Acmetek
A Trusted Advisor of Security Solutions and Services

SiteLock

Practical Guide to Choosing a DDoS Mitigation Service

WHITEPAPER

From massive volumetric attacks to sophisticated application level threats, DDoS attacks are bigger, smarter and more dangerous than ever. Given today's threat landscape and the availability of inexpensive, "Do It Yourself" DDoS tools, online businesses need to take DDoS mitigation seriously. These attacks can cripple a website or online application in minutes, resulting in lost revenues, reputation damage and reduced customer confidence.

This white paper provides online businesses of all sizes with practical guidelines for choosing a DDoS mitigation solution. It outlines several important considerations, useful tips and key requirements to be used for evaluating potential solutions. The document also includes an overview of the SiteLock DDoS Protection solution, showing how it helps online businesses mitigate high-volume and sophisticated DDoS attacks without disrupting the user experience.

DDoS: Who's at Risk?

The answer to the question of who's really at risk from a DDoS (Distributed Denial of Service) attack is quite simple: any business with a web presence. DDoS attacks today target both large and small companies, organizations, government offices, and even individuals with a prominent web presence.

Imperva's "2015-2016 DDoS Threat Landscape Report," points to a 240% increase in DDoS botnet activity over the space of one year. Among the driving forces behind the proliferation of DDoS are the simplicity and low cost of putting an attack in motion, and the relative impunity attackers enjoy. Simple, low-cost DDoS toolkits, such as Dirt Jumper and its variants, leave no website or network safe.

While hacktivist attacks, such as those perpetrated by the QCF against leading US banks in 2014-2015 often get the most headlines, the majority of DDoS attacks are executed by criminal botnet services. Botnets-for-hire, composed of thousands of compromised devices, are readily available on the Internet and provide the foundation for launching devastating attacks against online businesses. The fees for these services start at $50 for small attacks, but some researchers have seen DDoS prices as low as $9. To attract customers, botnet owners advertise their services in underground forums and mailing lists.

Another trend ratcheting up the risk to commercial sites is the fact that DDoS attacks are increasingly being used as a competitive business tool, designed to create chaos and level damage to competitors' sites. As such, DDoS attacks, which used to focus mainly on high-profile websites, now also target mid-sized enterprises and SMBs.

Preliminary Precautions

Given today's threat landscape, any business owner with a website should take DDoS mitigation seriously. In particular, organizations with significant online financial or reputational assets should take immediate action with respect to implementing a DDoS mitigation solution.

Even those still considering their DDoS mitigation options should at the very least conduct ongoing monitoring to be aware of threats, and have an idea of possible remedies. This means that today you should:

- **Conduct online reconnaissance**
  Take note of online buzz about your organization, and look for hints of budding hacktivism focus. Subscribe to free security assessment reports that cover DDoS incidents and emerging DDoS techniques.

- **Understand the basics of mitigation**
  Once you know of relevant threats, take note of basic mitigation recommendations like implementing content filtering rules or modifying your firewall settings. In the event that you are attacked, prepare a communications strategy in advance that will let your customers know what's going on, and what you're doing about it.

- **Evaluate alternatives to absorb DDoS bandwidth peaks**
  Over-provisioning Internet bandwidth is one of the most common measures to alleviate DDoS attacks, but it is also probably the most expensive, especially since DDoS attacks can be 10 times or even 100 times greater than standard Internet traffic levels. An alternative is to use a security service that scales on-demand to absorb and filter DDoS traffic. DDoS protection services are designed to stop massive DDoS attacks without burdening businesses' Internet connections.

- **Know where to get help**
  You should at least know how to find a DDoS mitigation service, if you're under attack and need a quick remedy. Services like SiteLock can deliver reasonably-priced protection in just minutes – keeping your site from crashing in the event of an attack, or at least minimizing downtime.

Choosing a DDoS Mitigation Solution – Practical Tips

Once you're ready to get serious about implementing DDoS mitigation, you'll need to delve deeper into the nature and types of solutions out there.

