RSA WEB THREAT DETECTION

Innovative and Effective Online Threat Detection

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 is web session intelligence and it can be used to identify

- Account Takeover
- DDoS
- Robotic Attacks
- Password Guessing
- Wire Transfer and ACH Fraud
- Random Deposit Fraud
- Credit Card Fraud
- Site Probing
- Validating Stolen Credentials
- Mobile Session Hijacking
- Man-in-the-Middle
- HTML Injection
- Incentive Abuse
- Gift Card & Coupon Code Guessing
- Site & Inventory Scraping
- Architecture Probing
- Man-in-the-Browser

Cyber Crime is Prevalent and Costly

Today's evolving threat landscape makes it difficult for organizations to adequately detect and respond to online threats. New and increasingly sophisticated attacks from DDoS to malware to Man in the Middle to account takeover are constantly being developed and deployed, making it extremely difficult to keep pace. Adding to this burden is the fact that web users 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 users and disruptive or criminal users, can have major consequences.

Complex cyber attacks and fraud schemes cost websites billions of dollars annually. In addition to direct financial losses, organizations can suffer negative publicity, further impacting their bottom line.

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 web session intelligence to distinguish legitimate users from criminal ones.

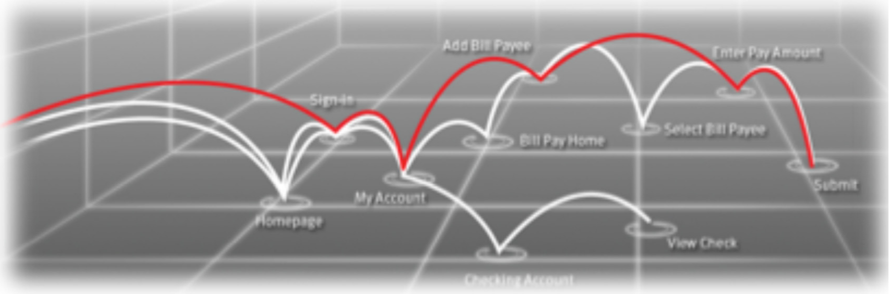
Monitoring and analyzing how individuals interact with your site is a highly effective way to identify disruptive users because criminals do behave differently than legitimate customers.

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.

RSA identifies all types of anomalous behavior in real time, offering total visibility into the web session and providing actionable information so that you can stop threats quickly, before they escalate.



Disruptive Users Navigate a Site Differently than Legitimate Users

DATA SHEET

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

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 Web Session Intelligence to Identify Behavioral Anomalies

RSA constructs behavioral profiles to support the identification of 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.

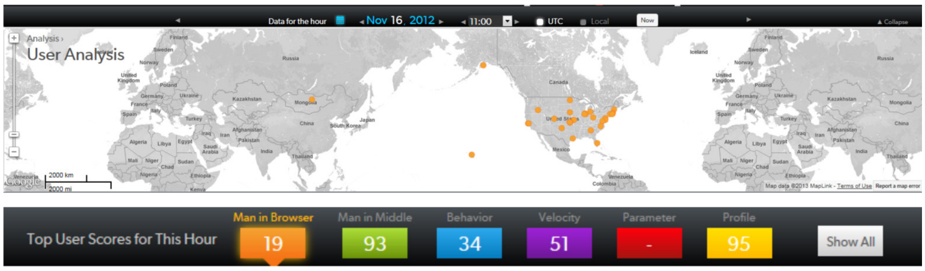
RSA captures and analyzes click stream data to build these profiles. Behaviors that don’t conform to the profiles are flagged as suspicious – RSA’s rules engine allows you to respond to different levels and types of threats.

Similarly, RSA can compare current behavior against past behavior for individual known users. So for example if an authenticated user always logs in from one of two IP addresses in the greater Boston area but suddenly logs in from an unrecognized IP address in Eastern Europe a red flag is raised.

This is all done in real time so that you can respond in real time.

The use of dynamically created profiles to help identify online threats represents a critical divergence from the traditional approach – rather than trying to intuit activities or sequences of events that would indicate disruptive behavior, RSA allows anomalous behavior to expose itself.

This is imperative in an environment where what constitutes legitimate use may look slightly different from site to site and even from day to day on the same site.



Top User Scores for This Hour

Man in Browser	Man in Middle	Behavior	Velocity	Parameter	Profile
19	93	34	51	-	95

RSA Web Threat Detection

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.

www.emc.com/rsa