netwrix

Hitting a Moving Target

Why GDPR Compliance is an Ongoing Process

Ann Barrett
GDPR Consultant
https://www.linkedin.com/in/annbarrettdublin

Dave Matthews
Systems Engineer at Netwrix
Dave.Matthews@netwrix.com

Disclaimer

- The information contained in these slides and their presentation is based generally on data protection law, regulations, codes of conduct etc.
- It is not intended to provide a comprehensive or detailed statement of the law and does not constitute legal or professional advice.

Agenda

- Business Context
- Quick Review of GDPR
- Trends
- Challenges
- Looking Forward

Brief History

Tim Berners Lee uploads first web-page - 12th November 1990.

WWW switched on - 23rd August 1991.

The Data Protection Directive (DPD) was enacted in 1995.

The GDPR was ratified mid 2016 and immediately became law. Member states had a 2 year implementation period. Enforcement commenced on 25th May 2018.

The law aims to give citizens more control over their data and to create a uniformity of rules to enforce across the European Union.

Demand for Security Products and Services

Detection, Response and Privacy Driving Demand for Security Products and Services

Worldwide spending on information security products and services will reach more than $114 billion in 2018, an increase of 12.4% from last year, according to the latest forecast from Gartner, Inc.

In 2019, the market is forecast to grow 8.7% to $124 billion.

"Security leaders are striving to help their organizations securely use technology platforms to become more competitive and drive growth for the business. Persisting skills shortages and regulatory changes like the EU's Global Data Protection Regulation (GDPR) are driving continued growth in the security services market."

Siddharth Deshpande, research director at Gartner

Source: Gartner, 15th August 2018

Demand for Security Products and Services

A 2017 Gartner survey* revealed that the top 3 drivers for security spending are:

- Security risks
- Business needs
- Industry changes

Privacy concerns are also becoming a key factor. Gartner believes privacy concerns will drive at least 10% of market demand for security services through 2019 and will impact a variety of segments, such as

- Identity and access management (IAM)
- Identity governance and administration (IGA)
- Data loss prevention (DLP)

An increased focus on building detection and response capabilities, privacy regulations such as GDPR, and the need to address digital business risks are the main drivers for global security spending through 2019 – see table on next slide.

Source: Gartner, 15th August 2018

* In September and October 2017, Gartner conducted a survey to gain insights about current and planned security spending. A total of 480 respondents participated in the survey, from 8 countries: Australia, Canada, France, Germany, India, Singapore, the U.K. and the U.S.

Worldwide Security Spending by Segment (in mil USD)*

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	101,544	114,152	124,116

Source: Gartner, August 2018

* Effective July 2018, Gartner added segments to the security software forecast and transitioned to reporting end-user spending. New segments were added to the forecast scope, including integrated risk management software, tokenization, threat intelligence, vulnerability assessment and others. This broadened scope and revised methodology mean this forecast cannot be directly compared to previous Gartner forecasts.

Key trends affecting Information Security spending in 2018-2019

At least 30% of organizations will spend on GDPR-related consulting and implementation services through 2019.

Organizations are continuing their journey toward compliance with the GDPR that has been in effect since 25 May 2018. Implementing, assessing and auditing the business processes related to the GDPR are expected to be the core focus of security service spending for EU-based organizations, and for those whose customers and employees reside there.

Risk management and privacy concerns within digital transformation initiatives will drive additional security service spending through 2020 for more than 40% of organizations.

Consulting and implementation service providers have retooled their service offerings over the past several years to support customers on their digital transformation journey. Security is a key factor in the uptake of that transformation process for regulated data, critical operations and intellectual property protection spanning public cloud, SaaS and the use of Internet of Things (IoT) devices.

Source: Gartner, August 2018

Key trends affecting Information Security spending in 2018-2019

Services (subscription and managed) will represent at least 50% of security software delivery by 2020.

Security as a service is on the way to surpassing on-premises deployments, and hybrid deployments are enticing buyers. A large portion of respondents to Gartner's security buying behavior survey said they plan to deploy specific security technologies, such as security information and event management (SIEM), in a hybrid deployment model in the next two years. Managed services represented roughly 24 percent of deployments, on average.

