THREATS AND MITIGATIONS

A GUIDE TO MULTI-LAYERED WEB SECURITY

Akamai
FASTER FORWARD

TABLE OF CONTENTS

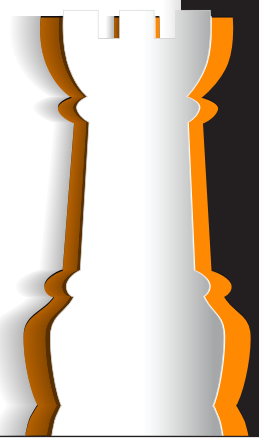
INTRODUCTION - Out of the Fortress and Into the Fire

WHY SHOULD I READ THIS GUIDE?

The data center perimeter is dead. But its memory lives on in the way many IT departments continue to secure their infrastructure. The meteoric rise of the Internet brought with it an ever-changing landscape of new attacks and completely disrupted organizations' old models of guarding their IT infrastructure. Previously, information assets that needed protection all resided in a fortress that IT controlled, namely a secured data center. Attacks typically came from outside the data center's four walls or from insiders abusing their privileges. Companies placed protections, such as firewalls, at the border crossings and guarded against inside attacks through strict roles and access privileges.

Websites and applications, however, increasingly live outside the data center in the cloud.

How can you protect a perimeter that no longer exists? First, you need to understand which of your assets are most at risk and determine your company's tolerance for risk. Then you need to manage that risk by extending security controls to the cloud and by guarding against the types of attacks that occur over the Internet.This guide will detail the threats common to websites and web applications and what you can do to mitigate them.



CHAPTER 1
Looks at the types of security threats you'll face online.

CHAPTER 2
Describes components necessary to secure websites and applications.

CHAPTER 3
Explores the types of solutions available.

CHAPTER 4
Talks about what to look for in a web security solution.

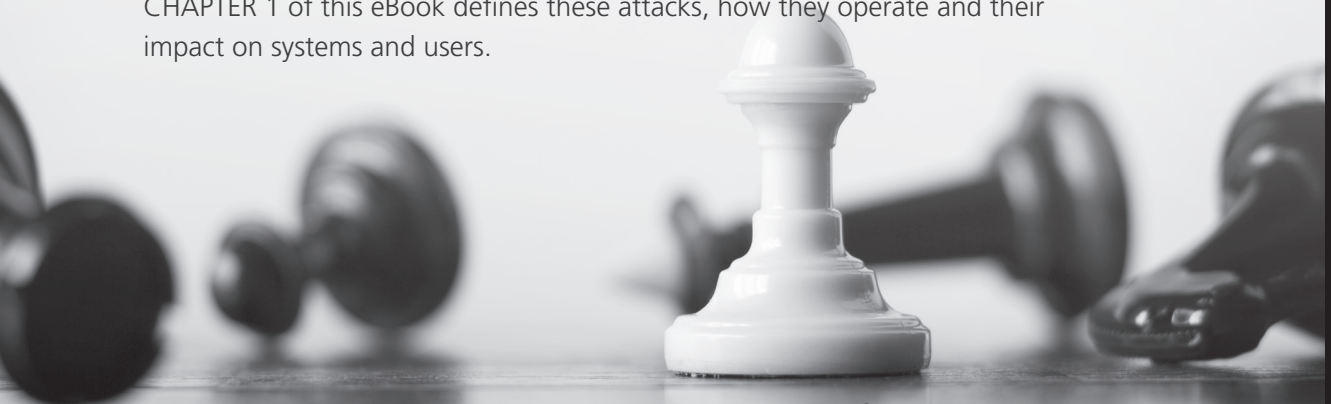
CHAPTER 5
Details what you can do to minimize vulnerabilities in your websites and applications.

Defining **TODAY'S WEB THREATS**

With the skyrocketing popularity of websites and web-based applications has come a corresponding explosion in the numbers, types, magnitudes, and costs of attacks that specifically target the vulnerabilities of these systems. Generally, these attacks fall into two categories:

- Denial of Service (DoS) / Distributed Denial of Service (DDoS)
- Hacks that steal data, such as SQL injection and other command injection attacks

CHAPTER 1 of this eBook defines these attacks, how they operate and their impact on systems and users.



COST OF CYBER CRIME

Ponemon Institute, October 2013

$1,288,710
Minimum

$11,559,057
Mean

$58,094,571
Maximum

The most costly cyber crimes are those caused by denial of service, malicious code and web-based attack. These account for more than 55% of all annual cyber crime costs for organizations.

LINK ▸

DoS/DDoS
Attacks Against the Network

DoS attacks are among the most common threats to Internet operations. These attacks saturate network bandwidth to make the network unavailable to its intended users. They involve blasting a site with enough traffic to flood the connections between the Internet and the business. Often multiple nodes are used to send traffic to a site in a distributed denial of service (DDoS). DDoS attacks reduce the amount of traffic that any one attacking system needs to send while increasing the impact on the target.

A mind-boggling array of DoS and DDoS attacks occur at the network layer. These can be grouped into two broad categories: simple flooding and amplification attacks. Several tools are available that automate the process of creating both types of attacks, allowing people with no technical background to quickly and easily threaten their choice of website.

THE EXPLODING SIZE OF DOS/DDOS ATTACKS

Ponemon Institute, October 2013

The size of volumetric DoS and DDoS attacks has been growing exponentially.

One of the first publicly documented DoS attacks took place in September 6, 1996 against Panix, a New York City ISP. Unidentified attackers used a SYN flood to exhaust available network connections and prevent legitimate users from connecting to Panix servers. The attack used three computers to generate 48 Kbps of network traffic.

In contrast, a hacktivist organization known as Izz ad-Din al-Qassam Cyber Fighters (QCF) launched a series of attacks against US financial institutions that began on March 5, 2013 and used 3,200 bots to generate 190 Gbps of peak network traffic.

Akamai predicts that by 2020 the average DDoS attack will generate 1.5 Tbps of network traffic.

Patrikakis, Charalampos, Masikos, Michalis, Zouraraki, Olga (Dec 2004). Distributed Denial of Service Attacks. The Internet Protocol Journal – Volume 7, Number 4. Retrieved from http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

Litan, Avivah (Mar 2013). Are the ongoing DDoS attacks against U.S. banks just the calm before the storm? Gartner. Retrieved from http://blogs.gartner.com/avivah-litan/2013/03/14/are-the-ongoing-ddos-attacks-against-u-s-banks-just-the-calm-before-the-storm/

Who is Launching DoS/DDoS Attacks and Why?

