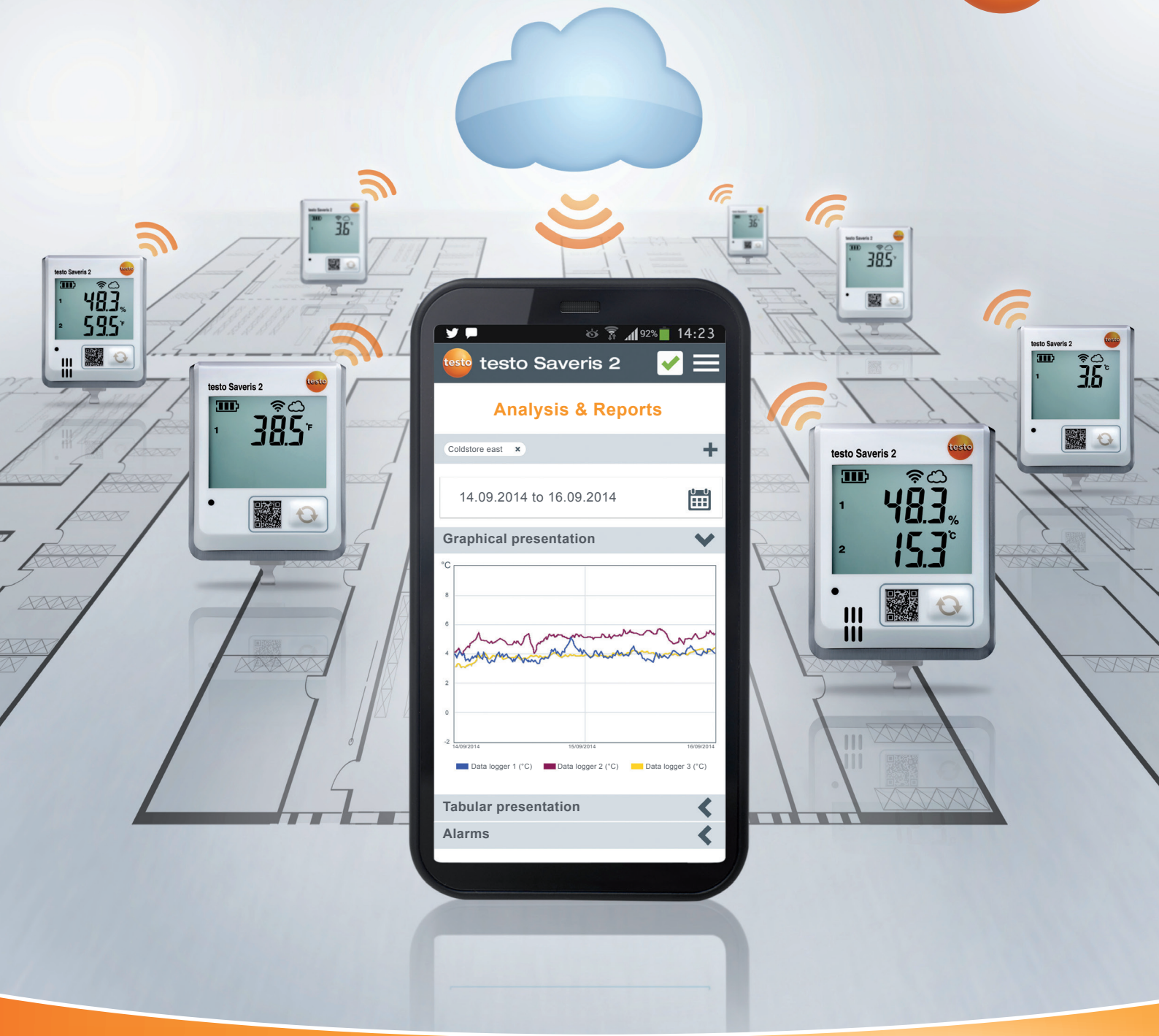
We measure it. testo



testo Saveris 2
Досье по безопасности

Нам важна Ваша безопасность

Защита данных и конфиденциальной информации с testo Saveris 2

Для того чтобы гарантировать сохранность и неприкосновенность Ваших персональных данных и данных измерений, компания Testo AG совместно с IT-разработчиками создала систему testo Saveris 2, соответствующую высочайшим стандартам, директивам и законодательным нормам в сфере информационной безопасности.

В этой брошюре Вы найдете все необходимые сведения по защите данных и конфиденциальной информации. При возникновении каких-либо вопросов Вы всегда можете обратиться к представителю нашей компании.

