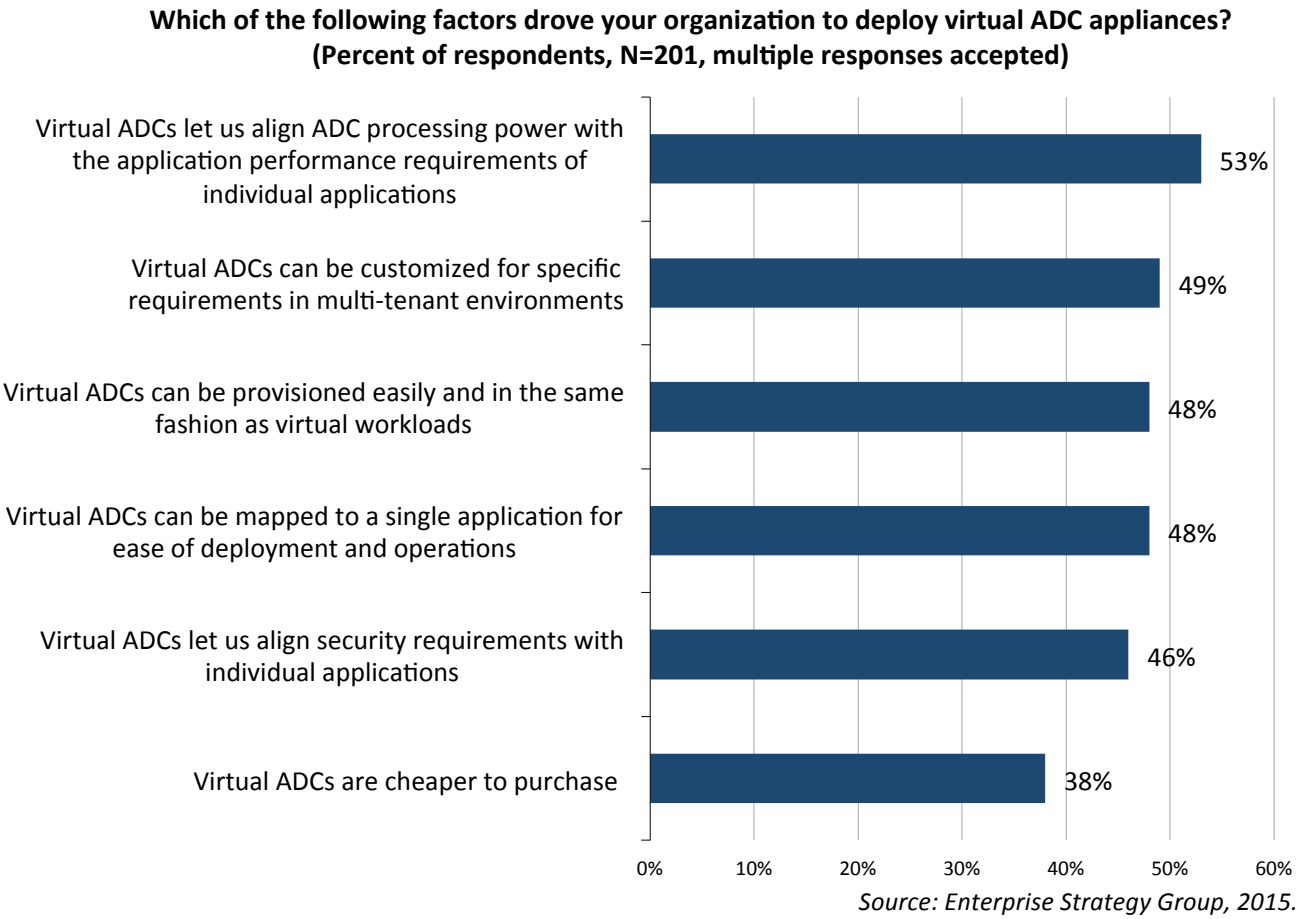
- More than half (51%) of enterprise organizations surveyed have at least 21 ADCs in use today.
- Eighty-two percent (82%) of organizations believe that the total number of ADCs will increase substantially or increase somewhat at their organizations.