"On-premises deployments are still the most popular, but cloud-delivered security is becoming the preferred delivery model for a number of technologies"

Siddharth Deshpande, research director at Gartner

Source: Gartner, August 2018

Why GDPR is a Good Thing

- 87% of consumers believe it is important for companies to safeguard the privacy of their information

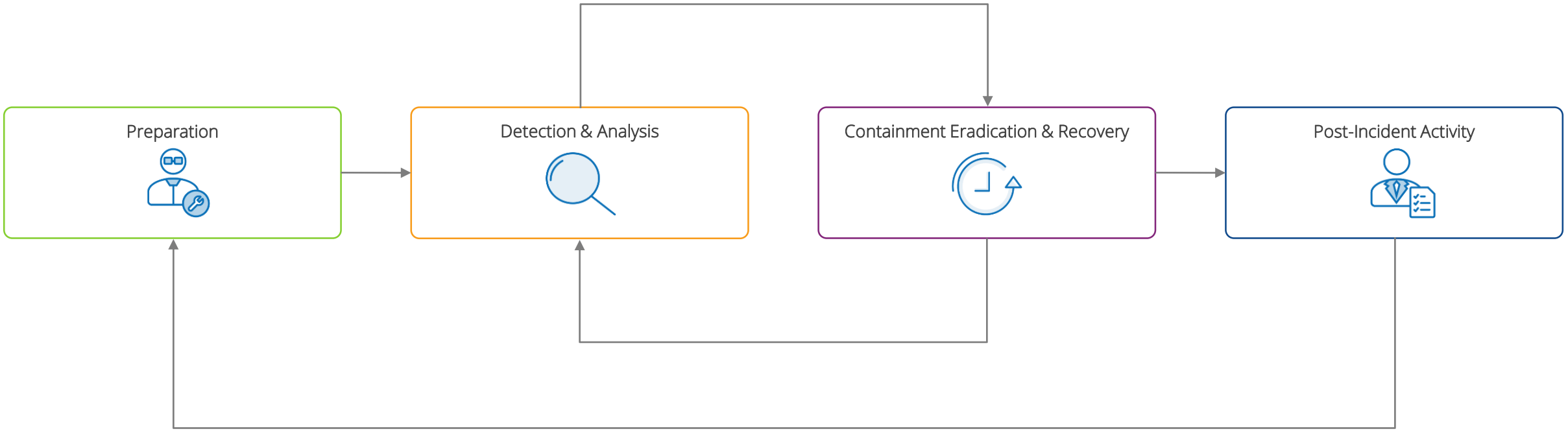
- Consistency in how data is protected
- 'Making sure you are compliant with GDPR gives you key operational efficiencies' through better management of personal data.
- Those processors who can demonstrate compliance will win business - procurement companies need the right level of evidence that their processor could comply with GDPR - this is about performing the correct due diligence on your supply chain.
- 'Helping' companies 'in their due diligence processes when tendering for business'

Sources:
Accenture, 2017
CEO Today Magazine, May 2018

6 Principles of GDPR (Article 5)

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality (Security)

Importance of Early Detection



The GDPR – 12 Steps

1. Becoming Aware

Review and enhance your organization's risk management processes – identify problem areas now.

2. Becoming Accountable

Make an inventory of all personal data you hold. Why do you hold it? Do you still need it? Is it safe?

3. Communicating with Staff and Service Users

Review all your data privacy notices and make sure you keep service users fully informed about how you use their data.

4. Personal Privacy Rights

Ensure your procedures cover all the rights individuals are entitled to, including deletion and data portability.

5. How have Access Requests changed?

Plan how you will handle requests within the new timescales – requests must be dealt with within one month

6. What we mean when we talk about a 'Legal Basis'

Are you relying on consent, legitimate interests or a legal enactment to collect and process the data? Do you meet the standards of the GDPR?

7. Using customer consent as a grounds to process data

Review how you seek, obtain and record consent, and whether you need to make any changes to be GDPR ready.

8. Processing Children's Data

Do you have adequate systems in place to verify individual ages and gather consent from guardians?

9. DPIA and Data Protection by design and default

Data privacy needs to be at the heart of all future projects

10. Reporting data breaches

Are you ready for mandatory breach reporting? Make sure you have the procedures in place to detect, report and investigate a data breach.

11. Data Protection Officers

Will you be required to designate a DPO? Make sure that it's someone who has the knowledge, support and authority to do the job effectively.

