PREPARING FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

WHITE PAPER

TABLE OF CONTENTS

PREPARING FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

INTRODUCTION

WHAT IS GDPR?

The continuing digitization and globalization of our economy is becoming increasingly reliant on the control and processing of personal data. And while this presents enormous opportunities for business, it accompanies a growing public awareness and concern for the importance of personal data protection.

According to a recent global survey by KPMG International, more than half (55%) of consumers said they had abandoned online purchases due to privacy concerns. The survey also found that less than 10% of respondents currently felt they had control over the way organizations handle and use their personal data.

The European Union's General Data Protection Regulation (GDPR) is a response to this concern. Acknowledging the value of such data, the regulation imposes a cost to its collection, storage and usage by holding organizations accountable for its protection and forcing them to return control and ownership to the individual.

In contrast to the existing data protection directive 95/46/EC, which was translated into individual national laws, GDPR is a single regulation to strengthen, unify, and enforce personal data protection across the EU. With more stringent criteria, additional obligations, and higher non-compliance penalties (up to 4% of worldwide turnover or 20M Euros, whichever is greater), both the effort of attaining compliance and the risks associated with non-compliance, will undoubtedly increase with GDPR. The good news is that it will, for the most part[1], be a consolidated effort covering an organization's data protection responsibilities across all EU member states.

[1] Legislators have provided local governments the ability to add or adapt provisions to fit local data protection needs.

The **General Data Protection Regulation (GDPR)** is the European Union's response to the massively increased role that technology now plays in everyday life. GDPR was ratified by member states in April, 2016 and **goes into effect on May 25, 2018.** Although an EU regulation, it also applies to any organization regardless of their physical location if they are collecting personal data of EU residents.

The objective of the new regulation is to **ensure that adequate data protection is incorporated into the process of collecting personal data "by default and by design".** This starts with collecting only the minimum amount of data needed for a specific purpose and when it is no longer needed the data is erased. Another important aspect of GDPR is that the data subject, the source of the personal data, is the owner of their personal data. As the owner, the data subject must be able to withdraw their consent to the collection of the data as easily as it was to give permission. The data subject also has the "Right To Be Forgotten" (RTBF) and to take their personal data with them.

GDPR also sets out the conditions of when notification must be made in the case of a data breach and sets out two levels of penalties depending upon the severity of the breach.

Due to the rapid change in technology, GDPR also places the burden of "continuous risk assessment" on the collecting organization – data controller - and requires that any outside organization processing data – data processor – be GDPR compliant.

WHO IS AFFECTED?

GDPR applies to any organization, in any country, that collects, stores, or processes the personal data of EU residents. This data can be from employees, business partners or prospects and customers. In regulation terminology, such organizations are defined as either 'controllers', who determine how and why the personal data is processed, or 'processors', who act on the controller's behalf. Both have increased obligations under GDPR, and both could face penalties in the event of a breach.

WHAT ARE THE IMPLICATIONS FOR GLOBAL BUSINESSES?

For most organizations, the implications are both significant and far-reaching, necessitating changes that encompass data processing workflows, organizational structure, business processes and ultimately, information and security technologies.

INDIVIDUAL RIGHTS

At its core, the GDPR defines the rights of the individual as they relate to data protection. These rights can be broadly summarized as follows:

- **Informed Consent**
  The right to be clearly informed why the data is needed and how it will be used. Consent must be explicitly granted and can be withdrawn at any time.
- **Access**
  The right to access, free of charge, all data collected, and to obtain confirmation of how it is being processed.
- **Correction**
  The right to correct data if inaccurate.
- **Erasure and the Right To Be Forgotten (RTBF)**
  The right to request erasure of one's data.
- **Data Portability**
  The right to retrieve and reuse personal data, for own purposes, across different services.

The first challenge towards GDPR compliance is therefore to audit, and if necessary modify, the way the organization collects, stores and processes personal information in accordance with these rights. Just reaching a point where the organization can precisely locate all instances of an individual's personal data across the entire infrastructure (sometimes referred to as the 'Where is my data?' problem) will be a major part of this challenge.

For some organizations, this will present an opportunity to streamline operations, eradicating unnecessary data collection and limiting processing to only that which is essential to the core business goals. Either way, the transition to compliance is likely to be a significant undertaking.

