SysKit

IT Guide to GDPR Compliance & Security

General Data Protection Regulation

Coming: May 25, 2018

GDPR is a European Union-driven **regulation** (specifically the European Parliament, the Council of the European Union and the European Commission) that will **strengthen data protection laws** throughout the EU.

- GDPR brings a new set of "digital rights" and aims primarily to give control back to EU citizens and residents over their personal data
- Regardless where your business is located, if you process, store or manage personal data of any EU resident – you must be GDPR compliant

Key Definitions

Data Subject — An **identified or identifiable natural person** 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

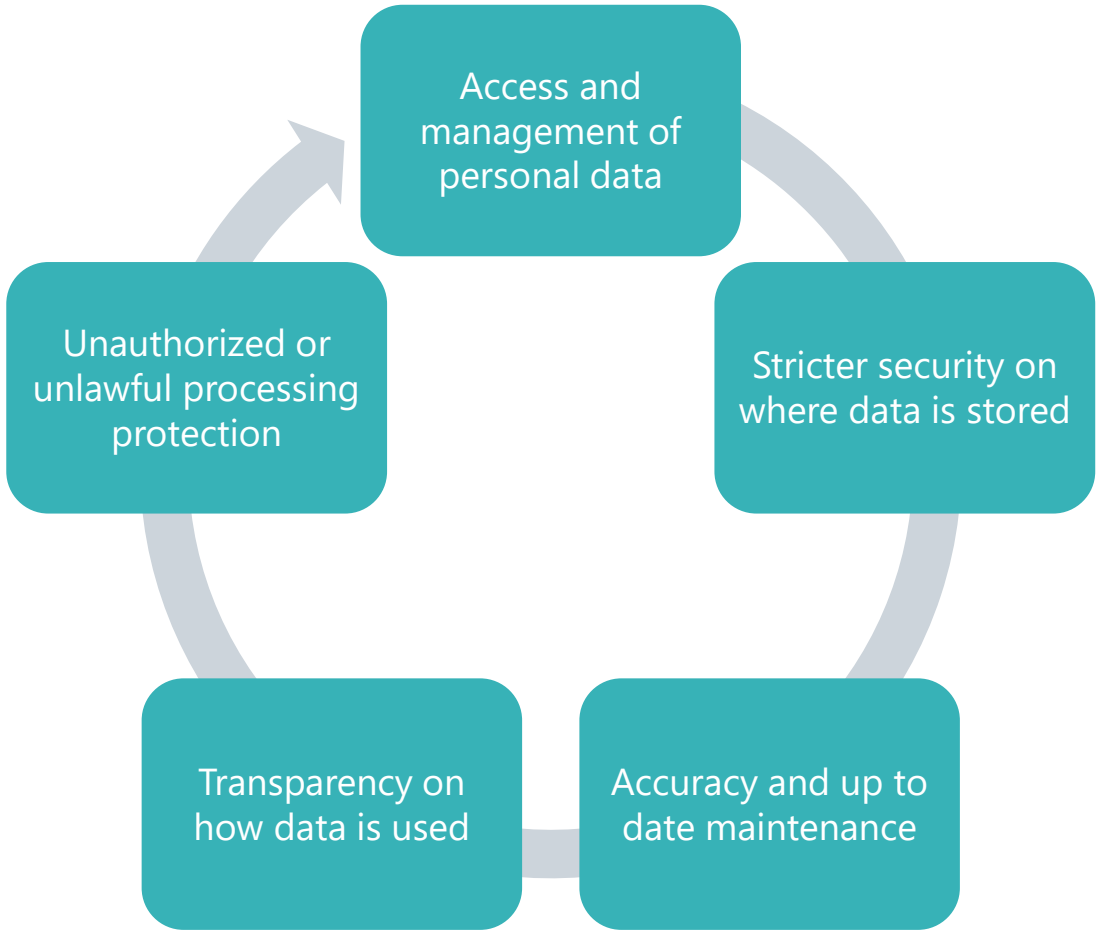
Personal Data — Any information **relating to a Data Subject**, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership

Processor — A natural or legal person, public authority, agency or any other body which **processes Personal Data** on behalf of the controller

Processing — Any operation or set of operation which is **performed on Personal Data** or on sets of Personal Data

Controller — The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the **purposes and means of the processing of Personal Data**

Benefits for my Business



Did you now?

Security is the core of GDPR's data protection requirements!

Meet security requirements with an intelligent solution!

Key changes to address GDPR bring many advantages for business

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater)!

