ADC Survey

GLOBAL FINDINGS

IT agility. Your way.®

CONTENTS

Executive Summary

Information security has always been an arms race between IT and hackers. The bad guys launch a threat, IT counters with safeguards and the bad guys develop a new threat that gets around the safeguards.

Currently the front line has shifted from layer 4 to layer 7 attacks. While most traditional safeguards can handle layer 4 threats like SYN Flood DoS attacks, layer 7 threats, such as SlowLoris, are trickier. They get by layer 4 defenses because they look like legitimate traffic.

In effect, hackers have raised the ante. It is now IT's turn to respond.

Application Delivery Controllers (ADCs, sometimes called next-generation load balancers) are, in many ways, perfectly suited to the task. They understand the context of the traffic they manage at all levels (including layer 7). They have the compute power required plus deep packet inspection to react to advanced, persistent and distributed threats. And they have the ability to react and mitigate attacks.

F5 designed the **2011 ADC Security Survey** to explore this issue. Specifically, the survey explores:

- **Threats -** What are the hardest threats IT currently has to defend against?
- **Effects -** what is the effect of this new breed of threat on global organizations?
- **Safeguards -** How are traditional safeguards, such as firewalls, faring against the new threats?
- **ADC Security -** How does IT feel about using ADCs to augment traditional safeguards?

Executive Summary continued

The survey was fielded in September 2011 to 1,000 large organizations in 10 countries and showed that IT is currently locked in a battle with advanced, persistent threats against which traditional safeguards are not enough. Of the threats IT rated as most worrisome, 4 of the top 5 were threats traditional safeguards have trouble defending against.

In fact, a third (36 percent) reported they had seen their firewalls fail under the load of an application-layer denial of service attack. A similar number said their traditional safeguards struggled defending against complex blended threats.

The effect on organizations is profound. All the organizations surveyed reported losses from cyber attacks. Productivity, data and revenue were the most common losses.

The typical cost to the organizations we surveyed was $682,000 within the past 12 months.

So, how does IT feel about enlisting ADCs in their battle against hackers? Enthusiastic, as it turns out. Just 1 in 12 felt their traditional safeguards were sufficient against this new breed of threat. Nearly all (97 percent) are discussing using ADCs in a security role and half already do so.