ACCOUNTABILITY AND GOVERNANCE

The organization then needs to be able to demonstrate compliance through appropriate governance measures, including detailed documentation, logging, and continuous risk assessment. There is an added expectation here of 'data protection by design and by default', meaning that security should, as far as possible, be an integral part of all systems from the outset, rather than something applied in retrospect, although this clearly presents an enormous challenge where legacy systems are concerned. Such cases highlight the essential role of network level security as the first layer of defense, since until the huge number of legacy systems still in use can be redesigned with inherent data protection measures, it may be their only defense against data breach.

Due to the rapid pace of technological change - as witnessed in the domains of Internet, mobile devices, applications and the digital economy for example - and the subsequent evolution of cyber threats that will continue to exploit such changes, the regulation is necessarily vague here about the exact technology measures needed to comply. Beyond the most obvious precautions of data encryption, pseudonymization[2], etc., the GDPR uses terms such as "appropriate" and "state of the art" to convey the requirement for continuous risk assessment and the updating of compliance measures. As new vulnerabilities are discovered, the security technology or data protection practices considered compliant today may need to be changed to remain compliant in the future. While this undoubtedly leaves room for legal challenges over interpretation, organizations will nevertheless need mechanisms to ensure their efforts keep pace with the latest changes in technology and threats.

[2] Pseudonymization is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms

BREACH NOTIFICATION

GDPR also introduces a new obligation on organizations to notify relevant authorities of any personal data breach[3] likely to result in a risk to "the rights and freedoms of individuals"[4]. Where that risk is deemed 'high', notification must also be extended to the affected data subjects. Notifications must be made 'without undue delay' and where feasible, within 72 hours of the event discovery.

Even in the absence of any explicit reference to specific data protection and network security technologies, the transition to compliance must begin with ensuring that the underlying network is sufficiently protected across all possible attack vectors.

NETWORK SECURITY CHALLENGES

MAINTAINING 'STATE OF THE ART' DEFENSES

Keeping pace with the evolving threat landscape is a challenge even without the GDPR's stipulation for 'State of the Art' defenses. The enormous revenue from cybercrime, not to mention its potential for state-sponsored terrorism, ensures a level of resource and innovation that can be hard for any individual company or even national government to match.

Part of the problem comes from the way cyber security has evolved, with the discovery of each new attack vector spawning yet another security solution to be added. Although each such addition may fulfil its role as intended, it does so mostly in isolation, with little or no interaction with the rest of the security infrastructure. This is not only hard to manage, but can easily lead to gaps and inconsistencies in the response to new threats – especially across a multi-vendor environment.

The challenge is compounded by the adoption of trends such as mobility, cloud computing, and the Internet of Things, all of which expand the effective attack surface, exposing new vulnerabilities, and eroding the traditional concept of a network border.

One response to new threats is to increase processing and controls, but as anyone familiar with airport / border security can testify, increased controls can soon lead to unacceptable chaos and delay. Additional processing also adds complexity, multiplying the number of data points to be aggregated and interpreted when evaluating the best response to any detected event.

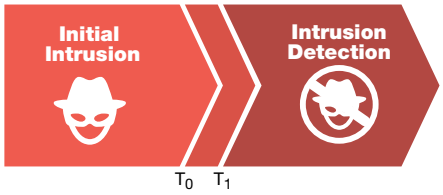
Any solution worthy of the term, 'State of the Art', will not only need to overcome the above challenges, but continually adapt to changes in the usage of technology and in the evolving threat landscape.

REPORTING BREACHES WITHIN 72 HOURS

The first challenge to the GDPR's breach notification requirement is to detect when a qualifying breach has taken place and determine which assets might be at risk. Almost by definition, any successful external security breach must have either evaded detection entirely, or was not detected quickly enough. This means it either exploited an attack mechanism unlike any previously encountered, or the flags that it did raise were missed.

Indeed, in 2016, the average time taken for organizations to become aware of a typical breach was almost five months[5]. Fortunately, the GDPR 72-hour notification window opens at the moment of detection, not the moment of intrusion. Yet since the financial impact of a breach correlates strongly with the length of time the hacker has access, shortening the time to detection is still imperative.

