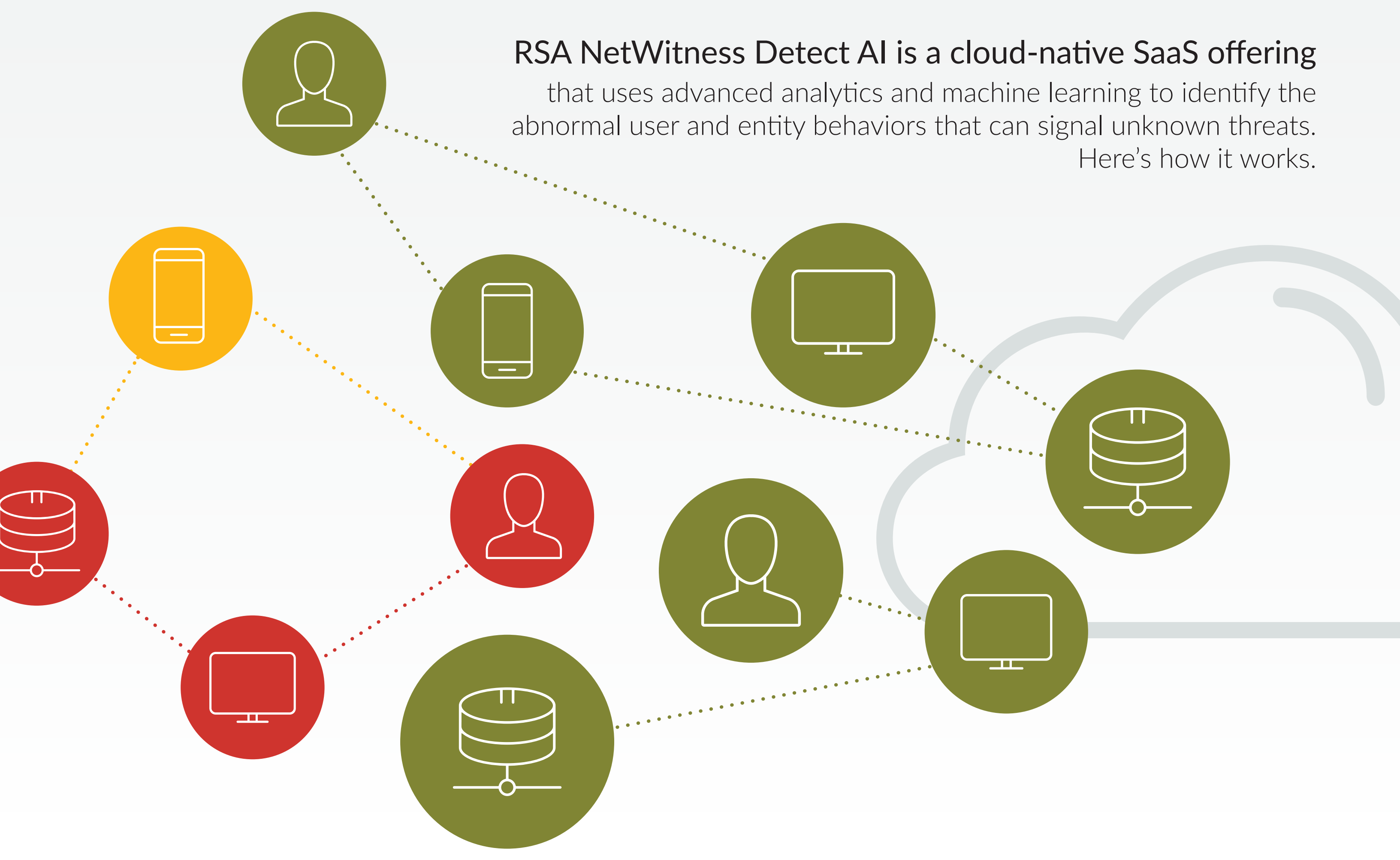
RSA

RSA NetWitness® Detect AI

Identify Anomalies Early, Resolve Threats Faster

Advanced analytics and threat detection
with the power and scale of the cloud

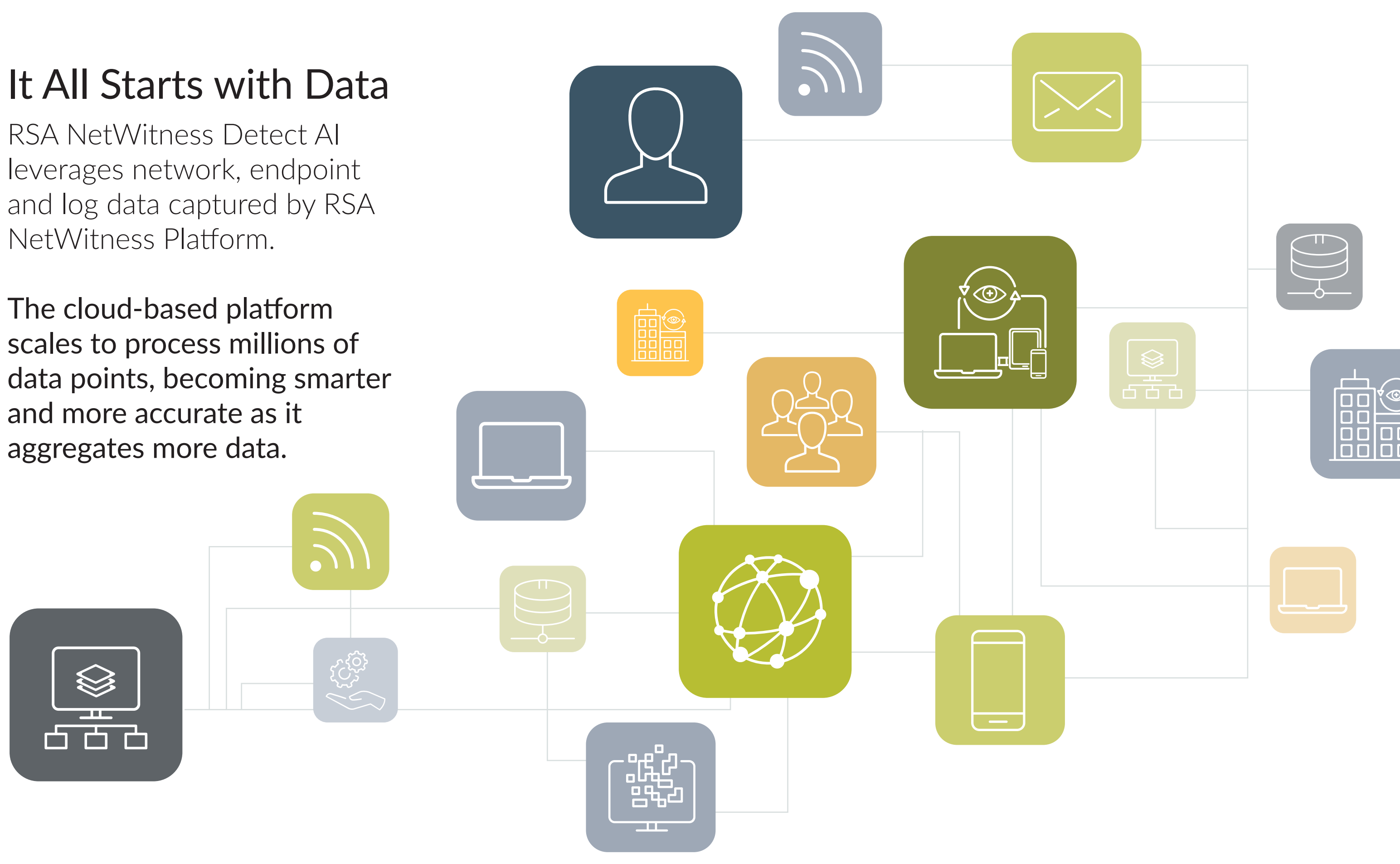


RSA NetWitness Detect AI is a cloud-native SaaS offering that uses advanced analytics and machine learning to identify the abnormal user and entity behaviors that can signal unknown threats. Here's how it works.

It All Starts with Data

RSA NetWitness Detect AI leverages network, endpoint and log data captured by RSA NetWitness Platform.

