BIZETY

WHITE PAPER

Website Defense in Depth – Casting Akamai, Imperva, CloudFlare, F5 and Distil Networks in Their Starring Roles

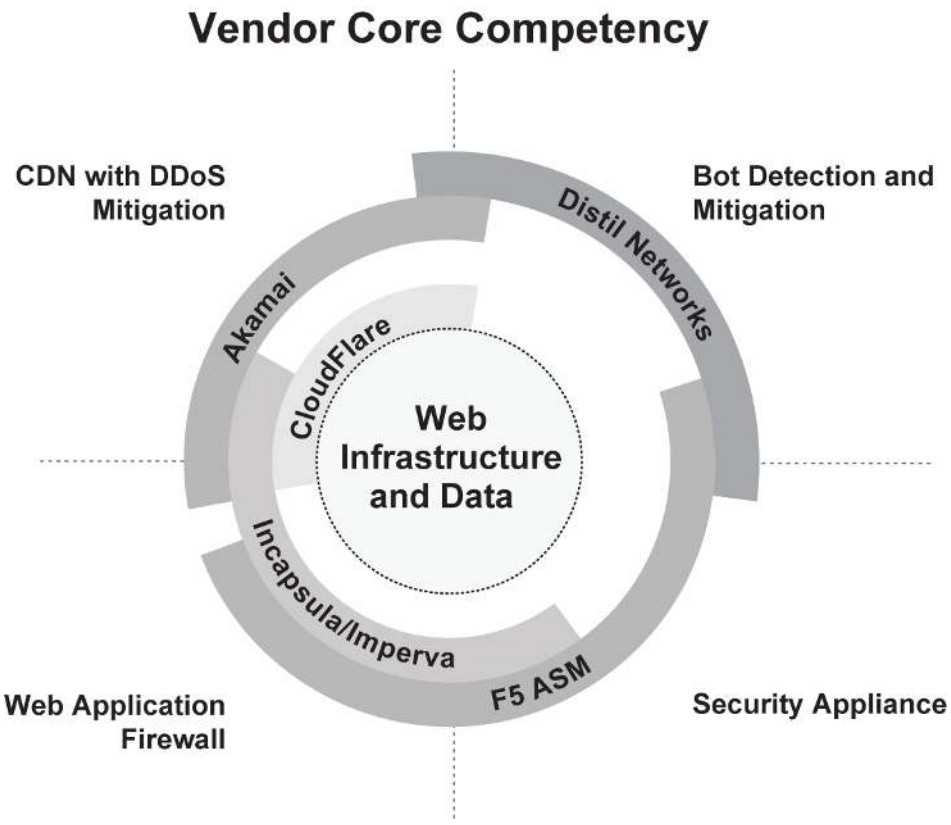


Table of Contents

Executive Summary

The potential threat of sophisticated new online attacks has vastly increased the burden on every category of security vendor. In this challenging new environment, CDNs struggle with dynamic content and enormous DDoS attacks, while WAFs contend with undocumented access requests. Many security appliances can't assess and adapt to threats in real time, and potentially block legitimate traffic. Recent website breaches also demonstrate that traditional WAFs, CDNs, and DDoS mitigation solutions have failed to keep pace with the variety, volume and sophistication of today's bot and botnet attacks. To address this security threat, bot detection and mitigation services must evolve beyond absorbing rare volumetric attacks into scrubbing centers, or simplistic IP – and user agent-based detection.

This paper examines five major vendors – Akamai, Imperva, CloudFlare, F5 and Distil Networks - and outlines how their products can coordinate to successfully secure web infrastructure and online data. Each company's 'Corporate DNA' leads to a degree of specialization, and attendant limitations.

Defense in Depth – Achieving Comprehensive Protection through Core Competency Integration

As data operations move onto the Internet, companies must increasingly turn to third party providers to protect their information, and to address the increased vulnerability of distributed information.[1] Rather than relying on a single security provider, the modern approach requires a Defense in Depth strategy, organized around specialized security structures.[2]

Defense in Depth is based on the original 'Protect, Detect, React' paradigm proposed by the National Security Agency. When correctly executed, it offers the most comprehensive model for information security. At its core is the concept that no single defensive technology will be able to protect against all intruders. To combat this, Defense in Depth proposes discrete layers of attack prevention and mitigation, situated at all levels of online infrastructure. Vulnerabilities are directly addressed with specialized products, with integrated redundancy to increase dependability. Defense in Depth relies on awareness of the challenges inherent to network security, and on quick response to newly emergent threats.