The DDoS threat has pushed vendors to the limits of their creativity. As a result – there's good news and bad news. The good news is that there ARE good solutions, technologies, and ideas out there; the bad news is that there are A LOT OF THEM to choose from, each representing a different approach to protection. Some notable approaches include:

- **Appliances deployed within the data center**
- **Hardened hosting platforms**
- **Cloud-based DDoS mitigation services**

Regardless of the approach, when choosing a DDoS mitigation solution, you should make sure the solution adheres to the following fundamental guidelines.

Transparent Mitigation

Your users don't need to know and don't care that you are under attack. People should be able to access your site without delay, without being sent through holding areas or splash screens, and without receiving outdated cached content. Find a solution that protects your realm invisibly, yet effectively.

Absorb Volumetric Network DDoS Attacks

Network level DDoS attacks continue to grow in size. These types of attacks, the largest of which have exceeded 200 Gbps, are growing at a rapid pace, fueled in part by the widespread availability of cloud infrastructure. Amplification-based attacks are popular with attackers because they can deliver a massive flood of data at the target while requiring only a relatively small output from the source.

You need to be able to absorb arbitrary – yet massive - amounts of traffic. Service providers do this by building large 20 gigabyte data centers and distributing traffic among them, when possible. Appliance vendors deal with it by stacking and cloudifying their appliances. Find the path to absorption that works best, and is most cost-effective, for your needs.

Identify Sophisticated Application Level DDoS Attacks

Application level DDoS attacks typically mimic legitimate user traffic to evade an organization's common security measures (including barebone anti-DDoS solutions). Application attacks are dangerous because they don't require high volumes to succeed. It takes no more than 50-100 targeted requests per second to bring down a mid-sized server. Most importantly, because application level DDoS relies on human-like bots and (in some cases) actual browsers, they're much harder to mitigate – even once detected. To mitigate application level attacks, you need a solution with the "brains" to profile incoming traffic and distinguish between humans and bots.

Leave a Path to Redemption

One of the key challenges in mitigating applicative DDoS attacks is minimizing false-positives and business disruption. Legitimate visitors to your site should never be shut out without the possibility of redemption. What if they were wrongly accused of being a bot? As a last resort, legitimate users should be given a chance to prove they are human by filling out a CAPTCHA. Find a solution that ensures the best possible user experience.

Preserve the User Experience

Even when struggling to prevent DDoS attacks, remember that indiscriminately blocking all bot traffic can have serious repercussions for your business. For example, blocking Googlebot or McAfee ScanAlert bot can harm your site in the short and long term. Effective DDoS protection should revolve around pinpoint-accurate identification. Your DDoS protection solution should recognize and respect good bots, allowing them continuous and uninterrupted access to all areas of your site.

Always On Protection

In a global economy, your online business never shuts down, which means that your DDoS protection strategy must be based on accurate 24x365 monitoring. This is something that human operators should support but, in practice, simply cannot deliver reliably. Moreover, hit & run attacks can wreak havoc with DDoS mitigation solutions that need to be manually turned on and off at every burst. Find a solution that protects you automatically, without the hassles and risks of manual activation.

Monitor Application and Network Traffic

Monitoring application and network traffic provides IT security administrators with instant visibility into DDoS attack status. Security administrators should be able to review traffic levels, application performance, anomalous behavior, protocol violations and Web server error codes. Real-time traffic monitoring enables data-driven response to DDoS threats and any other unwanted scenarios.

