Отличия версий продуктов	ESET NOD32 Antivirus Business Edition	ESET NOD32 Smart Security Business Edition
Антивирус и Антишпион Детектирование всех типов вредоносного программного обеспечения и проверка репутации приложений до их запуска на базе облачной технологии.	ДА	ДА
Контроль устройств Автоматическое сканирование подключаемых внешних устройств и настройка правил работы со съемными носителями информации для каждого пользователя.	ДА	ДА
Антифишинг Данная технология защищает пользователей от потери логинов и паролей, банковских реквизитов, данных кредитных карт и другой информации вследствие подмены надежных вебсайтов поддельными – фишинговыми.	ДА	ДА
Оптимизация для виртуальной среды Функция ESET Shared Local Cache позволяет значительно ускорить сканирование виртуальных машин за счет хранения информации о ранее просканированных общих файлах.	ДА	ДА
Защита от эксплойтов Блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее не известных эксплойтов и уязвимостей нулевого дня.	ДА	ДА
Расширенное сканирование памяти Технология позволяет обезвреживать зашифрованные вредоносные программы, которые устанавливаются на компьютер скрыто от пользователя.	ДА	ДА
Централизованное управление Продуктом ESET Endpoint Antivirus для Microsoft Windows можно удаленно управлять при помощи ESET Remote Administrator.	ДА	ДА
Минимальные системные требования ESET Endpoint Antivirus обеспечивает эффективную защиту рабочих станций, сохраняя при этом больше системных ресурсов для выполнения других задач	ДА	ДА
Настраиваемый графический интерфейс Интерфейс продукта можно полностью отключить, чтобы не отвлекать конечного пользователя от его непосредственных задач	ДА	ДА
Простая установка При установке специальный компонент ESET AV Remover автоматически определяет и предлагает удалить любое программное обеспечение, которое будет конфликтовать с антивирусным продуктом.	ДА	ДА
Веб-контроль Возможность настроить корпоративную политику безопасности и ограничить доступ пользователей к веб-сайтам по категориям или управлять отдельными списками адресов.	НЕТ	ДА
Щит уязвимости Технология обнаружения уязвимостей в распространенных протоколах, таких как SMB, RPC и RDP, является важным слоем защиты от вредоносных программ и сетевых атак.	НЕТ	ДА
Файервол Фильтрация всего входящего трафика, включающая настраиваемую систему обнаружения внешних вторжений HIPS (Host-based Intrusion Prevention System) и защиту от ботнетов.	НЕТ	ДА
Защита от ботнетов Помогает контролировать сетевую активность и обнаруживать вредоносные программы посредством анализа сетевых коммуникационных моделей и протоколов	НЕТ	ДА