Традиционные МФА и Silverfort

Характеристика	Традиционные МФА	Silverfort
Архитектура	Требует установки агента, прокси или интеграции с **каждой отдельной** защищаемой машиной. **Если агент удален – защиты нет**	Легкое внедрение без агентов и прокси. Постоянная непрерывная защита, которую нельзя обойти
Защита протоколов интерактивного входа (RDP и аналоги)	**Да, если существует агент или интеграция**	**Да**
Защита всех других протоколов (более 100 для Windows, в том числе протоколы командной строки psexec / smb, wmi, powershell, которые обычно и используют злоумышленники)	**Нет**	**Да**
Защита систем и устройств, на которые нельзя установить агент (IoT / OT, гипервизоры, legacy, file shares, самописное ПО и пр.)	**Нет**	**Да**
Защита сервисных УЗ	**Нет**	**Да**
Мониторинг и анализ всех попыток аутентификации и доступа ко всем ресурсам во всех средах организации	**Нет**	**Да**
Адаптивная политика МФА на основе AI, уровня риска , без закидывания пользователей постоянными запросами на второй фактор	**Нет**	**Да**
Выявление и блокирование атак на УЗ (аномалии, брутфорс, криптолокеры, нацеленные хакеры и пр.)	**Нет**	**Да**
Единая система аутентификации для всех кейсов (VPN, Windows, Linux, облака, веб и пр.)	**Нет**	**Да**
Простота лицензирования, отсутствие множества модулей для разных протоколов	**Нет**	**Да**