RSA® WEB THREAT DETECTION
GET AHEAD OF AUTOMATED ATTACKS & DIGITAL FRAUD THREATS
New and increasingly sophisticated ways to perpetrate fraud are constantly being developed, making it extremely difficult to keep pace with the individual fraud attempts targeting an organization’s website. Organizations consider it a challenge to identify and respond to fraud until account takeover or other losses occur.

Over 70% of organizations state it takes days—or longer—to identify the source of fraudulent activity on their website. This occurs because cybercriminals are able to mask their activities alongside legitimate web traffic. In addition, organizations are concerned with adding new security measures that could potentially impact the user experience.

**RESPOND FASTER THAN FRAUD**

RSA Web Threat Detection is a fraud detection platform that leverages a combination of behavioral analytics and rules to identify high-impact fraud threats—without impacting the user or website performance. Web Threat Detection observes everything in the clickstream across users and devices, starting from the moment a new web session starts to the point of transaction and logout.

Detect. Web Threat Detection offers numerous out-of-the-box fraud detection rules to deliver immediate time to value. Rules can also be customized to address high-impact areas, including application security, account takeover, password guessing and automated attacks. Threat scores for common attack types and anomalies can also be used to enrich rules.

Review. Web Threat Detection “sessionizes” all web and mobile traffic, allowing easy drilldown into individual sessions and visitors and full visibility into malicious or disruptive behavior. In only a couple of clicks, fraud and security teams can have all session and user data at their fingertips, drastically reducing the time spent on manual review.

Respond. Threat scores, elements from the clickstream and imported data files such as RSA intelligence feeds, including compromised IPs and emails and mule accounts, can be used to enrich, customize and create new rules for improved detection. Data, cases, and alerts can also be pushed to external applications, including email, syslog, case management, analytics and authentication platforms.

Web Threat Detection provides for a continuous feedback loop to help organizations grow their understanding of the threat landscape and potential site vulnerabilities. In addition, Web Threat Detection allows rules to be written and deployed in seconds, giving organizations the flexibility to respond in near real time to emerging fraud.
Web Threat Detection deployment options include:

- On-premises deployment
- Public cloud deployment. Customers who deploy their website in a public cloud can deploy Web Threat Detection to monitor their websites for potential fraud threats.
- Technology service providers can utilize a multitenant deployment of Web Threat Detection and offer it to their customers as a managed security service.

Web Threat Detection also provides data streaming capabilities, which allows organizations to extract session data into their existing fraud detection ecosystem.

RSA and the RSA logo, are registered trademarks or trademarks of Dell Technologies in the United States and other countries. © Copyright 2017 Dell Technologies. All rights reserved. Published in the USA. 10/17 Data Sheet H16155.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.