1. Продукт должен поставляться как виртуальное устройство (VA-virtual appliance) или физическое устройство (HW-оборудование), любой тип поставки должен быть сделан в виде единой платформы, которая не требует использования стороннего системного или прикладного программного обеспечения (операционные системы, программные приложения, системы управления базами данных и т.д.) для его имплементации.  
2. Продукт должен иметь функционал дополнительного подтверждения (одобрения) подключения к целевой системе привилегированных пользователей ответственным лицом.  
3. Продукт должен иметь встроенный механизм защиты от несанкционированного доступа к информации что сохраняется. Данная защита должна обеспечивать использование специального ключа защиты (пароля) при каждом запуске Продукта (после выключения или перезагрузки).  
4. Защищенное хранилище должно использовать стандартные крипто алгоритмы уровня не ниже AES-256.  
5. Настройка и администрирование Продукта должно осуществляться через отдельный веб-портал администрирования с использованием любого современного браузера (IE, Mozila, Chrome и т. д.) без необходимости установки дополнительных компонентов (плагинов, приложений и т. д.). Использование веб-консоли на основе технологии Flash или Java (JRE) не допускается.  
6. Продукт должен поддерживать запись действий привилегированных пользователей встроенными средствами без необходимости установки любого компонента (агента, сервиса, драйвера и т. д.) как на конечные рабочие точки привилегированных пользователей, так и на системы, к которым подключаются привилегированные пользователи (целевые системы).  
7. Продукт должен иметь функционал создания политик о возможности просмотра отдельными привилегированными пользователями пароля (-ей) к целевым системам, к которым они подключаются, в случае если такой пароль им неизвестен. Продукт должен иметь функционал принудительного запроса причин просмотра отдельными привилегированными пользователями пароля (-ей) к целевым системам, к которым они подключаются. Продукт должен иметь функционал дополнительного подтверждения (одобрения) просмотра отдельными привилегированными пользователями пароля (-ей) к целевым системам, к которым они подключаются. Продукт должен иметь встроенные механизмы просмотра таких паролей в любое нужное время (в прошлом) в случае, если они (пароли) изменялись с помощью соответствующего функционала Продукта (парольной политики).  
8. Администрирование Продукта должно поддерживать ролевую модель управления Продуктом и надзора за привилегированными пользователями.  
9. Продукт должен иметь встроенное безопасное хранилище для хранения записанных сессий привилегированных пользователей, реквизитов доступа (логин, пароль, ключи, доменные имена и т. д.) к Продукту, целевым системам и журналам событий. Безопасное хранилище должно использовать стандартные криптоалгоритмы, не ниже AES-256.  
10. Продукт должен иметь возможность создания отказоустойчивых конфигураций на базе встроенных технологий, использование сторонних (внешних) средств для построения таких (отказоустойчивых) конфигураций - не допускается.

11. Продукт должен иметь функционал добавления администраторов через веб-портал администрирования Продукта с возможностью выбора ролей, срока действия учетной записи, языка и способа аутентификации администратора.  
Для каждой учетной записи администратора должна быть поддержка по нескольких методов аутентификации:  
♣ С помощью статического пароля, хранящегося в безопасном хранилище Продукта;  
♣ Одноразовый пароль, генерируемый внешними службами (например, RADIUS-сервер);  
♣ С помощью внешнего каталога пользователей (AD/LDAP)    
♣ С помощью ключа SSH.  
12. Продукт должен иметь функционал добавления привилегированных пользователей через веб-портал администрирования Продукта с возможностью выбора ролей, срока действия учетной записи, языка и способа аутентификации администратора.  
Продукт должен иметь функционал добавления привилегированных пользователей следующим образом:  
♣ в ручном режиме;  
♣ Синхронизация с существующим каталогом пользователей (AD/LDAP)  
♣ Через интерфейс API.  
Для каждой учетной записи должна быть поддержка по крайней мере нескольких методов аутентификации:  
♣ С помощью статического пароля, хранящегося в защищенном хранилище Продукта;  
♣ Одноразовый пароль, генерируемый внешними сервисами (например, RADIUS-сервер);  
♣ Использование внешнего каталога пользователей (AD/LDAP)    
♣ Использование ключа SSH.  
13. Продукт должен иметь следующие возможности для работы с реквизитами доступа (логины, пароли, доменное имя, SSH ключи и т. д.), используемых привилегированными пользователями для подключения к целевым системам:  
♣ Ручное создание и хранение реквизитов доступа в защищенном хранилище Продукта;  
♣ Использование внешних систем аутентификации (включая внешние специализированные хранилища паролей);  
♣ Анонимный доступ (без необходимости ввода реквизитов доступа).  
В случае ручного создания и хранения реквизитов доступа для подключения к целевым системам, Продукт должен иметь функциональность полной маскировки от привилегированных пользователей данных реквизитов (за исключением случаев, когда такой пересмотр допускается отдельною парольною политикою).  
Продукт должен обеспечить функционал дополнительной (повторной) принудительной аутентификации на целевых системах, даже в том случае, если реквизиты доступа привилегированных пользователей на Продукте и целевых системах полностью совпадают.

