SOLUTION BRIEF

BUSINESS-DRIVEN SECURITY: THREAT DETECTION & RESPONSE
A CHANGING LANDSCAPE REQUIRES A NEW APPROACH

You have a lot of options if you’re implementing or augmenting a threat detection and response program. There are many viable vendors and options, and some fairly diverse approaches to the process.

At RSA, our view is clear. We espouse the idea of Business-Driven Security – integrating security as a core part of your business. We believe this approach improves security in two important dimensions. It makes security teams more operationally effective and empowers teams to more strategically manage security risks.

Business-Driven Security is an important evolution in the way organizations think about protecting their IT infrastructure, driven by rapid changes inside and outside an organization, and the fact that legacy approaches to security have become far less effective.

Security professionals know that traditional approaches are no longer reliable when it comes to protecting an organization’s most essential assets – its reputation, intellectual property, and customer relationships. In fact, 75% of organizations are unsatisfied with their current ability to detect and investigate threats, while only 11% of organizations say that they can investigate attacks very quickly. As the security goalposts have moved, it creates both a need and an opportunity to adopt a business-driven approach to protecting your organization from cyber threats.

First, from an IT perspective, the corporate perimeter has been obliterated by the explosion of cloud, virtualized, and mobile computing innovations. The whole idea of inside vs. outside has lost coherence, which means perimeter-centric tools like firewalls, virus scanners, and IPSs become inherently less effective. And if you’re looking at threat detection and response solutions, you realize this already.

But there’s also a business perspective, where global and external factors change the conversation about where security fits into your strategic plans. The impact of security breaches can be so large these days that no responsible board or CEO can fail to take these risks into account. A very good example is the European Union’s pending Global Data Protection Regulation (GDPR), which can impose penalties in the billions of dollars for failure to apply appropriate measures to protect user data.

SECURITY THAT UNDERSTANDS YOUR BUSINESS GOALS

RSA NetWitness® Suite is a leading threat detection and response platform which is noted for its robust technical architecture and its extreme visibility into threats anywhere they lurk within your infrastructure. Its scalable,
determined design, and deep analytics capabilities, make it the choice for security-conscious organizations around the globe. Its ability to monitor logs, packets, and endpoints across physical, virtualized, and cloud platforms, embraces the perimeter-less enterprise model.

However, RSA NetWitness Suite goes an important step beyond traditional threat detection and response: it supports the integration of security and business processes. At RSA we call this “bridging the gap of grief” – aligning the goals and vocabulary across the organization, and making security a core business dimension.

Here are some real-life examples of how RSA NetWitness Suite helps bridge the gap of grief in organizations:

- **Asset criticality.** As the volume of data to analyze explodes, so does the need to prioritize assets that present the most risk to an organization. It’s important to understand that the CIO’s personal laptop inherently exposes more risk than the web server hosting the cafeteria menu. Having that vital context as part of the security analytics process makes threat detection and response much more effective.

  How does the system know these things? RSA NetWitness is designed to incorporate data from a vast variety of sources, including governance, risk, and compliance (GRC) solutions such as the RSA Archer® Suite. Asset criticality is just one of the data points that can be integrated; any such data can be fed into the RSA NetWitness Suite analytics engine. This capability adds a layer of intelligence protect organizations from the threats that matter most.

- **Security Integration.** Another Business-Driven Security capability is the ability to connect to enterprise authentication systems such as the RSA SecurID® Suite. Why is this important? Consider that the job of RSA NetWitness Suite is to keep the wrong people out, while the job of the RSA SecurID Suite is to let the right people in. Traditionally this binary system has favored one goal at the expense of the other, but that’s no longer appropriate.

  When your disparate security systems integrate for the benefit of business, that’s Business-Driven Security. In this example, say a user account fails repeated attempts to log in. Traditionally that would cause a threat detection and response solution to trigger an alarm and potentially take that user off the network until it can be proved that this isn’t a malicious actor abusing a hijacked account.

  But that could create a business issue, if a legitimate user is prevented from doing her job while you investigate. In a Business-Driven Security approach, that alert will trigger step-up authentication for that user, requiring multifactor or some other challenge that a real user could be expected to pass. This way there’s no disruption to the user, or to the business, and any potential or legitimate attack would be thwarted.
DESIGN, OPERATION, AND INCIDENT RESPONSE EXPERTS

Business-Driven Security is practiced across RSA, including within the RSA Global Services team, which is comprised of over 650 cybersecurity experts delivering services in over 100 countries. RSA Global Services offering combine the deep security skills and broad business knowledge to help bridge your organization's gap of grief:

- RSA Professional Services provides implementation, tuning, and training services to deliver business value fast.
- Within the RSA Risk and Cybersecurity Practice, two groups provide critical security capabilities:
  - The RSA Advanced Cyber Defense (ACD) Practice delivers services to assess breach readiness, Security Operations Center (SOC) or (CIRC/CIRT) assessment and design, incident response planning and testing, and “Expert on Demand” services.
  - The RSA Incident Response (IR) Practice helps customers design, manage, and perform the Incident Response function, with both proactive and reactive services. Available on both retainer and ad hoc bases, the RSA IR Practice extends your organization’s security skills to deal with security incidents of all types and severities.

YOUR CHOICE FOR BUSINESS-DRIVEN SECURITY

Business considerations continue to drive rapid and accelerating changes in computing models. The cloud, virtualization, and mobile revolutions have obliterated the IT perimeter forever. IT Security can no longer be isolated from all the other systems and processes. In this new world, RSA NetWitness Suite and the RSA Business-Driven Security approach makes your security teams and cyber risk management more effective.

As you narrow your choices in Threat Detection and Response platforms, measure your options by both attributes: how well they protect your strategic assets, and how they’re able to support your strategic business goals.

For more information or to get started with the RSA NetWitness Suite, visit rsa.com/domore or the RSA Link Community.

1 RSA Threat Detection Effectiveness Survey 2016
2 EU GDPR: General Data Protection Regulation Organization