ACALVIO

Achieving GDPR through Autonomous Deception

Delivering Operationally Efficient Compliance

Executive Summary

The European Union's General Data Protection Regulation (GDPR) has forced significant changes in the way organizations handle the personal data of EU citizens. GDPR mandates a broad range of principles, requirements and notifications that are very difficult to avoid. Massive penalties for non-compliance give the GDPR punitive teeth other compliance regimens lack. Although the implementation of GDPR is still a work in progress, there are clear steps organizations should take now to protect their reputation. In particular, active adversarial monitoring and response as exemplified by Acalvio ShadowPlex both protects in-scope data, and demonstrates to regulators a high level of commitment to data protection.

Highlights

- The GDPR establishes a detailed framework for data privacy for all EU citizens, independent of location.
- GDPR includes requirements for security and availability, and heavy fines for non-compliance
- Acalvio ShadowPlex helps meet the security and availability requirements of GDPR by monitoring and reacting to attempts to access personal data.
- Acalvio delivers monitoring and response controls in a more cost-effective and operationally efficient manner than alternative approaches.

General Data Protection Regulation - Fundamentals and Penalties

GDPR was created by the European Union in response to the frequency and impact of data breaches, and because it was apparent that citizens had little control over how their data was being used. To this end, the GDPR reclassifies data protection as a human right, as opposed to just a consumer right. The GDPR further defines a number of data privacy rights fundamental to this position. All entities that handle the data of EU citizens must respect these rights in their data processing. Crucially, the location where the data is processed is irrelevant. If the data can be associated with a particular EU citizen, it is in-scope for GDPR.

To encourage compliance, the GDPR mandates heavy penalties for violations. These can include fines of up to 20M Euros or 4% of a company's worldwide revenue, whichever is higher. Also breach notification (to either the relevant government or to the public) may be required, in some cases not later than 72-hours. This tight deadline means that organizations need to have strong monitoring controls in place, so that they can quickly determine if notification is required or not.

GDPR - Rights and Principals

GDPR advances the concepts of both rights and principles. The core rights of EU citizens defined by the law is extensive, and includes things such as:

- Affirmative consent from the person authorizing the use of their personal data in a way that is clearly stated;
- Providing information on what data is being collected, how it is being used, and how long it will be stored;
- The right to have one's data provided to the citizen, or deleted upon request.

Obviously complying with these rules is more than a technical issue: it affects the business model and policies of many organizations.

Beyond the definition of rights, the GDPR also defines "principles", which are primarily conditions required for data processing. They are the "how" data may be processed and a key principle is that of data security, which is defined in Article 32 of the GDPR:

"The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. The pseudonymisation and encryption of personal data;
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

Note that both security and resiliency are required. It is not enough to protect data; steps must be taken to ensure that the data is accessible. Finally it must be noted that GDPR takes a risk-based approach to security controls:

> *"In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."*
> *GDPR, Article 32*

The effect of this approach is provide organizations flexibility in how they build out their controls, commensurate with the risk inherent in the relevant systems or processes.

Codes of Conduct and National Exceptions

GDPR is very light on detail when it comes to compliance, making it difficult for companies to establish any point of reference for what an acceptable approach to GDPR might be. GDPR Article 40 acknowledges this, and establishes the concept of codes of conduct to help. These are guidelines drawn up by non-governmental bodies, such as trade associations.

"Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to…the measures to ensure security of processing referred to in Article 32." GDPR, Article 40

Unfortunately, very few such codes of conduct exist, making this suggestion moot at the time of writing. For an example of one of the very few exceptions, see the Cloud Security Alliance Code of Conduct.

A further complication is the national exceptions. One of the goals of GDPR was to harmonize data privacy rules across all the countries in the European Union. However, GDPR allows national governments to set their own rules that supersede GDPR, and they appear to be in the process of doing exactly that. The result is that organizations will have to monitor for country-specific additional rules that may affect their data processing, either directly or indirectly through service and cloud providers.

Acalvio and GDPR

GDPR is relatively new, and there is no experience from previous audits that can be used to establish a reasonable baseline control set. However, what is clear is that there will be an expectation that organizations have implemented adequate security controls relative to the risk of data processing. As a leader in distributed deception, Acalvio is a perfect example of such a solution.

The table below summarizes Acalvio's support for controls expected of organizations in compliance with GDPR.