12. Cross-border processing and the one stop shop

The GDPR includes a 'one-stop-shop' provision which will assist those data controllers whose companies operate in many member states.

Source: Data Protection Commissioner: Dublin and Portarlington

Initial Focus Areas

- Privacy Notices
- Requesting Consent from Data Subjects
- Identifying Personal Data
- Process and Procedure definition/refinement
- Contract amendments

Trends & Items of Note

- The UK Information Commissioners Office (ICO) analysed enforcement actions against the 8 principles of the Data Protection Act 1998. Their findings concluded that over half of the enforcements were due to poor data security measures implemented within organisations and a third of enforcement actions were due to inadequate data retention policies.
- UK ICO has seen a doubling in the number of queries since the introduction of GDPR
- ECJ's importance
- Wirtschaftsakademie Schleswig-Holstein and Facebook
    - Controllership – Facebook and WSH deemed to be co-controllers (Article 26)
    - Independence of Data Protection Commissioners
    - Establishment
- Privacy notices
- Contract amendments
- Absence of substantial case law leads to ambiguities

Tech firms lead the laggards as GDPR compliance stalls

- More than one in three businesses (37%) confess they are still not following GDPR nearly three months after the regulation came into force, with technology companies the worst culprits.

- So says a new survey of just over 1,000 UK workers carried out by digital marketing agency MarketingSignals.com, which also showed that nearly one in five (17%) admitted they are still unsure as to what the benefits of being GDPR-compliant are.

Source: dataIQ, August 2018

Google fights plan to extend 'right to be forgotten‘

- The European Court of Justice is hearing evidence on the matter and will rule in 2019.
- Google argues that extending the law could turn it into a tool for censorship, in "less democratic" regimes.
- France's regulator said that Google is currently not respecting the rights of citizens to have information erased.

Source: BBC, September 2018

Challenges

- Absence of clarity on how Data Protection Commissioners will use powers
- Limited Case Law at this time
- Complying with requests from Data Subjects

Privacy Shield

- The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.
- The European Commission passed the data-sharing privacy framework on July 12, 2016, after its precursor, Safe Harbor, was struck down by the European Court of Justice on October 6, 2015.
- Is based on the now defunct EU directive 95/46, which the European Union General Data Protection Regulation replaced when it went into effect on May 25, 2018.

- Official Website: https://www.privacyshield.gov

Privacy Shield Status Unclear

- MEPs adopted a resolution calling for the suspension of the EU-US Privacy Shield – July 2018, although a full suspension is unlikely
- Press Response to above:

"United States, you have 2 months to sort Privacy Shield … or data deal is for the bin – Eurocrats"

The Register, 2018

"EU parliament calls for Privacy Shield to be pulled until US complies"

TechCrunch, 2018

" Are you Ready for the End of Privacy Shield?"

CMS WiRE

DPC vs Facebook, April 2018 (11 questions referred to ECJ)

- Whether provisions of EU law related to national security, public security, defense, and state security apply to transfers of data outside the EU under SCCs;
- Whether relevant EU law or EU Member State laws are the appropriate comparator for determining if a violation of individual rights occurred (and whether to include EU Member States' national security practices in that comparator);
- Whether the assessment of a third country's level of privacy protection should include administrative, regulatory and compliance practices, policy safeguards, procedures, protocols, oversight mechanisms, and non-judicial remedies;
- Whether transfer of personal data from the EU to the U.S. under valid SCCs violates the rights of individuals under Articles 7 and/or 8 of the Charter of Fundamental Rights of the European Union (the Charter) (note – these articles state the rights to data protection and privacy);
- Whether the level of protection afforded by the U.S. respects the essence of an individual's right to a judicial remedy for breach of data privacy rights as guaranteed under the Charter, and if so, whether limitations imposed by U.S. law on access to judicial remedies are necessary and proportionate for national security in a democratic society according to Article 52 of the Charter;

DPC vs Facebook, April 2018 (11 questions referred to ECJ)

- What level of protection is required for personal data transferred to a third country pursuant to SCCs in light of the Data Protection Directive and the Charter, and what factors should be reviewed in determining the adequacy of the level of protection offered by a third country;
- Whether the SCCs can include additional safeguards per Article 26(2) of the Data Protection Directive sufficient to cure any deficiencies for third countries where national authorities may require a data importer to make personal data received under an SCC available for national security purposes;
- Whether a data protection authority (DPA) can use its own discretion in determining whether to suspend data flows to a third country data importer if the DPA believes that country's surveillance laws conflict with relevant EU law;
- Whether the Privacy Shield Decision constitutes a finding that the U.S. has an adequate level of privacy protection, and if not, what relevance the Privacy Shield Decision has in assessing the adequacy of U.S. privacy safeguards related to SCCs;
- Whether the provision of the Privacy Shield ombudsperson under the Privacy Shield Decision, in combination with existing U.S. law, ensures a remedy compatible with Article 47 of the Charter;
- Whether the SCC Decision violates the Charter.