To meet these challenges, a variety of vendors have begun offering online security services, either integrated with existing products, or as stand-alone solutions. The overlapping nature of the services, combined with the lack of perceived product differentiation, has led to significant market confusion. While vendors may claim to offer complete protection from online threats, in actuality their protection can be limited by platform constraints. Vendors may feel the need to introduce features to cover a perceived market need, but these features are sometimes inadequate derivatives of their core competencies.

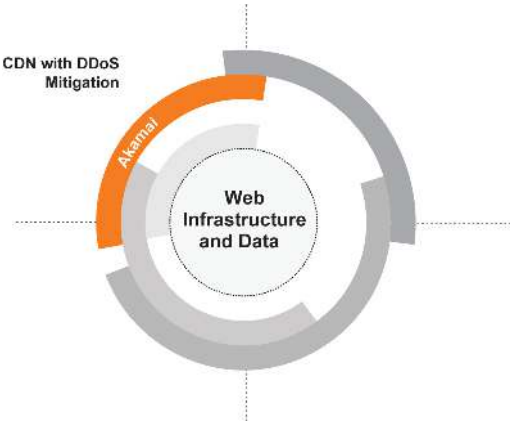
Vendors and Solutions – Building a Defense in Depth Website Security Platform

Many IT security vendors seek to address the security risks inherent in online operations. Industry leaders like Akamai, Imperva, CloudFlare, F5 and Distil Networks serve as exemplars for how an IT security vendor's corporate heritage defines its core competency and capabilities. Each of these five vendors excels in particular aspects of online defense, or has tried to capture a specific segment of the market (e.g., SMBs). However, the diverse demands of website security require comprehensive protection, as market confusion can lead to gaps in security. This paper will outline how each vendor can play an essential role in providing a Defense in Depth platform to protect your online data and web infrastructure.

[1] http://eval.symantec.com/mktginfo/downloads/21187913_GA_WP_SecuringtheCloudfortheEnterprise_05%2011.pdf
[2] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Industry Leaders – An All-Star Approach

Akamai – CDN Titan, Security Generalist



Akamai has risen to prominence as the pre-eminent CDN and cloud services provider in North America and much of the world. Founded in 1998, Akamai is the largest global content delivery network, and deals primarily with large organizations, such as Apple, Facebook, the Department of Defense and the U.S. healthcare system. In the past, there have been times when Akamai has struggled with secure connections and SSL intermediaries.[3] However, Akamai has made strides since 2009 to enhance their network security approach, including the introduction of Kona Site Defender as a Web Application Firewall. Given its industry stature, Akamai adopts the role of security generalist for large-scale clients, providing a packaged suite of base-level security applications.

Specialization:

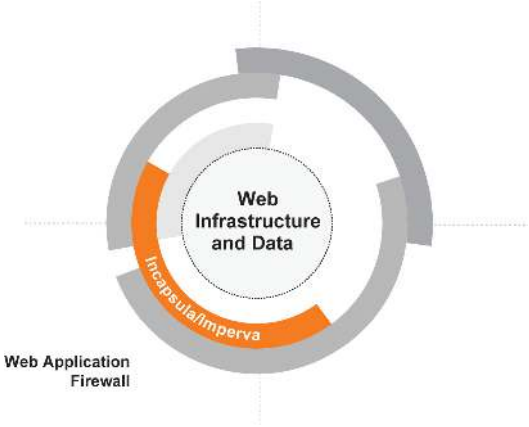
- Fastest Global Enterprise CDN, with complementary security products
- Excellent DDoS mitigation capabilities (Prolexic) to handle the largest volumetric attacks
- Embeddable WAF Services (Kona Site Defender)
- High-scalability and regional availability for global projects

Limitations:

- High cost puts Akamai out of reach for many small and medium enterprises
- Akamai's focus on content delivery leaves it less focused on emergent security threats
- Kona doesn't provide on-premise security appliances, and lags behind other specialized WAF vendors in regards to advanced capabilities and customization options
- Basic, rules-based, IP-centric bot blocking solution

