RSA

THE POWER OF ANALYTICS IN DIGITAL RISK MANAGEMENT

USING ANALYTICS TO FOCUS ON THE **THREATS THAT MATTER MOST**

On one hand, you want to enable your global workforce to work from anywhere on any device, with the digital access they need. On the other, you must constantly guard against an increasingly sophisticated range of possible cyber attacks including identity-based and pervasive unknown threats. Addressing such threats to your business requires you to understand the financial, operational and reputational risk you face, then develop and execute a coordinated response that minimizes business impact. Security analytics play a critical role in the ability to understand and prioritize business risk—allowing you to focus on the threats that matter most.

Not all threats—and not all responses—are created equal. Disconnected prevention, monitoring, investigation and response technologies can create more work during times of crisis. To respond quickly and decisively to high-priority threats, security teams need a comprehensive, collaborative solution that uses powerful analytics in both detection and response.

ANALYTICS HELP
MITIGATE CYBER RISK

RAPIDLY DETECT INCIDENTS

Cut through the noise to pinpoint the threats that matter most.

ASSESS THE INCIDENT

Identify the scope, severity and overall impact of the incident.

COORDINATE THE RESPONSE

Facilitate a prioritized, automated and coordinated response.

A HOLISTIC APPROACH TO **CYBERSECURITY**

Responding to today's security threats requires three essential components:

Complete visibility into all users and devices.
Continuous network and endpoint monitoring provides up-to-date information on every device and user.

Ecosystem-wide threat detection.
Capture insights from networks, logs, endpoints, user behavior, and identity and fraud data from across digital, cloud and on-premises environments. Enrich this data with business context information and threat intelligence to investigate high-priority threats.

Automated, optimized prevention and response.
Automate and orchestrate workflows from early identification to close-loop remediation, allowing security analysts to do more with less.

THE BENEFITS OF USING ANALYTICS IN YOUR **DIGITAL RISK MANAGEMENT STRATEGY**

FEWER FALSE POSITIVES

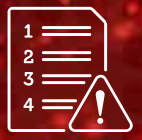
IMPROVED RESPONSE TIME

ACCELERATED THREAT DETECTION

REDUCED BREACH IMPACT

FASTER IDENTIFICATION OF SUSPICIOUS OR RISKY USERS

REDUCED DWELL TIME



PRIORITIZED INCIDENT RESPONSE

AUTOMATED RESPONSE

USE CASES

- Insider threat
- Brute force
- Account takeover
- Compromised account
- Privileged account abuse and misuse
- Elevated privileges
- Snooping user
- Data exfiltration
- Abnormal system access
- Lateral movement
- Malware activity
- Suspicious behaviors

THE THREE MOST POWERFUL ANALYTIC TOOLS FOR **DIGITAL RISK MANAGEMENT**

User and entity behavior analytics

Unsupervised machine learning

Endpoint detection and response

Behavioral analysis, machine learning, and endpoint threat intelligence help analysts detect and resolve both known and unknown attacks before they can disrupt your business.

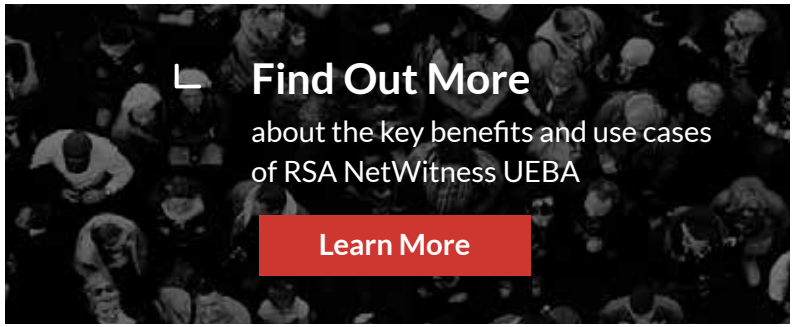
BENEFITS OF ANALYTICS: **UEBA**

What it delivers:

- Fewer false positives
- Accelerated threat detection
- Faster identification of suspicious or risky users
- Reduced dwell time

How it works:

With the proliferation of networks, devices, remote users and accounts, making sure your users are who they claim to be is a full-time job. User and entity behavior analytics (UEBA) develops a baseline behavior profile for each user, then uses this baseline to identify suspicious activities, such as login misuse. With smart, actionable and fully automated alerts, UEBA helps you zero in on abnormal behaviors, so your team can focus on high-risk threats rather than wasting time on unnecessary alerts.



BENEFITS OF ANALYTICS: **UNSUPERVISED MACHINE LEARNING**

What it delivers:

- Fewer false positives
- Accelerated threat detection
- Improved response time

How it works:

Meet the ideal: a threat monitor that never needs a coffee break and gets smarter over time. Continuous automated monitoring speeds detection of rogue insiders and cybercriminals without the need for rules, signatures or manual analysis. Instead, it baselines “normal” behavior, then applies both static rules and statistical analysis to detect suspicious activity. Using artificial intelligence, data science and mathematical data models, machine learning automates and orchestrates the entire incident response lifecycle, doing more with less human work.

