Protect Your Site From Online Attacks
RSA can detect even the most sophisticated online attacks by monitoring and analyzing how users interact with your site.

This web session intelligence can be used to identify:
- Robotic Attacks
- Password Guessing
- Account Takeover
- Gift Card & Coupon Code Guessing
- Credit Card Fraud
- Mobile Session Abuse
- Man-in-the-Middle
- HTML Injection
- Session Hijacking
- Incentive Abuse
- Site & Inventory Scraping
- Denial-of-Service
- Architecture Probing
- Man-in-the-Browser

Cyber Crime is Prevalent and Costly
Today’s evolving threat landscape makes it difficult for ecommerce sites to adequately detect and respond to online threats. New and increasingly sophisticated attacks aimed at defrauding ecommerce sites are constantly being developed and deployed, making it extremely difficult to keep pace. Adding to this burden is the fact that online shoppers have little tolerance for any security measure that slows access or impedes activity on the site.

The inability to detect threats in real time, in effect the inability to distinguish between legitimate customers and disruptive or criminal users, can have major consequences on ecommerce sites in particular.

Complex cyber attacks and fraud schemes cost these sites billions of dollars annually. In addition to direct financial losses, ecommerce sites can suffer negative publicity, making online shoppers wary of patronizing particular sites.

Mitigating Cyber Crime by Distinguishing Customers from Criminals
RSA Web Threat Detection can help organizations meet the challenges posed by the ever-evolving threat landscape through the use of behavioral analysis to distinguish legitimate users from disruptive users.

Monitoring and analyzing how individuals interact with your site is a highly effective way to identify disruptive users because criminals do behave differently than legitimate customers.

That becomes apparent when you compare how quickly criminals move through the site, where they access your site from, even how they navigate through the site. They also leave tell-tale signs such as IP addresses and user-agent strings that indicate their presence.

For example, visitors to an ecommerce site may typically browse from product page to product page interspersed with visits to their shopping cart. A web session in which pages are visited in alphabetical order is likely one initiated and controlled by a bot.

The difficulty comes in seeing that anomalous behavior when it is just one among the millions of legitimate behaviors occurring simultaneously.
Why RSA Web Threat Detection?
RSA allows criminal and disruptive users to identify themselves through their online behavior — that way you can leave your legitimate customers alone

- No disruption of the customer experience or site performance
- Self learning risk engine continuously adapts to recognize new threats
- Real time detection allows real time response
- Almost immediate time to benefit
- Rapid deployment
- Highly scalable

Using Behavioral Analysis to Identify Behavioral Anomalies
RSA uses behavioral profiles to identify anomalous behavior. These behavioral profiles reflect what constitutes legitimate behavior on your site and are built dynamically based on how users actually interact with your site. This enables potentially fraudulent or disruptive behavior to expose itself.

RSA continuously monitors the click stream, looking at each and every click a user performs during a web session. The software automatically creates behavioral profiles based on click stream data, analyzing how quickly users move among web pages or enter data, the sequence in which they navigate web pages, etc.

RSA then compares individual user behavior against the population profile to determine if that user is engaging with the web site in a way that is expected. Each time the user clicks during the web session a threat score is calculated - behaviors that don’t conform to the profiles and/or other parameters are assigned higher threat scores.

These threat scores can be consumed by RSA’s rules engine to allow you to determine how to respond to different levels and types of threats. If for example the velocity score exceeds a particular threshold you can receive an alert and/or use the RSA API to terminate a web session.

RSA Web Threat Detection for Ecommerce
RSA Web Threat Detection extends visibility into web and mobile-application traffic and delivers actionable web session intelligence. The software monitors all clicks and HTTP/HTTPS stream and scores each click. This visibility into data in every web session, providing complete intelligence context in real time and one-click incident investigation, saving valuable engineering resources and avoiding impact to legitimate users.

RSA Web Threat Detection uses targeted rules to detect, alert, and communicate events to other network devices in real time, enabling you to instantly block IPs and users that are deemed malicious, including Denial-of-Service, site scraping, horizontal password guessing, and others. An API is also available to prompt suspected bot-like activity with CAPTCHA or strong authentication mid-session.

RSA Web Threat Detection Profile Analyzer
Profile Analyzer examines the behavior of website and mobile-application users and models it against past usage to determine if activity is legitimate or suspicious. Deviations from historically “normal” usage patterns are automatically flagged. Combining Profile Analyzer with the population-based modeling provided by RSA Web Threat Detection enables increased accuracy and faster response times to online threats.

“We found very quickly that these scripted attacks stuck out like a sore thumb when examined with RSA…”
ROBERT CAPP S, SENIOR MANAGER OF TRUST AND SAFETY, STUBHUB