Introduction

Website security is tightly intertwined with website performance optimization. Insufficient security measures can result in attacks that slow your website experience, expose customer data, and damage your relationship with customers. At the same time, stringent security measures that are poorly applied can slow the website experience even when no attacks are taking place. Consider how the airport security line would look if TSA conducted the most rigorous security procedures - background checks, interviews, fingerprinting - on each passenger upon check-in. Yottaa's eCommerce Acceleration Platform delivers advanced security measures that are applied intelligently against your traffic in the right sequence, allowing you to deflect harmful traffic and attacks while ensuring legitimate customers receive a fast experience.

Security & Performance Threats

eCommerce security is challenging because web applications live in the wild, outside the enterprise's protective walls, and attacks are becoming more challenging and frequent every day. Anyone can attempt a request to a web application. The request can take virtually any form and contain any content. And the application may offer any number of interfaces ready to handle these requests with virtually any kind of logic.

Almost all these requests may originate from legitimate users. The hard part is filtering out requests that are not legitimate and dealing with them appropriately — such as challenging the request, serving a 404 error page, or dropping the connection entirely. The attack logic will be disguised to resemble a legitimate user request in order to avoid detection and do the most harm. As a result, the best countermeasures must be advanced enough to identify and thwart these disguised attacks, yet allow through the requests that are legitimate. These countermeasures must also appear invisible to your legitimate visitors, and preserve the speed and quality of their experience on the website. A secure website that no one visits because it takes 10 seconds to load while each request is scrutinized is not a realistic solution.

The most critical web application security and performance vulnerabilities facing eCommerce sites can be simplified into five categories:

Bots – A web robot ("bot") is an application that runs a series of automated tasks, such as requesting and scraping content on your website. Today a large proportion of web traffic to eCommerce websites are bots, ranging from the beneficial (e.g. search engine spiders), to questionable (e.g. price comparison engines, competitors), to the outright malicious (e.g. denial of service attacks). But no matter what their intent, bots represent a large volume of requests that can draw resources away from legitimate visitors and slow or even block the website experience.

Volumetric (DDoS and Slow & Low) - Volumetric attacks are designed to overwhelm the target server with so many requests that it crashes. Two key strategies typify this style: distributed denial of service (DDoS) and Slowloris ("slow & low"). DDoS attacks utilize automated agents distributed around the Internet to simulate human users hitting the target server with potentially millions of simultaneous requests for service. Slow & low attacks are similar, except that each automated agent's requests are spread out (i.e., are slower) so that a connection with the target server is maintained as long as possible without the connection timing out. Ultimately the target can't service all the requests so it crashes. Slow & low attacks are particularly hard to detect because the request rate is slower than the typical DDoS attack.

Injection - These attacks exploit an application's syntax - SQL, PHP, Java Script, OS shell commands, etc. - in order to execute malicious instructions injected as data in a command or query. These instructions trick the web application into doing things the application's owners might not willingly permit — for example, to access private customer data.

Cross-site scripting - Cross-site scripting happens when a web server sends malicious code to users' web browsers which causes the web browsers to do things the user didn't intend — like defacing a target website or redirecting the user to a malicious site.

Session hijacking - Related to cross-site scripting, session hijacking occurs when attackers intercept or predict a user's session ID, allowing them to view and even take over the communication between a website and that user. As a result, the attacker can masquerade as the user to obtain private data or take any actions that the user is normally authorized to do.

Yottaa Platform: Tiered Security Approach

Just the five types of threats described above require a variety of different steps to effectively counter them. Denial of service, for example, is a very different kind of threat than session hijacking, and requires very different methods of detection and mitigation. Although security approaches to all these types of attacks do exist, they must be choreographed correctly or else these security efforts would impede the speed of the website by holding up legitimate traffic while it's being analyzed and filtered. Yottaa's platform leverages our Context Intelligence technology in conjunction with a Web Application Firewall to provide the highest level of security against OWASP top 10 security vulnerabilities while delivering the fastest possible experience.