Since it is clearly impossible to detect the undetectable, security administrators should accept and prepare for the inevitable, occasional intrusion, while striving to minimize such occurrences and hasten their detection through every means possible. As previously noted, the GDPR does not require notification for all security breaches, only those that present a risk to the rights of individuals. Consequently, if the data accessed through a breach has been adequately obfuscated through encryption or pseudonymization, and if the duration of unauthorized access is kept short, then the risk to those rights should be minimal.



[3] A personal data breach is defined here as any security violation resulting in the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
[4] GDPR Article 32, "Security of Processing"
[5] 2016 M-Trends Report

However, the fact that a specific attack profile has not been encountered before does not necessarily render it undetectable. With the right combination of distributed traffic analysis and threat intelligence, together with technologies such as sandboxing, previously unseen attacks can still be blocked. The challenge for such advanced detection techniques is to distinguish the relevant signals from all the other noise.

This challenge is similar to that faced by antiterrorist organizations throughout the world who must extract the tell-tale signs of an unfolding attack from the actions and communications of thousands of surveillance subjects across multiple jurisdictions and national boundaries. Without extensive collaboration and automated pattern recognition technologies, such efforts would stand little chance of success.

Similarly, the traditional approach to network security of having multiple isolated solutions report to, and then rely on, the decision-making abilities of a single human administrator, is rapidly becoming untenable. As both network complexity and the frequency of security events increase, a degree of collaboration and intelligent automation across the security infrastructure is essential.

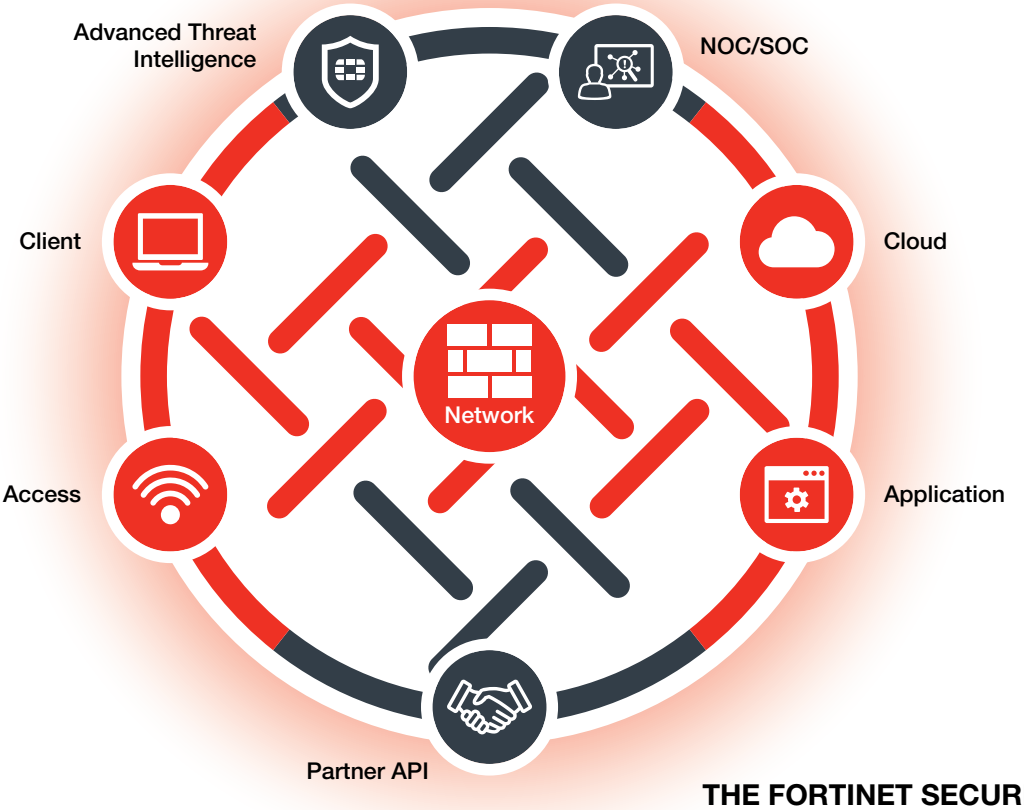
THE FORTINET SOLUTION – SECURITY BY DESIGN

While GDPR compliance is not something that can be achieved through technology alone, the provision of 'State of the Art' network security is clearly an essential first step. To reduce exposure to the potentially crippling implications of a serious data breach, it is necessary to minimize both the number of network intrusions, and their time to detection. And it is here that Fortinet can contribute most to an organization's overall compliance efforts.

