RSA

WHITE PAPER

Business-Driven Security & the GDPR

GDPR data protection & the RSA NetWitness® Platform

Introduction

The new European privacy law, the EU General Data Protection Regulation (GDPR), goes into effect on May 25, 2018. The GDPR represents a major evolution in global data security and privacy practices, and companies will need to thoroughly review, and in many cases drastically change, the way personal data is handled going forward.

That's because it's not just EU-based companies that will be affected; The GDPR is explicitly "extraterritorial." If your company does any business at all within the European Union, or has relationships with organizations that do, the GDPR will apply to you.

And the EU is ensuring that everyone takes this law as seriously as they do. The GDPR imposes very detailed and specific requirements, enforcing them with major penalties for violations – fines ranging up to €20 million, or 4% of a company's total annual sales, whichever is greater.

The EU has always been more privacy-oriented than most regions; the 1995 Data Protection Directive (DPD) embodied the EU's stance on personal data and privacy, and served as the framework for various laws and policies throughout the continent. But the DPD was more policy than law; its interpretation was left to member states.

In contrast, the GDPR makes this a core legal tenet across the EU. It enshrines data protection and privacy as a fundamental human right for EU citizens and residents. From an operational perspective, the driving principle is that any data that specifically relates to a person, belongs to that person — not to the organization creating, holding, or processing it.

Yet while the GDPR imposes substantial new requirements and penalties, there's also a big benefit to organizations. Compared to the DPD, the pan-EU nature simplifies compliance greatly. As a Regulation, the GDPR holds much broader power than the previous Directive ever did, but normalizes data law across the entire EU.

The GDPR requirements will impact every part of an organization. The law specifically states that:

- All new and existing processes and systems must conform to the principle of privacy by design
- Personal data collection must be kept to the minimum necessary, and solely in context of the activity taking place
- Organizations must obtain and record explicit consent for the data to be held or processed
- Users must be able to see any information about them, to request corrections, and to delete or move that data as they wish
- Data breaches must be reported to authorities within 72 hours of discovery
- All requirements apply to any personal data related to an EU resident, whether they are customers, employees, partners, shareholders, or others

So while the primary goal of user privacy may be simple, the impacts on companies are extraordinarily broad and complex, and creates challenges that only business-driven solutions can address.

Importantly, organizations must also take concrete steps to assure that personal data is protected from unauthorized access. Some of the most severe sanctions apply to instances where breaches result from insufficient or inadequate data protection efforts by the breached organization.

Data protection

It's critical to understand that data protection – not data privacy – is what the "DP" in GDPR stands for. This is because, no matter how well implemented are the processes of consent and control over a data subject's personal information, if it's lost in a breach, nothing else matters. Therefore, the protection of personal data is absolutely key to compliance with the GDPR – and is subject to the full force and effect of the penalties contained in the regulation.

Most organizations have deployed data protection infrastructure, ranging from firewalls and spam filters, to Data Loss Prevention (DLP) solutions and Intrusion Prevention Systems (IPSs). Still, we hear constantly about data breaches that affect millions of users.

The EU is clear that such breaches will be dealt with harshly under the GDPR, with strict new rules about disclosure to ensure reputational punishment, and massive fines to punish offenders financially. The GDPR recognizes that the threat environment has changed dramatically, and organizations must step up their game to protect EU residents.

Breaches continue because, as security infrastructure became standardized, threat actors have become adept at targeting attacks and evading defenses. Commercial-grade exploits are easily obtained from hacker marketplaces, and nation-states have developed weaponized attacks, often using zero-day vulnerabilities. The operating presumption these days must be that your

organization's IT infrastructure is under continuous attack, and likely already compromised in multiple ways.

This shifts the conversation from threat prevention, to threat detection and response. And it requires a different approach, using a different set of tools.

RSA NetWitness Platform is a leader in this fast growing market. Because it can monitor logs, packets, and endpoints, RSA NetWitness scans your entire infrastructure for indications, often subtle or obfuscated, that exploits are active. Through behavioral analysis and machine learning, the system correlates indicators and assigns risk scores that identify anomalies that warrant investigation.

Unlike traditional prevention systems, RSA NetWitness Platform helps your organization hunt for the threats that have successfully invaded your organization. Undetected, such exploits can wreak havoc on your infrastructure and intellectual property, and can create the types of data breaches that the GDPR specifically targets.

