Is Your Organization Ready for GDPR?

GDPR Checklist for Service Provider

Arbor Security Solutions for Service Providers Can Help

The General Data Protection Regulation (GDPR) calls for unprecedented changes in the way organizations collect, process and protect the personal data of EU citizens. The GDPR requirements are not limited to organizations physically located in the EU. GDPR explicitly applies to any business collecting or processing personal data (controllers and processors), whether directly, or indirectly as a third-party. In fact, the regulation highlights requirements for protecting the flow of personal data across borders.

For security operations, GDPR Recital 49 defines the appropriateness of processing personal data within security solutions for the purposes of "ensuring network and information security." It goes further: "This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems." Arbor security solutions help ensure your networks are available and protected against advanced attacks targeting personal data. The checklist below can help you assess your preparedness for GDPR, ensure service availability for your customers, even help your customers with GDPR compliance.

GDPR Section 2: Security of personal data, Article 32: Security of processing

For the security professional, Article 32 goes to the "heart of GDPR" — the requirements called for in the protection of personal data.

Article 32 calls for:

- "The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services." (Article 32: 1(b))
- "The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident." (Article 32: 1(c))
- "A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing." (Article 32: 1(d))

Check for these vulnerabilities in your network security posture:	Arbor DDoS Protection Solution provides:
Lack of real-time information needed to detect potential outages from network hotspots, BGP hijacks, DDoS attacks or network misconfiguration	Pervasive network visibility and the ability to automatically detect network anomalies and DDoS attacks in as little as 1 second
Inability to perform root cause analysis to quickly diagnose and resolve issues	Protection of the integrity of your network by quickly diagnosing and preventing misconfigurations, flash crowds or malicious threats
Relying exclusively on stateful devices (load balancers, firewalls, IPSs) which are vulnerable to state exhaustion DDoS attacks	Carrier-class threat management to automatically help identify and stop volumetric, TCP state exhaustion and application-layer DDoS attacks on your infrastructure or your customers' networks
Cannot protect your peering/transit points or data center Internet connections from saturation due to new, DDoS volumetric attacks	Wide range of mitigation platforms and capacities from 2U appliances (500Mbps–160Gbps), 6U chassis (10–100Gbps) and Cisco ASR 9000 Router embedded (10–60Gbps) and virtual
Inability to detect stealthy "lo and slow" application layer and multi-vector DDoS attacks that crash servers	Arbor Cloud provides multiple Tbps of aggregate, centrally-managed mitigation capacity per deployment for extra mitigation capacity and expertise
Limitations on helping customers mitigate the effects of DDoS attacks due to time lost identifying illegitimate traffic and coordinating with customer	Arbor Cloud Signaling™ that intelligently and automatically connects local DDoS protection with Arbor Cloud DDoS Protection Services for volumetric mitigation
Difficulty updating DDoS threat intelligence and DDoS policies	Service enablement features such as APIs, customizable user portals and multi-tenancy enable delivery of managed DDoS protection services
Lack of global threat context to help prioritize security resources to respond to breaches	In-box SSL decryption capabilities to identify threats hidden in encrypted traffic
	ATLAS Intelligence Feed (AIF): continuously updated DDoS protection with the latest global threat intelligence from Arbor's Security Engineering & Response Team (ASERT)

GDPR Section 2: Security of personal data, Article 33. Notification of a personal data breach to the supervisory authority

GDPR notification requires:

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…" (Article 33: 1).
- The degree of compliance can affect the level of financial penalties. The Supervisory Authority takes "…into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;" (Article 83: 2 (d)) and "the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement." (Article 83: 2 (h)).

Check for these vulnerabilities in your network security posture:	Arbor Spectrum provides:
Relying on perimeter protection in critical data centers to detect and block data breaches from complex/stealthy advanced threats	Provides streamlined security workflows to detect and investigate network-wide threat activity faster than traditional solutions
Inability to detect a data breach in real-time. Limitations on analyzing massive amounts of log data; sidetracked by "false positives"	Real-time visualization of Indicators of Compromise (IoC) of trends in new indicators and network activity
No visibility into the full extent of a data breach	Identification of cyber threats for all impacted hosts and network connections to gain visibility into the full extent of a data breach
Difficult to correlate past activity with current breach	Workflow for investigation of past breach activity from full packet-level network archive
Lack of global threat context to help prioritize security resources to respond to breaches	Detection based on ATLAS Intelligence Feed's Internet threat visibility and high fidelity attack campaign indicators applied to your internal network activity

GDPR Section 1: General obligations, Article 25. Data protection by design and by default

"By design and by default" attempts to enforce security planning from the ground up, in the planning of your security systems and procedures. You are required to:

"…implement appropriate technical and organisational measures …which are designed to implement data-protection principles …in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." (Article 25:1).

Check for these vulnerabilities in your network security posture:	By design, Arbor solutions provide:
Reliance on manual and event-specific security processes against DDoS and advanced attacks	Surgical, automated mitigation, removing only attack traffic without interrupting the flow of non-attack business traffic
Insufficient real-time, global network visibility and fragmented traffic engineering tools	Analysis of NetFlow, SNMP and BGP routes that allows you to better plan and engineer network integrity and availability
Lack of global threat context to help prioritize security resources to respond to breaches	Automation of policies and processes such that, by default, data protection against DDoS and advanced threats, is built in, e.g., • Automatic detection and mitigation of attacks • Key incident response and security operations workflows • Integrated on-premise and cloud DDoS protection
Inadequate network traffic data to optimize configuration for protecting network availability	Embedded, continuously updated ATLAS global threat intelligence for the context you need for a proactive security posture against DDoS and advanced threats
Network design slow to scale or reconfigure so you can offer new DDoS protection services	

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECMD_002_EN-2001 03/2020