To secure your infrastructure strategically, you need to understand who's most likely to attack you and what tactics they'll use. Various types of adversaries include:

- **EXTORTIONISTS** - Extortionists threaten to (or do) disable a website and then demand ransom money to prevent (or halt) an attack.
- **EXFILTRATORS** - Exfiltrators use a DoS attack to divert attention from their real objective—stealing data they can monetize, whether that's intellectual property or credit card numbers.
- **HACKTIVISTS** - Hacktivists are different than other types of attackers. They are angry and seek to make a political statement or shine a spotlight on a cause. Their attacks can seem random and are often incited by a particular news story. But they are angry at you, which means that when they run into your security controls they're unlikely to back off and find an easier target. Sometimes, hacktivists are used as a scapegoat, allowing other types of adversaries to hide behind their politically based attacks.
- **COMPETITORS** - Your competitors may disable your site to gain an advantage; or they might screen scrape information on your site, for example, to determine and beat your pricing.

◀ Back to Table of Contents

If your company has been the target of a DDoS attack, there's a 1 in 4 (25%) chance that you'll be attacked again within 3 months and greater than a 1 in 3 (36%) chance you'll be targeted again within the year.

- Akamai Research

In 2013, half of all companies responding to a recent Ponemon Institute survey had experienced a denial of service attack, a 29% increase over 2012.

DoS attacks represented 21% of the total annualized cost of cyber crime.

2013 COST OF CYBER CRIME STUDY: United States

Ponemon Institute, October 2013

LINK to Report ▸

"If you know your enemies and know yourself, you will not be imperiled in a hundred battles... if you do not know your enemies nor yourself, you will be imperiled in every single battle."

Sun Tzu, The Art of War

Simple Flooding

Most DoS attacks flood the network or infrastructure. Floods take advantage of specific protocols, such as TCP, ICMP, or UDP to send large numbers of requests to a target and overload network capabilities.

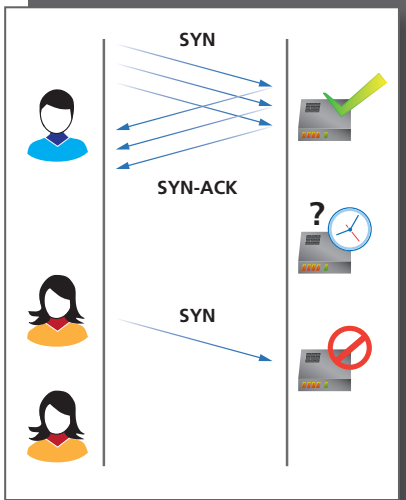
Some of the ways DoS attacks can wreak havoc include:

- Consuming network bandwidth
- Overwhelming available computational resources, memory, disk space or processor time
- Disrupting configuration information, such as routing information
- Interrupting state information, for example by resetting TCP sessions

DNS Flooding Attacks

DNS has become a favorite target for DoS flooding attacks. DNS maps domain names that a human can understand to the IP address computers use to find the resources they need. Whenever you access a website, a DNS server looks up the IP address for the domain name. DNS servers come in two types: authoritative servers that contain a database of IP addresses and recursive servers that query the authoritative server on behalf of the client. Many organizations deploy only a small number of DNS servers. This makes DNS especially vulnerable to volumetric attacks. When attackers flood DNS, they needn't take down any web servers. Instead, they take the DNS server offline, which prevents users from finding the websites they're looking for.

Anatomy of a Simple Flooding Attack



TCP SYN flooding is a popular example of a simple flooding attack. In TCP SYN flooding, the attacking system sends a TCP SYN request with a spoofed source IP address to a host. While these TCP SYN requests look legitimate, the spoofed address refers to a client that doesn't exist so the final ACK message is never sent to the victim host. The result is half-open connections at the victim site. A backlog queue stores these half-open connections, which bind the server's resources so that no new legitimate connections can be made, resulting in Denial of Service.

Amplification Attacks

Attackers are constantly looking for ways to increase the size of floods. Two commonly used methods of amplifying attacks take advantage of the DNS and NTP protocols:

DNS Reflection and Amplification Attacks

Three characteristics of DNS servers leave them particularly vulnerable to reflection and amplification attacks:

- Some recursive servers answer queries from any client.
- DNS relies on the Universal Datagram Protocol (UDP), a connectionless protocol that doesn't validate source IP addresses,which makes these addresses easy to forge.
- A small DNS request can solicit large amounts of data in a response.

To conduct an attack, an adversary sends a set of DNS queries to the recursive server, altering the source address on the requests to that of the chosen target. The requests are designed to have a much larger response, directing about eight times as much traffic at the target as they receive. For more information on Distributed Reflective Amplification Denial of Service (DrDoS) attacks, refer to the case study in Prolexic's Q3 2013 Global DDoS Attack. **Report here.**

NTP Amplification Attacks

At the beginning of 2014, NTP-based attacks emerged as an important tool in the DDoS arsenal. NTP is the Network Time Protocol that machines connected to the Internet use to set their clocks. Like DNS, NTP is a simple UDP-based protocol that is prone to amplification attacks because it will reply to a packet with a spoofed source IP address and because one of its built-in commands sends a long reply to a short request. The monlist command, which can be sent to an NTP server for monitoring purposes, returns the addresses of up to the last 600 machines with which the NTP server interacted. If a server responds with the maximum number of addresses, a request of 234 bytes could yield a response of 100 packets for a total of more than 48K—an amplification factor of 206x.

In February of 2014, attackers used an NTP reflection attack to launch one of the largest recorded DDoS attacks ever—just shy of 400 Gbps.

LINK ▸

Lucian Constantin, "Slew of spoofs used in massive, record-breaking DDoS attack," PC World, February 11, 2014.

Tools for Launching DDoS Attacks

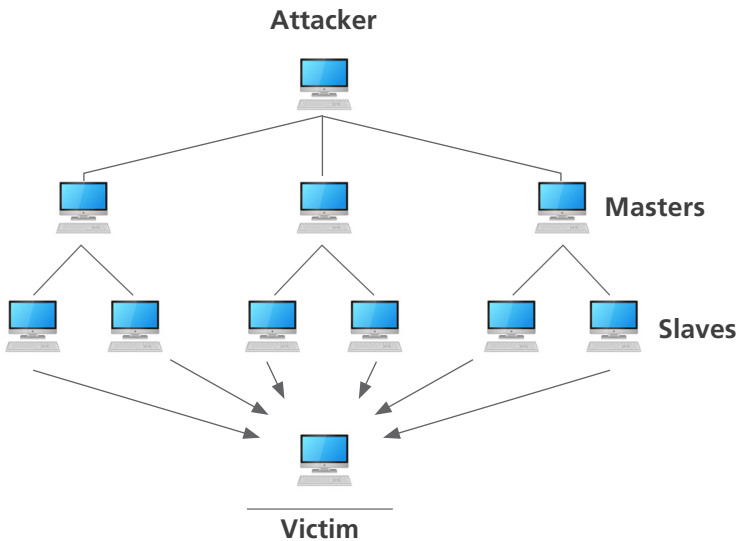
Virtually anyone can launch a DDoS attack within seconds using one of many readily available and easy-to-use tools. These tools can be used to launch both simple flooding and amplification attacks.