Fortunately, even if a threat has evaded an organization's defenses, for it to have any value, it must then do something. Examples include "phoning home" to a command and control (C2) server for instructions, or attempting privilege escalation, or network traversal intended to infect additional systems, and/or locate targeted high-value assets.

These activities look very different from "normal" behavior, which solutions like RSA NetWitness Platform are designed to detect by using behavior analytics. Exploit creators often engineer their software to hide among normal traffic, making it extremely difficult to isolate the bad activity from the good activity. Therefore, binary "positive/negative" detection becomes impractical, because the risk of blocking a legitimate activity, and disrupting your business becomes too great.

This is where a business-driven solution like RSA NetWitness Platform can dramatically raise your security effectiveness, and make your security investments go much farther. The GDPR is clear that organizations without a proactive security posture will be viewed harshly if personal data is lost, but the benefits of doing so go far beyond fine avoidance. RSA NetWitness Platform may help organizations satisfy the GDPR data protection requirement for "appropriate technical and organisational measures." And certainly effective threat protection can minimize the chances of data loss, and all the costs and disruption that goes with it. But to deliver real value, a solution must align with your business imperatives, not the least of which is to not disrupt the way people work.

There may be a very good reason, for example, that someone's ID is accessing an external resource via telnet, over a nonstandard port. But it's also a typical way for an exploit to behave, so alerting your Security Analysts is prudent. RSA NetWitness Platform will use the full context – seeing the full "scope of threat" – to highlight the likeliest problems for your analysts. For example, telnetting externally on a nonstandard port is much more likely to be malicious if the user ID belongs to an HR employee than your CTO. The "risk score" considers many such factors, including additional indicators of compromise (IOCs) that may apply.

In this way, RSA NetWitness Platform is able to take on the "needle in a haystack" problem, removing the hay until the needles are laying in plain sight. It's fundamentally different from traditional defenses, which operate on a reactive model, based primarily on software signatures of known exploits as they are discovered. Instead, RSA NetWitness gains effectiveness as it's used, as it learns what "normal" looks like in a particular organization, and as analysts tweak and tune the solution in the threat hunting process.

In fact, quickly discovering undetected threats is what RSA NetWitness Platform is all about. 70% of companies reporting a compromise in the previous year[1], and 90% are unsatisfied with incident response time[2]. RSA NetWitness Platform is focused on minimizing "dwell time," or the period when an exploit operates undetected before discovery. Dwell time has a high correlation to the damage wrought by an attack, and thus finding and responding quickly is the most critical variable in a threat detection and response program.

All of this is why, as an organization plans out its GDPR strategy, data protection should be at the top of the list. Protecting against data breach is good business any time, but it's particularly important to have a threat protection solution in place and operational before the GDPR takes effect in May, 2018. While the GDPR carries penalties of up to €20 million or 4% of a company's total annual sales for violations, it carries penalties of up to €10 million, or 2% of a company's total annual sales for simply failing to comply – which includes inadequate security efforts, even if no breach occurs.

Fortunately, implementing a threat detection and response solution is a straightforward process, and one that can be implemented now. Companies will have a lot of complex activities to research and design – for example the comprehensive privacy orchestration component of the GDPR. Moving first on the data protection solution will avoid resource contention during the "crunch time" before the GRDPR takes effect in May, 2018.

RSA NetWitness Platform, for example, can be implemented flexibly for any combination of logs, packets, or endpoints. Professional services from RSA or partners can quickly set up, train internal analysts, and even perform Incident Response (IR) if anything is found during implementation – which is often the case.

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

A user role in RSA NetWitness Platform allows it to be configured to limit exposure of privacy-sensitive metadata and raw content (packets and logs) using a combination of techniques, including:

[1] RSA Cybersecurity Poverty Index 2016

[2] RSA Threat Detection Effectiveness Survey 2016

- 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

Conclusion

The GDPR will drive fundamental changes in the way most organizations process personal data. Privacy and data protection will no longer be "nice to have" benefits; lacking them will become critical risks, both financial and reputational.

While many of the requirements of GDPR will require lengthy analysis and planning, RSA NetWitness Platform for threat detection and response can be implemented immediately. As you plan the sequence of activities needed to become compliant with the GDPR, start with your biggest and fastest win.

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational 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**.