RSA BUSINESS-DRIVEN SECURITY™

YOUR JOURNEY TO EVOLVED SIEM

THE MISSION

Even with increasing focus on security, breaches still occur at record rates. Whether it's outsiders stealing and misusing personal data, phishing or malware attacks through company emails, or nation-states trying to disrupt critical services, cybercriminals are constantly evolving their craft in attempts to stay undetected as long as possible.

These serious threats to your finances and reputation make it critical that your organization embrace an equally important mission: to continuously evolve security information and event management (SIEM) as the centerpiece of your security operations.

Evolved SIEM gives you deeper visibility into endpoints and network traffic, accelerates threat detection and response, and incorporates business context to prioritize threats and security incidents.

Pervasive Visibility

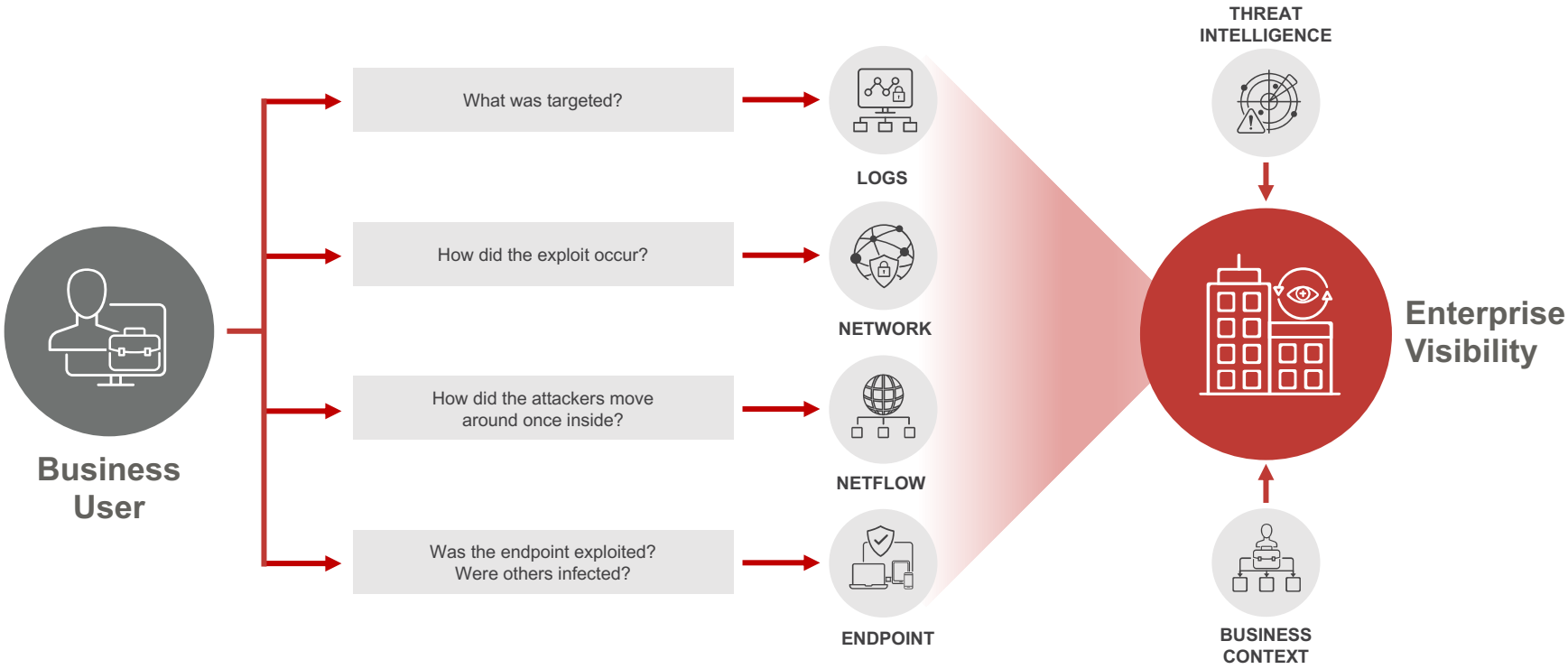
Advanced Attack Detection

Investigation and Response

Connection to the Business

PERVASIVE VISIBILITY

To get a complete picture of your enterprise security and answer all of the important questions, you need visibility—and context—across logs, packets, NetFlow and endpoints. That includes the ability to collect and normalize data from on-premise, virtual and cloud infrastructures.



