Bitdefender®

Endpoint Detection & Response (EDR)

How to safeguard customers' personally identifiable information under the GDPR

Table of Contents

Intro

More data records were lost or stolen in the first half of 2017 than in all of 2016 [1]. And in 2017, Gartner found organizations were gravely underprepared for the European Union's General Data Protection Regulation (GDPR). More than half of companies affected by the regulation will not be in full compliance when it takes effect in May, the group said [2].

With only two months to go before the regulation is enforced, studies show little has changed. Yet the pressure of complying with the upcoming law weighs more heavily on everyone's shoulders by the day. Fortunately, solutions are readily available to businesses big and small seeking to ensure cyber resilience on their way to GDPR compliance.

> "The GDPR will affect not only EU-based organizations, but many data controllers and processors outside the EU as well. Threats of hefty fines, as well as the increasingly empowered position of individual data subjects tilt the business case for compliance and should cause decision makers to re-evaluate measures to safely process personal data." -- Bart Willemsen, research director at Gartner.

Context

Personally identifiable information has a central role in Digital Economy versus traditional business, and the biggest players are in the former camp. To protect personal rights in the digital space, both against abuse and against ever increasing cybercrime, the EU in 2012 decided to revise its existing data protection laws and create a unified framework by which every data processor should abide.

Negotiations between the European Parliament, Council and Commission resulted in a joint proposal in 2015. One year later, in April 2016, the EU Parliament adopted and approved the GDPR. The GDPR didn't require any new government legislation, so it was set to take effect May 25, 2018.

Although the law specifically aims to protect EU residents from data theft, companies both within and outside the Union have an obligation to comply with the new regulation **if they hold "personally identifiable information" (PII) of EU citizens**. Failure to comply will draw fines of up to 20 million euros, or up to 4% percent of the organization's annual turnover, whichever is greater.

According to the Information Commissioner's Office (ICO), many concepts and principles behind the GDPR are the same as those in the current Data Protection Act (DPA). Organizations currently in compliance with the DPA are well on their way to be compliant with the GDPR as well. However, organizations targeted by the new law should not take the GDPR lightly, nor should they rely solely on current procedures. Rather, they should use everything they know about protecting customer data as a starting point to build from.

Despite the availability of GDPR documentation toolkits containing so-called compliance "templates," experts at IDC warn that no template should be 100% applicable because of the sheer discrepancies between the operations of different businesses – even if those organizations are players in the same industry.

Developing a solid understanding of what the GDPR entails means to fully review your data, understand where it's located and how it's structured, how it flows and, most importantly, what it contains. This whitepaper offers a general look at the EU's agenda for the GDPR, with a focus on solutions available today that can help businesses achieve compliance.

GDPR key changes

The main purpose of the GDPR is to strengthen and unify data protection for all individuals within the European Union (EU). It compels data processors and custodians to be fully aware of the data they collect, store, process and move around, and imposes mandatory disclosure in case of a breach, assessments, and immediate action based on those assessments. And key changes in the GDPR give rise to these obligations:

Personally identifiable information (PII)

GDPR targets any organization that collects, processes and manages "personally identifiable information" of EU residents – or information that can be used (either on its own or in tandem with other information) to identify, contact or locate a single person, or to identify a person in a given context.

Jurisdiction

The biggest change to the regulatory landscape of data privacy is the extended jurisdiction of the GDPR. It applies to all companies processing PII of subjects residing in the Union, regardless of the company's location. A business could be operating in Antarctica (for the sake of the argument) yet still have to abide by the regulation if it collects and processes data belonging to EU residents.

Penalties

There is a tiered approach to fines. A company can be fined 2% of annual global turnover for not having their records in order, not notifying the supervising authority and victim about a breach, or not conducting an impact assessment. Lacking sufficient customer consent

to process data or violating the core of Privacy by Design concepts can spell a fine of up to 4% of annual global turnover or €20 million (whichever is greater) in penalties.

Consent

Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. Data Subjects must also be able to withdraw their consent as easily as they gave it.

Data Subject Rights

Data subjects are entitled to new rights under the regulation, including

- Breach notification – mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals."
- Right to access – obtain confirmation from the data controller that their personal data is Ăor isn't) being processed, where and for what purpose.
- Right to be forgotten (aka Data Erasure or the right to erasure) – entitles data subjects to oblige the data controller erase their personal data, cease further dissemination of the data, and even have third parties halt processing of the data as well.
- Data Portability – the right for a data subject to receive the personal data concerning them, which they have previously provided in a "commonly used and machine-readable format" and have the right to transmit that data to another controller.

Privacy by Design

This calls for the inclusion of data protection from the onset of the designing of systems (instead of an addition / amendment / patch / fix).

Data Protection Officer (DPO)

Most Member States have different notification requirements, leading to bureaucratic chaos every time a breach occurs. This is about to change as the GDPR requires data processors to appoint a Data Protection Officer (DPO) whose core attributes will be to conduct regular and systematic monitoring of data. This person must be an expert in data protection law and practices, and will report directly to top management. The role can be appointed internally but can also be outsourced.