Botnets

A botnet is a collection of PCs infected with malware and controlled centrally by a botmaster. The botmaster directs these slave machines using a command and control server—a central location from which infected machines receive instructions. Infected machines in a botnet can easily number in the thousands or tens of thousands. The botmaster can harness all of them to submit as many requests as possible to a single Internet computer or service, overloading it and preventing it from servicing legitimate requests.

Low Orbit Ion Cannon

Low Orbit Ion Cannon (LOIC) was initially developed by Praetox Technologies as an open source network stress testing tool and was later released into the public domain. LOIC makes mounting a DoS attack quick and simple. The software gives a potential attacker an intuitive graphical user interface. The hacker uses the GUI to enter a URL, choose an attack method (TCP, UDP, HTTP), and submit the request. It takes all of 60 seconds to download the tool and use it



A botnet attacks its victim

LINK

to open multiple connections to the target server and send a continuous sequence of messages. This tool was the weapon of choice for the infamous hacker group Anonymous, who claimed responsibility for attacks against Sony, the FBI and other US security agencies. LOIC was also used in highly publicized attacks against PayPal, MasterCard and Visa.

High Orbit Ion Cannon

High Orbit Ion Cannon (HOIC) is a powerful upgrade to LOIC. Instead of repeatedly sending out a single visit to a site from a fake user, HOIC targets sub pages. HOIC's fake users visit the welcome pages, help pages, article pages and anything else on a victim site. This tactic prevents some firewalls from recognizing what is happening as an attack. Even if the firewall does figure it out, it'll have trouble shutting the connection because HOIC sends multiple fake users to multiple pages within a domain. A threat report on HOIC can be downloaded from **Akamai's website**

Brobot

Operation Ababil, a DDoS initiative believed to have been perpetrated by the hacktivist group Izz ad-Din al-Qassam Cyber Fighters is using a modified Russian script toolkit known as Brobot to target U.S. banks. The group identifies vulnerable software extensions on computers linked to high-bandwidth websites and web-hosting data centers. It then compromises and controls these

ECONOMIC DDOS

When a cloud service provider hosts your application, the cloud infrastructure can expand to handle bursts of traffic during a DDoS attack. Typically you pay for the bandwidth you use. If a DDoS attack consumes significant resources, your servers may stay up—but you may not be able to afford to keep them running. The cost of CPU or bandwidth in hosted environments, such as Amazon Web Services, can be massive.

computers by inserting near-invisible embedded code into the extensions' HTML. These high bandwidth botnet slave computers can then bombard banks' websites with DDoS attacks as powerful as 190 Gbps. A threat report on the itsoknoproblembro toolkit with detection rules to identify infected web servers (bRobots) can be downloaded from **here**

The Top 10 DDoS Trends for 2013

2013 set a record in distributed denial of service (DDoS) attack activity, as shown in this DDoS trends infographic.

Compared to a year earlier, DDoS attack volume increased 32 percent according to Prolexic research.

DoS/DDoS
Attacks at the Application Layer

The network layer is no longer the only target of DoS attacks. Increasingly popular application layer attacks look like legitimate requests yet cause denial of service by exhausting the capabilities of the web application servers. These attacks may cause the server to use significant computing resources for each request, perform sub-optimally, or return different results for each request to avoid caching on the server.

High-Bandwidth Attacks

High-bandwidth application-layer attacks typically bombard resource intensive pages with either GET or POST requests and reset the connection over and over to exhaust the server's session and memory capacity. Alternatively, they make complex, compute-intensive requests or ask for large files from the website, such as PDFs. The result is overconsumption of resources that effectively knocks down servers to prevent them from responding to legitimate traffic. Examples include attacks that:

Akamai customers reported

768 application-layer attacks in 2012 and 1153 in 2013, a 50% increase year over year.

For more information see Akamai's State of the Internet Report: http://www.akamai.com/stateofthe internet/

LINK ▸

Veracode predicts

that three out of four companies will be targeted at some point by web application exploits and that web applications represent 54% of the total hacking based data breaches.

DuPaul, Neil (July 2013). The Real Cost of a Data Breach Infographic. Retrieved from http://www.veracode.com/blog/2013/07/the-real-cost-of-a-databreach-infographic/

- **Exploit SSL** – The traffic for some pages, such as the login page, must be encrypted using SSL to protect user credentials in motion. It takes nine steps to establish an SSL handshake, many requiring complex cryptographic and key generation operations. If an attacker uses a botnet to establish numerous SSL sessions simultaneously, the application becomes unavailable because the system gets hung up processing previous requests.
- **Overwhelm the database** – A database driven page such as a store locator needs to hit the database for every request. That typically involves a large number of different or complex database transactions as well as field level validation and other techniques for defending against other application layer attacks. Sending such requests repeatedly will overwhelm the database server.
- **Attack a form page** – Form pages need to access a database with every request. Attackers can cause unnecessary database processing, for example, by using random numbers in place of real zip codes or by submitting huge passwords.

Low-Bandwidth Attacks

Many application-layer attacks exploit the hacker's knowledge of the application and how to break it. These attacks can be far more efficient than blasting the network because they require far fewer attack nodes and less bandwidth. Moreover, because attackers often take advantage of legitimate application features, it's not always obvious what's an attack and what's legitimate traffic. This makes defense considerably harder.

Some examples of low-bandwidth attacks include those that keep resources open and shopping cart attacks:

Attacks that Keep Resources Open

Some attacks keep resources open on the server to exhaust server connection pools and resources. This approach is far more efficient than the GET flood. It requires only hundreds of requests at regular intervals rather than thousands continuously and a single device can knock down a large site. For example:

- **Slowloris** slowly delivers request headers, forcing the webserver to keep connections open without completing the requests. This rapidly exhausts the server's connection pool.
- **Slow HTTP POST** delivers the message body slowly to exhaust web server resources.
- **Slow Read** shrinks the TCP window on the client side.This forces the server to send data to the client very slowly. The server must keep connections and other resources open to ensure the data is sent, which means it can be quickly overwhelmed.

Abuse of Shopping Carts

An attacker might put several items into a shopping cart, abandon it for a while, and then come back and refresh the cart, putting off the session expiration and forcing the database to reload the cart. If the attacker puts large numbers of products in the cart, this consumes substantial resources.

Attacks that Steal Data

While DoS/DDoS attacks render your site unusable, attacks that steal data can also have a direct impact on your bottom line. Organizations face an increasing number of attacks designed to steal data. These attacks usually take advantage of vulnerabilities in web applications and can be difficult to detect because they generate application traffic that appears legitimate to traditional network-layer security tools.

Attempts to steal data are most likely to take the form of Command Injection attacks. With these types of attacks, a hacker injects commands into a vulnerable application. The attacker can then execute these commands to view data, wipe out data, or take over the machine. Injection flaws occur when the application lacks correct input data validation, which allows the attacker to manipulate input to include untrusted data in a command or query. The most common types of command injection attacks include SQL Injection, Remote File Inclusion and Local File Inclusion:

Sometimes DoS attacks work in conjunction with attacks on data, acting as a distraction while the hacker steals data. Dell SecureWorks Counter Threat Unit reported that a popular DDoS toolkit called Dirt Jumper was being used to divert bank employees' attention from attempted fraudulent wire transfers of up to $2.1 million.