Clearly, this data demonstrates that ADCs are used extensively in large and small enterprises, supporting hundreds of web applications for business analytics, CRM, e-mail, and HR. Organizations also report that ADCs can deliver numerous other benefits as well—49% say that ADCs deliver higher levels of availability, 47% believe that ADCs provide improved response time, 44% state that ADCs offer better access to applications, and 36% associate ADCs with an enhanced security posture.

ESG research also contradicts the image of ADCs as chassis-based hardware devices. While physical ADCs are most common, two-thirds of organizations have deployed a combination of physical and virtual ADCs. Furthermore, virtual ADCs' popularity will only increase over the next few years. Why are virtual ADCs becoming so prevalent?

- IT professionals are implementing virtual ADCs because they let them align ADC processing power with application performance requirements.
- Virtual ADCs can be customized for specific requirements in multi-tenant environments, and for alignment with provisioning virtual workloads (see Figure 1).

Figure 1. Factors Driving the Deployment of Virtual ADCs



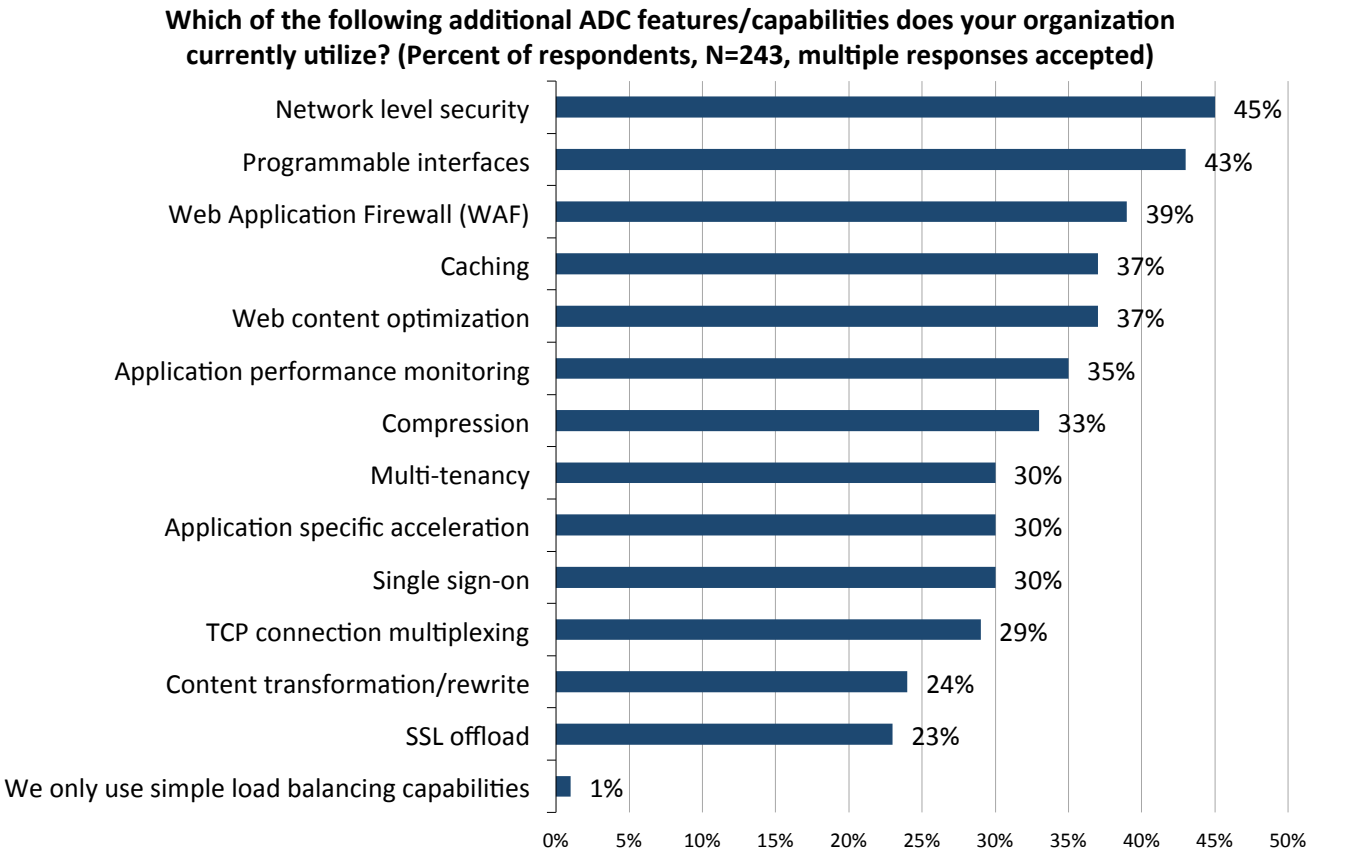
Source: Enterprise Strategy Group, 2015.