California Consumer Privacy Act, A.B. 375

Grants California residents unprecedented control over the collection, use, and sale of personal information. Many have already speculated that other state legislatures will follow suit and adopt a similar law in their own states, as has occurred in the wake of past California laws on data privacy and security. A copy of the law can be found here.

Among other provisions, the law states that:

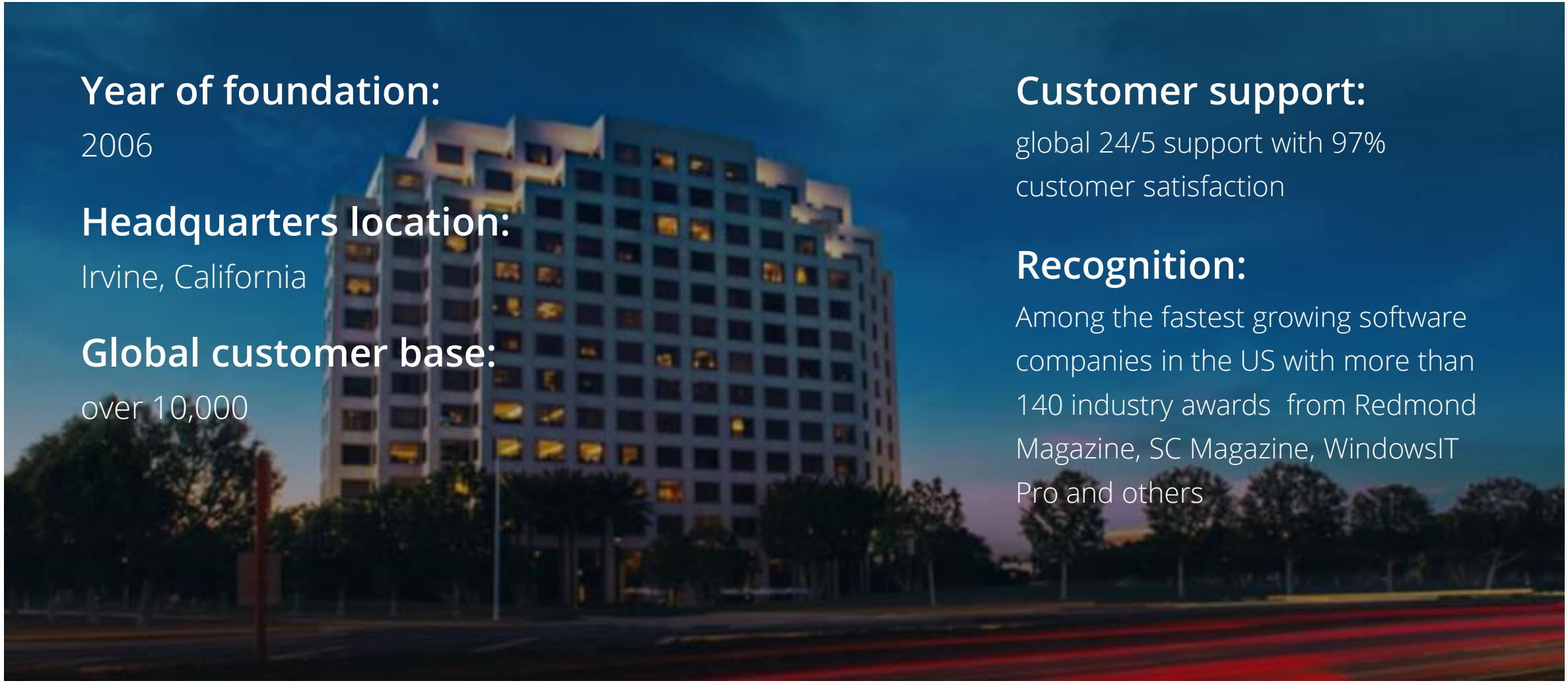
- Californians have the right to request that a business that collects a consumer's personal information disclose what categories and specific pieces of personal information the business has collected;
- Californians have the right to request that a business delete any personal information about the consumer;
- Californians have the right to direct a business not to sell the consumer's personal information, which is referred to as the right to opt out; and
- Californians can bring a private right of action against a company if there is an unauthorized breach of non-redacted or non-encrypted personal information.

