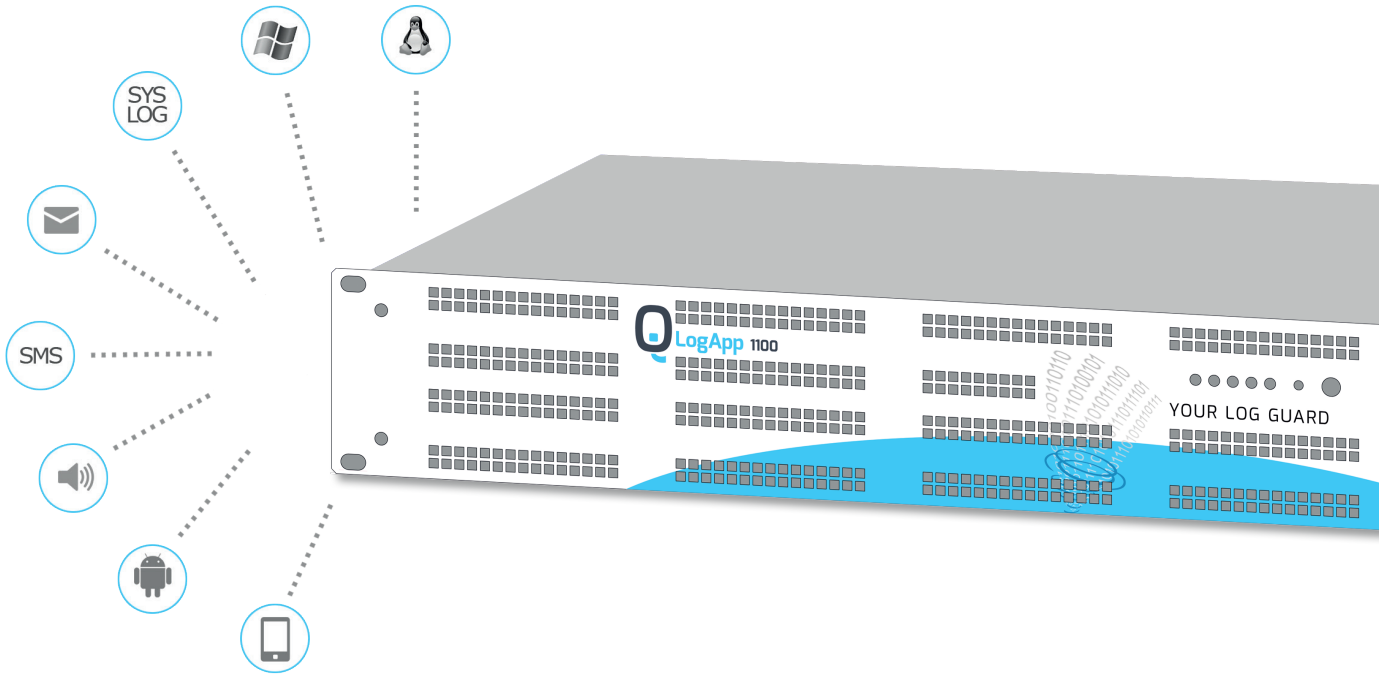
LogApp – regulation compliant logging
The tool for IT security and compliance

iQSol
Security made in Austria.



LogApp

Guaranteed compliance and security in office, data center and production through central logging!

Who had when and where (il)legally access?

Latest security requirements call for logging of numerous events from different systems. Also the European General Data Protection Regulation requires complete documented evidences of access, changes, transfer and deletion of sensitive data within the company networks.

LogApp collects, normalizes and analyses events with LogAgents and over syslog. Integration possibilities from ERP/CRM systems and many other applications and databases make it easier to see who had when and where (il)legally access. This aspect is one of the central criteria for the data protection authority. The objective is the proof of data privacy compliance through automated procedures without any additional effort.

TIP!

A full and tamper-proof archiving of all collected events and created alerts meets further compliance requirements.

If security-critical events are detected, an alarm is created in real time and sent to the operations team via e-mail or an alerting solution.

