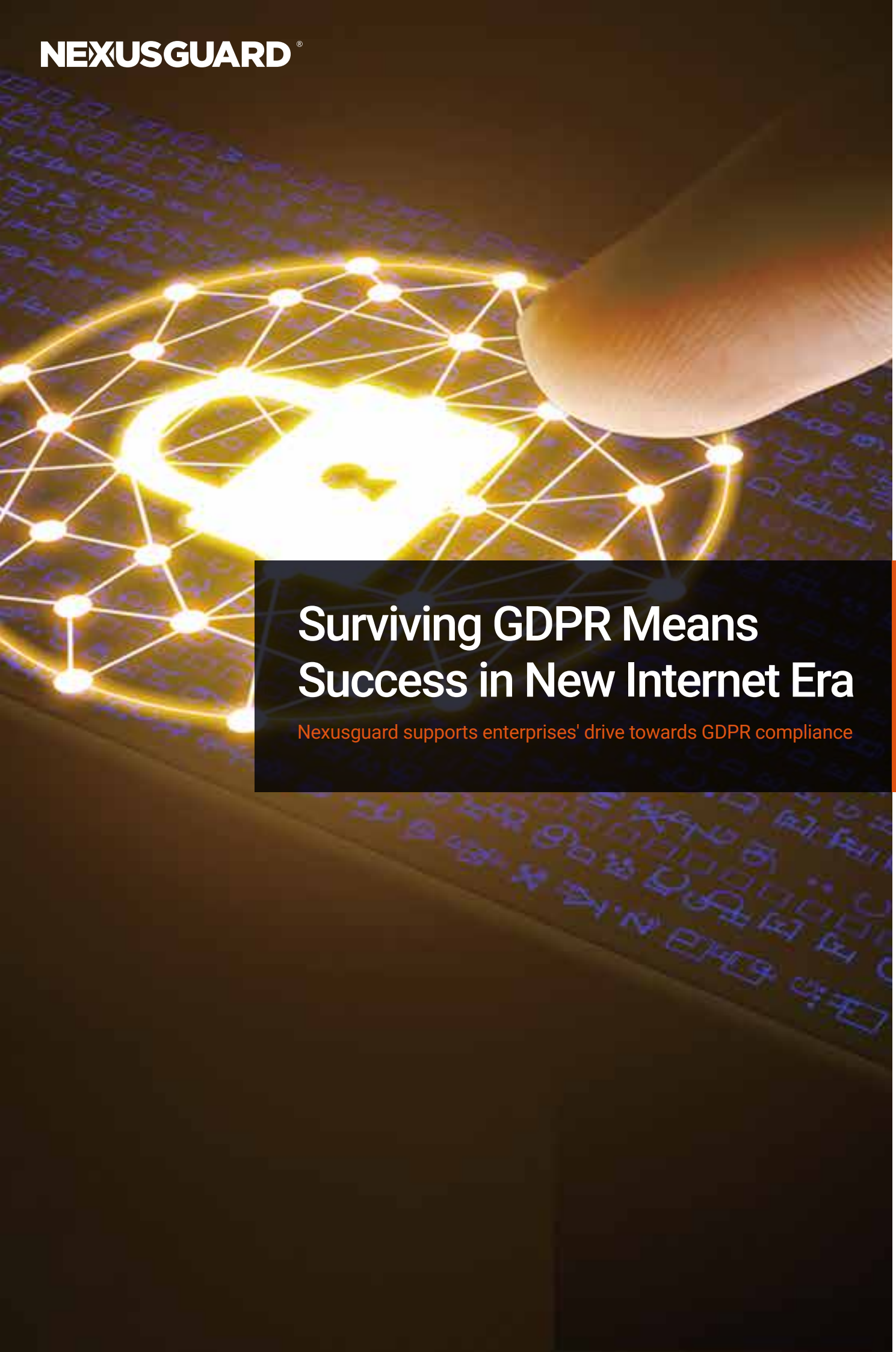
NEXUSGUARD®



Surviving GDPR Means Success in New Internet Era

Nexusguard supports enterprises' drive towards GDPR compliance

WHITE PAPER

Introduction

Effective from 25 May 2018, the General Data Protection Regulation (GDPR) imposed by the European Union (EU) is undeniably daunting and part of it is deliberately vague for online businesses to comply with. Generally speaking, the legislation empowers web users from the EU to opt out of having their data collected by websites or service providers, with hefty penalties for non-compliance.

To survive the GDPR data rules, businesses must prepare themselves with technology that can defend them against data breach, intrusion and service disruption. What's more, once GDPR proves to be successful and effective in protecting personal data, the odds are that it will become a global standard for other jurisdictions to follow suit. This implies that overcoming this challenge will help you succeed in a new era in data protection heralded by GDPR.

What is GDPR?

The General Data Protection Regulation (GDPR) that applies to all EU countries and citizens is a game-changing milestone. Businesses, from social media giants to independent food joints, are now required to take "appropriate technical and organizational measures to ensure a level of security appropriate to the risk" as long as they conduct business of any kind within the EU countries or with EU citizens. Failure to comply with GDPR can yield a hefty penalty--the maximum fine can go as high as 4 percent of the company's global annual revenue.

Definition of Personal Data under GDPR

According to Art. 4 GDPR, "personal data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In other words, anything that is deemed sensitive in nature and that can directly or indirectly identify an EU citizen immediately falls under the umbrella of protection. The most obvious ones are names, addresses, credit card numbers, credentials, pictures, travel records, sexual orientation, political affiliation, biometric data tracked by their smart watches, etc. Web data such as search engine records, IP addresses, cookie data and RFID tags also fall under this umbrella. EU citizens now have the right to know what data is collected about them, to opt out and to be forgotten.