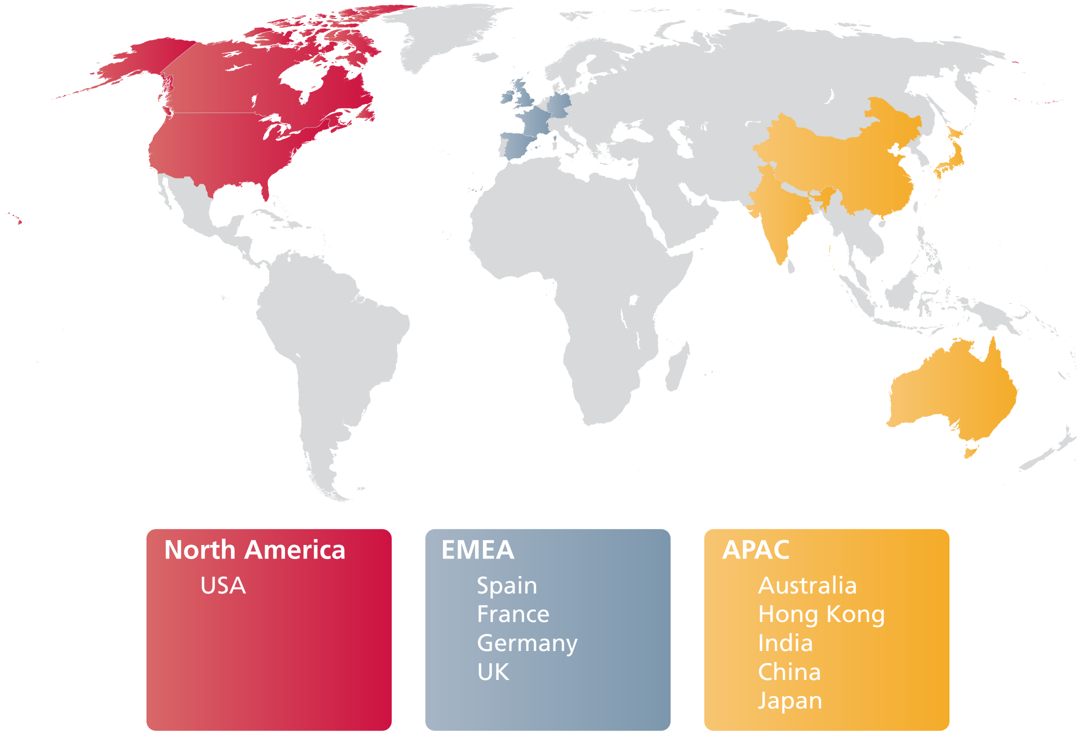
Methodology

The telephone survey was fielded by Applied Research in September of 2011. They surveyed 1,000 large organizations in 10 countries around the world. Applied spoke with senior IT management from a variety of roles.

All respondents reported that at least 25 percent of their role was security. Of that pool, we split five equal groups of respondents that reported 50% or more of their role was:

- Network infrastructure (one fifth)
- Endpoints (one fifth)
- Applications (one fifth)
- Security (not compliance related) (one fifth)
- System administration (one fifth)

What did the respondents tell us?



Finding 1

Attacks Getting More Difficult to Defend

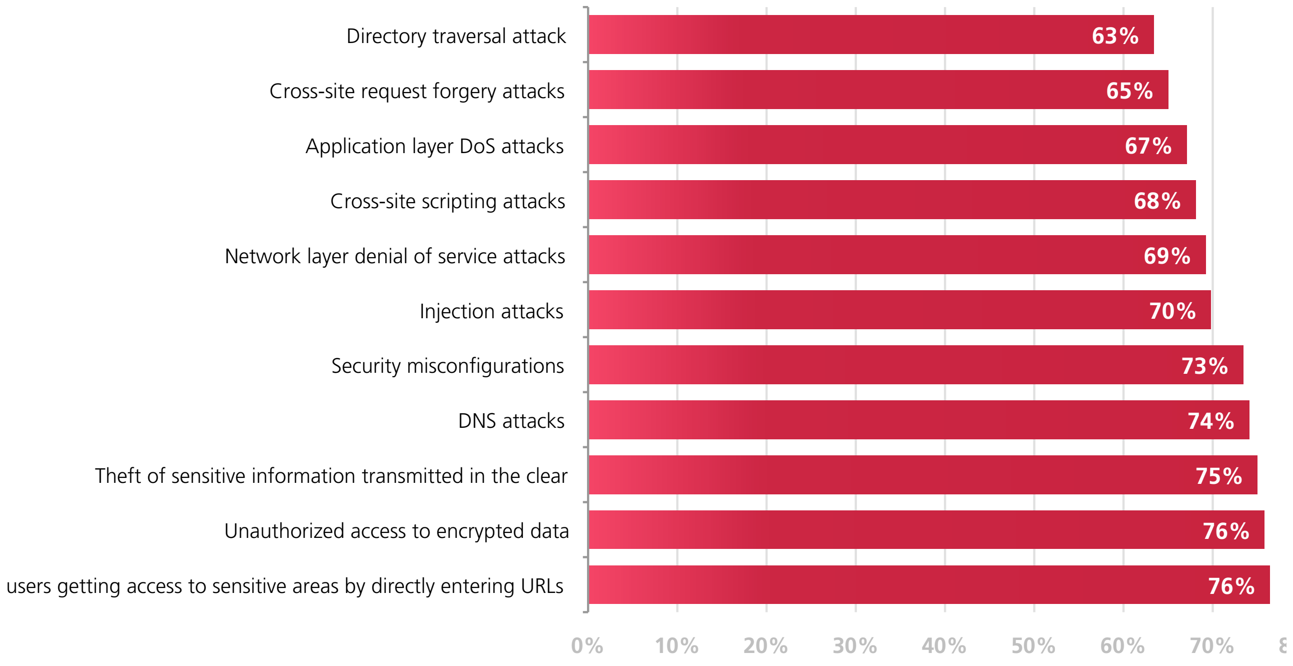
To better understand how organizations can best defend themselves against security threats, we must first know where the most critical threats lie. We asked several questions about the various types of attacks IT sees. We supplied the following list of attacks:

- Network layer denial of service attacks (DoS) (such as SYN flood)
- Application layer DoS attacks (such as Slowloris)
- DNS attacks (DoS, spoofing, cache poisoning, etc.)
- Injection attacks (such as SQL injection, LDAP injection, etc.)
- Cross site scripting attacks
- Security misconfigurations
- Directory traversal attack
- Cross-site request forgery attacks
- Unauthorized access to encrypted data (passwords, credit card data, etc.)
- Unauthorized users getting access to sensitive areas by directly entering URLs
- Theft of sensitive information transmitted in the clear

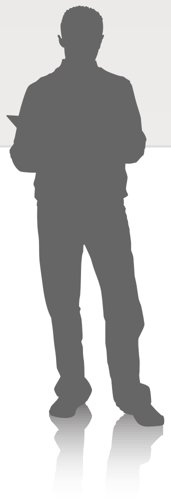
By combining the results of several questions, including ranking the top three attacks in terms of frequency, difficulty protecting against, and impact to your organization, we created the "Cyber Attack Index." This index is a measure of frequency, difficulty to defend, and impact to the organization.

Finding 1 continued on page 12

Q13: How familiar are you with each of these types of attacks? (Somewhat/Completely familiar)



> "It's been a really big deal for us. We've had some notable public attacks, both DDoS and scripting issues. We've changed our entire policy and our infrastructure in the past year because of these things."
>
> Director of Technology



Finding 1 continued

Four of the top five cyber attacks (in terms of the cyber index) are complex attacks that are difficult for traditional safeguards to defend against. They include the following:

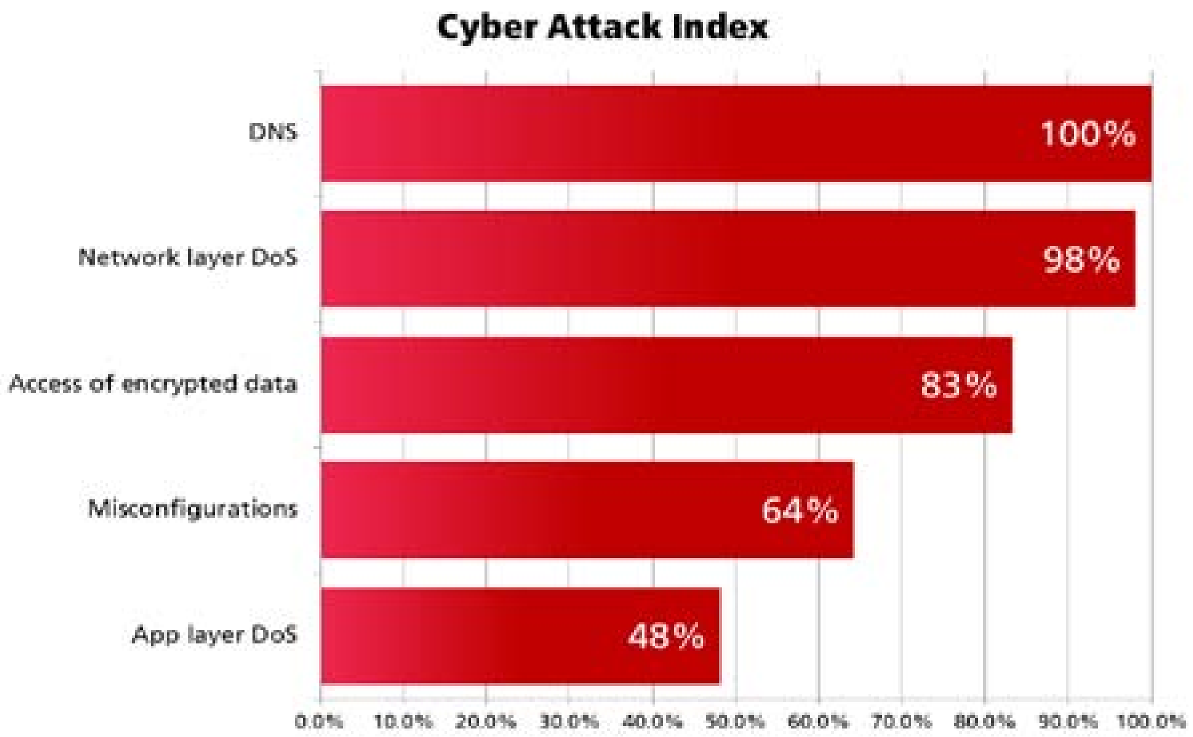
- DNS (100 percent)
- Network layer DoS (98 percent)
- Access of encrypted data (83 percent)
- Misconfigurations (64 percent)
- App Layer DoS (48 percent)