Brenner, Bill (August 2013), DDoS Attacks Used as a Cover for Other Crimes

LINK ▸

In one high-profile attack, a hacktivist group used SQL injection to steal information for more than 1.6 million accounts belonging to US government organizations, including NASA, the FBI and the Pentagon.

VII. Newton, Casey (Dec 2012). GhostShell claims breach of 1.6M accounts at FBI, NASA, and more. Retrieved from http://news.cnet.com/8301-1009_3-57558338-83/ghostshell-claims-breach-of-1.6m-accounts-at-fbi-nasa-and-more/

SQL Injection

SQL Injection takes advantage of improper coding of web applications to allow hackers to inject SQL commands into, say, a login form to allow them to directly query the data held within a website. Features such as login pages, support and product request forms, feedback forms, search pages and shopping carts are all susceptible to SQL Injection attacks.

Remote File Inclusion

Remote File Inclusion (RFI) is a website vulnerability that allows an attacker to use a script to include a remote file on the web server. This permits the hacker to do everything from executing code on the web server for temporary data theft to taking over a vulnerable server.

Local File Inclusion

Local File Inclusion (LFI) is similar to a Remote File Inclusion vulnerability except instead of including remote files, only local files, i.e. files on the current server, can be included.

Account Checker Attacks

Account checker is another popular attack that targets customer data. These attacks occur when cybercriminals use automated attack tools and scripts called account checkers to determine valid user ID/password combinations. Once the account is breached, the attacker collects the user's personal data and credit card information to use in further fraud. Attackers hide their attacks by cycling through a list of open proxies. Account checker attacks can also cause a DDoS condition when the attacker fails to properly configure their tools; the tools will try user-names and passwords as quickly as possible, overloading target servers.

DNS Attacks

DNS is a weak link in web security. In addition to DDoS and amplification attacks, DNS is subject to threats that include registrar hijacking and redirection/cache poisoning.

Registrar Hijacking

The domain name registrar manages the reservation of Internet domain names. Registrar hijacking attacks use social engineering against the registrar's customer support staff. If an attacker can use a phishing attack to compromise an organization's account with their registrar, it gains control over the domain name and can point it to servers of their choice, including name servers, web servers, email servers and so on. The domain could even be transferred to a new owner.

Redirection/Cache Poisoning

In DNS redirection attacks, the attacker redirects queries for DNS names to servers under the control of the attacker by advertising a false routing protocol to redirect traffic to the attacker's servers. Alternatively, attackers pollute the cache of a DNS server with erroneous DNS data that directs future queries to servers under the attacker's control.

In the third quarter of 2013, the Syrian Electronic Army (SEA) a hacktivist group that supports the regime of Syrian President Bashar Hafez al-Assad, claimed credit for launching a series of phishing attacks against the DNS registrars of multiple enterprises. One such attack compromised an administration account for a third-party content discovery engine. As part of the attack, malicious code was injected into content served to customers. These attacks allowed the SEA to redirect traffic for legitimate domains to one they controlled. Any visitor to an affected website was sent to syrianelectronicarmy.com, a propaganda page for the SEA.

Akamai Q3 2013 State of the Internet Report

LINK ▸

AKAMAI PREDICTS THAT **BY 2020**, THE AVERAGE DDOS ATTACK WILL GENERATE

1.5 TBPS

OF NETWORK TRAFFIC

CHAPTER 2

A Multi-Layered Approach to **SECURING WEB APPLICATIONS**

DoS/DDoS attacks targeting the network layer and the application layer use different techniques. Your company needs to defend against both. Whatever tool you use, your company needs to take a multi-layered approach to secure web applications from denial of service attacks and data theft. Efforts to minimize application vulnerabilities will protect against both application-level DoS attacks and attempts to steal data.

Defending against **DoS Attacks at the Network Layer**

Defending against network-layer DoS attacks demands a two-pronged approach. First, you need enough network bandwidth to easily deal with massive amounts of traffic. You also need a way to filter attack traffic to allow legitimate traffic through while discarding attack traffic.

Protecting Applications from **DoS Attacks and Data Theft**

You can eliminate many application-layer vulnerabilities by practicing good web-application hygiene and using a secure software development lifecycle. For example, you should harden each application through secure configuration and timely updates and patches. Developers should keep security in mind throughout the application requirements, architecture and design phases. They should also build security protections into the software such as providing sufficient input validation to make sure the application can't be attacked using command injection techniques. All configurations and applications should be tested thoroughly for vulnerabilities. For more information on how to ensure good web application hygiene, **see Chapter 5.**

Internet hygiene, however, is rarely perfect. It makes sense to guard against any unprotected vulnerabilities by also using a Web Application Firewall. The WAF can provide virtual patching; you can program rules into the WAF to protect against new vulnerabilities until your IT staff can apply the actual patch. The WAF also delivers another line of defense against both threats to data (such as SQL Injection attacks that take advantage of application layer vulnerabilities) and application-layer DoS attacks (such as Slowloris-type session manipulation). Of course, a lone WAF is as likely as any other device to be overwhelmed by a DoS attack; this means the WAF also needs anti-DoS capabilities and architectural protections to shield it from brute force attacks. For more information on what to look for in a WAF, **see Chapter 4.**

Exploring
YOUR OPTIONS

Security solutions aren't one-size-fits-all.

It's important to understand your assets and your risks and find the right solution for your company. Commercial solutions are available to help with the various aspects of web-application security described in Chapter 2 of this guide. These include on-premises hardware and Cloud-based services.

On-Premises Hardware

Most organizations rely on hardware, installed on-premises in their data centers, such as network firewalls, DDoS mitigation and a WAF to stay secure. Installing and implementing these on-premises devices requires large up-front capital expenditures with a typical hardware lifecycle and depreciation of two-to-three years. With the current skills shortage, hiring experts with the right skillsets to successfully use this hardware to mitigate these attacks can be costly and difficult.

Defending against application-layer attacks can be resource-intensive. WAFs require large amounts of computing resources and processing, which can reduce performance.

Most devices represent a single point of failure; they can't absorb DDoS attacks without failing. Moreover, by definition on-premises hardware attempts to stop a DDoS attack only after it's entered the data center. This presents a single point of failure against one of the most prevalent security threats out there. Furthermore if your organization doesn't have a sufficiently large Internet link, the attack will saturate the available bandwidth causing an outage for the entire data center. Alternatively, an attack can bring down other data center infrastructure such as routers, network firewalls or load balancers. Even when the solutions defend against attacks, bandwidth-intensive attacks may degrade the performance for legitimate users. As the scale of DDoS attacks grows, organizations will have to continue provisioning additional bandwidth to ensure sufficient scale; if they have multiple data centers, costs can increase exponentially.

