servereye

servereye Data sheet

servereye

IT monitoring with servereye means monitoring hardware, software, networks and communication channels. servereye offers solution approaches with which partners can optimally serve the requirements of their customers. The monitoring software monitors all processes around the clock and detects faults immediately. In addition, it informs everyone who is responsible for it - no matter where he or she is located worldwide.

System requirements

The system requirements for using servereye are listed in the knowledge base.

>> Click here for the system requirements <<

Encryption of communication

servereye treats all your data and measured values with the utmost confidentiality.

This starts with the transport of the data from the OCC-Connector to our servereye Cloud. We rely on the industry standard TLS/SSL with a 2048bit key.

All communication channels are additionally secured with Perfect Forward Secrecy (PFS) standard. Perfect Forward Secrecy is a protocol for generating TLS session keys. This procedure enables a secure exchange of the keys and prevents that in case of loss of the master key, all session keys created with it become decryptable.

We use the HTTP Strict Transport Security (HSTS) method. HSTS ensures that our Online Control Centre can only be accessed via HTTPS connections. Our domain is already registered for HSTS in all common browsers (HSTS Preloading).

We use further measures to process your data as securely as possible. Every machine installed with servereye has a private and a public key. The private key is only known to your machine and is used to decrypt the passwords. The public key is known to the OCC and encrypts all passwords when they are saved.

servereye

servereye Data Centre

Our servers are located in a high-security data centre. The computer centre is located in Germany.

ELECTRICITY, CLIMATE, FIRE AND WATER PROTECTION

- Redundant air conditioning of the racks
- Uninterruptible power supply with redundant building supply
- Protection against voltage fluctuations
- Emergency power supply via UPS and diesel generators (n+1)
- Fire alarm systems with early detection
- Hardware-friendly firefighting through gas extinguishing
- A leakage warning system is installed in the data center to protect against water
- A drip tray in the underfloor, which can hold all the water in the cooling circuit in the event of a leak, fully protects the systems operated above it from water ingress

SECURITY

- Data centre area designed as security zone
- mechanical/electronic access control
- 24 h security personnel on site
- Video surveillance and recording in the building and on the outside
- Monitoring of the complete infrastructure
- Use of state-of-the-art firewall technology and intrusion prevention/detection systems
- When accessing the OCC from the browser, additional servers in other data centres are used. These servers are only used for faster delivery of static content. No access data or measured values are transmitted to these servers. For the statistical analysis of accesses

With the help of technology used according to the latest security standards, we ensure that no external access to your network is possible through the use of servereye. All measured values, system parameters and system statuses collected in your network flow exclusively from the inside to the outside, so that no opening of the firewall is required.

Which data are transmitted

**Only the results of the monitoring configured by the user will be displayed.
to the online instance for processing and preparation. These are exclusively measured values and information on monitored systems and system states, which are sent to our OCC in an appropriately encrypted form.**

How long are data stored

Alarm messages are stored for 24 months. Individual measured values are stored for 24 hours. All measured values older than 24 hours are only available in grouped form. With increasing age of the data, they are grouped more and more. After 30 days, only one data record is available for every 12 hours of measured values.

For billing purposes, the number of sensors used per customer is counted every night between 2 and 3 o'clock. After 24 months, only the monthly maximum is stored. Invoice data is stored in accordance with the legal regulations.

If you have any further questions on the subject of security, our colleagues from the support department at support@server-eye.de will be happy to help you.