A Parting Thought

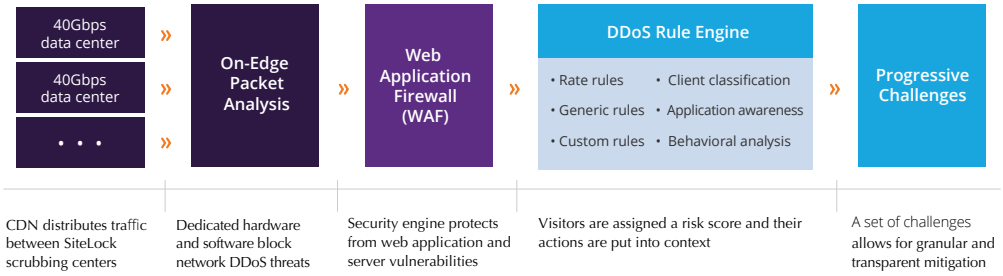
DDoS is a reality that your business needs to face. When choosing a DDoS mitigation service, following the guidelines above can help your business not only weather the flood of DDoS attacks, but even survive and thrive in the dangers of the virtual jungle.

Cloud-Based DDoS Protection

SiteLock is a cloud-based service that stops all types of DDoS threats, including network, protocol and application level attacks – with minimal business disruption. Leveraging a high-capacity global CDN, This "always on" DDoS mitigation service scales on demand to stop multi-gigabit attacks without requiring businesses to purchase expensive Internet connections or deploy additional networking equipment. DDoS Protection can be rolled out without the need for hardware, software, integration or web application code changes. Customers can provision this service simply by changing their website's DNS setting.

The service detects and mitigates advanced attacks that exploit applications, web server, and DNS server vulnerabilities. Ironclad network defenses detect network attacks like SYN floods and DNS amplifications. SiteLock detects sophisticated application level attacks that bypass traditional DDoS security services by implementing advanced and progressive challenge mechanisms. These defenses differentiate between bots and legitimate application users by validating whether the client browser can execute JavaScript, store cookies and perform other basic browser functions.

How It Works



Key Features & Benefits

Comprehensive DDoS Protection

SiteLock protects your website against all types of DDoS threats, including network-based attacks, like Sloworis, ICMP or TCP & UDP floods, and application level attacks, such as GET flood, that attempt to overwhelm server resources. The service detects and mitigates advanced attacks that exploit application, Web and DNS server vulnerabilities, hit-and-run DDoS events and large botnets.

High-Capacity Network

As the size of network DDoS attacks, such as SYN flood and DNS amplifications, continues to increase, organizations require robust network capacity to mitigate any threat that might come its way. Our global CDN offers high capacity to thwart the largest volumetric DDoS attacks.

Zero Business Disruption

SiteLock protects your site not only from complete denial of service, but also from disruptions related to DDoS attacks, mitigation false-positives, etc. We offer transparent mitigation with less than 0.1% false positives, and without degrading the normal user experience in any way. This lets you enjoy true DDoS protection, even from lengthy attacks, without affecting legitimate users.

Infrastructure Protection

Infrastructure Protection lets you protect core infrastructure (e.g., web, email, FTP servers) on demand across entire subnet ranges. In the event of an attack, traffic is re-routed through SiteLock scrubbing centers using BGP announcements. From this point on, SiteLock acts as the ISP and advertises all protected IP range announcements. All incoming network traffic is inspected and filtered, and only legitimate traffic is securely forwarded to the enterprise network via GRE tunneling.

24x7 Managed Security Service

A dedicated team of SOC engineers monitors your attacks and is available before, during or after attacks to ensure your site is up and running and performing optimally.

Collaborative Security

SiteLock protects websites using collective knowledge about security threats, including new and emerging DDoS attack methods. Using crowdsourcing techniques, new security information is aggregated across the entire network and new mitigation rules are applied in real-time, across all protected websites.

About SiteLock

SiteLock is a cloud-based application delivery service that protects websites and increases their performance, improving end user experiences and safeguarding web applications and their data from attack. SiteLock includes a web application firewall to thwart hacking attempts, DDoS mitigation to ensure DDoS attacks don't impact online business assets, a content delivery network to optimize web traffic, and a load balancer to maximize the potential of web environments.

Only SiteLock provides enterprise-grade website security and performance without the need for hardware, software, or specialized expertise. Unlike competitive solutions, SiteLock uses proprietary technologies such as client classification to identify bad bots, and big data analysis of security events to increase accuracy without creating false positives.