[3] http://revealingerrors.com/akamai_ssl

Imperva and Incapsula – Guarding the Gateway with Appliance and Cloud WAF



Imperva, founded in 2002, has focused on delivering on-premise Web Application Firewall products (SecureSphere). Incapsula, a spin-in of Imperva, was established in 2009 to provide cloud-based WAF solutions via a CDN. By routing client's web traffic through centrally orchestrated servers, Incapsula is able to detect malicious content and filter out threats. Incapsula also bundles in affordable DDoS protection that's within reach for most SMBs. WAFs in general excel at disabling hazardous scripts and preventing unauthorized access. Incapsula in particular has lead the way in adapting its WAF to current generation threats, and has scored highly in comparative penetration testing analysis.[4]

Specialization:

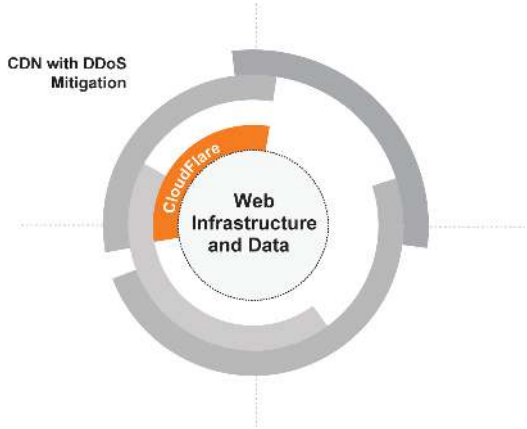
- Affordable WAF services for businesses at all levels
- Robust Protection from SQL Injections, Client-side scripting attacks (XSS), and OWASP Top 10 Attacks
- Quick and easy deployment of WAF protection
- Offers both on-premise (Imperva) and CDN-delivered (Incapsula) options
- Complementary security services like DDoS mitigation for budget conscious SMBs

Limitations:

- Inherent restrictions on Imperva's ability to protect against business logic flaws or SQLi/XSS outliers
- WAFs are an effective component of security strategy, but not a complete risk shield
- Limited effectiveness in preventing site-scraping[5]
- Due to registry mechanics, WAFs are most effective against documented threats, but can struggle with real time threats, such as bot-driven brute force login attacks

[4] http://zeroscience.mk/files/wafreport2013.pdf
[5] http://www.itwire.com/business-it-news/security/60604-seek-goes-for-imperva-to-protect-data

CloudFlare – WAF, CDN, Managed DNS and DDoS Mitigation for the People



Since their launch at TechCrunch 2010, CloudFlare has burst onto the security scene as a disruptive innovator and effective element of online protection. As an inexpensive bundled security provider, CloudFlare competes with Incapsula for budget-conscious small and mid-sized companies. CloudFlare originated as a reverse proxy and DNS change service. By operating in conjunction with a community-based DNS System, CloudFlare can prevent harmful attacks while optimizing load speed. CloudFlare has surged in popularity, thanks in part to offering its core services for free. However, this 'opening of the gates' has left some businesses uncomfortable about sharing IP's with unsavory content.

Specialization:

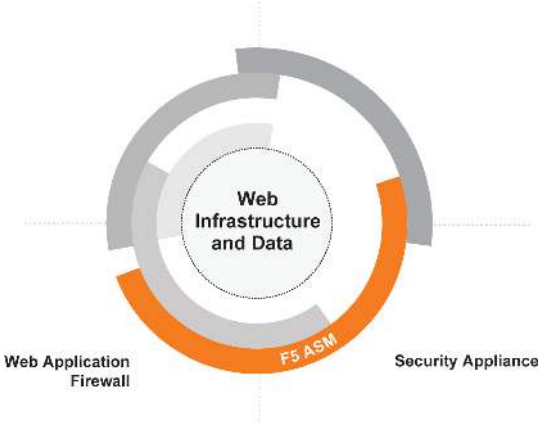
- Highly affordable security services for even the smallest webhosts
- CDN integration may have associated improvements (faster load times, increased server availability)
- Community intelligence offers collective benefits

Limitations:

- Potential downtime due to route leakage[6]
- Cloud-only deployment model means that any issues with the CloudFlare network can lead to problems on your website
- Limited reporting for attack data
- Requires Full DNS control and management
- False positives can block legitimate traffic

