Helping Breach Response for GDPR with RSA Security

Addressing the ticking clock of GDPR compliance

The European Union (EU) General Data Protection Regulation (GDPR) that takes effect in May 2018 will bring changes to organizations that handle personally identifiable information (PII) of European residents. This regulation is intended to strengthen the protection of PII with in the EU, and anywhere it is transferred outside of the EU. The scope of the GDPR encompasses all businesses based in the EU as well as any business that controls or processes personal data related to individuals in the EU. These requirements apply regardless of where the organization is based, making GDPR a truly global compliance requirement.

Non-compliance with GDPR requirements carries with it the potential for significant negative impacts; failure to achieve and maintain compliance is expected to result in fines up to 4% of an organization's annual world-wide revenue or 20 million Euros, whichever is greater. Without a holistic approach to GDPR compliance, organizations are likely to prematurely exhaust available human and capital resources and take an unnecessarily long time to prepare for the impending regulation.

Data protection is one of the key elements of the GDPR. After all, what good are all the GDPR's personal privacy enhancements if you can't keep the data secure and safe from misuse or theft? The GDPR sets forth requirements for data protection, and introduces new responsibilities that organizations must meet.

Breach Response is a key responsibility under the GDPR. Article 33 of the regulation lays out specific requirements for notification of a personal data breach to the supervisory authority. Notifications must take place generally within 72 hours after the organization becomes aware of the breach. That's not much time to perform forensics that will answer the important question: What's the impact? The answer to that question will help to determine whether you must notify everyone who was affected. Accomplishing this objective will require a combination of processes and technical capabilities including security incident management, security operations and breach management, as well as tools for deep monitoring and analysis of security data, including strong forensics tools.

RSA: Supporting a holistic approach to addressing data breaches

RSA offers business-driven security solutions that uniquely link business context

Preparation for GDPR is essential

The EU GDPR imposes interrelated obligations for organizations handling personal data of EU citizens, including:

- Adopting policies and procedures to ensure and demonstrate that PII is handled in compliance with the regulation
- Maintaining documentation of all processing operations
- Assessing electronic and physical data security risk to personal data including accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Implementing appropriate technical and organizational controls to ensure a level of security appropriate to the risk
- Implementing procedures to verify the effectiveness of the controls which align with the results of the risk assessment
- Performing data protection impact assessments on planned processing of highly sensitive personal data
- Providing transparent notice to EU residents at the time information is collected, upon later inquiry
- For some organizations, appointment of a Data Protection Officer charged with the responsibility of monitoring the organization's compliance with the EU GDPR requirements

with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to help organizations effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, all essential steps in helping an organizations develop a holistic strategy for responding to GDPR.

With GDPR requirements as context, let's take a closer look at the RSA product and service portfolio, and how these offerings can help organizations prepare for GDPR.

RSA NetWitness® Platform

The RSA NetWitness Platform is a leading threat detection and response platform that is designed to allow security teams to detect and understand the full scope of a compromise. RSA NetWitness Platform is differentiated from competitive solutions by two important characteristics:

- **Visibility** – by leveraging logs, packets, and endpoints, RSA NetWitness Platform enables you to see across your organization's data, including cloud and virtualized environments. This unmatched breadth of visibility is what enables RSA NetWitness customers to correlate seemingly unconnected alerts and events, to focus on the threats that matter.
- **Productivity** – With an all-new security analyst user experience, RSA NetWitness Platform provides visual cues to threats. Advanced threat intelligence and analytics are engineered to find the threats and create a prioritized investigation queue, while rich visualization capabilities make anomalous activity "pop" within the sea of legitimate data. Pivot tools permit analysts to quickly drill down on specific data to isolate and eliminate exploits.

For the GDPR, RSA NetWitness Platform offers specific capabilities that will help organizations detect and report security incidents. Its rich analytics capabilities are also great in assisting with compliance, which is about documenting your efforts and reporting accurately on what has taken place. In those important 72 hours before reporting a breach, RSA NetWitness Platform can document what happened, who was affected, and what was the impact. The GDPR is clear that organizations must implement appropriate security controls, and those that don't will be called into account for it in the event of a violation.