LogApp

Core Features

- available as appliance or Virtual Machine
- central management with tamper-proof archiving
- LogAgents for Windows Server, Linux Server, Windows Clients
- syslog interface for networking devices and other syslog-sources
- SNMP interface for networking components
- possibility to cascade LogApps
- optionally encrypted communication between LogAgent and LogApp
- alerting via e-mail or iQSol Alert Messaging Server (SMS, Voice)
- comprehensive reporting (Enterprise Reporting Services)
- 4-eye-principle for events and alerts (online and archive)
- comprehensive role concepts

LogAgent

LogAgents collect events from Windows- or Linux-Servers and forward them to a LogApp. Archiving, correlation and alerting are completely taken over by LogApp.

All **events** are **transmitted over an encrypted channel to LogApp**. Geographically dispersed scenarios can be depicted efficiently and safely. LogAgents are available for Windows and Linux and do not have any special demands to the system resources.

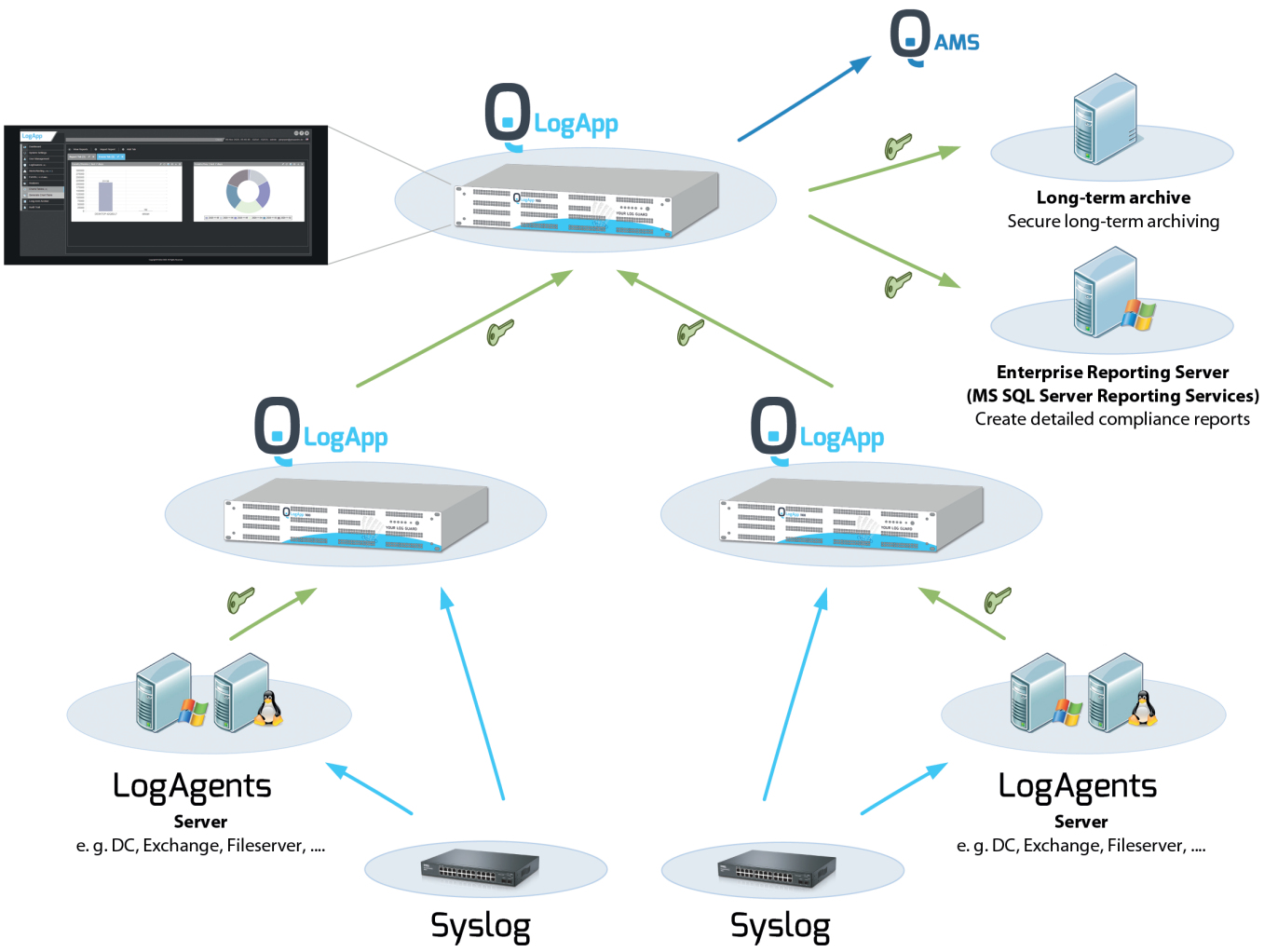
Agent Features

- Log formats
  - Windows Event Logs (application, security, setup, system, ...)
  - Linux System Logs (user authentication, ...)
  - Log Files (flatfiles, XML, CSV, ...)
- File Integrity Monitoring
- Windows Change Auditing
- Syslog and SNMP proxy functionality
- buffer function
- encrypted transmission (optional)
- remote or local installation

Syslog

Events from networking devices and other syslog sources can be sent directly to LogApp. The syslog interface accepts and processes events analogous to events from a LogAgent. Optionally, LogAgents can also be configured as syslog and SNMP proxies in order to collect events decentral in more complex network architectures.

LogApp Architecture



Through the possibility of cascading LogApps, numerous scenarios regarding event collection, alerting and archiving can be depicted. Both the consolidation of all events of the subordinate LogApps and selective forwarding of safety-critical events is configurable. Alerts can be triggered on the subordinate LogApps or also only on the hierarchically highest LogApp.