ADCs Move Beyond Load Balancing

Another common misperception is the view that ADCs are no more than network load balancers—in spite of years of innovation and a track record of additional features/functionality. The ESG research indicates that enterprises are using many ADC features today—far beyond load balancing alone (see Figure 2). For example:

- Forty-five percent (45%) use ADCs for network-level security tasks like firewalling and network segmentation. This indicates that ADCs have a role within network engineering and operations.
- Forty-three percent (43%) use the programmable interfaces on their ADCs. This functionality is often used by DevOps to align application requirements with ADC capabilities for performance tuning, application monitoring, and security.
- Thirty-nine percent (39%) use ADCs for web application firewalls to protect critical applications from attacks like SQL injections, cross-site scripting, and buffer overflow attacks.

Figure 2. Common ADC Features/Capabilities Utilized by Enterprise Organizations



Source: Enterprise Strategy Group, 2015.

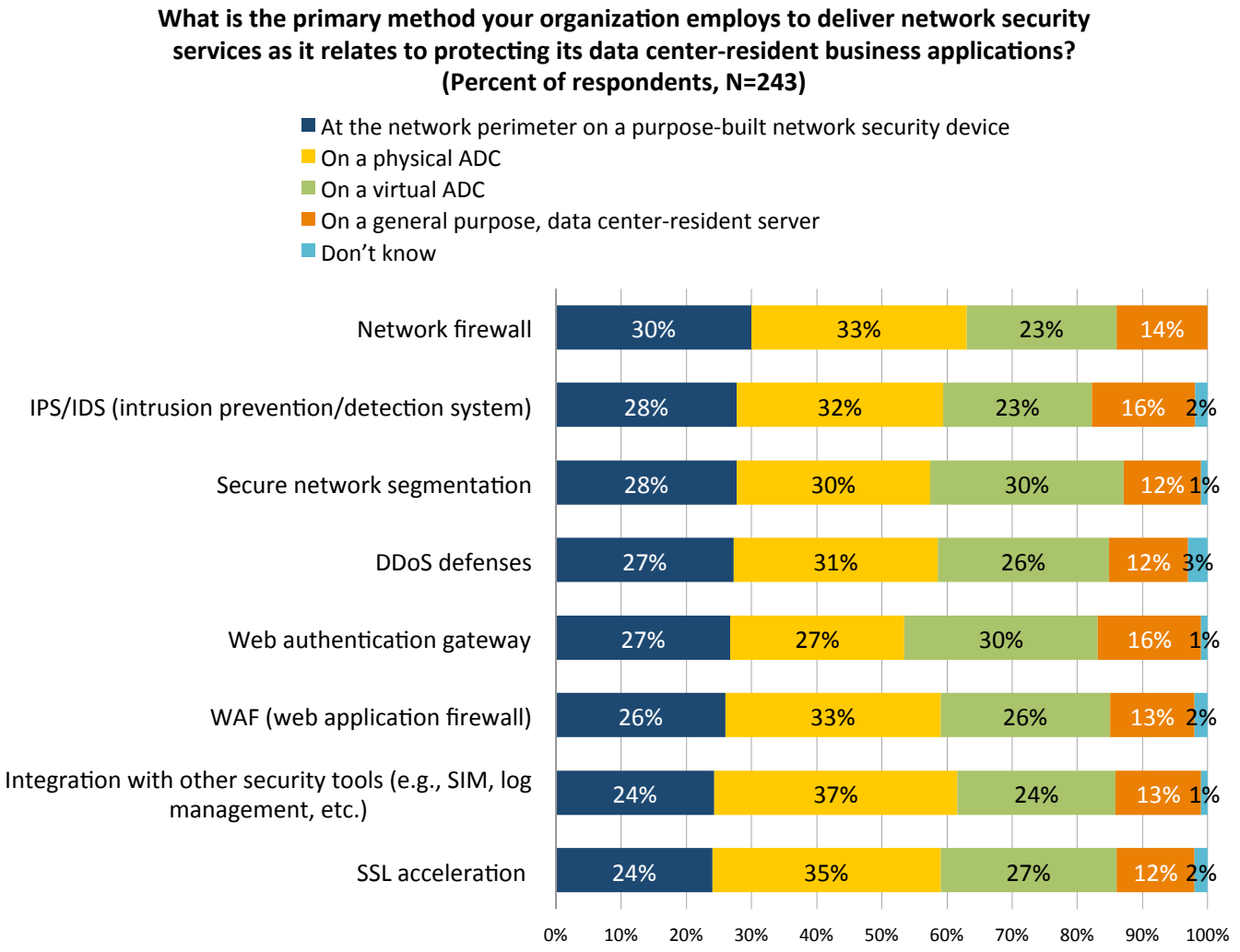
ADCs Have Become a Critical Security Control

