

Пакетные предложения по настройке и поддержке продуктов безопасности Microsoft для заказчиков малого и среднего бизнеса

(до 300 пользователей)



Киберпреступность становится бизнесом, хакеры объединяются в преступные группировки, которые имеют достаточное финансовое обеспечение. Киберугрозы находятся в центре внимания организаций и правительств во всем мире, а денежные и репутационные риски становятся всё выше. Softline предлагает воспользоваться решениями по безопасности, входящими в состав Microsoft 365.

BASIC

Единократовая настройка и отработка инцидентов:

- Многофакторная авторизация (SMS + мобильное приложение Authenticator)¹
- Условный доступ для MFA
- Портал самостоятельного сброса пароля
- Политики защиты Outlook на мобильном устройстве²
- Консалтинг³

¹25 пользователей (не более 300)

²1 устройство на сотрудника

³5 часов поддержки

Доступно для следующих лицензий:

EMS E3/E5, Microsoft 365 Business Premium/A3/A5/E3/E5

Стоимость пакета Basic – **75 000 ₽**

Дополнительные 25 пользователей – **7 500 ₽**

SMART

Все сервисы из пакета Basic, а также:

- Условный доступ для Outlook на мобильном устройстве¹
- Политики защиты MS Office на мобильном устройстве²
- Единый вход³
- Политики защиты Exchange Online
- Windows Hello for Business
- Консалтинг⁴

¹25 пользователей (не более 300)

²1 устройство на сотрудника

³1 SaaS приложение на организацию

⁴10 часов поддержки

Доступно для следующих лицензий:

Microsoft 365 A3/A5/E3/E5

Стоимость пакета Smart – **120 000 ₽**

Дополнительные 25 пользователей – **12 000 ₽**

SUPPORT

Инцидентная поддержка технического пользователя, удаленные подключения, эскалация обращений.

Объем работ:

10 часов, срок 1 год, до 300 пользователей

- Прием и регистрация обращений в Service Desk исполнителя (телефон, почта, портал) от технического пользователя заказчика
- Сессии удаленных подключений с целью оказания помощи в решении инцидентов (по запросу, в рамках объектов сопровождения)
- Эскалация обращений и взаимодействие с Microsoft
- Предоставление регулярной статистики по обращениям по форме исполнителя

Стоимость пакета Support – **36 000 ₽**

OUTSOURCING

Помощь техническому пользователю заказчика по управлению облачным тенантом, Exchange Online, Teams, OneDrive, SharePoint Online, Office 365 ATP, Azure Information Protection, Microsoft Endpoint Manager, сессии удаленных подключений по запросу, контроль статуса выполнения работ, подготовка отчета.

Объем работ:

24 часа, срок 1 год, до 300 пользователей

- Администрирование учетных записей, групп, ролей, подписок и лицензий
- Администрирование почтовых ящиков, групп рассылки и потока почты
- Администрирование политик решений по безопасности

Стоимость пакета Outsourcing – **70 000 ₽**

Дополнительные 12 часов – **35 000 ₽**

Многофакторная авторизация (MFA)

Пароли легко потерять или взломать. В большинстве атак с целью кражи удостоверений не играет роли, насколько длинный и сложный у вас пароль. MFA сразу же повышает защищенность вашей учетной записи, так как при входе в приложение для подтверждения своей личности вы проходите несколько форм проверки. MFA можно использовать для защиты доступа как к приложениям, расположенным локально, так и в облаке.

Условный доступ (Conditional Access)

Периметр безопасности вышел за пределы сети организации. Conditional Access позволяет принимать решение о предоставлении доступа пользователю, используя такие сигналы идентификации как его учетная запись, расположение, устройство и приложение с которого он пытается получить доступ.

Портал самостоятельного сброса пароля (SSPR)

Самостоятельный сброс пароля (SSPR) позволяет пользователям изменить или сбросить пароль без участия администратора. Если учетная запись пользователя заблокирована или пользователь забыл пароль, выполнив несложные инструкции, он сможет выполнить разблокировку и вернуться к работе. Эта возможность снижает количество обращений в службу технической поддержки и минимизирует время простоя из-за невозможности войти на устройство или в приложение.

Политики защиты Outlook на мобильном устройстве

Outlook для iOS и Android предоставляет пользователям быстрый, интуитивно понятный интерфейс электронной почты и календаря. Очень важно защитить данные компании или организации на мобильных устройствах пользователей. Также вы можете запретить сотрудникам использовать Outlook для iOS и Android, если это не соответствует политике безопасности в организации.

Политики защиты MS Office на мобильном устройстве

С помощью политик защиты вы можете ограничить возможности сотрудников при работе с приложениями Office на мобильных устройствах. В частности, они позволяют: удалять рабочие файлы с устройства, которое не активно более указанного количества дней, обеспечить сохранение корпоративных файлов только в OneDrive для бизнеса, шифровать рабочие файлы, запрашивать пин-код или отпечаток пальца для доступа к приложениям Office.

Единый вход (SSO)

Настройка единого входа — это существенный этап в развитии процесса получения доступа пользователей к приложениям и работы с ними. С единым входом пользователи входят один раз, используя одну учетную запись, и получают доступ к присоединенным к домену устройствам, ресурсам компании, приложениям SaaS (программное обеспечение как услуга) и веб-приложениям.

Политики защиты Exchange Online

Microsoft Exchange Online Protection (EOP) — это облачная служба фильтрации электронной почты, она помогает защитить организацию от нежелательной почты и вредоносных программ, передаваемых через email. EOP может упростить управление вашей средой обмена сообщениями и облегчить многие сложности, которые связаны с поддержкой аппаратного и программного обеспечения.

Windows Hello for Business

Windows Hello для бизнеса заменяет пароли на компьютерах и мобильных устройствах, которые имеют строгую двухфакторную проверку подлинности. Для контроля в этом случае используется новый тип учетных данных пользователей, привязанных к устройству и основанных на биометрических данных или PIN-коде.

Контакты:

+7 495 232-00-23
info@softline.com
www.softline.ru

softline[®]
We know we can