BENEFITS OF ANALYTICS: **ENDPOINT DETECTION AND RESPONSE**

What it delivers:

- Fewer false positives
- Accelerated threat detection
- Faster identification of suspicious or risky users
- Reduced dwell time
- Automated response

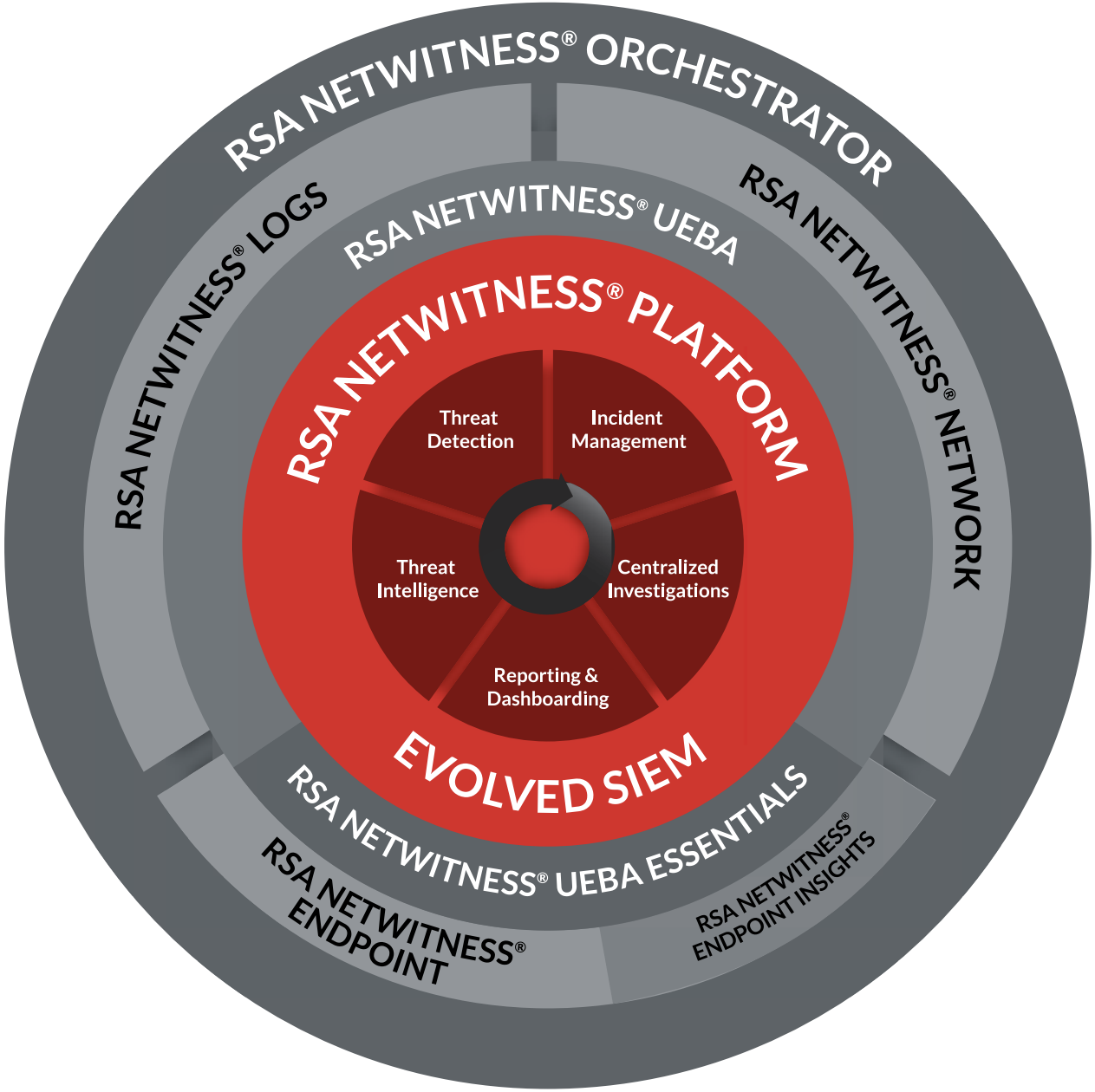
How it works:

Always on and never tiring, endpoint behavioral monitoring uses advanced machine learning to identify attacks that other security solutions miss. It quickly and automatically gathers critical data and provides powerful analysis needed to clarify the scope and breadth of each attack, so your team can launch an effective, targeted investigation and response.

RSA NETWITNESS PLATFORM

The RSA NetWitness® platform empowers security teams to quickly detect and respond to threats. It seeks out and identifies active exploits across logs, network, endpoints and NetFlow. And it uses deep analytics—including machine learning, advanced threat intelligence and UEBA—to boost analyst productivity.

With better, more proactive threat monitoring and protection, the organization can focus on growing the business, knowing that security threats will be held in check.



ABOUT RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to **rsa.com**.

RSA