Cloud-Based Services

Cloud-based services live outside of a company's data center in order to secure traffic before it reaches company infrastructure. There are two primary types of Cloud-based anti-DoS/DDoS services: those that route suspicious traffic to a centralized location where malicious traffic is filtered out, and Website Protection Services that utilize Content Delivery Networks (CDNs) to absorb and inspect malicious traffic across a distributed network of servers to shield company websites and applications.

DDoS Mitigation Providers

DDoS Mitigation Providers operate "scrubbing centers" that use a mix of equipment, technical rules and direct human interaction to provide protection against DoS & DDoS attacks. These private data centers are equipped with high bandwidth to process inbound floods and keeps sites available.

These companies provide some of the most comprehensive protection against DoS/DDoS attacks, as they handle all types of attacks from simple floods to those that take advantage of HTTP/S, FTP and other non-web applications.

These services operate either "**always-on**" or "**on-demand**."

- **Always-on services** continually monitor your traffic for suspicious activity that indicates an attack. Always-on mitigation is like a shock absorber that protects the customer from taking that first big hit on their network when a DDoS attack strikes — and consequently provides stronger protection against costly site downtime.
- **On-demand options** offer better performance and greater affordability. Using standard IP routing protocols, it is simple to intercept incoming traffic and inspect it for anomalies using out-of-band mitigation services. Outgoing traffic is not inspected, but allowed to take its normal path. Legitimate traffic is identified and forwarded-on while malicious attack traffic is dropped or "scrubbed."

Both types of services have potential issues to consider. Always-on SOC services are more expensive; and, continuous traffic inspection further degrades site performance. When using an on-demand solution your company must determine when to

activate the service, and contact the vendor to activate the service. On-demand solutions are also unable to detect attacks that occur over time, such as SQL Injections. This leaves organizations exposed to attacks focused on data theft or brand damage.

Website Protection Services

Website Protection Service providers utilize CDNs to provide network- and application-layer security for websites and applications. As a cloud-based proxy, these networks sit in front of your IT infrastructure and deliver traffic from your end-users to your websites and applications. The cloud platform examines network traffic for known attack patterns and passes only legitimate traffic to the web app.

These solutions operate inline so your organization is protected at all times without any human interaction. They can mitigate attacks that are new and not seen previously. Some services include WAF technology and protect against application attacks such as SQL injection.

CDNs by their nature are built with a distributed architecture – that is, they are comprised of servers located across the world. For a DoS attack to succeed, it would have to target and overwhelm every one of those servers simultaneously. CDNs are specifically built to handle large volumes of traffic, making this a difficult task for attackers. At the same time, these solutions offer acceleration services to simultaneously reduce performance impact and improve the end-to-end performance of the web application.

A potential problem for CDNs is that some of these solutions come from smaller vendors that don't have the infrastructure required for either global protection and/or protection from large DDoS attacks. In recent years several vendors experienced major outages and customers were affected by large DDoS attacks against other customers. Limited or no customer support may also leave customers managing their own attack response. In addition, some CDNs do not include WAF technology, and some that do may not provide sufficient protection against many application layer attacks.

CHAPTER 4

How to Choose **A SOLUTION**

Every business is different. You need to find the right solution for yours. This section is a guide to help you ask the right questions so that you can make the right decisions for your organization.

Guarding Against
DoS and DDoS Attacks at the Network-Layer

Defending against volumetric DoS attacks occurring at the network layer requires a resilient network architecture that can absorb large blasts of traffic and that filters all traffic so that only web traffic is permitted onto the network. The following are key considerations:

Does it offer positive protection?
Many DDoS attacks at the network level can be stopped by only allowing legitimate HTTP traffic onto the network (e.g. Port 80 (HTTP) or Port 443 (HTTPS)). The solution should drop all other non-application traffic, such as Excessive TCP SYN Packets, floods of ICMP packets or UDP packets without application payloads.

Does the solution absorb all attack traffic?
Not all attacks target web applications or services. Some will attempt to sneak in through FTP or non-web ports. For comprehensive protection, look for a solution that can evaluate all of your traffic.

Is the solution always on?
Security controls only protect your website or application if they are up and running. You need to determine the availability level promised by the solution and how it's delivered. Do you need to purchase multiple redundant versions of a security control to ensure availability? Does the solution provider guarantee availability with a service level agreement?

IDG Research found that it takes an average of ten hours before a company can even begin to resolve a DDoS attack. On average, a DDoS attack isn't detected until 4.5 hours after its commencement, and an additional 4.9 hours passes before mitigation can commence. With outage costs averaging $100,000 per hour, a DDoS attack can cost an Internet-reliant company $1 million before the company even starts to mitigate the attack.

Source: http://www.infosecurity-magazine.com/view/35238/a-ddos-attack-could-cost-1-million-before-mitigation-even-starts

LINK ▸

Does the solution deliver scalable bandwidth to handle the volume of the attack?
A garden variety DDoS attack might produce the amount of traffic a site normally receives in two years. To keep the site available, the solution needs to handle all that traffic. While you may not be able to purchase enough capacity on your own because it will go unused most of the time, many cloud service providers give you access to the extra bandwidth you need to absorb an attack when you need it. Ask the provider what peak flows it can accommodate.

Does the solution thwart economic DDoS attacks by capping fees for peak traffic?
When cloud service providers furnish additional bandwidth to thwart a DDoS attack, they often charge for all the extra traffic. Thus even if your cloud service provider is capable of protecting your site, you may not be able to afford the cost of doing so. Look for a service provider that caps service fees.

Does the solution stop attacks before they reach your data center?
Consider the potential impact of an attack on your entire data center. Cloud solutions are designed to stop an attack before it ever reaches your data center. This means you need not be concerned about DDoS attacks impacting your data center. In contrast, on-premises devices protect you once the attack reaches the device, which means the attack will invade your data center. If you have an on-premises solution, you'll need to provision enough resources throughout your data center infrastructure (network bandwidth, routers, and firewalls) to withstand an attack.

DDoS attacks have become one of the most common triggers of data center outages, causing 18% of those experienced at the 67 U.S. data centers that participated in a December, 2013 study by Ponemon Institute. When Ponemon first polled data centers on outages in 2010, DDoS attacks accounted for just 2% of outages.

Source: http://www.networkcomputing.com/next-generation-data-center/news/servers/ddos-attacks-wreak-havoc-on-data-centers/240164503

LINK ▸

Does the solution impact performance?
Ecommerce and media streaming applications demand excellent performance. Yet many security controls require a tradeoff between security and performance. For example, a web application firewall examines all application traffic from every user to the application. The more traffic and the more attack types, the more rules you need and the more hardware is necessary to process packets without compromising performance. To maintain good performance, look for a solution that's architected for both performance and security.

