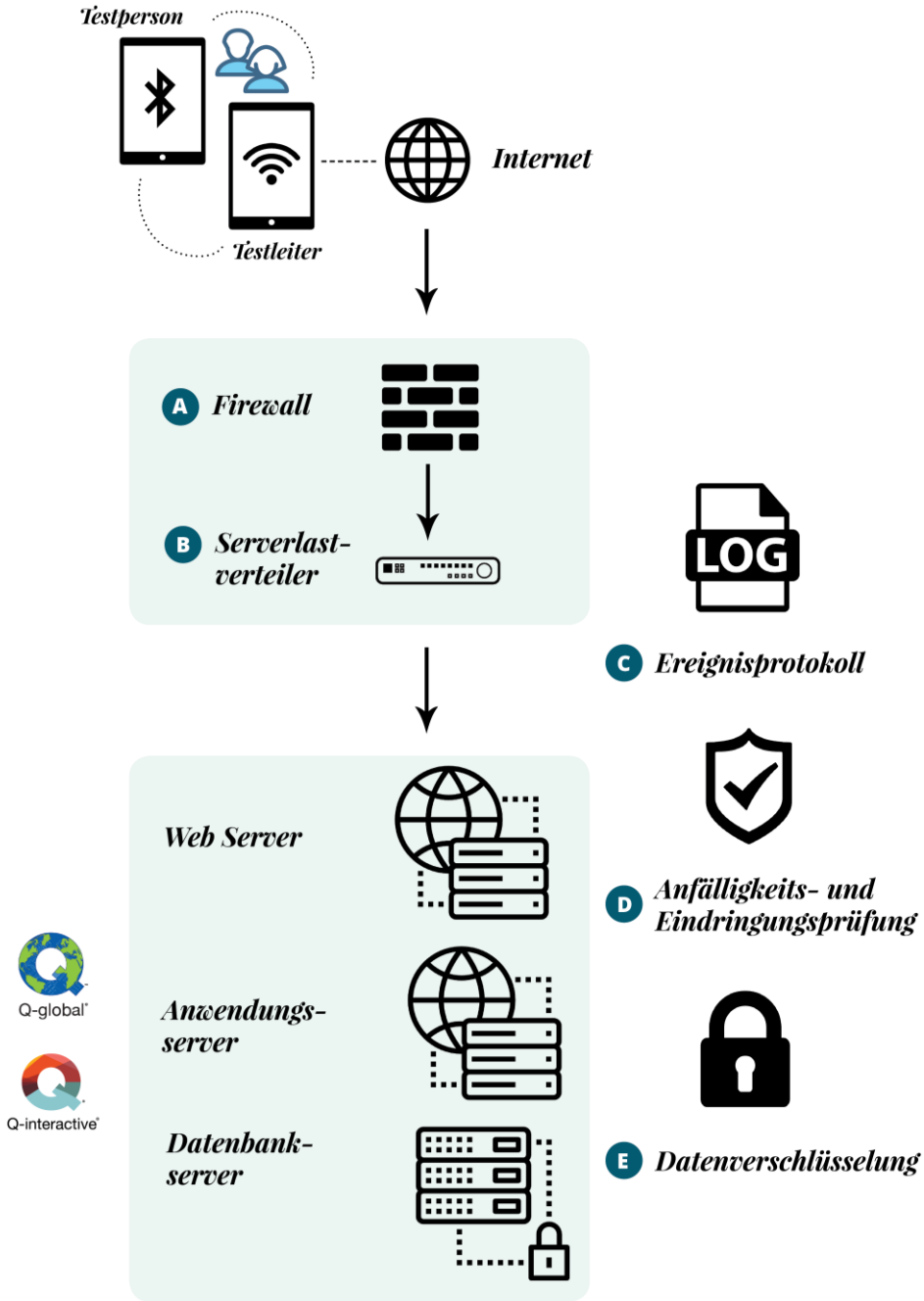
Informationen zur Systemarchitektur von Q-global und Q-interactive

Die Instandhaltung einer sicheren Infrastruktur und einer Umgebung, welche die vollkommene Sicherung von Daten und personenbezogenen Informationen unserer Kunden sicherstellt, hat höchste Priorität. Das folgende Dokument beschreibt die Architektur und Sicherheit, welche Q-global und Q-interactive nutzen, um diese Daten zu schützen.