Road to compliance

GDPR can be viewed as a huge public service for data subjects and, at the same time, a major pain for businesses. However, think tank PwC recommends that organizations view GDPR and NIS (the EU's Directive on Security of Network and Information Systems) as opportunities to stay ahead of the curve [5].

> "CEOs should see GDPR and the NIS directive not as compliance drills but rather as strategic opportunities to align their business for success in a data-driven world. In addition, companies should be reaching out to regulators to build relationships and lines of communication before compliance deadlines arrive." -- Grant Waterfall, PwC's Europe, Middle East and Africa Cybersecurity and Privacy Leader.

To that extent, to comply with the GDPR, aggregators of EU customer data will have to hone their breach-detection and breach-response skills to unprecedented levels. In fact, according to the Information Commissioner's Office (ICO) – the UK's independent data privacy watchdog – a key requirement to complying with the regulation is setting systems and procedures in place to minimize the risk of a breach. In other words – implement a sturdy incident response plan. Starting May 25, an incident response program is no longer just good to have, but a must-have for data processors and custodians, or anyone in between.

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. – Information Commissioner's Office: Preparing for the General Data Protection Regulation (GDPR) | 12 steps to take now) [6]

Following industry best-practices is key, as GDPR requires evidence of accountability. If a breach occurs, at the very least an organization must be able to limit the damage, reduce the penalties and avoid getting its image tarnished.

Your typical attack cycle / attack kill-chain

Probably the most infamous breach of 2017 was the Equifax incident. The breach occurred simply because the firm's IT department did not make it a priority to patch known vulnerabilities in Apache Struts – an open-source framework for developing Java EE web applications. Attackers took full advantage of that oversight and proceeded to breach the consumer credit reporting agency and compromise the personal and financial data of more than 143 million US customers. The incident prompted the immediate firing of two executives, and weeks later the CEO stepped down as well. The biggest damage, however, was to Equifax's image.

The illustration below offers a typical attack scenario (similar in many ways to how the Equifax incident allegedly occurred), described further down in a little more detail.

1. Reconnaissance – Intruders select a target, research it and attempt to identify vulnerabilities in the targeted infrastructure.

2. Weaponization – Intruders use a known exploit (or create one themselves, in some cases) to weaponize the malware they are about to deploy.

3. Delivery – Intruders deploy weapon to target (either via social engineering, e-mail attachments, spoofed websites or even physically via USB flash drives).

4. Exploitation – Malware weapon's program commences on target endpoint to exploit vulnerability.

5. Installation – Malware weapon installs access tools (for example, a "backdoor") usable by the attacker.

6. Command & Control Center – Malware establishes back-and-forth route allowing intruders persistent access to targeted infrastructure.

7. Actions on Objective – Intruders act to achieve their goals (data exfiltration, data destruction or encryption for ransom).
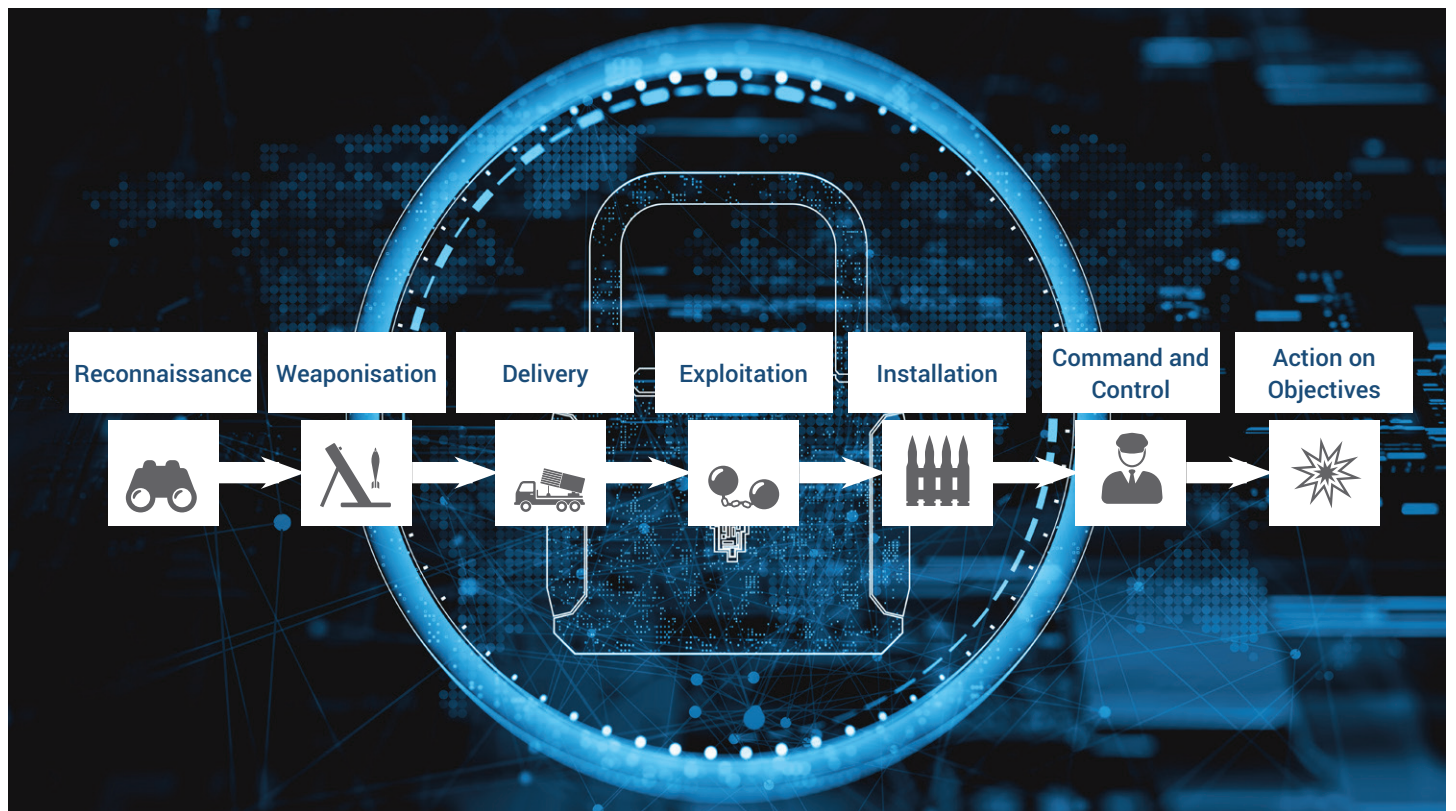
Endpoint Detection & Response (EDR) – an instrument for your Incident Response team