WHAT TOOLS AND PROCESSES DO I NEED?

Log monitoring

Network traffic analysis and forensics

Endpoint detection and response (EDR)

Cloud and virtualized environment support

WHERE ARE YOU ON THE PATH TO PERVASIVE VISIBILITY?

Examine the breadth and depth of your current visibility across:

- Logs, network, endpoints and NetFlow
- On-premises, virtualized and cloud environments
- Integrations and parsers

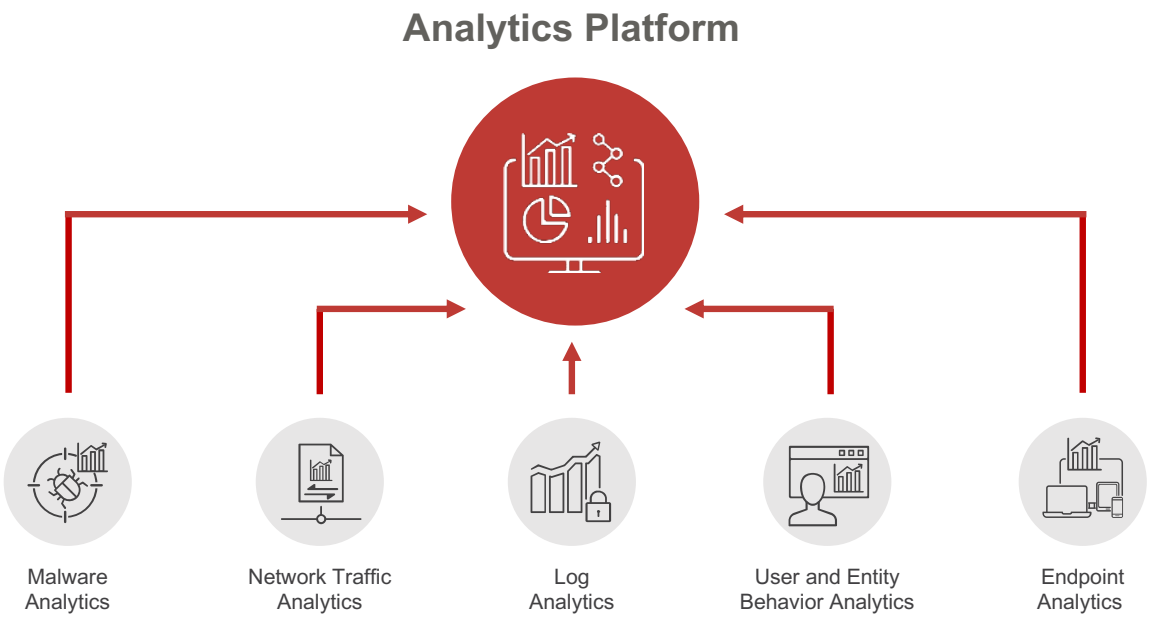
Evaluate your collection strategy:

- Do you have multiple repositories?
- Is the data normalized for analysis?
- Do you apply metadata at collection time?
- How do you store and manage data over time?

ADVANCED ATTACK DETECTION

To detect attacks, you need a multifaceted analytics approach that:

- Detects anomalous user behavior—even across a large number of events—to find unknown threats
- Uses unsupervised statistical anomaly detection to identify unknown threats
- Applies advanced correlation rules across all data to identify known threats
- Keeps a library of known threat indicators
- Interacts with third-party and community threat intelligence



WHAT TOOLS AND PROCESSES DO I NEED?

Security analytics applied to logs, network and endpoint data

Threat intelligence

User and entity behavior analytics (UEBA)

HOW WELL CAN YOU DETECT ADVANCED ATTACKS?