Ihr Kontakt zu uns: Pearson Beratungsservice | Tel.: 069/756 146-17/-25/-28/-32 | beratungsservice.de@pearson.com

Architektur:
Q-global und Q-interactive sind web- bzw. iPad-basierte Anwendungen, welche für klinische Diagnostiker entwickelt wurden, die einfach, zuverlässig und sicher Testverfahren durchführen und auswerten möchten.

A) Dedizierte Firewall

Eine dedizierte Firewall fungiert als erste Verteidigungslinie und kontrolliert den Datenverkehr zwischen vertrauenswürdigen und nicht-vertrauenswürdigen Netzwerken. Sie filtert und blockiert unwesentlichen Datenverkehr anhand von Ports sowie Protokollen und ermöglicht nur angemessenem sowie gewolltem Datenverkehr den Zugang zum Netzwerk.

B) Serverlastverteiler

Ein Load Balancer (Serverlastverteiler) dient nicht nur zur Entlastung für den Server und zur Verwaltung der Datenlast der Plattform, sondern verwaltet auch den Datenverkehr und verdeckt den Verbindungsendpunkt, um vor unbefugtem Zugriff und Evasion des Netzwerks (Überbrückung eines Informationssicherungsgeräts, um z. B. eine Netzwerkattacke auszuführen) zu schützen. Er ermöglicht zudem die Beständigkeit von HTTPs-Sitzungen zwischen Servern, um sicherzustellen, dass jegliche Daten sicher zu Q-global/Q-interactive übertragen werden.

C) Ereignisprotokoll

Das Log Management (Ereignisprotokoll) hilft bei der Erkennung von nicht-autorisierten Zugriffsversuchen. Die verwendeten Informationssysteme führen spezifische Ereignisprotokollierungen auf der Anwendungsebene durch, um potenzielle Angriffe zu identifizieren. Das Ereignisprotokoll ermöglicht so eine schnelle sowie sichere Überwachung und Reaktion auf nicht-autorisierte Zugriffsversuche.

D) Anfälligkeits- und Eindringungsprüfung

Anfälligkeits- und Eindringungstests werden regelmäßig durchgeführt und ermöglichen die Identifizierung von möglichen Schwachstellen. Die Tests können in verschiedenen Intervallen durchgeführt werden, um sicherzustellen, dass durchgeführte Konfigurationsänderungen, Patches oder Funktionalitätsverbesserungen nicht zu Sicherheitslücken führen. Diese Form des Testens ist eine proaktive, präventive Kontrolle, die das Auffinden und Korrigieren (Verbessern) von Anwendungs- und Infrastrukturschwächen ermöglicht.

E) Datenverschlüsselung

1. Bei Übertragungen

Alle Daten, die an die Q-global/Q-interactive Plattform übermittelt werden, werden über eine sichere und kodierte 256-Bit-TLS-Verbindung übertragen. Der Webbrowser prüft das HTTPs-Zertifikat und generiert eine Ausnahme, falls das Zertifikat ungültig sein sollte.

Ihr Kontakt zu uns: Pearson Beratungsservice | Tel.: 069/756 146-17/-25/-28/-32 | beratungsservice.de@pearson.com

2. Im Ruhezustand

Kundendaten werden auf Q-global/Q-interactive in einer Datenbank verschlüsselt, welche sich in einer dedizierten, sicheren Server-Umgebung befindet. Diese Umgebung ist zugriffsbeschränkt und der physische sowie virtuelle Zugriff ist nur durch autorisiertes Personal möglich (Datenbankadministratoren). Lese- und Schreibprüfinformationen werden für den Zugriff und für Änderungen in der Datenbank gespeichert.

Ihr Kontakt zu uns: Pearson Beratungsservice | Tel.: 069/756 146-17/-25/-28/-32 | beratungsservice.de@pearson.com