

1. Сегментируем сеть на подсети DMZ, Inside. Возможно даже разделил бы на подсети сегмент 2 – кластер Oracle+ БД Estaff отдельно, внешнее приложение отдельно, сервер DWH + почта и отдельно рабочие места.
2. Между интернет сегментом и DMZ установить firewall/waf.
3. Между DMZ и 2 сегментом также установить firewall/waf.
4. На почтовом сервере установить почтовый антивирус.
5. Рабочие места оснастить антивирусными продуктами. Сервер управления антивируса оставить в инсайде при условии, что рабочие места пользователей находятся в локальной сети.
6. Развернуть сервер резервного копирования критичных данных.
7. Внедрение SIEM системы.
8. Установить сканер безопасности для мониторинга инфраструктуры. Регулярные пентесты.
9. Для мониторинга рабочих мест необходима система DLP.