When asked to identify their most common challenges in meeting application service-level agreements (SLAs), the most common challenge selected was "security problems" (chosen by 39% of IT professionals). It should come as no surprise then that ESG research reveals that ADCs are assuming a growing role as critical security controls. For example:

- Nearly half (49%) of organizations leverage the security capabilities/functionality on all ADCs while 44% leverage the security capabilities/functionality on ADC-supported applications containing sensitive data.
- ADC security has become a robust layer of a defense-in-depth network security architecture (see Figure 3). For example, many organizations use ADCs for firewalling, IDS/IPSs, and network segmentation that sits behind similar security controls residing at the network perimeter.

Why make ADCs another layer of network security defense? To block attacks that circumvent perimeter security controls. This is not an uncommon scenario for enterprise organizations—58% of organizations believe it is extremely likely or somewhat likely that a malicious attack could penetrate the network perimeter leaving the ADC as a last line of defense. Clearly, ADC-based security can help lower risk in this situation.

Figure 3. ADCs Have Become a Layer of Defense Behind Network Perimeters



Source: Enterprise Strategy Group, 2015.

Finally, ADC-based security appears to be gaining momentum for enterprise organizations, as 76% of organizations say that their use of ADC security capabilities/functionality will increase significantly or increase somewhat in the future.

The Bigger Truth

When it comes to ADCs, perception is not reality. For example, many IT professionals still think of ADCs as hardware-based load balancers but the ESG research presented in this brief indicates a different situation. ADCs are being deployed as virtual appliances and this will only increase as organizations embrace private and hybrid cloud architectures. Furthermore, most organizations use ADC functionality well beyond load balancing alone as they utilize them for API integration, caching, web content optimization, etc.

While the role of ADCs is certainly expanding, ESG research reveals that this is especially true with regard to information security. In fact, CISOs are using ADCs in an assortment of security use cases such as network firewalls (OSI layers 3 and 4) all the way up to web application firewalls (OSI layer 7). Furthermore, ADCs have become an additional layer of defense beyond perimeter security devices.

The IT professionals surveyed for this project understand and are taking advantage of the fundamental strength offered by ADCs. Unlike general-purpose network appliances, ADCs marry network and security functionality with specific web application requirements. As such, they can be fine-tuned at the IT infrastructure, security policy, and even business level, providing a degree of flexibility that is difficult or impossible to implement in other IT technologies.

There is a lesson to be learned here: The ESG data suggests that enterprise organizations can be creative with their ADC deployments for performance tuning, application-specific services, and critical system protection. CIOs, CISOs, application owners, and network engineers can benefit by applying ADCs in this fashion.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com