Web Interface for LogApp

- simple administration of LogAgents and syslog sources
- user and group management with Active Directory access
- extensive filtering and search function in alerts and events
- import and export of rules
- dashboard with system information and reports
- detailed system protocol
- multitenancy
- multilingual support

Technical Specification

	LogApp 2600	LogApp 1100	LogApp 600	LogApp VM
Hardware				
Cores	10	8	8	min. 4
RAM	64 GB	32 GB	16 GB	min. 4 GB
HDD-Capacity	8x 1.8 TB SAS 10k	4x 2 TB SATA 7.2k	4x 1 TB SATA 7.2k	min. 250 GB
RAID	RAID 10	RAID 10	RAID 10	-
LAN	4x Gigabit Ethernet	4x Gigabit Ethernet	4x Gigabit Ethernet	1-2x Gigabit Ethernet
Dimensions	19“ 1U	19“ 1U	19“ 1U	-

LogApp 2600 is the highest performing LogApp appliance. Sufficient resources are provided for high load event collection and correlation. A raid controller and one redundant power supply ensure maximum reliabiltiy. Because of its high-performance, LogApp 2600 is perfect for large companies with a geographically dispersed network and a large amount of LogAgents and syslog-sources.

LogApp 1100 and LogApp 600 ensure reliable detection of anomalies in small and medium-sized organizations. LogApp can operate as virtual machine alternatively.

Supported Operating System

LogAgent for Windows	Windows 10 / 11, Windows Server 2022 / 2019 / 2016 (older versions on request)
LogAgent for Linux	Red Hat Enterprise Linux and CentOS form version 7 upwards (older versions on request) Ubuntu from version 14.04 upwards (older versions on request) SUSE Linux Enterprise und OpenSUSE from version 12 upwards (older versions on request)

Further Benefits

- licensing on the number of servers and applications
- available as Managed Security Service
- cost-effective entry possible with log management
- legal certainty with European software
- auditable archiving
- four eyes principle for real-time data and archive

iQSol GmbH, Petrusstrasse, A - 3312 Oed T: +43 7472 207 67 E: office@iqsol.biz W: www.iqsol.biz