Is the solution inline?
Inline solutions work continuously to monitor and protect against attacks, whether you're aware of the attacks or not. However, to reduce the impact of security controls on performance, some organizations choose an out-of-band solution that only swings into action once you realize an attack is underway. These out-of-band solutions won't proactively prevent an attack from impacting your systems. And because they are not always available, these solutions also fail to guard against less obvious attacks like malicious code being inserted onto systems to steal data.

What is the total cost of ownership?
Many security managers look at the price of a solution but not the total cost of ownership. When determining TCO, consider the cost of the device, of redundant systems to ensure availability, and of managing the solution. Also weigh the expense of a data breach compared with the effectiveness of the solution in guarding against those attacks.

UK industry analyst firm OVUM recently published a white paper entitled "Delivering Effective DDoS Protection." The author, Principal Analyst, Security, Andrew Kellett noted that not all security solutions are capable of providing the required level of DDoS protection. He recommends that organizations evaluate DDoS mitigation providers against 10 enterprise criteria:

1. **Depth of experience**
2. **Provision of dedicated mitigation network capacity**
3. **Proven ability and global resources to mitigate the Internet's largest and most complex attacks**
4. **Innovation in DDoS mitigation technology**
5. **Human expertise on the front lines of DDoS**
6. **Speed to mitigation and service level agreement (SLA) guarantees**
7. **Mitigation at the SSL layer**
8. **Flexibility of service delivery**
9. **Threat intelligence**
10. **Real-time network visibility**

Guarding Against Application-Layer Attacks

Application-layer attacks require a more nuanced approach than defending against network layer attacks. Many attacks at the application layer, whether they're DoS attacks or attempts to steal data, are based on legitimate traffic. For example, both application layer DDoS attacks and legitimate application transactions start with a simple application request.

Most organizations address these attacks in one of two ways:

1. Close down vulnerabilities in the applications by following a secure software development lifecycle and good Internet hygiene, as discussed in **Chapter 5.**
2. Front-end applications with a WAF.

Our recommendation? Do both.

Of course, a WAF can be targeted and overwhelmed just like any other network component so it needs all the anti-DoS capabilities and architectural protections discussed in the previous section.

You should become familiar with the features and capabilities of your WAF—either an in-house appliance or as a service managed by your ISP—and how the firewall will perform against different types of attack vectors. You should also know what will happen to network performance when you use stateful inspection, such as SYN cookies, versus stateless blocking on your on-premise firewall.

Keep in mind that a firewall will usually offer limited protection against UDP and ICMP floods and no protection against a SYN flood of 2 or 3 Gbps or application-layer attacks.

Firewalls also provide little or no protection against low speed application layer attacks that involve HTTP and HTTPS requests through the firewall. In addition, there is a limit to the protection provided by a cloud-based ISP firewall. Not every type of ISP firewall can handle every type of DDoS attack and certain ACLs can fail, especially if they are deployed on a small number of devices close to your server.

Whether you have an on-premises firewall or use ACLs at the ISP layer, managing firewalls as part of an internal DDoS defense strategy is a challenging process that requires making a lot of complex rule changes during a DDoS attack. By moving all of these complex processes to a cloud-based DDoS mitigation service, you can do away with the time consuming processes of firewall reconfiguration and interfacing with your ISP during a DDoS attack.

Considerations when selecting a WAF include the following:

1. How flexible and comprehensive are the WAF rules?

WAFs perform deep packet inspection of HTTP/S Requests/Responses and their payload to identify and protect against attacks such as SQL injections, RFI and so on. WAF rules examine the formats of requests and addresses and determine whether they match certain patterns that are known to signify an attack. If it identifies these patterns, the WAF flags and/or blocks them. Look for a WAF that offers the following types of rules:

- *Rules that identify known issues*
  Many attacks have been around for a long time and are well defined, such as SQL Injection attacks or requests that come from automated tools that don't use browsers. Most solutions come with rules for well-understood attacks.
- *Rules for emerging attacks*
  Attacks are constantly evolving. No one company with a website can see all the attacks and develop rules to defend against all these emerging attacks. But some cloud service providers see significant amounts of traffic and can therefore detect new types of attacks as they appear, create new rules to diagnose these attacks, and make them available to all their customers globally.
- *Custom rules/virtual patching*
  Organizations should always install new versions and patches of their software. However, these patches must be tested before they can be installed, which can take time. A solution that allows you to create custom rules can serve as "virtual patches" that prevent attackers from exploiting the vulnerability until you're able to put the patch in place.
- *WAF rules for situational awareness*
  In some cases, you don't necessarily want to block a particular activity, but it may become suspicious and require further investigation when combined with other actions. You may want rules in place to alert you to these occurrences. Say you know that a certain eCommerce app has a vulnerability in *basket.php*. While a normal Google search won't arouse suspicion, you may be interested if a web search targets "nurl:basket.php" because the search could indicate that an attacker is looking to exploit the basket.php vulnerability. You should be able to configure the firewall to allow someone who's performed an innocuous Google search through, but block someone who searched on "nurl:basket.php".

2. What types of network layer controls does the WAF offer?

Does the WAF provide network layer controls to allow or restrict requests from certain IP addresses to protect the origin server from application-layer attacks? Look for a WAF that provides the following types of controls:

- *Black lists*

  A negative security model espouses "accept all except that which is explicitly denied." Does the WAF enable you to define a list of IP addresses to be blocked?

- *White lists*

  A positive security model says "deny all except that which is explicitly trusted." Does the WAF support the ability to define a list of IP addresses or IP address ranges to be allowed?

- *Geo blocking*

  Geo blocking filters traffic originating from specific geographic locations to mitigate localized DDoS attacks. Once specific IP addresses are identified, traffic can be blocked or throttled from those IP addresses before it reaches the application. Does the WAF support geo blocking?

3. Does the WAF provide behavioral controls?

Most WAFs block traffic based on particular signatures or rules. But behavior-based WAF rules look at and respond to the behavior of a requestor, an IP address, or a user both in the present and over time. For example, you could write a behavior-based rule to look at how many requests a user is making per given time period and block users who make more than a specified number of requests during that time. You could also block users who make more than a specified number of requests that result in a 404 page-not-found error message.

4. Does it offer origin cloaking?

One back door into a web server occurs when someone knows its IP address and enters it directly. A solution that offers "origin cloaking" shields the website or application server from the Internet, preventing users from directly connecting to it. Instead, the service provider will allow only the origin to directly connect to servers on the provider's own network. Access control lists in the customer's WAF determine which servers are allowed to send traffic to the origin.

Guarding Against DNS Attacks

You can address DDoS attacks against DNS servers and DNS reflection and amplification attacks using the same security controls that mitigate any other network-based DDoS attacks. But dealing with cache poisoning and registrar hijacking requires two additional capabilities:

Does the solution support DNS Sec?
Attackers using cache poisoning/redirection attacks can hijack any step of the DNS lookup process and take control of a session, for example, to direct users to their own deceptive websites for account and password collection. The solution is end-to-end deployment of the DNS Security Extensions (DNSSEC). DNSSEC should be used to digitally sign data to ensure its validity and be deployed at each step in the lookup process to guarantee that the end user is connecting to the actual website or service that corresponds to a particular domain name. To take advantage of DNSSEC you need an internal key management system or a service provider that delivers key management and can serve DNSSEC traffic.