Data Breach

A breach of security leading to the **accidental or unlawful destruction**, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

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!

Personal Data includes:

- Name
- Bank details
- Location
- IP address
- Email content
- Pictures
- Recordings of security cameras
- HR or CV databases
- Cookies
- Social Media Posts
- Medical information

How do I get started?

Detect all the **personal data you possess** and discover where it resides

Discover

Govern the **use and access** of personal data, restrict certain data from further processing

Manage

Establish security controls, **detect, prevent, respond** to vulnerabilities and data breaches

Protect

Manage data requests, **report data breaches**, and keep required documentation

Report

What solution should I use?

SysKit Monitor

Enterprise Server Monitoring & Administration Tool

Smart. All-Powerful. Robust.

MONITORING

DOCUMENTATION

REPORTING

MANAGEMENT

How can SysKit Monitor help me?

Monitor User Activitiy

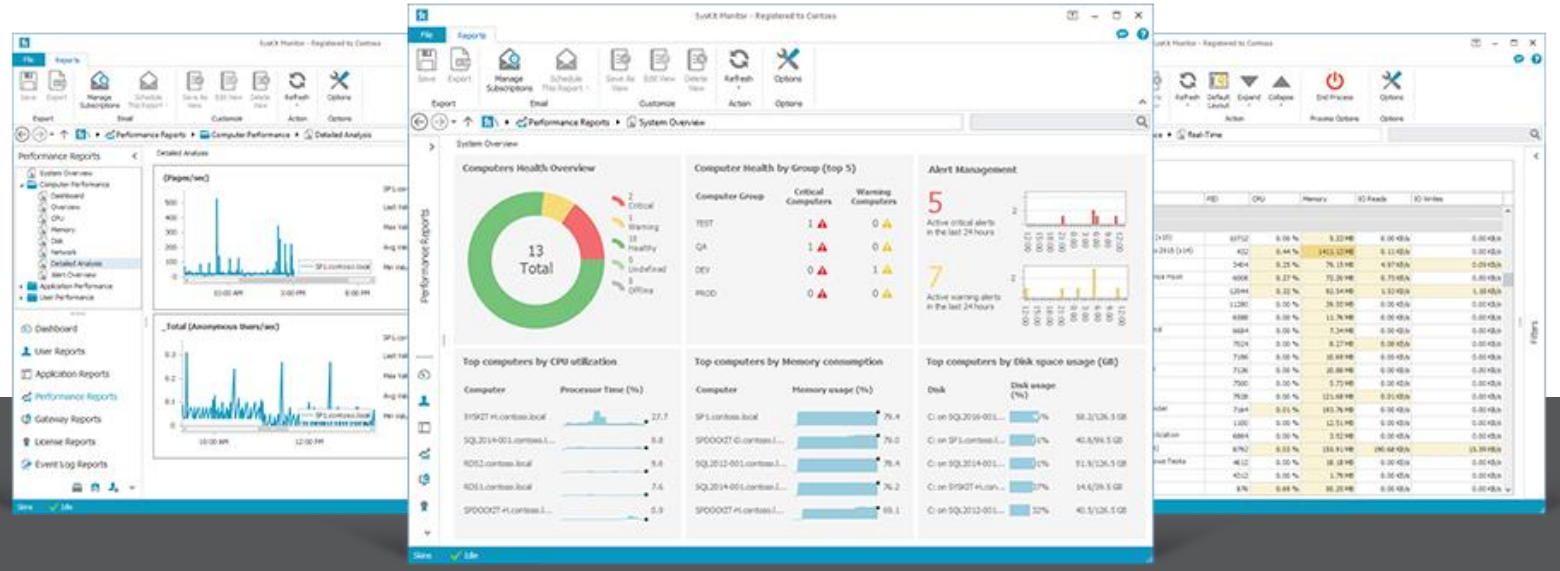
Monitor who has accessed to your system where personal data resides.

Audit Logon & File Access

Audit failed logon attempts on your Windows or Citrix servers and avoid possible intruders from entering your company domain.

Track RD Gateway Connections

Check who uses your RD Gateway to access your corporate network from the outside.