To determine if a respondent's role affected their answers, we performed a crosstab analysis across all the roles, including Network Infrastructure, Endpoints, Applications, Security (non-compliance related), Compliance and System Administration. Only security views cyber attacks slightly differently from the other roles, as noted below:

- DNS (100 percent)
- Network layer DoS (97 percent)
- Access of encrypted data (91 percent)
- Misconfigurations (70 percent)
- App layer DoS (36 percent)

In other words, they are less concerned about App layer DoS and Access of encrypted data and more concerned about misconfigurations.

So, what are the impacts on organizations of these attacks?



Finding 2

Attacks Driving High Costs to Organizations

The effects of cyber attacks can be crippling. Every respondent reported costs from cyber attacks within the past 12 months, with the most frequently-cited costs being the following:

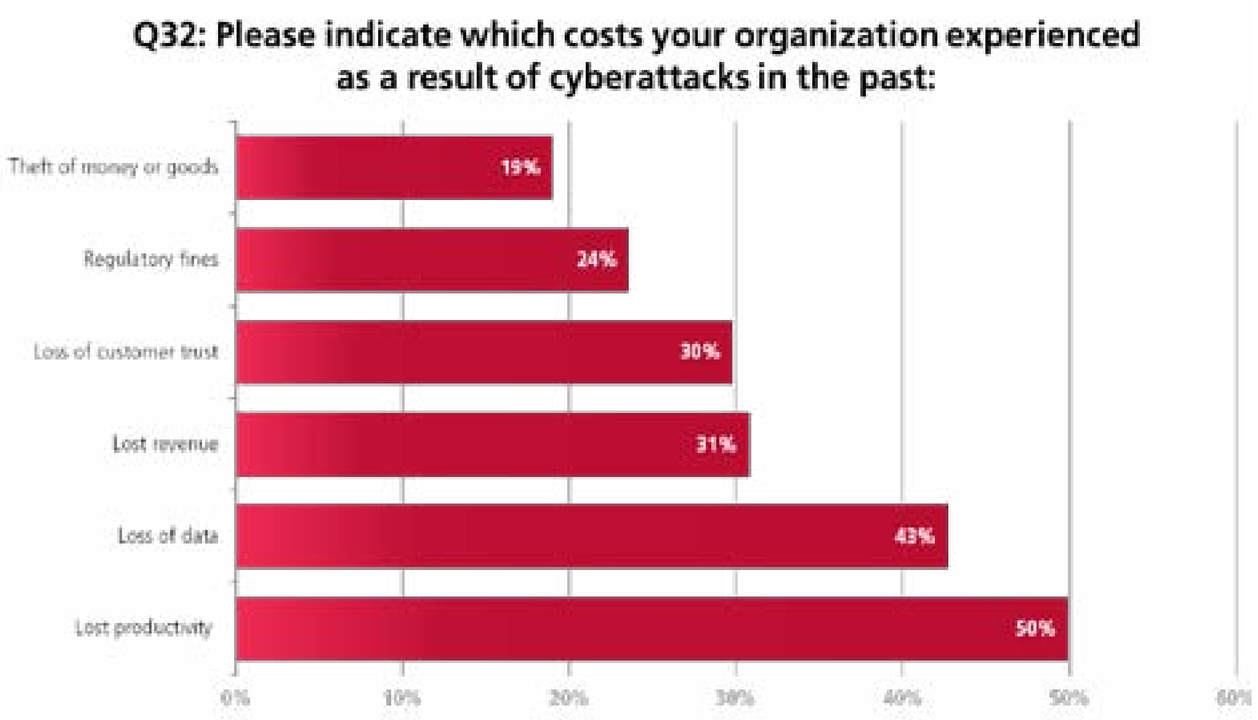
- Lost productivity
- Loss of data
- Lost revenue