Does the service provider use a trusted registrar?

Many registrars do not have foolproof business processes to guard against phishing attacks that result in the site being moved off the registrar. Look for a cloud-based Web application security provider that offers its own registry services with tight controls to prevent social engineering attacks.

For More on WAFs:

1. **Cloudification of Web DDoS Attacks:**
   https://blogs.akamai.com/2014/04/cloudification-of-web-ddos-attacks.html/
2. **What a web attack looks like to Akamai's Professional Services team:**
   https://blogs.akamai.com/2014/03/what-a-web-attack-looks-like-to-akamais-professional-services-team-lessons-from-the-defense-of-a-rec.html/
3. **A DDoS Checklist:**
   https://blogs.akamai.com/2014/03/a-ddos-checklist.html/

CHAPTER 5

INTERNET HYGIENE:

Common Web Application Vulnerabilities and What to Do About Them

No one security solution addresses every security challenge. You'll need to take a multi-layered approach. The optimal Internet security solutions combine purchased security solutions with internal measures to minimize vulnerabilities in your websites and applications.

What are **the Most Prevalent Vulnerabilities?**

The first step in addressing web application vulnerabilities is to understand where they come from and which are most likely to affect your systems. Vulnerabilities can be found in both custom (in-house developed) applications and those that occur in third party software.

Vulnerabilities in Custom-Built Applications

Organizations that write their own applications are subject to application vulnerabilities through insecure design or implementation.These vulnerabilities are referred to as unknown or application-specific vulnerabilities because they're unknown to hackers before the hacker interacts with the application.

Vulnerabilities in Third-Party Software

While hackers could go after vulnerabilities in custom software, it's far easier to attack vulnerabilities in third-party software.

Most web applications use some off-the-shelf software, such as plug-ins, web forum software, or blog software, that has vulnerabilities. Security researchers discover weaknesses in these popular products, notify the vendor, and then send out a public advisory about the issue.

Anyone, including hackers, can access these publications. Hackers take these known issues and scan the Internet for machines with them, particularly SQL Injection, Remote File Inclusion and Local File Inclusion vulnerabilities. Since administrators and site owners usually take awhile to patch their sites, attackers can always find vulnerable machines.

Recently, hackers have discovered that it makes more sense to take over web servers (rather than user machines) because they have greater bandwidth and can be used to generate much bigger attack volumes later.

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. The OWASP Top 10 List identifies the most critical risks facing organizations today.

1. **Injection**
2. **Broken Authentication and Session Management**
3. **Cross-Site Scripting (XSS)**
4. **Insecure Direct Object References**
5. **Security Misconfiguration**
6. **Sensitive Data Exposure**
7. **Missing Function Level Access Control**
8. **Cross-Site Request Forgery (CSRF)**
9. **Using Known Vulnerable Components**
10. **Unvalidated Redirects and Forwards**

How to Address **Common Web Application Vulnerabilities**

To minimize the vulnerabilities within your web applications, it's important to improve your Internet hygiene. This involves following best practices for application design, implementation, configuration, testing and maintenance:

Keep Software Up to Date and Install the Latest Patches

No code is perfect. Sooner or later defects will come to light. The most serious of these are security issues. Your first line of defense against malicious attacks is to have the most up-to-date version of your web server and application server software and install security patches as quickly as possible.

Software plug-ins and add-ons (such as Wordpress plug-ins) can be particularly vulnerable because they're often developed by inexperienced programmers or come from sources that don't always follow coding guidelines. Use only the plug-ins you need and make sure they're up-to-date.

Define Secure Configurations

Security misconfiguration can occur at any level of an application stack, including the platform, web server, application server, database, and custom code. Developers and system administrators need to work together to ensure that the entire stack is configured properly.

Items to consider for secure configuration:

- Appropriate use of encryption for data in motion and data at rest
- Removing unnecessary accounts
- Disabling or removing unnecessary services
- Following the principle of least privilege. It's easy to misconfigure a web server and allow malicious users to reach places you didn't intend them to reach—administration pages, directory listings, things normal users shouldn't see that allow hackers to mount a more serious attack. A well-configured system will only allow users to access what they absolutely need to access.

Develop a standard configuration and a repeatable hardening process to make it fast and easy to deploy systems and ensure they're properly locked down. Development, QA and production environments should all be configured identically using an automated process to minimize the effort required to set up a new secure environment. Run scans and do audits periodically to detect misconfigurations.

Write Secure Code

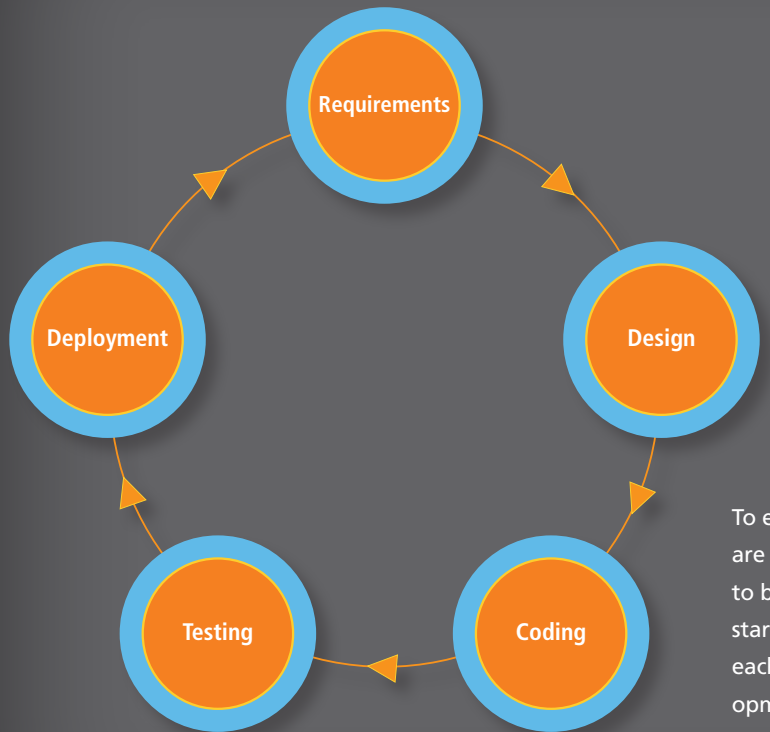
Keep security in mind both when developing software from scratch and when writing add-ins to existing software. Finding and remediating security issues early in the development lifecycle is less expensive than fixing the code once an application is in production.

You can prevent most faults and weaknesses by carefully and consistently implementing security during the application's requirements, architecture and design phases. For example, model threats up-front to identify the pages with the most logic and thus the longest load times, which would warrant additional DoS defenses. Be sure to train people who deliver web applications to build security into the software development lifecycle (SDLC) and put in place processes to guide their efforts.

