

Решения обеспечения безопасности Endpoint Detection and Response и Cloud Access Security Broker от Microsoft



Компания Информзащита предлагает защитить корпоративную информацию от новых типов угроз на базе современных средств защиты компании Microsoft.

Defender for Endpoint*

комплексное облачное решение для обеспечения безопасности конечных точек (Endpoint Detection and Response, EDR). Обнаруживает, автоматически анализирует и нейтрализует угрозы, а также предотвращает дальнейшие атаки.

CloudApp Security

брокер безопасного доступа в облако (Cloud Access Security Broker, CASB), работающий в множестве облачных сред. Обеспечивает широкие возможности визуализации, контроля над перемещением данных и сложной аналитики для обнаружения и устранения киберугроз во всех ваших облачных службах.

Пилотная группа
25 пользователей



Длительность
60 рабочих дней

Этапы пилотного тестирования:

- ▶ Определение пилотной группы
- ▶ Интеграция и настройка двух решений обеспечения безопасности
- ▶ Ознакомление с возможностями решений
- ▶ Демо-атака с анализом работы решений
- ▶ Регулярное взаимодействие по результатам работы решений обеспечения безопасности

По завершению пилотного проекта вы получите:

- ▶ Результаты обнаружения и реагирования решений Microsoft на угрозы в ходе демо-атаки
- ▶ Возможность ознакомиться с решениями для обеспечения безопасности компании Microsoft
- ▶ Полное понимание как решения Microsoft защищают вашу информационную структуру

Дополнительно возможно пилотирование следующих продуктов MS



Защита информации



Управление доступом



Защита от целевых атак и инфраструктуры



Защита почты

*ранее MDATP

Защита информации

Microsoft Information Protection, Azure Information Protection	Решения по классификации и защита документов и электронных писем используя метки
Microsoft 365 Endpoint DLP	Решение по защите от потери и предотвращению случайного предоставления доступа к конфиденциальным данным
Cloud App Security	Брокер безопасного доступа в облако
Intune	Решение по управлению мобильными устройствами (MDM) и управлению мобильными приложениями (MAM)

Защита от целевых атак и инфраструктуры

Microsoft 365 Defender	Единый пакет, в котором встроены функции обнаружения, защиты, исследования для обеспечения интегрированной защиты
Microsoft Defender for Endpoint	Облачное решение для безопасности конечных точек
Microsoft Defender for Office365	Решение по защите от угроз, которые могут быть получены через электронные сообщения, вложения, ссылки (URL-адреса) и средства совместной работы
Microsoft Defender for Identity	Облачное решение безопасности, которое использует сигналы локальной службы Active Directory для обнаружения и анализа угроз
Microsoft ATA	Локально решение безопасности, которое использует сигналы службы Active Directory для обнаружения и анализа угроз
Azure AD Identity Protection	Решение по автоматизации обнаружения и устранения рисков на основе удостоверений, исследование рисков и дальнейший анализ

Управление доступом

Identity Governance	Решение по защите, отслеживанию и аудиту доступа к критически важным ресурсам
Azure AD + Azure MFA	Решение по защите доступа к данным и приложениям за счет дополнительного способа аутентификации
Windows Hello for Business	Решение по защите проверки подлинности пользователя на компьютерах и мобильных устройствах

Защита почты

Exchange Online Protection	Решение по защите облачной почтовой службы
Microsoft Defender for Office 365	Решение по защите от угроз, которые могут быть получены через электронные сообщения, вложения, ссылки (URL-адреса) и средства совместной работы