Source: Lexology, June 2018

Looking Forward

- Clarification on how GDPR will be enforced, e.g. more case law
- Breaches / Fines
- Privacy Shield
- ePrivacy Regulation
- Brexit
- California Privacy Act
- 2019 – Politics may get in the way

About Netwrix Auditor



Year of foundation:

2006

Headquarters location:

Irvine, California

Global customer base:

over 10,000

Customer support:

global 24/5 support with 97% customer satisfaction

Recognition:

Among the fastest growing software companies in the US with more than 140 industry awards from Redmond Magazine, SC Magazine, WindowsIT Pro and others

About Netwrix Auditor

Netwrix Auditor

A **visibility** platform for **user behavior analysis** and **risk mitigation** that enables control over **changes**, **configurations** and **access** in hybrid IT environments.

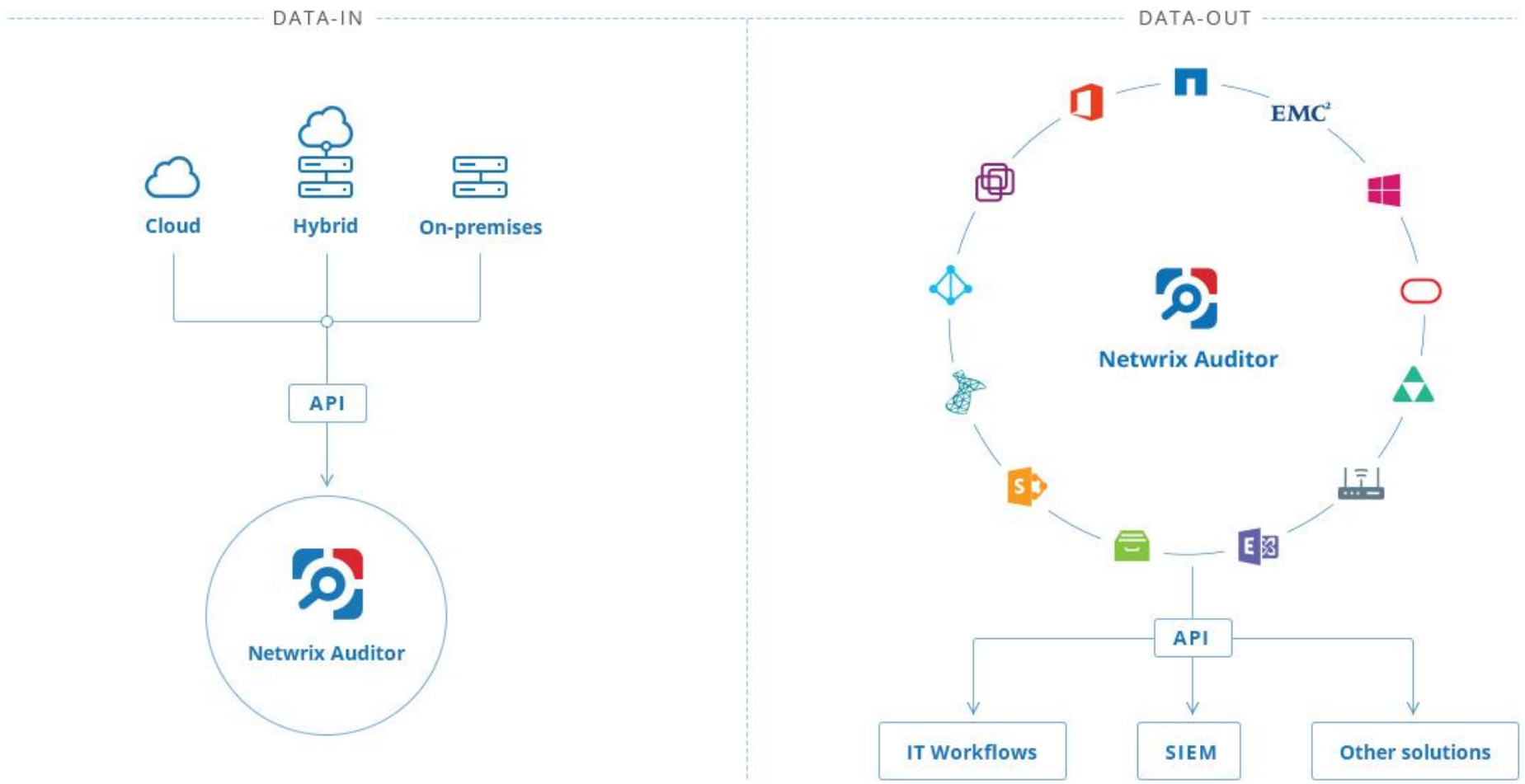
It provides security **intelligence** to identify security holes, **detect** anomalies in user behavior and **investigate** threat patterns in time to **prevent** real damage.