Monitor User Activitiy

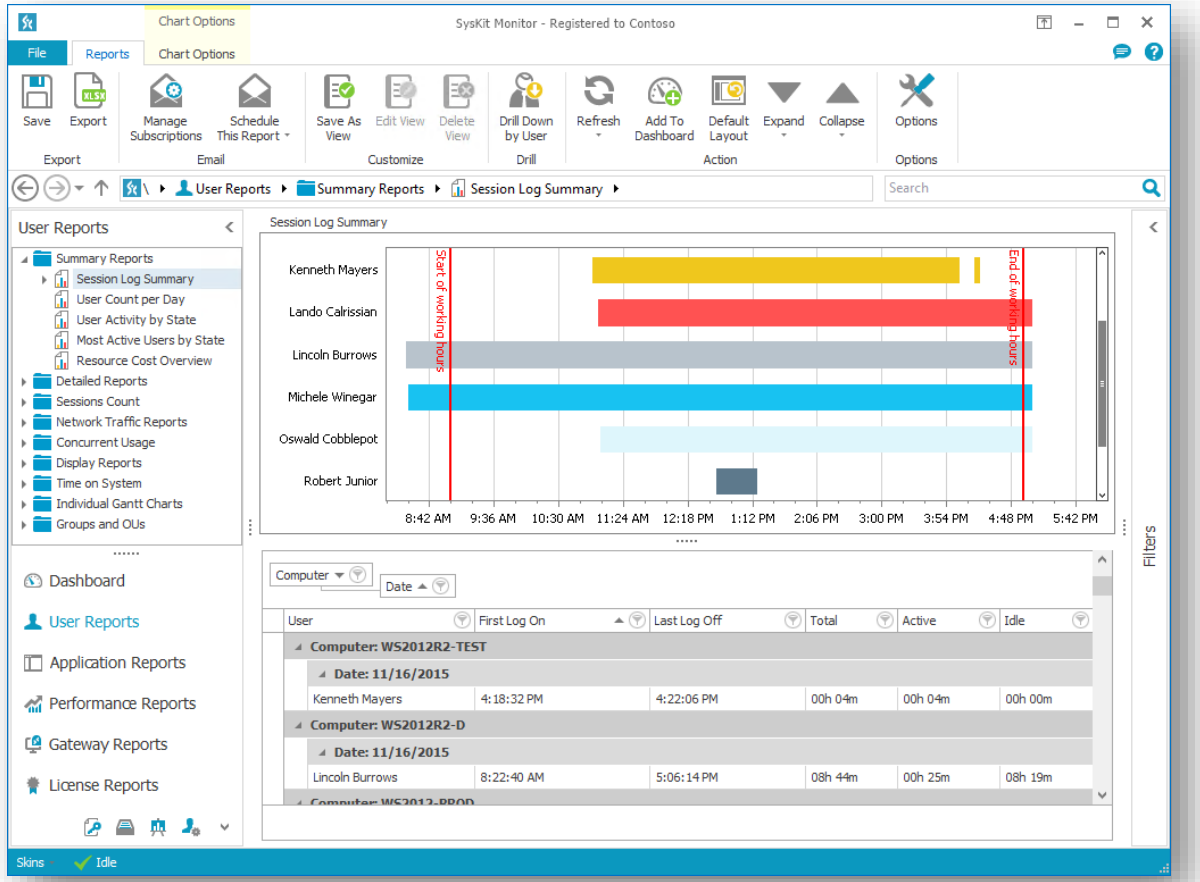
Meet GDPR compliance requirement

Data controllers must now constantly monitor user activity and detect risky behavior.

- Have an overview of all the users who have accessed the **business critical system to avoid personal data breaching** outside company
- Visualize users' access over the course of one day to sensitive data or **monitor users' live** (first log-on, log-off time, total time connected etc.)
- Schedule **daily or weekly email reports** on who exactly has accessed to the environment and how long he was active on any servers within the environment.

In case of a **personal data breach**, with SysKit Monitor you can track **who and when accessed different files** – once you become aware of a breach there is 72-hour limit to prepare the report.

Using SysKit Monitor, quickly and easily generate a **report for the controller or supervisory authority and avoid high penalties.**