The highest monetary loss was attributed to ‘loss of customer trust’, which topped out at $506,385, quickly followed by lost productivity ($492,334) and regulatory fines ($343,358).

Further, the average organization reported losses of $682,000 in the past 12 months.

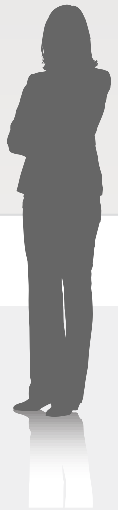
So, how are traditional safeguards faring at protecting against these more complex threats?

Attack Loses
$682,000



Q32: Please indicate which costs your organization experienced as a result of cyberattacks in the past:

> “We’re looking at the loss of time, productivity and data, maybe $100,000 a month.”
>
> Project Manager



Finding 3

Traditional Safeguards Falling Short

As the survey indicates, traditional safeguards are not enough to protect an organization from cyber attacks. Some of the more troubling findings indicating that traditional safeguards are falling short include the following:

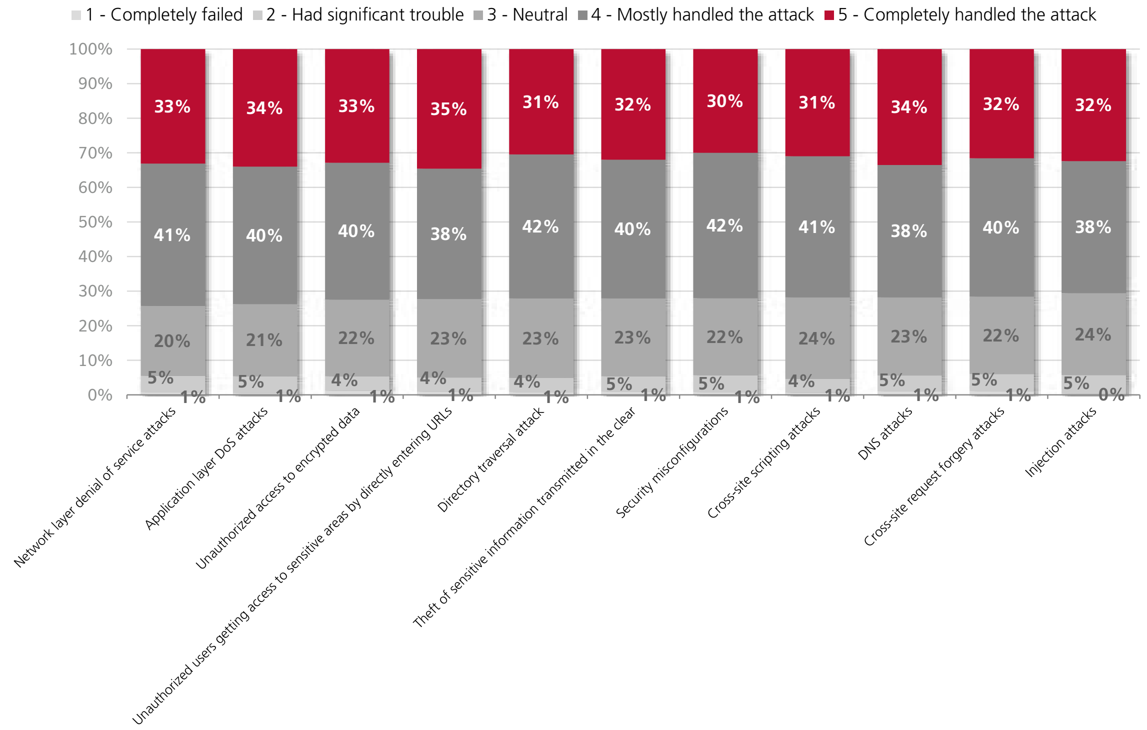
- 42 percent had a firewall fail due to high traffic loads in network-layer DoS at tacks (and 36 percent in app-layer DoS attacks).
- 38 percent said their traditional safeguards understand traffic context less than somewhat well.
- 36 percent protect against complex, blended threats less than somewhat well.