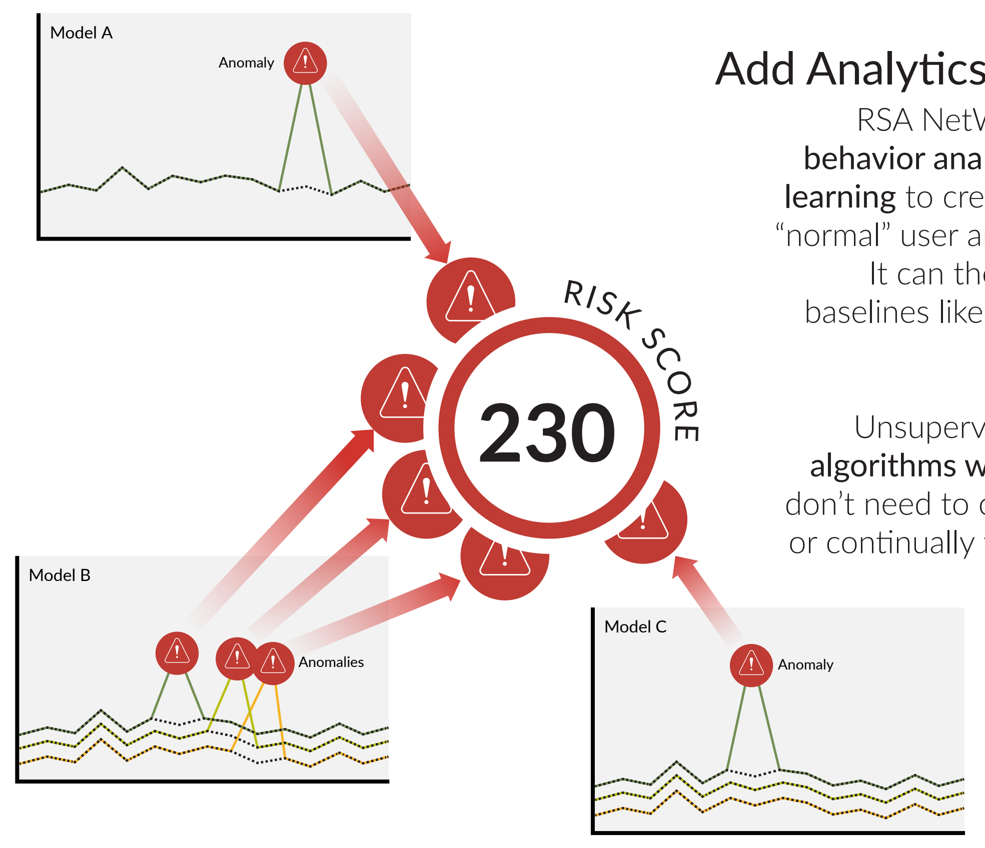
The cloud-based platform scales to process millions of data points, becoming smarter and more accurate as it aggregates more data.



Add Analytics and Machine Learning

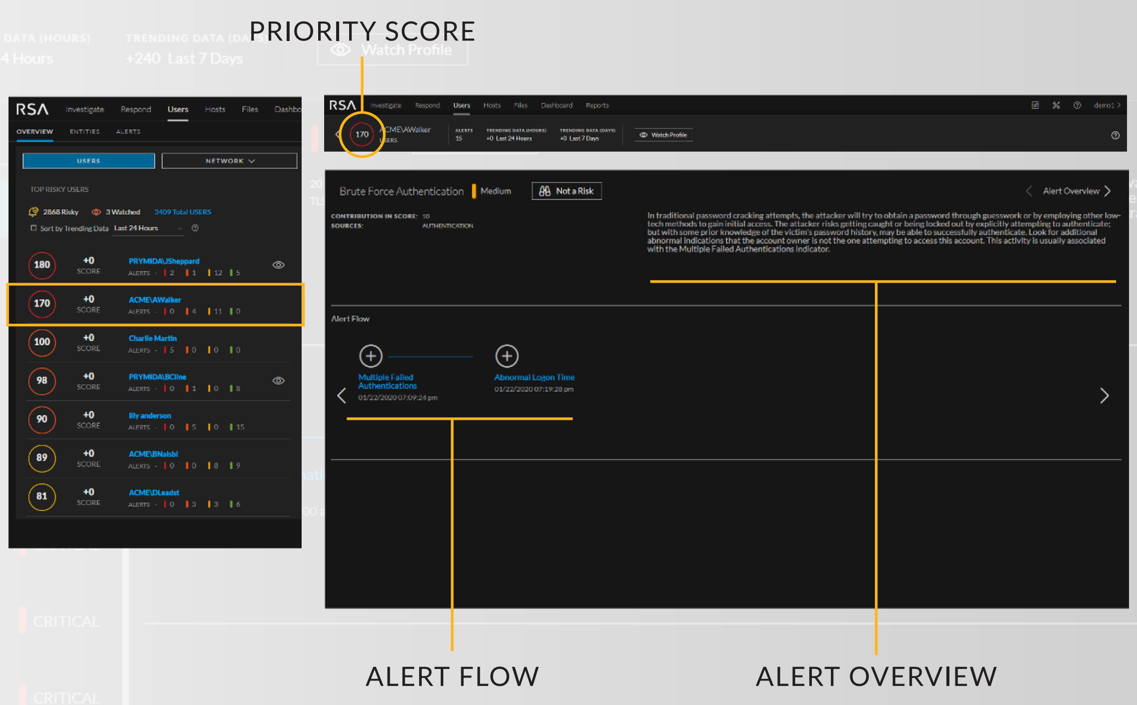
RSA NetWitness Detect AI uses **advanced behavior analytics** and **unsupervised machine learning** to create baselines of an organization's "normal" user and entity behaviors and IT usage. It can then identify deviations from those baselines likely to indicate suspicious behavior and sophisticated threats.

Unsupervised machine learning means **the algorithms work out of the box**. Your analysts don't need to create rules, customize metadata, or continually tune the underlying data models.