Implications of personal data protection and its impact on you:

While GDPR gives no concrete technology requirements or recommendations of the best practices on how to comply with the new rules, it emphasizes that "Data Controllers" and "Data Processors"[1] --the two roles given to those involved in the handling of personal data--must take "appropriate technical and organizational measures" to safeguard customer information. Organizations are also required to set up and maintain secure IT infrastructure that can "resist, at a given level of confidence, accidental events or unlawful and malicious actions". Two examples cited by GDPR (recital 49) are "preventing illicit access" and "stopping denial of service attacks and damage".

As such, the principle is quite clear. Not only are organizations required to make it transparent as to what data they collect [on EU citizens] and why they do so but they also need to prevent accidental or malicious incidents that compromise the "availability, authenticity, integrity and confidentiality of stored or transmitted personal data" by whatever means within their reach. The quintessential security measures include proper protection against intrusion and DDoS attacks on applications, websites and backend networks.

How Does Nexusguard Help You With GDPR Compliance?

Web Application Protection

As mentioned, the new rule has it that organizations must safeguard personal data against accidental events or unlawful or malicious actions. To comply with GDPR, implementation of a Web Application Firewall (WAF) is now mandatory. Nexusguard's cloud-based WAF can help you adopt the OWASP privacy and security best practices effortlessly, protecting your web applications or APIs from major threats on data security, such as cross-site scripting, SQL-injections and brute force passwords hacking.

[1] As a cybersecurity vendor, Nexusguard is a "Data Processor" under GDPR. In case of data breach, the Data Processor is required to notify the data controller of the incident, except where the controller has "implemented appropriate technical and organizational protection measures" that "render the data unintelligible to any person who is not authorized to access it, such as encryption".

Anti-DDoS Protection

While the GDPR is generally perceived as a legal framework to protect "personal data", the truth is that it also requires sufficient protection to maintain the "availability" of stored or transmitted personal data. In other words, protecting against DDoS attacks--a key threat to the accessibility of your network, and online services--is no longer an option.

Nexusguard is a leading DDoS protection solution provider built on the right mix of people, process, and technology. Our Cybersecurity Platform, underpinned by proprietary technologies and global cloud infrastructure, is crafted to mitigate volumetric and application attacks on websites, networks and DNS servers.

Article 32 of GDPR further stipulates that organizations must regularly test, assess and evaluate the effectiveness of data protection measures. Nexusguard's Application Protection (AP), Origin Protection (OP) and DNS Protection (DP) solutions, including WAF, are centrally managed and regularly updated to patch against latest threats and zero-day attacks.

PCI-compliant Cybersecurity Vendor

The GDPR stipulates that organizations must document and, upon request, be able to prove that personal data processed is appropriately and sufficiently protected. Hence organizations have to make sure that their security vendors defending their web applications and networks have the proven capability.

As a PCI-compliant (level 1) cyber security service provider, Nexusguard is committed to the protection of your and your customers' credit card data and sensitive information when they are stored, processed or transmitted across our platform. We are also certified for ISO 27001, ensuring that the highest standards of control are in place to address the confidentiality, integrity, and availability of customer information and assets, and to ensure compliance with the GDPR policies and other regulatory mandates.

Access to Log Data

It has been made clear that web data including customer IP addresses, geolocations, and even web cookies are subject to the GDPR rules. As a DDoS protection service provider, Nexusguard has to examine web traffic and maintain traffic log for us to mitigate DDoS attacks and other cyberthreats effectively. Typically, we collect, scrutinise and archive traffic log, raw application data, web proxies, search engine spiders and masked IP addresses, whereas each of them contains varied information in various formats. Together they give us a comprehensive picture of what is going on with our customer websites.

Nexusguard Customer Portal can help you move towards compliance for your website, and for your security log. Through the Portal, Nexusguard customers can download the raw log files of all requests, including legitimate and malicious ones, made to their website or network. Log entries include URLs requested access to, timestamps as well as source IP addresses of visitors.

Log Storage Policy

When traffic data pass through our mitigation services and VAS platform, they undergo a series of filtering, analytics and optimisation, before forwarding to your website. All such data are stored in-house and on the cloud (with encryption) for a limited period, after which the data will be eradicated. We implement stringent operational access and data control that follow the PCI-DSS Standard, while all our data centres comply with PCI-DSS requirements.

Log data are classified as “hot” and “cold”. Hot data, or frequently accessed data, lasts for no more than an hour, and they will be removed once statistics have been regenerated. “Cold data”, or less frequently accessed data, compressed (gzip) and encrypted (AES-256), are archived, in physically isolated servers for up to three months. Additionally, the tunnel for transmitting cold data is also encrypted, so that the data will not be stolen or tampered during transmission.

We manage and store all log data maintaining highest possible standards. We implement the most stringent security measures, governed by the ISO/IEC 27001:2005 certification of Information Security Management System (ISMS), to ensure its confidentiality, integrity, availability, and privacy.

Nexusguard Helps You Survive the New Era in Online Data Protection

GDPR is a turning point in personal data protection policies and has a far-reaching impact on organizations, especially those with an online presence in the EU. Although the data protection and security practices required by GDPR may look like a daunting challenge, you can turn it into an opportunity.

To succeed in the new era in online data protection, organizations must have the required security measures, including those provided by Nexusguard, in place to ensure the “availability, authenticity, integrity and confidentiality of stored or transmitted personal data.” Stand out from your competitors and make a name for protection of personal information. Gain competitive advantage over those who choose to quit the EU market as a result of GDPR.

About Nexusguard

Founded in 2008, Nexusguard is a leading cloud-based distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communication service providers to deliver DDoS protection solution as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

NEXUSGUARD®

www.nexusguard.com

20241015-EN-A4