FORESCOUT

Reduce GDPR Application Risk with Device Compliance and Network Segmentation

> **The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box-ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."**
>
> — Elizabeth Denham, Information Commissioner, UK

GDPR is intended to protect the privacy and freedoms of EU residents by extending greater control and transparency of processing of their personal data through heightened regulations and the imposition of significant fines and penalties for violations of those protections (the greater of €20 million Euros or 4 percent of annual global turnover).[1] GDPR also provides the benefit of harmonizing the data privacy laws across the European Economic Area.

Within months of GDPR coming into effect, high-profile breaches made headlines. During the breach of a major British airline, hackers took the personal and financial details of customers who made or changed bookings on the website or through the airline's application. The data included names, email addresses and credit card information. Approximately 380,000 transactions were affected. In addition, the airline was threatened with a class action lawsuit.[2]

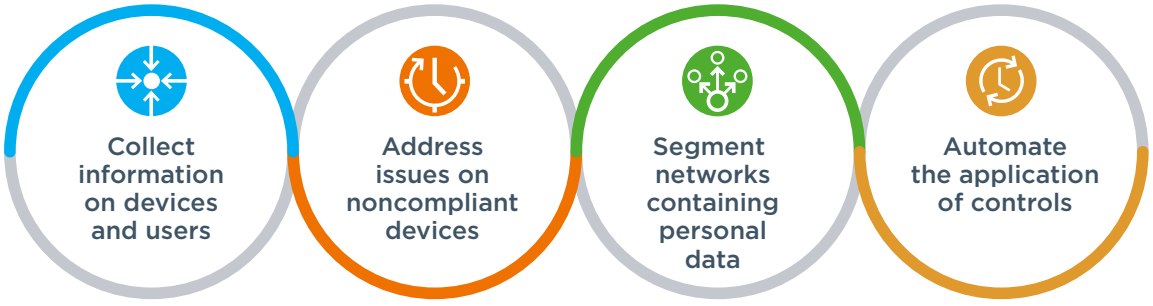
Reducing Risk Through Visibility

As a first step to becoming GDPR compliant, companies need to understand the control state relative to critical applications that access personal data. To do that they need to know the devices on their network, the access rights they have when they are connected and which data applications they are allowed to access. Organizations need proof that mechanisms on these devices to secure private data, such as encryption agents are operational. They also need visibility into the type of applications on devices that access private data.

Visibility is not limited to corporate-managed devices, but also includes a plethora of different bring your own device (BYOD) endpoints and Internet of Things (IoT) devices, as well as other systems that may be used by organizations everyday to conduct business.

Given the huge proliferation of devices, organizations need a different approach, as the traditional agent-based security solutions do not provide a complete solution. Instead, an organization's security tools must work in an agentless manner to see and manage all these different devices.

ForeScout visibility, control and orchestration capabilities within a GDPR environment.



[1] https://www.gdpreu.org/compliance/fines-and-penalties/
[2] https://www.bankinfosecurity.com/british-airways-faces-class-action-lawsuit-over-data-breach-a-11478

Reduce Privacy Breaches with these Seven Tips:

1. **Maintain continuous, in-depth asset inventory.** Accurate device visibility and context are paramount to understanding and improving security posture. Ever-changing networks complicate this process as compute, network, storage and mobility assets join and leave the network.

   Solution: Use a visibility platform that gathers asset intelligence continuously upon connection—without disrupting business operations—and shares real-time data with your configuration management database (CMDB).

2. **Consolidate governance and controls to manage risk.** Adding elastic compute, network, storage and mobility technology often requires highly specific, point-security solutions—fragmenting control and adding risk to your firm.

   Solution: Use the same people, processes and asset intelligence to build context and reinforce actions, and implement governance and policies leveraging segmentation and access controls.

3. **Implement granular network segmentation.** A well-formulated network segmentation strategy enables you to separate devices containing highly sensitive personal data and applications.

   Solution: Leverage real-time asset intelligence to create security policies and determine the optimal network segmentation zones in the cloud or in virtual environments. You may choose to segregate device types across the campus, data center servers and the cloud.

4. **Secure and manage privileged accounts and credentials.** Exploitation of privileged account credentials is a common way for attackers to access applications, sensitive personal data and credit card information.

   Solution: Use an agentless solution to gain visibility of accounts on all types of managed and unmanaged devices, including IoT devices. Next, automate policy-based access control and enforcement across all zone-enforcement technologies (Switches, NGFW, SDN, Cloud).

5. **Automate detection and response to strengthen defense.** Avoiding data privacy breaches is a top priority for all firms storing data of EU citizens, yet security teams are stretched thin working on too many alerts across too many tools.

   Solution: Expedite investigations with valuable information sharing about endpoints (control state, location, authentication, ownership). Facilitate faster mitigation through automated network controls.

6. **Maintain consistent security and streamline compliance.** Many point solutions rely on agents that are often broken or scans that are incomplete. This paints an incomplete picture of the risk to your critical applications.

   Solution: Extend continuous monitoring and security controls across your entire environment—from campus to data center to the cloud—to ease compliance. Use an advanced network visibility solution to discover noncompliant devices and trigger/enforce updates.

7. **Scale security without disrupting critical operations.** Regardless of the size of the organization, if it stores personal data of EU citizens, these data sources wherever they are (and no matter how many) must be secured. Flexibility and centralized management are key.

   Solution: Use a heterogeneous security solution that works across campus, data center and cloud environments—allowing you to manage a large number of endpoints with a single console for greater control and efficiency.

Learn more at
www.ForeScout.com

Learn More

- Addressing the EU General Protection Regulation (GDPR) Solution
- GDPR: A Europe Based Regulation with Global Impact White Paper
- 7 Ways Financial Services Firms Can Conduct Cybersecurity At Business Speed

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591