[6] https://blog.cloudflare.com/route-leak-incident-on-october-2-2014/

F5 Networks – Application Delivery Networking and Security Appliances for Onsite Protection



Known for popularizing network load-balancing with the BIG-IP product line, F5 Networks has been at the forefront of network appliances since its foundation in 1996. BIG-IP systems are deployed at thousands of Enterprise and Fortune 100 companies. F5's expanded series of modules for BIG-IP include a number of security focused add-ons. Most notable are the Application Security Manager (ASM) products, which are often bundled with Advanced Firewall Manager as BIG-IQ Security. ASM includes a robust Web Application Firewall and offers policy-based application security to help mitigate HTTP-based attacks. The modularity and on-site availability of these security products explain their obvious appeal for companies with large IT workforces. For extensive operations where transparency is essential, F5's security appliances offer tailored server support.

Specialization:

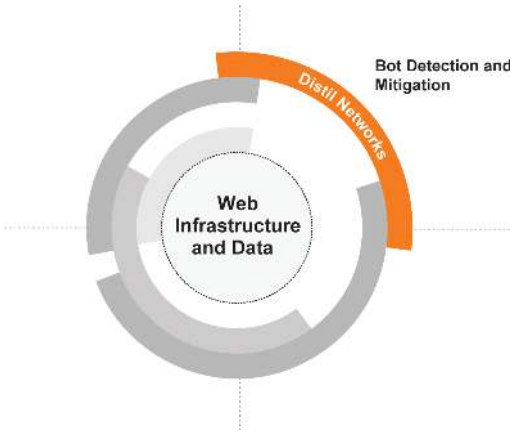
- Considerable experience with providing security solutions for large Enterprise customers
- Strong reputation as the leading load-balancing appliance on the market
- Web Application Firewall and DDoS mitigation services deeply integrated with load balancing core
- Web application focused security for Layer 7 protection
- Robust policy engine for swift and simple rule deployment

Limitations:

- Big-IP appliances are designed with corporate networks and data centers in mind, not the cloud
- Appliance can only be at one place at one time – scaling infrastructure requires additional appliances
- Product cycle confusion makes it difficult to determine the right modules for a particular infrastructure
- Issues with ease-of-use and startup documentation[7]
- Static IP-based security less effective against widespread attacks that come from multiple IPs or on Network Address Translated networks.

[7] http://www.scmagazine.com/f5-networks-big-ip-application-security-manager/review/3582/

Distil Networks – Dedicated Bot Experts



Distil Networks was founded in 2011 and from the outset concentrated on eliminating the malicious bots that are the root cause of many modern attacks. Since its inception, Distil has been at the forefront of anti-bot solutions, focused on identifying, tracking and mitigating bot attacks. To this end, Distil has developed industry-leading fingerprinting algorithms to instantly identify bots along more than five dozen data parameters. Fingerprints stick to a bot even if it attempts to reconnect from randomized IP addresses, or hides behind an anonymous proxy. By using these unique ID's in coordination with a globally updated Known Violators Database, Distil has immediate recognition and mitigation capabilities. With integrated machine learning techniques, Distil can automatically pinpoint behavioral anomalies specific to each domain.

Specialization:

- Easy and accurate defense against malicious bots without impacting legitimate users
- Solution can be deployed as a Cloud CDN or on-premises appliance
- Seamlessly integrates with enterprise CDNs and dedicated DDoS mitigation solutions
- State-of-the-art detection and mitigation neutralize emerging bot threats: web scraping, data theft, adaptive malware

Limitations:

- Singular focus on bot detection and mitigation may not make sense for SMBs with limited budgets looking for "all-in-one" protection from a single vendor
- Absorbs bot-driven application layer attacks, but not suitable for volumetric DNS-level DDoS attacks
- Threat prevention model does not include WAF capabilities such as monitoring for coding errors

Assembling Your Defense in Depth Infrastructure - Incorporating the Essentials

Defense in Depth constitutes a comprehensive, multi-point security architecture that actively addresses prevalent online conditions. Every business faces a wide range of online threats and must constantly deal with a variety of attacks. In order to secure network infrastructure, protect intellectual property, and avoid costly data breaches, companies should adopt a Defense in Depth strategy that deploys specialized security vendors in their most effective roles. By leveraging the core competencies of the vendors examined in this paper, a company can be confident in their ability to respond to any assault.