Netwrix Auditor Unified Platform

Netwrix Auditor Platform

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Azure AD
- Netwrix Auditor for Exchange
- Netwrix Auditor for Office 365
- Netwrix Auditor for Windows Server
- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Netwrix Auditor for SharePoint
- Netwrix Auditor for Network Devices
- Netwrix Auditor for Oracle Database
- Netwrix Auditor for SQL Server
- Netwrix Auditor for VMware

Netwrix API


DATA-IN
Cloud
Hybrid
On-premises
API
Netwrix Auditor
DATA-OUT
EMC²
Netwrix Auditor
API
IT Workflows
SIEM
Other solutions

Netwrix Auditor Add-On Store

Gain complete visibility into your AWS environment to **ensure data security and compliance**

Stay abreast of any suspicious access to your Linux systems to **avert potentially harmful activity**

Maximize visibility into the **actions of privileged users** across your Linux and Unix environment

RADIUS Server

Detect and analyze unauthorized access to your network with visibility into RADIUS logons.

What GDPR Requirements Does Netwrix Auditor Address?

CHAPTER II. Principles

Article 5. Principles relating to processing of personal data
§1 (f); §2

CHAPTER III. Rights of the data subject

Article 15. Right of access by the data subject
§1 (b)

Article 16. Right to rectification

Article 17. Right to erasure ('right to be forgotten')
§1

Article 20. Right to data portability
§1

CHAPTER IV. Controller and processor

Article 24. Responsibility of the controller
§1

Article 25. Data protection by design and by default
§1; §2

Article 32. Security of processing
§1 (b, c, d); §2; §4

Article 33. Notification of a personal data breach to the supervisory authority
§1; §3 (a)

Article 34. Communication of a personal data breach to the data subject
§1

Early Detection and Dealing with Incidents

Detecting **security incidents** in a timely manner

Investigating **anomalous activity** that is detected

Determining the **severity** of a **data breach**

netwrix

Netwrix Auditor

Demonstration

netwrix

Netwrix Auditor – DDC Edition

Data Discovery and Classification

Empowers risk, compliance and data security officers and IT security pros

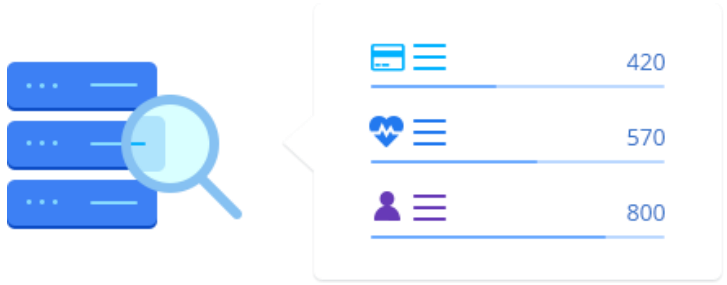
to **prioritize** their efforts and **secure** data in accordance with its **value** or **sensitivity**.