Audit Logon & File Access

Meet GDPR compliance requirement

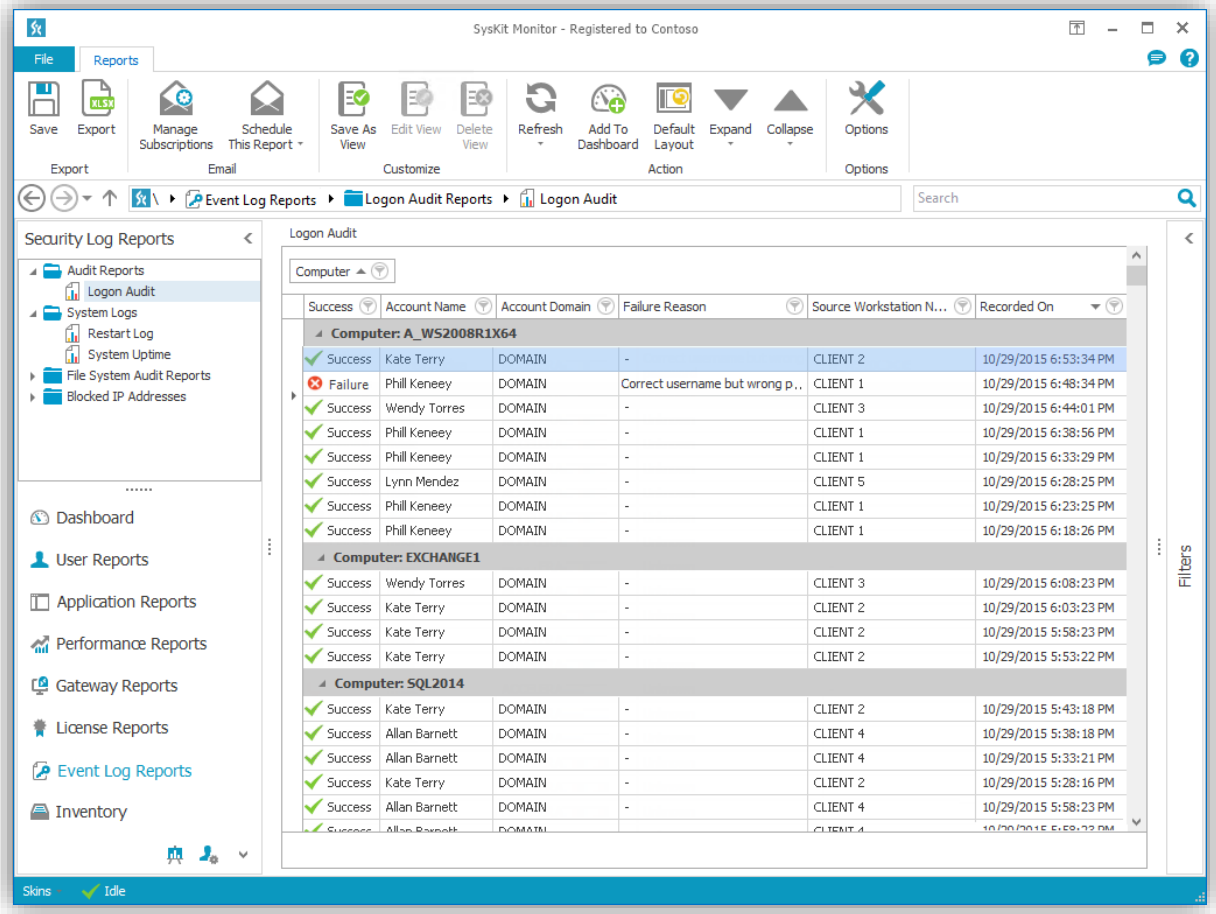
Audit data access and flow across their entire network, detect data breaches.

- **Detect failed logon attempts** if somebody tries to access your systems with personal data – detect treats on time
- Get a warning if there are **multiple logon attempts** to the servers or suspicious behavior

Auditing data breaches is the most important thing you need to do for the GDPR compliance - if there is a security breach by malicious attacker this **should be reported immediately to the supervisory authority** within 72 hours.

With SysKit Monitor you can provide Logon Audit report that shows a **complete logon history on who and when has accessed your environment**, how long he was trying that and if on end someone managed to log on your servers. Using this type of the report you can even **get the IP address of the remote attacker** and geo-locate the country or even city where the attacker is, and if you get asked by supervisory authority this details you will have those in your hand.

In SysKit Monitor, **File Access Auditing** allows you to see who **accessed**, **modified**, or **deleted files** - if any unauthorized user tried to open, modify, or delete any files, you will know. If you have configured file system auditing, SysKit Monitor provides you with a **clear view of file access history**.