RSA NetWitness Platform also helps organizations address GDPR requirements for user data protection in the threat discovery and response activity itself. The platform is designed to provide a range of controls, such as obfuscation, that security analysts can leverage to protect privacy-sensitive data, without reducing analytical capability.

The RSA NetWitness Platform is designed to be configured to limit exposure of privacy-sensitive metadata and raw content (packets and logs) using a combination of techniques, including:

- **Data Obfuscation** – Privacy-sensitive metakeys can be obfuscated for specified analysts/roles
- **Data Retention Enforcement** – Retain privacy-sensitive data only as long as needed

- **Audit Logging** – Audit trail for privacy-sensitive activities, e.g., attempts to view/modify data

RSA Archer Suite

The RSA Archer suite is an industry leading Governance, Risk & Compliance (GRC) solution that is engineered to empower organizations to manage multiple dimensions of risk with solutions built on industry standards and best practices on one configurable, integrated software platform. The RSA Archer Suite includes specific use cases designed to help organizations looking to improve capabilities related to responding to security issues.

- RSA Archer data governance is designed to provide a framework to help organizations identify, manage, and implement appropriate controls around personal data processing activities.
- RSA Archer privacy program management is designed to enable organizations to group processing activities for the purposes of performing data protection impact assessments and tracking regulatory and data breach communications with data protection authorities.

Security Incident Management

RSA Archer Security Incident Management enables the processes to address the flood of security alerts and implement a managed process to escalate, investigate and resolve security incidents. The use case includes a centralized system to catalog IT assets for incident prioritization providing business context (usage of IT assets) to prioritize events. Workflow for security incidents with built in reporting of security incidents streamlines the process and enables teams to work effectively through the incident response process. Issues related to incident investigations can be tracked and defined procedures to handle security events can ensure incidents are handled properly.

Security Operations & Breach Management

RSA Archer Security Operations and Breach Management extends the security incident process by monitoring of key performance indicators, measurement of control efficacy, and management of the overall security operations team. Workflow is included to address data breaches enabling the security and business teams to react quickly to a breach of personal information. Enabling a focus on the most impactful incidents helps lower overall security risk and supports reacting promptly and appropriately to data breaches.

RSA risk and cyber security practice

RSA offers a range of strategic services designed to help you craft a business-driven security strategy, build an advanced security operations center and revitalize your governance, risk and compliance (GRC) program. To complement our robust product offering, we also provide implementation and post-implementation support so that you can maximize your investment in our products.

RSA incident response practice

Obviously, a major requirement within GDPR is the efficient and effective management of incidents when they do occur. When organizations discover a security breach, they need to determine—in short order—exactly what happened, how it happened, the scope and impact of the compromise, and the steps needed to contain and remediate it. RSA's incident response team can help organizations quickly understand the details and necessary steps during a breach. Paired with other RSA Archer solutions, the Incident Response Practice can tailor those next steps to help organizations meet the unique requirements of GDPR.

RSA Advanced Cyber Defense Practice

The RSA Advanced Cyber Defense Practice can help security organizations develop the processes, procedures, workflows and automation that facilitate a prompt, decisive response to data breaches and other cyber incidents.

Conclusion

Globally, organizations are actively assessing the impact of GDPR on their business and data privacy and management operations. The deadline of May 2018 is looming, and any organization collecting PII of EU residents needs to work through the deployment of additional processes, policies and technologies to avoid the significant fines posed by the regulation. A breach of personal data can lead to significant consequences and organizations must implement a strategy to protect PII of EU citizens including the ability to identify and respond to security threats. With a unique scope of products and services targeting the critical areas of threat detection and security incident response, RSA can act as a strategic partner in any organizations journey towards GDPR compliance.

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.