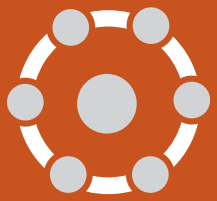
Underpinning the Fortinet solution is a new approach to security in which all key components of the security infrastructure are woven together into a seamless fabric.

FORTINET SECURITY FABRIC

Built upon three key properties - **Broad, Powerful, and Automated** - the Fortinet Security Fabric offers a unique response to the challenges of protecting today's borderless, high bandwidth and complex networks from the rapidly evolving menace of cyber-attack.



THE FORTINET SECURITY FABRIC



BROAD

Designed to cover the expanding attack surface of a modern enterprise network, the Fortinet Security Fabric provides protection, visibility and control over every part of the environment, from wired and wireless endpoints, across public and private cloud assets, to the datacenter, and even to the applications themselves.

Combined with dynamic network segmentation that logically separates data and resources, the Fortinet Security Fabric can reach deep into the network to discover new threats as they move from one zone to the next. This broad deployment and deep visibility is a crucial step to compliance, by helping monitor internal traffic and devices, preventing unauthorized access to restricted assets, and limiting the spread of intruders and malware.

Furthermore, the benefits of the Fortinet Security Fabric are not limited to the Fortinet portfolio of security solutions. With open application programming interfaces (APIs), open authentication technology, and standardized telemetry data, a growing ecosystem of Fabric-Ready Partners is emerging, enabling organizations to integrate existing security and networking investments into their own Fortinet Security Fabric.

POWERFUL

With the processing power of many traditional security appliances failing to keep pace with increases in network bandwidth and threat complexity, organizations are often faced with an unacceptable compromise. Either they must reduce the level of protection, which risks intrusion via an uncovered attack vector or through an unsecured part of the network, or they must accept a drop in application performance across the network.

By offloading security and content processing to dedicated, custom-built Security Processing Units (SPUs) that combine hardware acceleration with highly optimized firmware, Fortinet products have become the fastest in the industry, enabling organizations to establish comprehensive security without compromising on performance.

AUTOMATED

In addition to broad visibility across the entire attack surface and the processing muscle to delve deeper into every packet, the Fortinet Security Fabric can also muster the combined intelligence of its distributed components to rapidly correlate events and coordinate a fast, automatic response appropriate to the level of risk.

As rapidly as new threats are detected, the Fortinet Security Fabric can automatically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware. And as an organization's network grows and adapts to changing business needs, the Fortinet Security Fabric will grow and adapt with it, automatically extending the latest security policies to new devices, workloads, and services as they are deployed, whether local, remote or in the cloud.

SUMMARY

For many organizations, the initial transition to GDPR compliance is likely to be a lengthy and challenging process. Furthermore, as the digital revolution marches on bringing technological advances to both sides of the cybersecurity arms race, that compliance will require regular reevaluation based on continued reassessment of the risks.

Fundamental to this ongoing process will be the role of network security in preventing intrusion and minimizing the risk of serious breach, by reducing the time taken to detect new threats. To achieve this requires a broad, powerful, and automated approach to security.

The Fortinet Security Fabric is a collaborative technology vision that harnesses the collective power and intelligence of Fortinet's portfolio of security solutions to deliver benefits greater than those of its parts.

Designed around scalable, interconnected security, combined with high awareness, actionable threat intelligence, and open API standards, Fortinet's security solutions provide seamless protection to the most demanding of enterprise environments and have earned the most independent certifications for security effectiveness and performance in the industry. These solutions, the realization of the Fortinet Security Fabric vision, close gaps left by legacy point products and provide the broad, powerful, and automated end-to-end protection demanded by today's organizations across their physical, virtual and cloud environments.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

67717 0 1 EN