Examine your ability to identify attacks and compromises using:

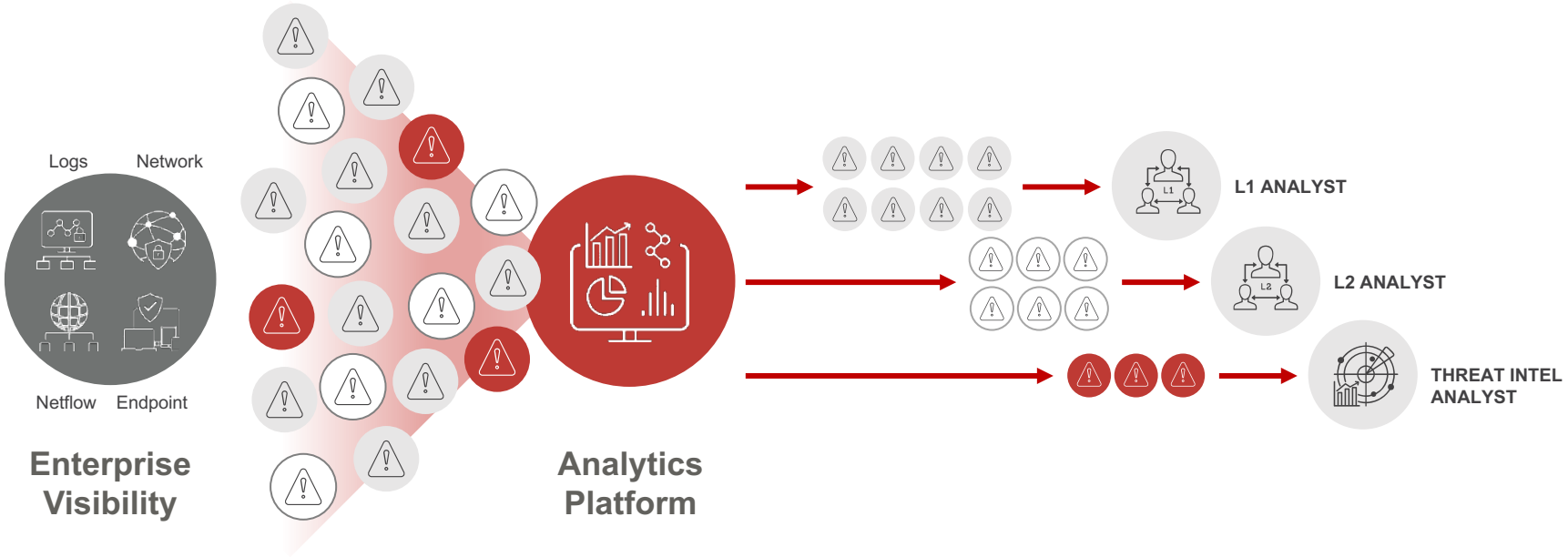
- People, processes and technology framework
- Computer science and AI (big data and machine learning)
- User and entity behavior analytics (UEBA)

Evaluate your readiness:

- What systems and tools are in place for threat detection?
- Have you deployed UEBA capabilities?
- How advanced are your current analytics? How well can they detect anomalies?
- Are you capturing all the data you need for effective detection?
- Are you fully leveraging threat intelligence?

INVESTIGATION AND RESPONSE

To eradicate attacks and mitigate business risks, you can't rely on technology alone. People and processes are just as important as tools. How well can you understand the full scope of an attack—and how quick and comprehensive is your response?



WHAT TOOLS AND PROCESSES DO I NEED?

Orchestration and automation

Playbooks and machine learning

Collaborative incident response

HOW RAPID AND ROBUST IS YOUR INVESTIGATION AND RESPONSE?