Diving into a more granular level, when asked to characterize how well their current security safeguards protect at the network versus the application layer, 19 percent of respondents responded ‘neutral’ (with 7 percent responding either ‘somewhat poorly’ or ‘extremely poorly’) in regards to the network layer and 21 percent responded ‘neutral’ (with 5 percent responding either ‘somewhat poorly’ or ‘extremely poorly’) in regards to the application layer.

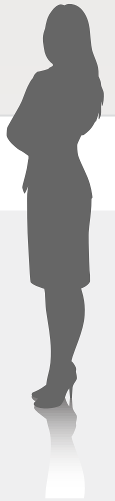
Finally, on a related note, more than half (53%) say network performance impact from security safeguards is somewhat or extremely challenging.

So, what is IT doing about these shortcomings?

Q17: How has your firewall performed in the past with each of these attack vectors?



> “I think traditional safeguards are no longer effective. For data loss, where we have a more experienced enemy, we’re seeing that we need to be far more advanced.”
>
> Director of Technology



Finding 4

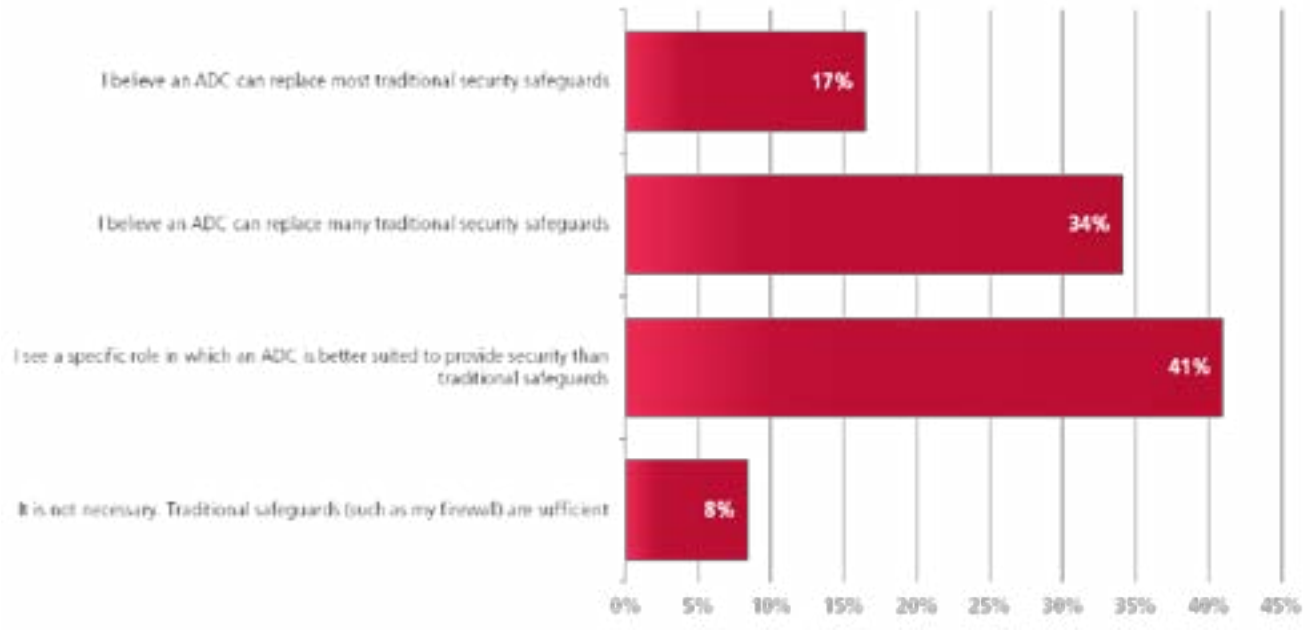
IT Sees Role for ADCs for Security