Among the most effective protections to build into software include implementing proper:

- **Input validation.** Most vulnerabilities are caused by lack of user input validation and proper sanitization of input. Never trust user inputs. Instead, include input validation on form fields to mitigate against buffer overflow, code injection, and other attacks that can break application logic.
- **Encryption.** Encrypt both data in motion and data at rest, using the latest industry encryption standards

A Secure Software Development Lifecycle



To ensure that your applications are secure, it's far more effective to build in security right from the start. Consider security throughout each phase of the software development lifecycle, shown here.

Source: http://resources.infosecinstitute.com/intro-secure-software-development-life-cycle/

Scan Your Code and Plug-ins

No matter how carefully you design and develop an application, there will always be weaknesses in the code. These are often not readily apparent and many are propagated as developers incorporate snippets of existing code into multiple applications. Vulnerability scanning offers a way to find application backdoors, malicious code, and other threats that may exist in purchased software and internally developed applications.

Two types of vulnerability scanning are available: **static-testing** and **dynamic testing**.

- **Static testing** – Static testing scours the source code in the application and tells you where the application is vulnerable to malicious input such as SQL injection. Static testing looks at every line of code and identifies the exact location of any weaknesses. Automated tools can even provide mitigation recommendations, reducing research time. However, the results are very theoretical and tend to contain both false negatives and false positives. In other words, you'll get a long list of vulnerabilities that hackers will likely miss, and the tools may miss some vulnerabilities.
- **Dynamic testing** – Dynamic testing identifies vulnerabilities in the runtime environment by mimicking how a hacker works. These scanners traverse websites, fill out forms, send requests, and analyze the structure of the application. They then start bombarding the application with malicious input trying to find vulnerabilities. The benefit is that this type of testing finds real vulnerabilities—and identifies vulnerabilities that may have been missed with static tools. The drawback is that they're limited. Web applications are very complex, and scanners find it difficult to traverse the entire application so you get less coverage than you would with static testing.

The best solution for finding most, if not all, vulnerabilities is to use a mixture of both types of scanners. Some scanning vendors offer both capabilities in the same solution.

Install a WAF

Installing a WAF gives you more time to fix vulnerabilities. You can use a WAF to virtually patch the application by developing a rule to block the new vulnerability until you can make a permanent fix.

When you implement a WAF, be sure to test, monitor, and update the default configuration with rules tuned to your specific application environment. Remember that no security tool is meant for "set and forget." Best practices dictate that you review and update your ruleset at a minimum on a quarterly basis or optimally on a monthly basis.

Analyze the Accuracy of the WAF

Be sure to analyze the accuracy of the WAF. Evaluate the WAF in terms of its ability

to block attacks and allow good traffic through by determining:

- How many real attacks were blocked (true positives)
- How many valid requests were allowed through (true negatives)
- How much valid traffic was inappropriately blocked (false positives)
- How many attacks were allowed through (false negatives)
- Learn about the Matthews Correlation Coefficient and how to apply it to your WAF (http://en.wikipedia.org/wiki/Matthews_correlation_coefficient)

Look for (or build) a WAF testing solution to assess the accuracy of your deployment. The tool should send both valid traffic and real attacks and allow you to easily add test-cases of both valid traffic and attacks. It should gather statistics accurately and provide you with rich information about each test, including the full request, response, expected behavior and the nature of the request. It should also provide reporting capabilities.

CONCLUSION

As you continue to move data and services to the Internet, you can no longer rely on strong perimeter protection to keep your systems and data secure. You need solutions designed specifically to address the security threats you face on the Internet—especially DoS/DDoS attacks at the network and application layer and attempts to steal data.

This eBook has mapped out the types of threats that plague Internet resources, the necessary elements of a solution, and the options available to you. Whatever solution you choose, take advantage of a multi-layered approach that provides sufficient bandwidth at the network layer and allows only HTTP traffic onto the network. At the application layer, follow secure development processes and good Internet hygiene as well as implement a comprehensive WAF to handle any attacks that might slip through the cracks. By putting in place a comprehensive set of security controls, your organization can minimize the risks of maintaining your Internet presence.

To get the most up to date information on the DDoS Landscape,
download the most recent Quarterly Attack Report here

For more information on the general security and Internet landscape,
download Akamai's State of the Internet Report

The cyber security landscape is constantly evolving. Akamai will continue to stay on top of market trends and keep you up-to-date with new thought-leadership.

For daily commentary on the security industry,
VISIT OUR BLOG ▸ http://blogs.akamai.com.

And if you'd like to speak with a representative
CALL: 1.877.425.2624 or

CONTACT OUR SALES TEAM ▸ today at:
http://www.akamai.com/html/forms/sales_form.html

Start Your Web Application Security Plan Now:

Follow These 5 Steps to Improve Your Web Application Security Profile:

1. Evaluate the security risks most likely to impact your websites and web applications
2. Inventory your existing security controls and assess the additional security controls necessary to mitigate your risks
3. Assess your web application vulnerabilities and follow Internet hygiene best practices to address them
4. Research your options
5. Implement your multi-layered solution

APPENDIX 1

VALUABLE RESOURCES:

12 Must-Know Security Experts - Need help better understanding the most recent trends in cyber security? The experts below are some of the top names in the industry, each with their own strong social media presence. Follow them to get your fill of InfoSec facts and an extra dose of witty repartee.

ANDY ELLIS	Akamai Chief Security Officer	**Twitter:** @CSOAndy
ANDREW JAQUITH	CTO of SilverSky	**Twitter:** @arj
BILL BRENNER	Akamai Security Evangelist	**Twitter:** @BillBrenner70
BRIAN KREBS	Investigative Journalist	**Twitter:** @BrianKrebs
CHRIS HOFF	VP Strategy and Planning, Juniper Networks	**Twitter:** @Beaker
JACK DANIEL	Technical Project Manager, Tenable	**Twitter:** @jack_daniel
JOSHUA CORMAN	CTO at Sonatype	**Twitter:** @JoshCorman
MARTIN MCKEAY	Akamai Security Evangelist	**Twitter:** @Mckeay
MICHAEL SMITH	Akamai CSIRT Director	**Twitter:** @rybolov
MIKE ROTHMAN	President, Securosis	**Twitter:** @securityincite
RICH MOGULL	CEO, Securosis	**Twitter:** @RMogull
STEPHANIE BALAOURAS	VP and Research Director, Forrester Research	**Twitter:** @sbalaouras

APPENDIX 2

FURTHER READING:

Global DDoS Attack Report
Keep up to date with trends on cyber security

Customer Case Studies
Read how other companies protect their websites from DDoS attacks

PLXsert Threat Advisories
Learn more about the current DDoS threats and steps to take for protection

Man, Machine & DDoS Mitigation
Find out why you need human cyber security expertise in today's DDoS threatscape

Ovum: Delivering Effective DDoS Protection
Read this analysts report on why DDoS protection should be a part of your security response plan