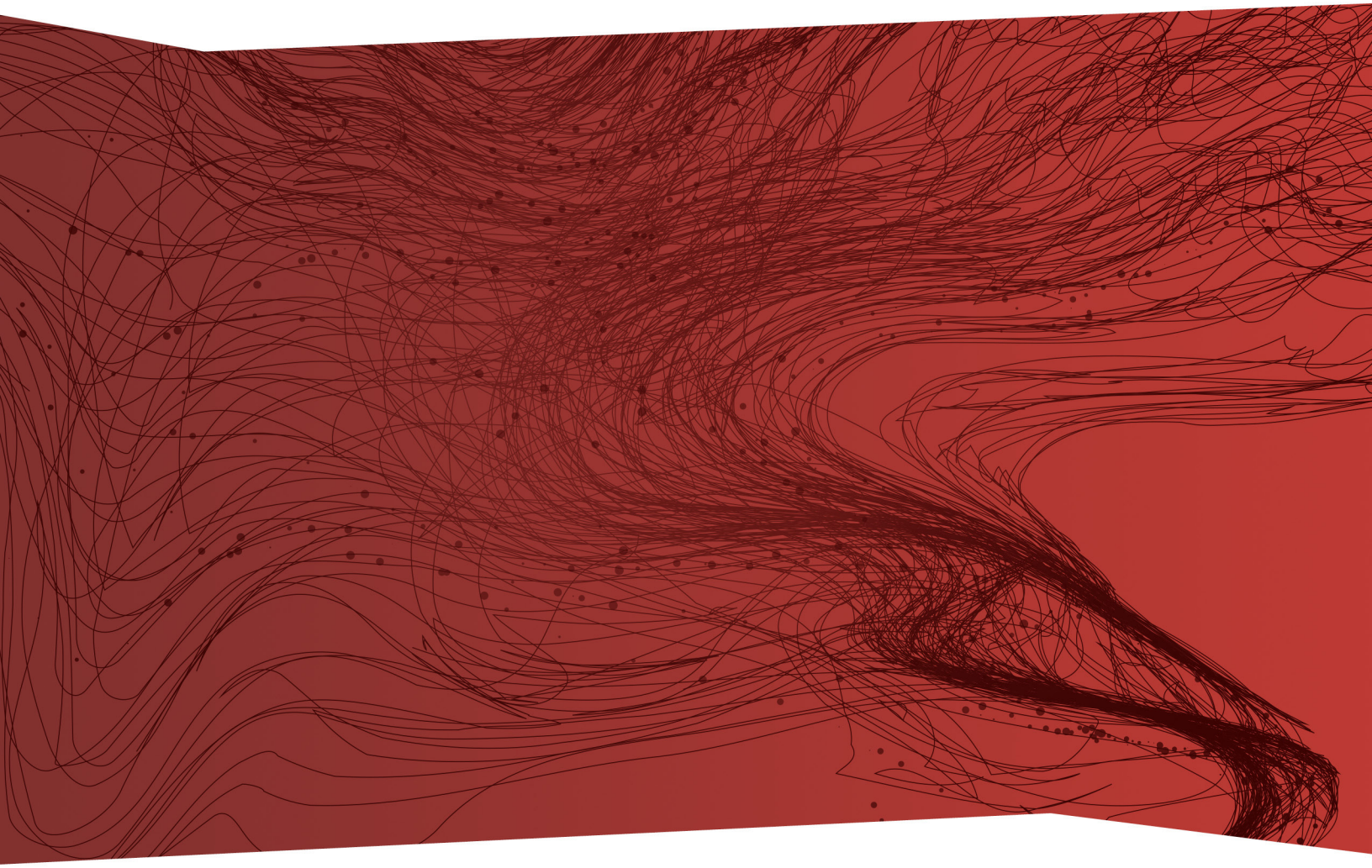
RSA



DATA SHEET

RSA® WEB THREAT DETECTION

GET AHEAD OF AUTOMATED ATTACKS & DIGITAL FRAUD THREATS

RSA

DETECT HIGH-IMPACT FRAUD THREATS

Web Threat Detection is a versatile platform that can identify even the most sophisticated fraud threats, automated attacks and other forms of disruptive online behavior, including:

- *Account takeover*
- *Fraudulent money transfers*
- *Password guessing*
- *New account fraud*
- *Credential harvesting*
- *Credential testing*
- *Mobile and web session hijacking*
- *Sophisticated malware*
- *Man-in-the—middle attacks*
- *DDoS attacks (application layer)*
- *Site scraping*
- *Vulnerability probing*
- *Business logic abuse*
- *Improper site functionality*

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.

RSA

WEB THREAT DETECTION DEPLOYMENT OPTIONS

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.*

MAXIMIZE VALUE WITH INTEGRATION

Web Threat Detection is part of the RSA Fraud and Risk Intelligence Suite of products that offers numerous points of integration across the portfolio to enhance fraud detection, including:

- **RSA eFraudNetwork.** Leveraging the eFraudNetwork, a global repository of confirmed fraud data, Web Threat Detection can receive feeds, such as known fraudulent IPs, as an input to the rules engine.
- **RSA FraudAction.** Web Threat Detection can leverage fraud intelligence collected from RSA FraudAction services as an input to the rules engine. One example would be known mule accounts.
- **RSA Adaptive Authentication** customers can leverage information captured by Web Threat Detection to monitor and score online transactions without integrating APIs to the web page.

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