A company that chooses Akamai as their CDN provider is assured of premier quality global delivery services, and a basic level of overall security. With Akamai's massive server base and Prolexic technology, they remain the industry leader for volumetric attack prevention. Alternatively, cost-conscious entities might select CloudFlare and obtain a substantial measure of security and data optimization benefits, for a fraction of the cost.

While CDNs offer associated security services, for secure coding measures, organizations should seriously consider layering additional WAF protection. Imperva has pioneered easily integrated WAF services, capable of blocking many common attack vectors. Companies with major IT infrastructure often choose to rely on F5 Networks to provide onsite protection through their popular ASM products. These security appliances offer extreme customization and transparency, enabling strategic control over enterprise security.

Finally, the rising sophistication of malicious bots has necessitated the reevaluation of bot related security measures. DDoS mitigation systems are ill-prepared to deal with threats beyond volumetric attacks, such as web scraping, data theft, and adaptive malware. Distil Networks provides essential bot defenses that are crucial to long-term online security. As bot attacks become increasingly severe and damaging, it is imperative that companies not neglect this layer of security.

The New Bot Horde – Preparing for Emergent Attacks

Due to the prevalence of under-secured networks, the potential pool of bot-susceptible systems is immense and growing. The relative ease of initiating a bot attack, and the relative lack of legal consequences, has interested parties across the globe. The economic model for attacks has shifted from ‘lone intruder’ to ‘corporatized criminal enterprise’. And the scope of attacks has expanded beyond simple denial of service assaults, now incorporating data-scraping, network disruption, private file access and system surveillance. Malicious bot services can be hired online and immediately put to these tasks. Meanwhile, beneficial bots such as Googlebot perform necessary tasks, but create false positives and confusion for Web Application Firewalls and Proxy services. In order to combat these alarming trends, companies should reinforce their security strategy with the addition of proactive bot detection and mitigation.

The Changing Threat Landscape

Though media attention tends to focus on denial of service attacks (DDoS) with sensational attack metrics, perhaps the more alarming threat lies in the emergence of advanced bots with adaptive behavioral patterns. These bots are capable of more accurately mimicking human users, and constitute a serious risk of infrastructure penetration and data capture. Even protected information is susceptible to concentrated scraping offensives. Bot-orchestrated breaches are increasingly common as criminal networks leverage computing power for illicit gain.

Along with the proliferation of bot attacks, the severity and damage of these attacks has similarly increased. Where earlier bot attacks were largely regarded as a nuisance, today’s bot attacks can paralyze website infrastructure, pirate entire online directories, and destroy a company’s competitive advantage. Click fraud and spam services can ruin a brand’s image and seriously impede customer loyalty. Web developers and security personnel using IP-centric network security tools as bot prevention systems are locked in a reactive cycle of detection and response, while their entire network hangs in jeopardy. This siege-mentality can overtax internal IT teams, degrading system responsiveness and disrupting traffic control. Any company without proactive bot detection and mitigation risks leaving its online presence in the hands of criminals.

While no aspect of data security should be overlooked, the dramatic increase in scale, scope and sophistication of modern bot attacks requires a rethinking of overall strategy. In addition to traditional defensive measures such as CDNs, WAFs, DDoS mitigation and security appliances, companies must attend to the increased threat posed by malicious bots. While the task can be overwhelming for ordinary IT Departments, specialized vendors have risen to the challenge, assembling the necessary technology and intelligence to combat the growing bot threat. By integrating bot-centric layers into a Defense in Depth strategy, corporations can better protect their invaluable data assets.

About the Author

Ernie Regalado drives telecommunication innovation as a technology analyst (formerly of Gigaom Research) and consultant for the CDN Industry. As the founder of Bizety.com, his research and insights reach thousands of global entrepreneurs and executives. Ernie's approach focuses on growing business value through game-changing strategies. During his 20 years in the infrastructure technology field, he has helped hundreds of the Fortune 1000, mid-market, internet, E-commerce, media and entertainment companies in developing revolutionary solutions. He is a recognized CDN expert, with deep knowledge in video streaming, small/large file delivery, e-commerce, information security, sales management, business strategy, marketing and product development.