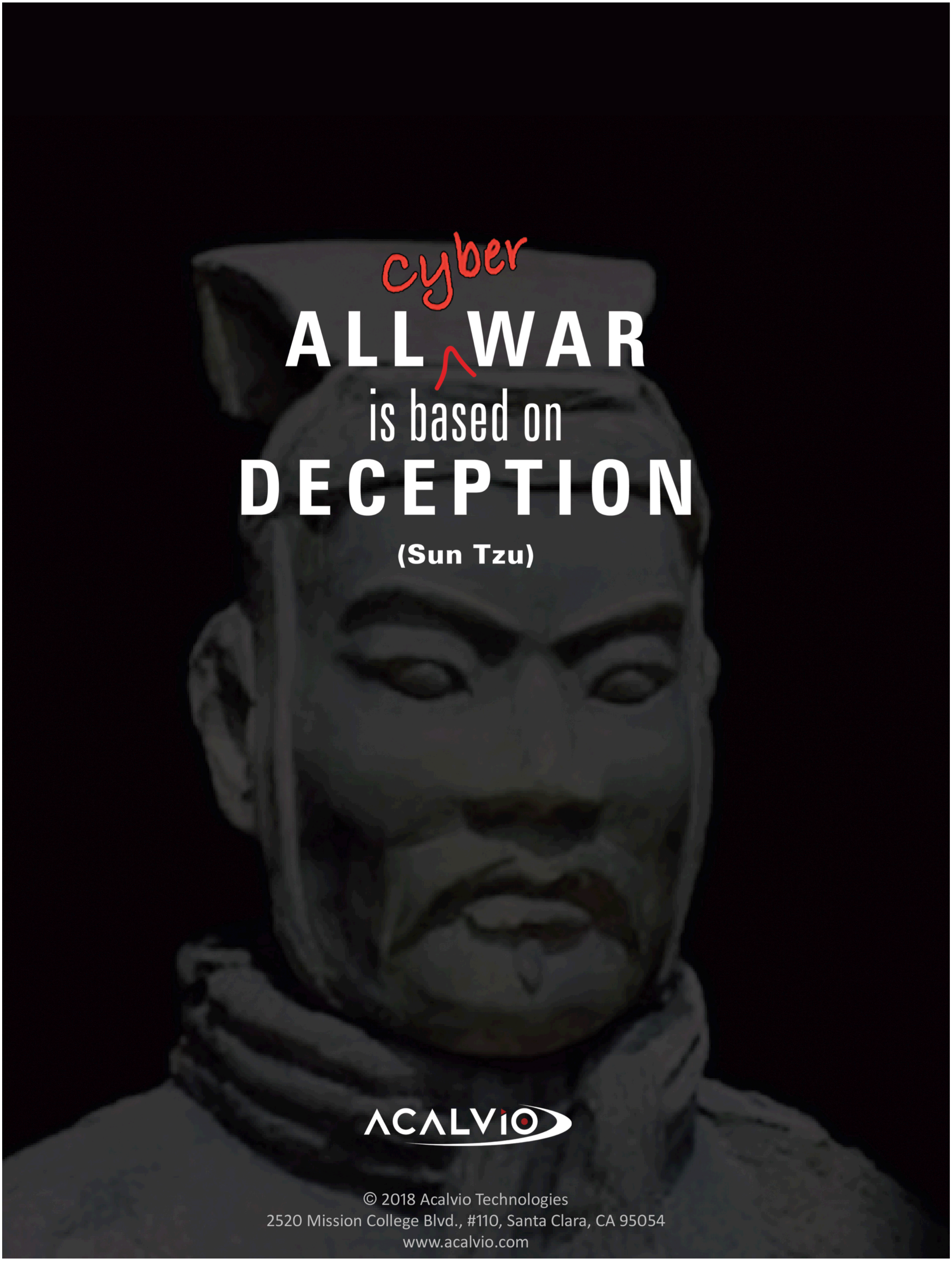
Cybersecurity Control Typically Relevant for GDPR	Acalvio ShadowPlex Support
Network monitoring for threat behavior	Acalvio decoys monitor network activity to detect all unusual events that suggest compromise. ShadowPlex Reflections Engines allow specialized systems (e.g. medical or SCADA devices) to be replicated virtually to enhance realism in non-standard, high-value networks. Deception Farms technology supports broad deployments with minimal operational overhead and cost.

Cybersecurity Control Typically Relevant for GDPR	Acalvio ShadowPlex Support
Threat identification	Using Deception 2.0 breadcrumbs and lures, Acalvio detects attacker activity in systems, servers and endpoints. Acalvio is also able to detect such activity through attempted communication to Acalvio decoys.
Threat forensics and methods gathering	Full documentation of attack actions and methods is gathered automatically. Based on those inputs detailed forensic information is obtained through deep engagement of the attacker's identity, techniques and motives.
Risk and impact determination	Acalvio delivers network-wide data related to device inventory and real-time threat activity, allowing organizations to assess both likelihood and potential impact.
Incident mitigation and containment	The Acalvio Shadow Network, or False Apparent Network, can contain an attacker and prevent compromise of sensitive assets. Acalvio can dynamically deploy lures relevant to an attacker's methods to obfuscate sensitive assets and delay attack propagation.
Control testing	Red team or Penetration exercises can leverage Acalvio capabilities and integrations to test organizational detection efficacy.

A crucial consideration for GDPR compliance is speed. The 72-hour breech notification window dictates that companies have internal monitoring solutions that can very quickly identify and scope adversarial behavior across the environment. This includes not only where the attack has been active, but also where it is not. The ability to define the scope of attack quickly is absolutely crucial to rapid assessment of the likely level of data loss. Without this intelligence, organizations may be forced into unnecessary breach notifications, causing major reputational impact.

Acalvio deception-based detection is superior to alternative approaches such as behavioral analytics because it is both more accurate (few false positives) and more efficient and easier to deploy. Furthermore, what separates Acalvio from all other detection solutions is operational efficiency at scale. Acalvio's technology supports broad application across the internal estate, while minimizing both capital and ongoing expenses and effort. Legacy "Deception 1.0" honeypot solutions simply cannot be scaled or operated easily. Organizations do not have unlimited budgets for implementing cyber security, and the more efficiently they can deploy funds, the more effectively they can build a robust defensive architecture.

> *"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss."*
>
> *GDPR, Article 25*



2520 Mission College Blvd., #110, Santa Clara, CA 95054
www.acalvio.com