Yottaa Web Application Firewall with Context Intelligence

Yottaa's web application firewall (WAF) leverages our Context Intelligence technology to apply rules-based logic that reads each request and processes it through escalating security procedures. Context Intelligence allows eCommerce teams to configure rules that trigger actions based on the context and attributes of each visitor, such as their location, browser, device, and interaction with web content. For example, when designed to accelerate the website, specific optimizations may be applied or content delivered based on the visitor's browser type and device screen size. When applied to website security, it allows specific security actions to be triggered based on visitor attributes such as geographic location, HTTP request header, request URL, user agent, and client IP.

The WAF with Context Intelligence delivers a high level of web security by rapidly identifying and filtering out unwanted web traffic, and saving the most stringent (and computationally intensive) security measures for a smaller volume of remaining traffic. As a result, Yottaa is able to eliminate threats while still delivering a highly optimized and fast experience for your legitimate visitors.

Staged Approach to Scrutinizing Traffic

The security actions taken by the WAF can be broken down into eight stages:

Stage 1: Intelligent traffic management & DDoS scrubbing

The Yottaa platform is built to scale with global infrastructure serving hundreds of clients across the world. If our edge servers determine that a volumetric attack is taking place, the platform can decide to deny the requests and simply drop the connection, and move traffic around any trouble spots. Alternatively, if the unusual spike in traffic is legitimate (e.g. due to a news item or special event), the platform can distribute the requests to multiple servers that are widely dispersed around the Internet, using techniques like border gateway protocol (BGP). BGP uses less of the IP protocol stack to make routing decisions, therefore requiring fewer compute cycles and less time.

Stage 2: Blocking traffic to non-web ports

Legitimate web traffic should only arrive over ports 80 (http) and 443 (https). All other ports are blocked. This blocking is performed first since there is no reason to examine traffic that arrives over an unauthorized port. By removing this traffic, it focuses the scrutiny of each security filter on a smaller amount of traffic.

Stage 3: Serving cached content

The Yottaa platform identifies all static content on our clients' pages so we can serve that content from edge cache locations and increase page load speed. The first time that static content is requested from the origin server, the request is scrutinized and validated before the content is returned and cached. As a result, all subsequent requests for that content can be served straight from the distributed cache locations without further scrutiny. This allows us to focus additional security measures on a smaller pool of requests – those for dynamic content from the origin server.

Stage 4: Client specific blocking

The volume of traffic undergoing security measures are narrowed further by triggering security rules based on attributes of the requester (e.g. geographic location, HTTP request header, request URL, user agent, and client IP). This can be performed several ways, including a rejection of traffic by IP range, or more granularly by blocks of IP addresses known as CIDR (Classless Inter-Domain Routing) blocks. This technique would apply, for example, if a website owner knows in advance that threats are likely to originate from a certain region, or if there are regions from which the owner does not expect legitimate traffic.

Stage 5: Validate user against a list of known attackers

By accepting requests on a global scale for hundreds of clients, the Yottaa platform quickly builds a comprehensive list of known bad actors. As a result, traffic that hasn't already been blocked by port or client attributes is then compared against the platform's blacklist to block known malicious traffic. The remaining traffic is then analyzed more thoroughly to determine if it poses a threat. For example, to prevent session hijacking, Yottaa will scan requests for the presence of suspect URLs and match those against a blacklist of known offenders including those "fingerprinted" during visits to various client sites.

Stage 6: Throttling and rate controls

As opposed to a high volume DDoS attack, the platform detects a slow & low attack by first monitoring traffic to determine what represents a “reasonable” number of sessions over a period of time for that specific site. With that calculation, the platform looks for variations from that “reasonable number” that would indicate a possible attack. A good example would be witnessing a user take two hours to conduct a transaction instead of the average five minutes, and launching 1,000 HTTP sessions instead of the typical five. In response, the platform can block those requests deemed unreasonable, or apply rate controls to reduce the number of requests allowed through over a set period of time.