1. Какие данные хранятся?

В системе хранится минимальная персональная информация, а именно: имя пользователя, все адреса e-mail и номера мобильных телефонов, вносимые в базу данных с целью получения оповещения при нарушении предельных значений. Таким образом, все личные данные используются только для информирования пользователя в случае превышения пороговых значений.

Каждые последующие измеренные значения документируются и хранятся в хронологическом порядке, а не записываются поверх предыдущих данных измерений. Таким образом, Вы можете получить сведения об измерениях в любой момент с возможностью восстановления четкой картины, в какой момент были зафиксированы определенные значения. Это, в свою очередь, дает возможность неограниченного отслеживания информации в случае возникновения чрезвычайных обстоятельств.

2. Где хранятся мои данные?

Все данные хранятся в Германии в центре обработки и хранения данных признанного во всем мире провайдера Host Europe, имеющего сертификат ISO/IEC 27001:2005. На все данные распространяется действие строгих немецких законодательных норм в отношении безопасности информации.

Провайдер Host Europe имеет сертификат соответствия стандарту ISO/IEC 27001:2005, выданный организацией TÜV Süd, на «Предоставление высокодоступной мощности центра обработки данных (ЦОД), включая сетевую целостность и функционирование». Благодаря протестированной организацией TÜV системы менеджмента информационной безопасности (СМИБ), Host Europe гарантирует превосходную безопасность данных и всеобъемлющее соблюдение принципов защиты данных.Таким образом, Вы получаете оптимальную защиту наряду с доступностью, конфиденциальностью, целостностью и подлинностью ваших данных и систем.

Сертификацию прошли не только существующие процессы, обеспечиваемые провайдером Host Europe, но и эффективные меры для соответствия стандартам безопасности в будущем. Меры по обеспечению безопасности данных включают следующее:

<u>Доступность</u>

Host Europe гарантирует доступность и удобство управления данными за счет:

- Ежедневного резервного копирования;
- Удаленного резервного копирования;
- Программного сканирования на вирусы;
- Регулярных обновлений системы безопасности и ПО.

<u>Конфиденциальность</u>

Меры, гарантирующие только санкционированный доступ к Вашим данным:

- Защита доступа к зданиям и данным;
- Различные зоны безопасности;
- Безопасное уничтожение данных и запоминающих устройств;
- Корпоративные тренинги по обеспечению безопасности.

<u>Целостность:</u>

Host Europe полностью защищает данные и сведения от несанкционированного внесения изменений за счет:

- Безопасности доступа;
- Защиты от несанкционированного хранения, обработки, использования и отправки данных;
- Закодированной передачи данных;
- Защиты от сетевых атак.

Подлинность:
Host Europe гарантирует надежность передачи данных и обмена информацией со сторонними партнерами благодаря:

- Многоуровневым процессам аутентификации;
- Безопасной идентификации пользователя;
- Упреждающему устранению пробелов в обеспечении безопасности.

Физическая защита
Более того, Host Europe проводит всестороннюю программу по защите центров хранения данных, например, за счет:

- Регулярных нагрузочных испытаний инфраструктуры, а также создания избыточности данных;
- Противопожарной защиты;
- Защиты от затоплений;
- Чрезвычайных планов действий на случай природных катаклизмов;
- Управления в критических ситуациях;
- Защиты от рисков для окружающей среды.

Надежное Облачное хранилище
С целью исключения организационных, юридических и технических рисков, связанных с использованием Облачной технологии компания-провайдер Host Europe решила обратиться в организацию TÜV TRUST IT для тестирования безопасности своих Облачных сервисов. Согласно обширному каталогу требований к Облачным сервисам организации TÜV TRUST IT, сервисы Host Europe были протестированы на уровне инфраструктуры (IaaS) в отношении безопасности данных, защиты данных и соответствия требованиям. В ноябре 2011 года Host Europe стали первым провайдером, награжденным сертификатом “Надежный Облачный Сервис” (“Trusted Cloud Service”). Для пользователей надежные сертифицированные Облачные технологии означают оптимальную доступность, конфиденциальность и целостность данных и систем.