Examine your ability to identify and react to attacks using:

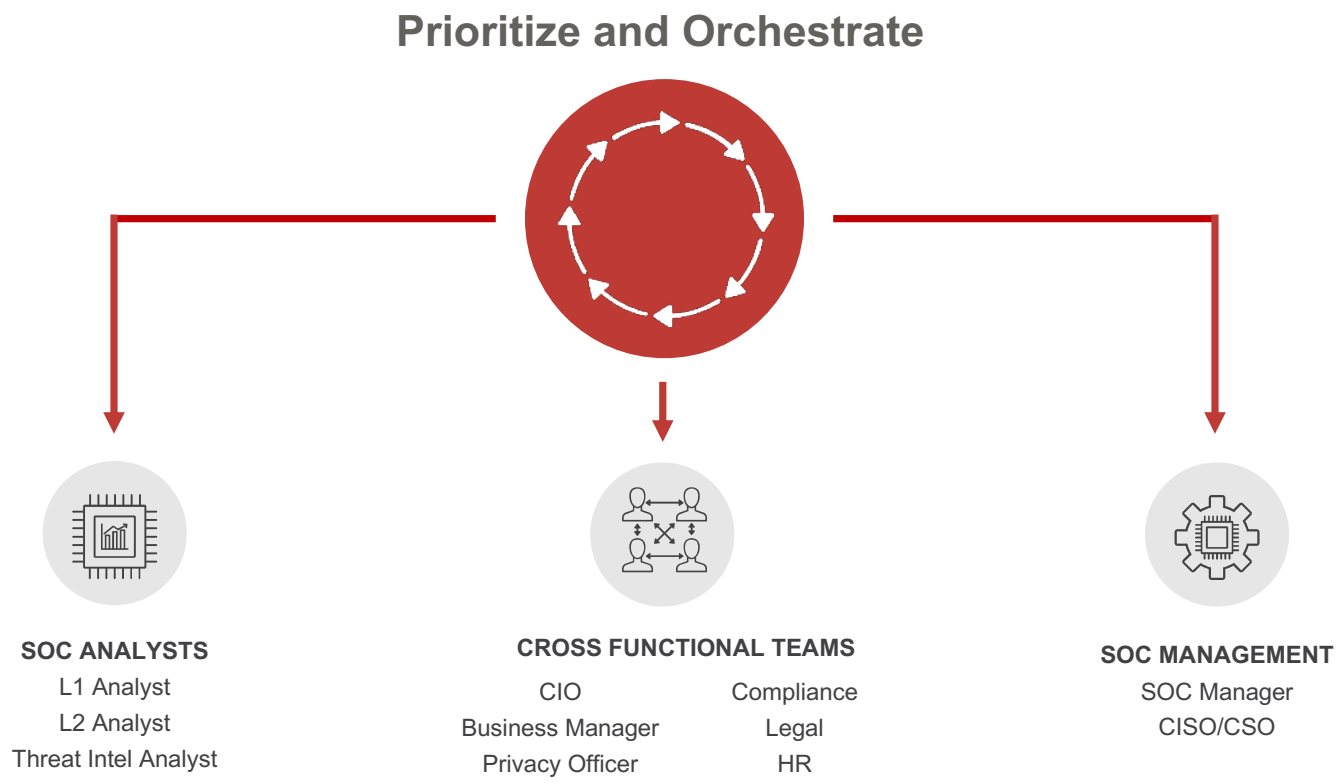
- Incident management
- Automation and orchestration
- Dashboards and reporting
- Security, Orchestration, Automation and Response (SOAR) framework

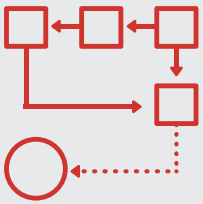
Evaluate your SOAR requirements:

- Can you manage incidents collaboratively?
- Can you automate common tasks effectively?
- Do you have an orchestration solution (leveraging security and nonsecurity tech)?

CONNECTION TO THE BUSINESS

Are your priorities for IT security aligned with business risk?





WHAT TOOLS AND PROCESSES DO I NEED?

Asset criticality assessment

Connections between risk and IT security teams

Cyber risk quantification

HOW WELL DO YOU CONNECT TO THE BUSINESS?