Stage 7: Advanced threat scrubbing

Up to this point, the traffic has not been analyzed for threats at the application level — i.e., for attacks attempting to use the logic of the application itself against the interests of the application’s owner, such as by SQL injection or site hijacking. These checks are more computationally intensive, so they are reserved for traffic that has successfully passed the other stages. At this stage, Yottaa’s Context Intelligence processes traffic through an extensive database of security rules that test for malicious activities and trigger the configured security response. For example, scanning incoming requests for keywords (“select,” “delete,” etc.) that indicate an injection style attack, or requests that resemble a malicious bot. If the answers are “yes,” the appropriate level of response is applied, such as interrogating the user, serving a 404 error page, or simply dropping the connection altogether. These rules are updated quarterly to stay current with emerging threats.

Step 8: Origin shielding

Yottaa provides a final tier of protection for attacks against our customers’ origin servers by broadcasting the Yottaa IP addresses so customers can block all traffic from other sources. This provides an additional security layer that prevents the origin server from being exposed to traffic that has not been scrubbed through Yottaa’s security measures.

By applying these tiered security procedures, the Yottaa platform quickly filters out the most threatening and problematic traffic, while focusing the most rigorous and computationally- intensive security measures against a smaller number of requests. As a result, websites on the Yottaa platform are protected from the most common security threats while preserving their ability to accelerate the speed of their online experience.

Comprehensive Security Services

Complementing this rigorous filtering of every request to your website, Yottaa enhances our security measures with additional services and certifications to provide ongoing support and enhancement of your eCommerce site.

Managed Security Services

Yottaa's Customer Success team provides an additional layer of security beyond the measures built into our platform. Our unique visibility into traffic across hundreds of websites gives us the ability to quickly detect and act against emerging threats. This layer of oversight is essential, as security threats change every day, and eventually new ones will emerge that existing measures may not detect and block. Yottaa's Customer Success team continually monitors traffic across all our customer sites, sends out alerts about new or unusual threats, and helps customers make adjustments that will block attacks while maintaining a high performing website for legitimate customers.

PCI Compliance

Yottaa has been certified as PCI DSS compliant by independent third-party PCI auditors. This certifies that Yottaa meets the requirements outlined by the Payment Card Industry Data Security Standard (PCI DSS) to provide online services to eCommerce and mCommerce businesses that store, process, or transmit payment card data. Yottaa undergoes recertification annually to stay current with the most recent standards.

Managed Rule Set Service

Customers can use Yottaa technology to configure rules that govern how security measures are applied. Our Customer Success team helps you configure those rules and set up custom rules. Additionally, customers can subscribe to our advanced security service that gives them access to more than 700 pre-configured rules for most known security vulnerabilities, updated quarterly. Our managed rule service includes false positive analysis, where our success team analyzes blocked traffic for examples of requests that should have been permitted, and uses those learnings to adjust your rule configurations. Additionally, our rules configuration interface allows customers to evaluate rules in "Learn" mode, which simulates how rules would have been applied against real traffic. You can view which type of requests would have been blocked when activating a particular rule, so any necessary adjustments can be made before setting it to "Active."

Security Analytics & Alerting

A real-time dashboard allows you to monitor traffic and view threats as they unfold throughout the day. You can monitor your traffic and threats across many different variables and views.

- Traffic and threat analysis by time, geography, IP, etc.
- Visibility into which rules are firing and blocking traffic
- Visibility into which rules would fire and block traffic if applied
- Visibility into all traffic and security logs for root cause analysis

By delivering this data in real-time, the Yottaa platform allows you to identify and respond to harmful trends as they unfold, rather than relying on daily reports that preserve large windows of vulnerability. Context Intelligence even gives you the ability to configure rules that trigger real-time push alerts via email and text when specific events occur. This access to real time data, full traffic logs, and alerting ensures that you will always be aware of threats to your website and are armed with the tools to defend it.

About Yottaa

Yottaa is the leading cloud platform for accelerating eCommerce. Purpose-built to solve the website performance challenges retailers face today, Yottaa enables retailers to deliver content instantly across all devices, pages, and browsers, through advanced acceleration and 3rd party application sequencing. Our cloud infrastructure and security procedures allow eCommerce organizations to protect against the most common attacks while improving the quality of the customer experience. To learn more about Yottaa technology, visit our website at www.yottaa.com.