Securing IT infrastructure for the typical global enterprise gets harder every year. With cyber attacks getting more complex, employees more distributed and infrastructure more complex, traditional safeguards are struggling to keep pace. Many are turning to ADCs to fill security gaps traditional safeguards cannot reach.

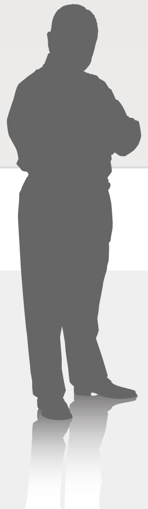
According to survey results, an overwhelming 92 percent of respondents see specific security roles for ADCs. Additionally, half say ADCs can replace many or most traditional safeguards. Clearly there is a need for ADCs to replace or supplement the security safeguards being used in today's organizations.

So, are they actually using ADCs for security?

Q55: Which statement best sums up your belief about the role of ADC in terms of providing security for your network?



> "With the ADC, at least if you do have an attack on the network, you can shut down that piece, and your entire network is not compromised. You can isolate it from the rest of the system."
>
> Senior Systems Analyst



Finding 5

Adopting of ADCs for Security is Growing

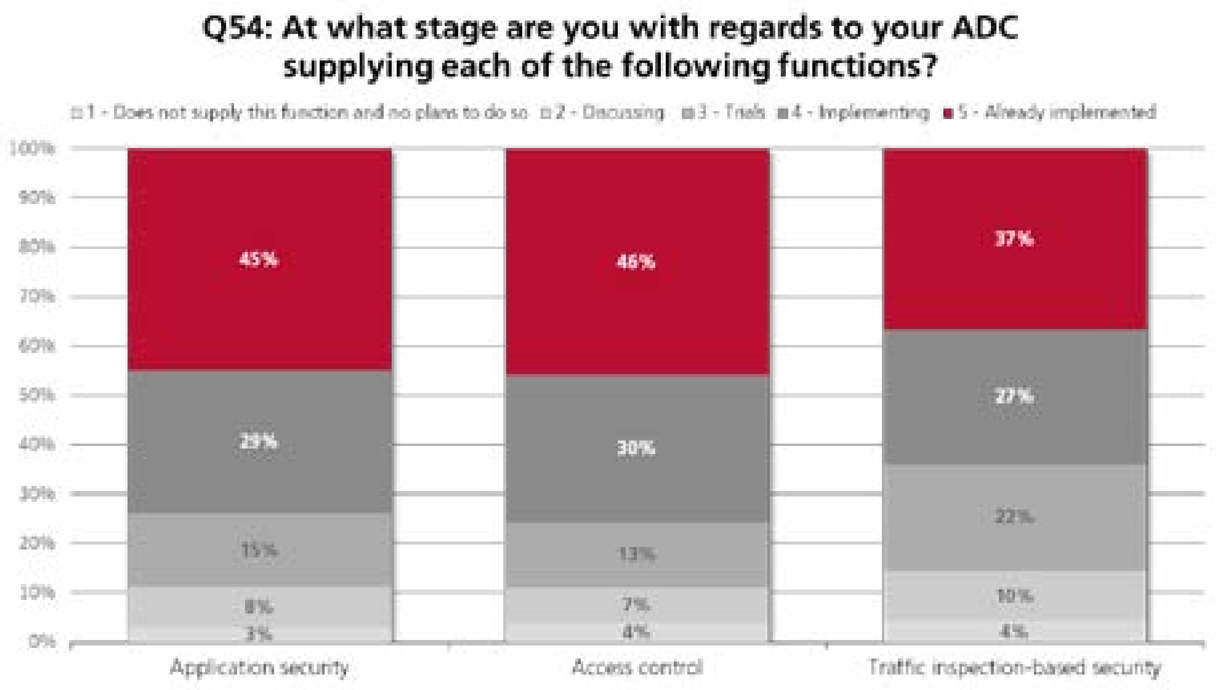
IT is increasingly turning to ADCs to bolster their organization’s cyber security. One-third to one-half are already using ADCs and almost all are discussing the possibility of implementing ADCs.