Like the attack kill-chain, the incident response team needs to respond with its own series of steps, such as prepare, contain, eradicate, as well as make a fast recovery following an incident. Endpoint Detection & Response (EDR) solutions are specifically designed to assist an organization's incident response plan.

EDR is built to detect, report, quarantine and neutralize an attack at every stage of the attack cycle (fig. 1). Ideally, IT departments should use a solution that has been built from the ground-up with a single-agent / single-console architecture, one that reduces the effort to deploy and effectively manage the security of endpoint infrastructure.

To have an incident response team in place with EDR capabilities means to have an organized approach to validating, addressing and managing the aftermath of a security breach or cyberattack. The goal is to handle the situation in a way that prevents, or at least limits, damage and costs, and reduces recovery time. Investing in an EDR solution is central to achieving these goals.

EDR not only enables the Incident Response team to act before the attack unfolds, it also assists the organization in reporting their course of action to data protection authorities. Data processors and collectors should make no mistake – if they get breached, they will be asked to demonstrate every bit of accountability as part of the 72-hour disclosure requirement.

Closing statements

80% of large organizations, 25% of midsize organizations, and 10% of small organizations are investing in endpoint detection & response, placing EDR as a technology on track to become a key security asset by 2020. (7) Demand for incident response tools that offer early visibility into advanced threats is further expanding the market, with expectations of a CAGR of 45.27% from 2015 through 2020. The EDR market grew from $238 million in 2015 to about $500 million in 2016. By 2020, it is expected to become a billion-dollar market, rivaling the multi-billion-dollar market for endpoint protection platforms (EPP).

Bitdefender Gravity Zone Ultra offers an easy-to-use, integrated next-gen endpoint protection and EDR platform that accurately protects enterprises against sophisticated cyber threats. It offers prevention, detection, automatic response, clear visibility into suspicious activities and one-click resolution capabilities. As the deadline for GDPR compliance approaches fast, investing in EDR solutions will become instrumental for every organization sitting on personally identifiable information (PII) belonging to EU residents.

To learn more about EDR and Bitdefender's offering to assist your incident response plan, visit https://www.bitdefender.com/business/ultra-security/.

Glossary

GDPR – General Data Protection Regulation

DPA – Data Protection Act

ICO – Information Commissioner's Office

DPO – Data Protection Officer

PII – Personally Identifiable Information

EDR – Endpoint Detection & Response

EPP – Endpoint Protection Platform

CAGR – Compound Annual Growth Rate

Resources

(1)   https://www.csoonline.com/article/3235684/data-breach/more-data-records-were-lost-or-stolen-in-the-first-half-of-2017-than-all-of-2016.html

(2)   https://www.gartner.com/newsroom/id/3701117

(3)   https://ico.org.uk/

(4)   https://www.idc.com/

(5)   https://press.pwc.com/News-releases/organisations-are-not-doing-enough-to-protect-data-privacy/s/b56bf806-5712-4462-98a1-161c1a3f9cbe

(6)   https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

(7)   https://www.gartner.com/newsroom/id/3744917

About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/