Innovative Statistical Analysis

RSA NetWitness Detect AI **aggregates multiple indicators of suspicious activity**, then applies a dynamic statistical risk scoring model. This approach alleviates analysts' burdensome workloads by producing **higher-fidelity alerts** triggered only when a risk score exceeds established thresholds.



TOP RISKY USERS

2868 Risky · 3 Watched · 3409 Total USERS

Sort by Trending Data · Last 24 Hours

Score	Trend	User	Alerts
180	+0 SCORE	PRYMIDA\USheppard	2 · 1 · 12 · 5
170	+0 SCORE	ACME\AWalker	0 · 4 · 11 · 0
100	+0 SCORE	Charlie Martin	5 · 0 · 0 · 0
98	+0 SCORE	PRYMIDA\BCline	0 · 1 · 0 · 8
90	+0 SCORE	lily anderson	0 · 5 · 0 · 15
89	+0 SCORE	ACME\BNaisbi	0 · 0 · 8 · 9
81	+0 SCORE	ACME\DLeadst	0 · 3 · 3 · 6

170 ACME\AWalker USERS · ALERTS 15 · TRENDING DATA (HOURS) +0 Last 24 Hours · TRENDING DATA (DAYS) +0 Last 7 Days

Brute Force Authentication · Medium

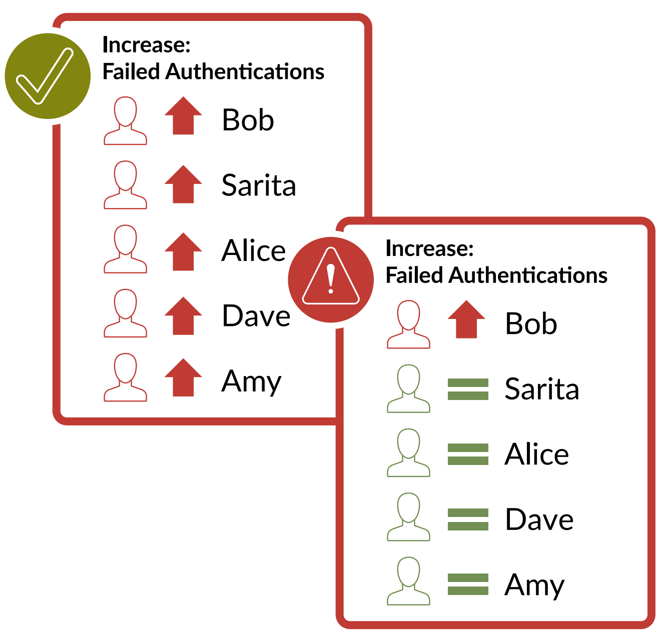
CONTRIBUTION IN SCORE: 10
SOURCES: AUTHENTICATION

In traditional password cracking attempts, the attacker will try to obtain a password through guesswork or by employing other low-tech methods to gain initial access. The attacker risks getting caught or being locked out by explicitly attempting to authenticate; but with some prior knowledge of the victim's password history, may be able to successfully authenticate. Look for additional abnormal indications that the account owner is not the one attempting to access this account. This activity is usually associated with the Multiple Failed Authentications indicator.

Alert Flow

Multiple Failed Authentications · 01/22/2020 07:09:24 pm

Abnormal Logon Time · 01/22/2020 07:19:28 pm



Intelligent Peer Grouping

Since user behavior varies based on an individual's role, responsibilities, location and other factors, **RSA NetWitness Detect AI creates peer groups and compares peers to detect deviations.** This also leads to more accurate alerts.

For example, if RSA NetWitness Detect AI sees that a user who normally never has a problem authenticating suddenly experiences several failed authentication attempts in a single day, it will look at similar users to see if they're having the same problem. If they, too, are showing failed authentication attempts, it's unlikely to signal a cyber threat.

Scalable SaaS Solution

RSA NetWitness Detect AI scales to process millions of events daily and analyze hundreds of thousands of organizational entities. Flexible licensing options accommodate the needs of both large enterprises and smaller organizations.

Easy to deploy and administer, with minimal hardware to install and manage.

Begins processing data within hours, so you can quickly baseline behavior, start detecting high-risk anomalies, and achieve fast time-to-value.

Automatically and regularly refines its machine learning algorithms to provide high-fidelity threat detection without burdening analysts with extra work.

RSA NetWitness Detect AI

- ✓ Prevents known and unknown attacks in an automated fashion
- ✓ Detects abnormal endpoint, user, and network behaviors
- ✓ Detects hard to predict threats without relying on traditional signatures
- ✓ Shrinks Mean-Time-To-Detect, -Investigate, and Respond (MTTD/I/R)
- ✓ Learns attacker's tactics, techniques, and procedures (TTPs)

For more information, visit **rsa.com/detect-ai**