Track RD Gateway Connections

Meet GDPR compliance requirement

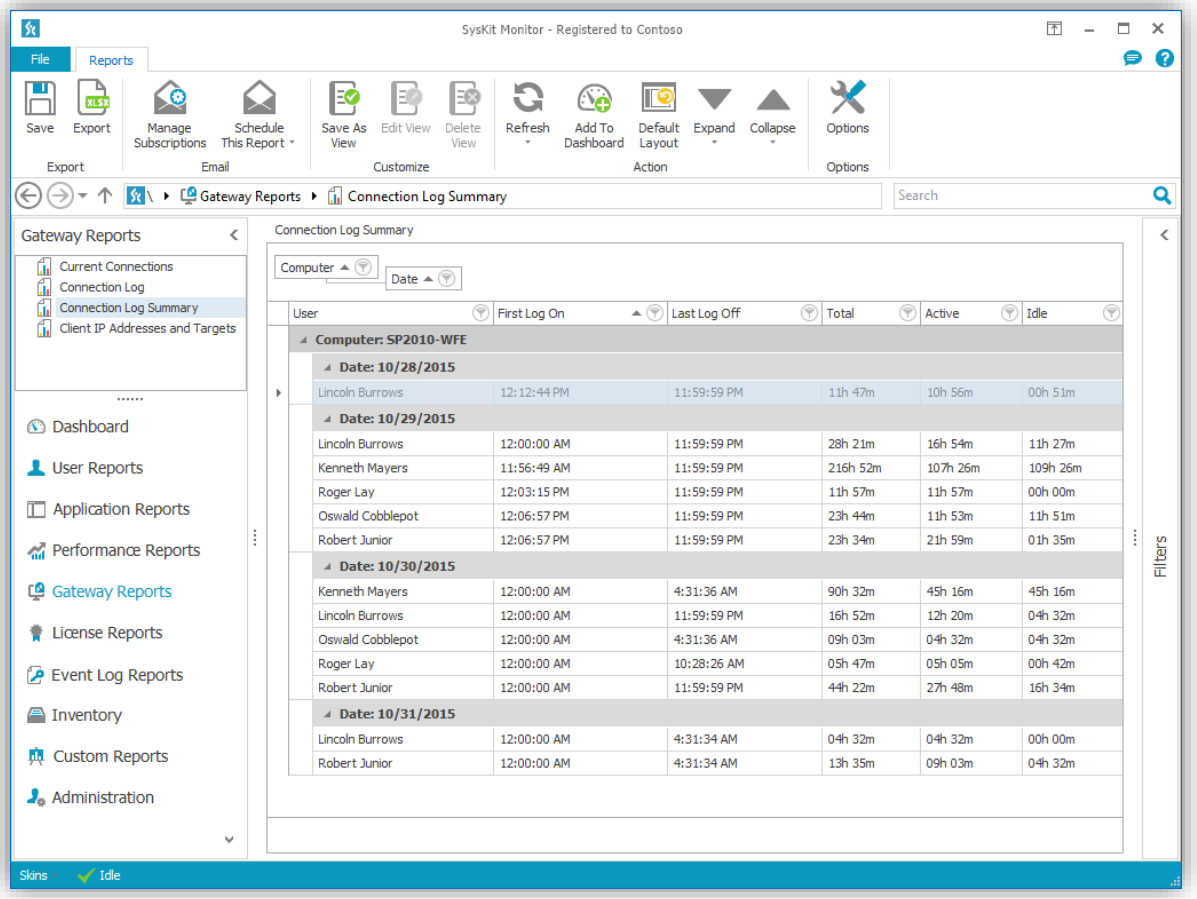
Identify and prioritize gaps in security and monitor risky connections to your network from the outside.

- Measure and monitor connections to your **servers or workstation** made via RD Gateway and **track their external IP address**
- Add **multiple RD Gateways** and track user activity
- Analyze both **real-time and historical data** about users and activities

RD Gateway Connection Monitoring is **crucial for the GDPR security** since outside user connections to your environment are extremely critical and risky. RD Gateway secures the servers behind the firewall – you will be aware **if somebody is attacking your RD Gateway** as well as if a malicious user manages to gain access to the internal resources.

RD Gateway is the single server (or in load-balanced scenarios more servers) that are exposed on the Internet and therefore a **single point of the security breach**.

To get access to the internal resources malicious attacker needs first to **break the RD Gateway** which needs to be **monitored with high priority** and all the users that are connecting through the RD Gateway. SysKit Monitor allows you to monitor RD Gateway connections on top of the RD Session host monitoring.



One tool to monitor them all!

Citrix XenDesktop and XenApp monitoring

SharePoint, SQL Server, and Windows Server monitoring

Remote Desktop Services and Gateway monitoring

The clock is ticking...

Start your GDPR journey today & prepare for May!

Download Free Trial

Relevant GDPR Articles:

- Article 28
- Article 32
- Article 33
- Article 34

Sources:

- Key Changes
- GDPR Terms
- General Info
- Principles