3. Мои данные в безопасности?
Защита конфиденциальной информации
Все данные попадают в Ваш интернет-браузер исключительно по закодированному протоколу SSL. Кроме того, серверы, на которых хранятся Ваши данные измерений, находятся в Германии и, следовательно, на них распространяется действие немецкого закона о защите данных – одного из самых строгих в мире.
Весь web-трафик регистрируется и хранится на web-сервере временно, максимум, в течение месяца. Однако это необходимо исключительно в сервисных целях или для обеспечения работы системы. Затем все данные удаляются или становятся анонимными.
В случае сетевых атак на инфраструктуру потоки данных временно перенаправляются через стороннего провайдера, обеспечивающего безопасность, который анализирует их, чтобы отфильтровать вызывающие конфликт запросы.
Защита от потери данных
Центр обработки данных имеет две изолированные друг от друга пожарные зоны. Термин “пожарная зона” здесь употреблен в буквальном смысле: в случае возникновения чрезвычайной ситуации и полного падения базы данных – из-за пожара, например – её функции переходят на другую пожарную зону. Вне сомнения, мы уведомляем своих клиентов о подобных случаях в максимально полной и открытой форме.
База данных с Вашими измеренными значениями – это многуровневый высокодоступный кластер. Она разделена на ведущую базу данных (master) и ведомую (slave), находящиеся в разных пожарных зонах. Ежедневное резервное копирование служит гарантией, что обе базы данных содержат текущие сведения, и в случае падения одной из баз можно будет в любой момент полностью восстановить все данные. Кроме того, все данные также архивируются на дистанционно расположенном сервере.
Помимо баз данных в каждой пожарной зоне находится кластер приложений, в котором содержится так называемый “брокер” – интерфейс между WiFi-логгерами данных и базами данных. Каждый кластер приложений используется максимум на 50%. Это обеспечивает безопасную передачу измеренных значений с WiFi-логгера в базу данных, даже если “брокер” не сработает из-за системной неисправности.

4. Кто имеет доступ к моим данным?

- Вы и те лица, которым Вы разрешили иметь доступ к Вашей учетной записи.
- Сотрудники компании Testo AG в Германии с целью осуществления сервисного обслуживания testo Saveris 2 и гарантии бесперебойной работы системы. Данные измерений не подлежат изменению или удалению.

5. Действие какого законодательства о защите данных распространяется на мои данные?

Серверы, на которых хранятся Ваши данные, находятся в Германии, следовательно, на них распространяется немецкое законодательство в отношении защиты данных.

6. Какие сертификаты действуют?

Host Europe имеет сертификат ISO/IEC 27001:2005.

ISO/IEC 27001:2005 является основным международным стандартом Систем Менеджмента Информационной Безопасности (СМИБ), применимым по отношению к частным коммерческим или общественным предприятиям, а также организациям. Данный стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы Менеджмента Информационной Безопасности.

Стандарт содержит требования к осуществлению подходящих механизмов обеспечения безопасности безотносительно сферы применения, которые необходимо адаптировать под отдельные требования соответствующих организаций. ISO/IEC 27001:2005 был разработан с целью гарантии выбора подходящих механизмов обеспечения безопасности для защиты всех информационных ресурсов компании.

7. Что нужно знать моему сотруднику IT-отдела?

- WiFi-логгеры данных системы testo Saveris 2 устанавливают соединение с брокером через порт 1883 по стандартному протоколу MQTT.
- Временная синхронизация логгеров данных с SNTP-сервером осуществляется через порт 123.
- Именование в службе DNS осуществляется через порт 53.
- Все три порта (1883, 123, 53) должны быть открыть только для выхода данных. Нет необходимости в использовании двунаправленных портов.
- Шлюз по умолчанию, который должен быть связан с зондом по протоколу DHCP или вручную, должен отвечать на ping-запрос WiFi-логгера данных. Примечание: В ходе первой настройки можно выбрать, что будет использоваться: протокол DHCP или статический IP. Выберите “экспертный режим”, чтобы получить актуальную информацию.
- Каждый WiFi-логгер данных системы testo Saveris 2 имеет свой уникальный MAC-адрес.
- Каждый WiFi-логгер данных системы testo Saveris 2 имеет динамический IP-адрес, который можно отдельно изменить на статический.
- testo Saveris 2 поддерживаает 2,4 гГц WLAN (IEEE 802.11 b/g/n).
- Метод кодирования, используемый для установления связи между WiFi-логгером данных и маршрутизатором – WPA2.
- Приложение для testo Saveris 2 доступно через любой интернет-браузер. Используются стандартные TCP-порты http (80) и https (443).

Российское отделение Testo AG – ООО “Тэсто Рус”
115054, Москва,
Большой Строченовский пер., д.23В, стр.1
Телефон: +7 (495) 221-62-13
Факс: +7 (495) 221-62-16
E-mail: info@testo.ru
http://www.testo.ru