БЕЗОПАСНОСТЬ TEAMVIEWER

Самые высокие стандарты безопасности Все подключения TeamViewer осуществляются через полностью закодированные каналы данных. Это также безопасно как интернет-банкинг.

Знак качества

Программное обеспечение TeamViewer сертифицировано в Германии "Bundesverband der IT-Sachverständigen und Gutachter e.V."(BISG e.V. , Немецкая экспертная ассоциация в области информационных технологий) со знаком качества "пять звёзд".
Независимые члены ассоциации BISG оценивают продукты известных компаний с точки зрения качества, безопасности и значимости.

Проверка безопасности FIDUCIA IT AG

Программное обеспечение TeamViewer прошло проверку безопасности, проводимую FIDUCIA IT AG (оператор центров обработки данных в 800 банках Германии) и получило разрешение на использование и внедрение в банковской системе.

Проверка безопасности GAD eG

Немецкая компания GAD eG (оператор центров обработки данных для 450 немецких банков) подтвердила характеристики безопасности TeamViewer. Одобрено использование TeamViewer на компьютерах банковской системы (WinXP).

Шифрование

TeamViewer включает полное шифрование данных, базирующееся на обмене личными/публичными ключами RSA и шифровании сеансов AES (256 бит). Эта технология основана на тех же стандартах, что и https/SSL, и считается абсолютно безопасной среди использующихся в настоящее время стандартов.
Обмен ключами также гарантирует полную защиту данных, передаваемых от клиента к клиенту. Это означает, что даже серверы-маршрутизаторы не могут контролировать поток данных.

Защита доступа

В целях обеспечения дополнительной защиты от несанкционированного доступа к системе TeamViewer, в дополнение к PartnerID (ID партнёра), также генерирует пароль сеанса, который меняется при каждом запуске программного обеспечения. Некоторые функции, влияющие на безопасность, – например передача файлов – требуют дополнительного подтверждения от удалённого партнёра. Также невозможно незаметное управление компьютером. В целях защиты данных лицо, сидящее за удалённым компьютером, должно иметь возможность определить, когда кто-то пытается получить доступ к машине.

Подпись кода

Все программные файлы защищены с помощью технологии подписи кода VeriSign. Это позволяет вам проверить источник полученных вами исполняемых файлов. Даже средства QuickSupport с заказным дизайном получают при создании динамическую подпись.