# Uncovering A Major Hidden Risk of GDPR Legislation

Companies in Europe today are focused on GDPR compliance. The smart ones are approaching the preparation for future compliance in a methodical and phased way, beginning with an assessment of the current data protection measures in place and identifying gaps or other threats to data security.

The legislation is incredibly hostile to business, yet it is a natural evolution of our changing society and the required balance that is constantly negotiated between industry and technology and their impact on people's lives. What is alarming about the GDPR legislation, as it is written, are the hidden risks that will threaten companies that believe themselves compliant, but may unwittingly be missing the bar for compliance.

The new law is focused on corporate actions required after the discovery of a breach, but fails to adequately define what constitutes a 'reasonable' period of time to discover a breach. Enterprises that are relying on defensive technologies alone – whether traditional defenses like endpoint protection and whitelisting or more modern defenses like EDR and SI (Security Intelligence) analysis tools – will face problems.

## The Impact for EU Businesses

The GDPR legislation defines a period of time, specifically 72 hours, following the discovery of a breach, to notify affected parties and authorities. That much is clear and defined.

However, the period of time to detect the breach remains undefined.

What constitutes a 'reasonable time' to discover a breach? With a lack of clear guidelines in the GDPR, the courts will likely decide. The issue is already working its way through courts of competent jurisdiction in the USA. In early 2016 a massive malware hack of fast casual dining chain 'Noodles & Company' impacted hundreds of thousands of customers' financial data, the problem exacerbated by the fact the malware persisted for months undetected.

In the autumn of 2016 American financial institutions filed a class-action lawsuit against 'Noodles & Company', in part claiming that the company should be held liable due to negligence because they 'let' malware persist undetected for four months.


## Allowing Breaches to Persist Opens Up Liability

European companies working to comply with GDPR, and believing themselves to be compliant – run the eventual risk of being found effectively non-compliant, if they allow a breach to persist for weeks, months or even years.

The GDPR, in its opening clauses specifically states (GDPR page 17 paragraph 87): "It should be ascertained whether all appropriate technological protection and organizational measures have been implemented to establish immediately whether a personal data breach has taken place..."

This language implies that as technology changes, enterprises have an obligation to modernize their discovery capabilities. This further compounds the risks inherent in lengthy gaps between breaches and the discovery of the breaches.

## Modernize Your Security Posture with Infocyte HUNT™

The breach detection gap – or dwell time – is defined as the period of time between first execution of malware and its discovery. Infocyte HUNT helps enterprises manage and mitigate their risk exposure, the solution enables organizations to define and manage this gap.

Stated another way – Enterprises using Infocyte HUNT are able to determine and enforce HOW LONG malware is allowed to persist undiscovered after it breaches existing defences. That period of time may be one week, one day, 12 hours or any period of time that an enterprise decides is appropriate.

Infocyte HUNT uses dissolvable agents that validate that each endpoint in an organization is 'clean' and malware free. HUNT uses volatile memory analysis, memory un-mapping techniques and more to collect the required information from each endpoint. HUNT then analyses the gathered data and delivers clear, easy to read reports that even junior IT administrators can work with to address potential breaches.

HUNT effectively delivers a solution that equips enterprises with the skill set of a highly specialised Forensic Analyst, executing the work in a fraction of the time and cost that a dedicated specialist would require.

## Harness the Power of Infocyte HUNT and Get Ahead of GDPR Specifications

Adopting Infocyte HUNT and the capabilities it offers, puts organizations in a best practice position. The functionalities are useful today, using HUNT Compromise Assessments will validate how effective your existing defences are and provide proof that you are malware free. HUNT also allows entities the flexibility to react easily to the inevitable clarification of what a 'reasonable time' is to detect malware that has breached existing defences.

- Manage and address risk
- Hunt malware that's hiding on your endpoints
- Uses Forensic State Analysis
- Find malware even if it's dormant or unknown
- Fast – Compromise Assessments can be done in hours
- Lightweight and Affordable
- Receive actionable reports
- Take action before a breach
- Created by ex US Military cyber hunters

Remove the uncertainty.  Find the threats.  Identify the holes in your defences. Prepare for GDPR the smart way.

Learn more about how Infocyte HUNT delivers the ability to define and manage your breach detection gap.

Infocyte®


CORPORATE HEADQUARTERS

110 E. Houston St. Floor 6

San Antonio, TX 78205

+ 1.844.INFOCYTE (844.463.6298)

sales@infocyte.com

www.infocyte.com

@InfocyteInc