When asked at what stage they are at in regards to their ADC supplying specific security functions, a large majority are already using or currently implementing ADCs for the following functions:

- Application Security (74 percent)
- Access control (76 percent)
- Traffic-inspection based security (64 percent)

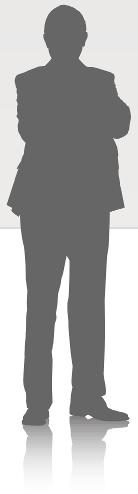
Similarly, when asked at what stage they are at in regards to their ADC supplying the security functions listed above, almost all respondents said they were at least discussing implementing ADCs.

So what should IT do?



Q54: At what stage are you with regards to your ADC supplying each of the following functions?

> “In the past 3 or 4 years we’ve expanded the use of our ADCs. We had two things that were driving it: security concerns and our ability to implement more Web 2.0 applications.”
>
> Director of Technology



F5 Recommendations

1. Unified Framework

Today's threats blend network, protocol, user, as well as application level attacks. So you need an integrated architecture that can handle L3-L7. One that can secure the network, access, endpoint, protocol and application. Why? First of all most attacks today are blended. And secondly because if all you're doing is network security, protocol security, user security or only application security in a silo you lose the context of how each is impacting the other and the vectors a particular attack is taking. By tying these together you get a full picture so you can effectively defend against these sophisticated threats. Unlike traditional security or so called next gen security technologies that narrowly focus on either network and protocol level or only on the application. That's like trying to defend against an attack where the navy, marines, infantry and air force don't communicate and you're not leveraging each effectively. In fact, you can create a lot of preventable collateral damage and you're still not protected, the attacker can more easily exploit this.

2. Must scale

Globalization and the Internet have made the need for cost-effective scale a necessity. Look at the recent anonymous and Lulzsec attacks. They are global and random in their reach. If the framework and the solution cannot scale to meet the global nature of attacks, all the unification, context, adaptability and community efforts are for naught.

3. Must understand context

Because today's attacks are blended across network, protocol, user, and application, unifying security across L3-L7 gives an organization the ability to better identify, defend and adapt. It gives the organization the edge, not the attacker. Because to exploit a vulnerability would present an attacker too many vectors to coordinate. If you have your army, navy, marines, and air force working in concert it becomes much more difficult to exploit a weakness in any one. By providing context of who, what, how, and when in real-time coordinated defense among all vectors becomes not only more manageable but effective.

F5 Recommendations continued

4. Must be extensible and adaptable

Because the attacks are blended and there are new exploits or vulnerabilities being introduced each week, the framework has to be able to respond quickly to new threats. It's not next generation it's a "now generation" solution. So the customers should seek solutions that can rapidly adapt and unlike traditional approaches not have to wait days, weeks, or months for an effective defense.

5. Must have a robust community – the "all in" strategy

It's the principle of many brains working toward a solution is better than one. Because no one organization has all the answers and no one solution approach can address it all, you need the power of community. Like-minded users who care about solving these issues and know that we're all in this together. It's like having the ultimate in visibility, command and control. If all the members are contributing, threat response and adaptability becomes not only practical but possible. A recent example is the Apache D exploit.