Examine collaboration between your IT security and business risk teams:

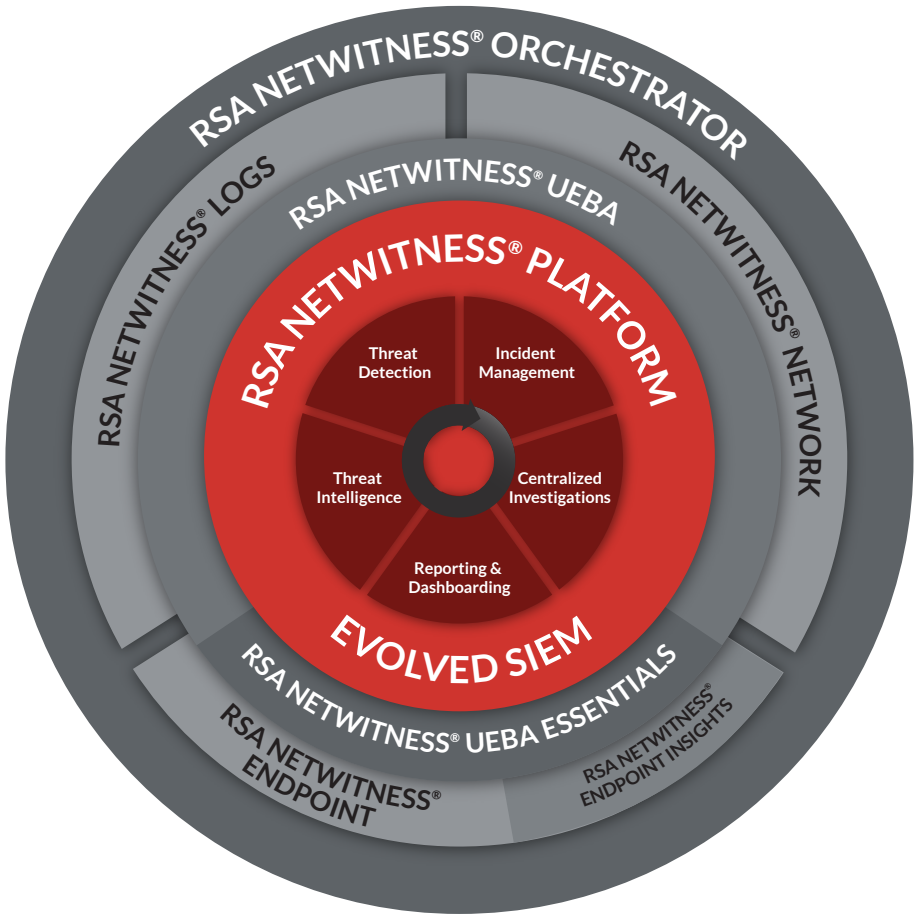
- Does your organization regard security breaches as a business risk, not just an IT risk?
- How's the working relationship between the two groups?
- Do business risk personnel feel responsible for IT risks (and vice versa)?
- Have you quantified the impact of various digital risks?

Evaluate your IT risk strategy against business risk imperatives:

- Do you have systems and processes that inform IT security about business risk strategy?
- Do your tools automatically integrate IT risk and business risk?
- Does executive management (CISO/CRO) prioritize collaboration at all levels?
- Do both IT and business risk manage your incident response plans?

RSA NETWITNESS EVOLVED SIEM

The RSA NetWitness® Platform uses an evolved SIEM approach that empowers security teams to quickly detect and respond to threats. It proactively watches for activities signaling the presence of active exploits across logs, network, endpoints and NetFlow. And it leverages deep analytics, with machine learning, advanced threat intelligence, and user and entity behavior analytics (UEBA), to improve analyst productivity.



Benefits of an Evolved SIEM

Rapid investigations

Automated behavior analytics

Integrated threat and business context

Single, unified platform for all your data

Flexible, scalable architecture

End-to-end security orchestration and automation

ABOUT RSA

RSA® Business-Driven Security™ solutions link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies take command of their security posture and thrive in an uncertain, high-risk world.
For more information, visit rsa.com