It enables them to **mitigate** the risk of PII, PHI, PCI and IP being stored outside dedicated locations

and apply controls and policies **consistently** and **accurately**,

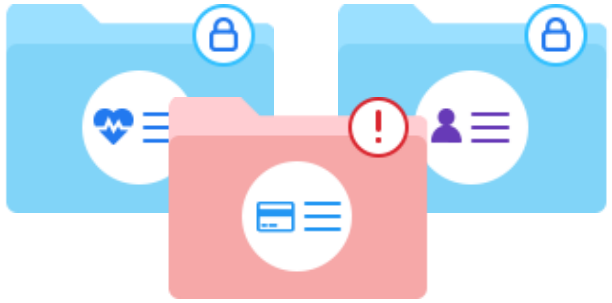
so their organization can ensure both data **security** and regulatory **compliance**.

Locating your sensitive files



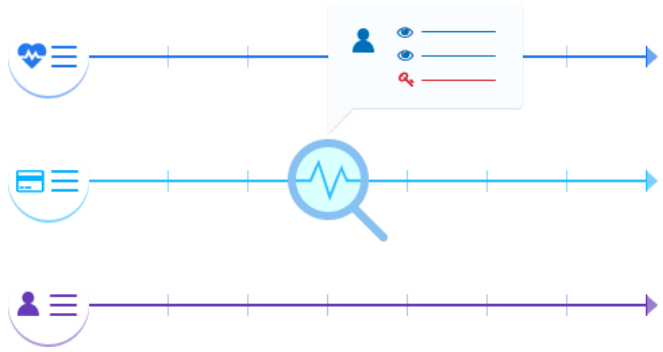
Gaining a **high-level view** of the **sensitive data** you store

Prioritising efforts and **spending** on the **most critical** assets first

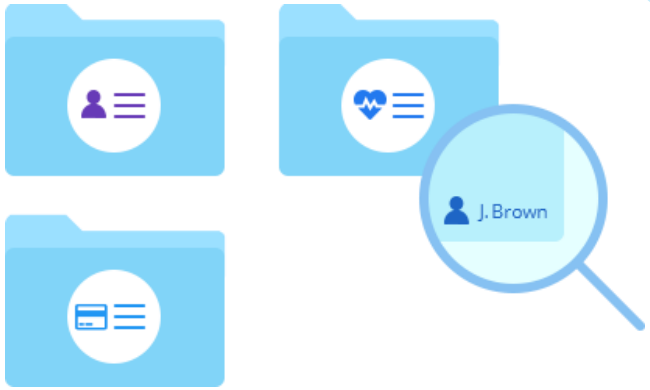


Discovering sensitive data stored **outside of a secure location**

Address Accountability principle and the Right to Be Forgotten



Detecting **unauthorized activity** around your sensitive data



Addressing **subject access** requests and complying with the '**Right to Be Forgotten**'

Useful Links

- Official pdf of the legislation
- European Court of Justice
- Irish DPC Website
- UK ICO's September Newsletter
- Latest GDPR News
- What's Changed so Far?
- Why GDPR is Good for Business

Next Steps

Contact Sales to obtain more information

https://netwrix.com/contactsales

Read blog post "Data Classification: What It Is, Why You Should Care and How to Perform It"

https://blog.netwrix.com/2018/03/15/data-classification-explained-what-it-is-why-you-should-care-and-how-to-perform-it/

Download eBook "What is GDPR: 10 FAQs"

https://try.netwrix.com/what-is-gdpr-ebook-nemea.html

Review GDPR Requirements and Netwrix Auditor Mapping

https://try.netwrix.com/gdpr-compliance-nemea.html

Questions?

Thank You!

Ann Barrett
GDPR Consultant
https://www.linkedin.com/in/annbarrettdublin

Dave Matthews
Systems Engineer at Netwrix
Dave.Matthews@netwrix.com

Appendix

What is Personal Data?

Article 4

- The GDPR applies to the processing of personal data that is:
- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

What is Personal Data?

- If personal data can be truly anonymised then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

Data Subjects' Rights

Articles 14 – 22

- To be informed
- Access
- Rectification
- Erasure ('right to be forgotten')
- Restrict processing
- Data portability
- Object
- In relation to automated decision making and profiling.

Consent is only one of six possible legal bases for data processing

Article 6 – Lawfulness of Processing

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Do we need to appoint a Data Protection Officer?

Under the GDPR, you **must** appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

Controllers and Processors

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Data Protection by Design and by Default

- The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is ‘data protection by design and by default’.
- In essence, this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as ‘privacy by design’, it has have always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR’s fundamental principles and requirements, and forms part of the focus on accountability.