14. Продукт должен иметь возможность принудительной замены паролей на конкретных целевых системах по данной парольной политике для отдельно назначенных учетных записей привилегированных пользователей.  
Такая парольная политика должна обеспечивать следующие возможности:  
♣ Длина пароля;  
♣ Сложность пароля (включая требования к большим буквам, цифровым символам, специальным символам);  
♣ Частота изменения пароля.  
♣ Ротация паролей по завершению активного сеанса.  
♣ Принудительное изменение пароля в соответствии с данной парольной политикой должно поддерживаться по крайней мере на следующих целевых системах:  
♣ Unix/Linux- операционные системы на базе (через SSH);  
♣ Операционные системы Windows (через WMI, LDAP);  
♣ Система Cisco (через SSH, Telnet).  
Преимуществом будет функционал безопасного обмена паролями между программными приложениями.  
15. Продукт должен иметь встроенный функционал для оценки эффективности работы с целевыми системами, как отдельных привилегированных пользователей, так и групп привилегированных пользователей. Функционал эффективности работы с целевыми системами должен предоставлять статистику об активных действиях привилегированных пользователей (время активной работы в отношении общего времени работы с целевой системой) возможность детализации и экспорта статистических данных на внешний отчет.  
17. Продукт должен иметь функционал временного или полного принудительного прекращения работы сессий привилегированных пользователей ответственными лицами в режиме реального времени. Также Продукт должен иметь возможность одновременно с прекращением сессии привилегированного пользователя блокировать учетную запись привилегированного пользователя сессия которого прекращается.

17. Резервное копирование должно использовать зашифрованный (защищенный) протокол обмена данными (например, на основе пары публичных и приватных SSH-ключей). Созданные резервные копии должны быть защищены от несанкционированного просмотра данных, что в них хранятся и от несанкционированного восстановления.  
18. Продукт должен иметь встроенные механизмы пересмотра результатов действий привилегированных пользователей, а именно - просмотр записанных сессий, вводимых команд и ответов целевой системы на такие команды. Просмотр результатов должен обеспечиваться в веб-портале администрирования без необходимости установки каких-либо средств (программных приложений, плагинов и т. д.). Продукт должен иметь встроенные фильтры поиска результатов действий привилегированных пользователей по различным критериям, по меньшей мере по имени привилегированного пользователя или пользователей, введенными командами, типу протокола, именем целевой системы, а также в заданном диапазоне дат. Продукт должен иметь возможность создания отчетов на базе полученных результатов с заданными фильтрами. Такие отчеты должны иметь возможность быть экспортировано в виде файлов формата CSV, PDF, HTML.  
19. Продукт должен иметь систему хранения и обработки событий в виде журналов, что хранятся в защищенном хранилище.  
Все журналы событий должны быть защищены от удаления, включая администраторов Продукта с самым высоким уровнем доступа (правами).  
Журналы событий должны содержать в себе по крайней мере следующую информацию:  
♣ События, связанные с производительностью Продукта (включая журналы отладки);  
♣ События, связанные с работой привилегированных пользователей в целевых системах;  
♣ События, связанные с администрированием Продукта.  
20. Продукт должен иметь встроенные механизмы просмотра результатов действий привилегированных пользователей, а именно просмотр записанных сеансов, вводимых команд и ответы целевой системы на эти команды. Результаты просмотра должны предоставляться на веб-портале администрирования без необходимости установки каких-либо средств (программных приложений, плагинов и т. д.).  Продукт должен иметь встроенные фильтры для поиска результатов действий привилегированных пользователей по различным критериям, по крайней мере, по имени привилегированного пользователя или пользователей, введенных командами, типу протокола, название целевой системы, и в заданном диапазоне дат. Продукт должен иметь возможность генерировать отчеты на основе результатов, полученных с помощью данного фильтра. Эти отчеты должны иметь возможность экспортироваться как CSV, PDF, HTML-файлы.  
21. Продукт должен иметь возможность предоставлять доступ третьим лицам к сессиям привилегированных пользователей, подключенных в режиме реального времени так и к сессиям что были сохранены (записаны). Такой доступ должен предоставляться с помощью уникального URL-ссылки с возможностью подключения третьего лица к заданной сессии без какой-либо дополнительной авторизации. При создании URL ссылки обязательно должна быть возможность задания времени действия такой ссылки и режима доступа (полный доступ к сессии или доступ только в режиме просмотра).  
22. Продукт должен иметь функционал просмотра ответственными лицами сессий привилегированных пользователей в режиме реального времени, без какого-либо явного информирования привилегированных пользователей во время такого просмотра.  
Кроме того, продукт должен предоставить ответственному лицу информацию о сеансе: имя и IP-адрес целевой системы, имя пользователя, тип используемого протокола, время начала сеанса.  
23. Продукт должен иметь функционал временного или полного принудительного прекращения сессий привилегированных пользователей, ответственными лицами в режиме реального времени. Также, Продукт должен иметь возможность одновременно с прекращением сеанса привилегированного пользователя блокировать учетную запись привилегированного пользователя, сессия которого прекращается.  
24. Средство должно иметь функционал поведенческого анализа, позволять анализировать поведение работы пользователей по следующим критериям: RDP сессии - анализ выполняемых действий с помощью компьютерной мыши; SSH сессии - анализ команд, Которые пользователи вводят с клавиатуры.  
25. Продукт должен обеспечивать контроль привилегированных пользователей, которые подключаются к целевым систем по протоколу RDP.  
Продукт должен иметь возможность контролировать подключение в различных режимах работы протокола RDP, в том числе - в режимах Enhanced RDP Security (TLS) и NLA.  
Продукт должен иметь функционал по принудительному ограничению разрешения и глубины цвета сессии RDP, принудительного отключения буфера обмена, ограничение доступа к целевой системе устройства, ограничения по работе с мультимедийными установками.  
Результатом контроля привилегированных пользователей, которые подключаются к целевым систем по протоколу RDP должен быть записанный графический видеоматериал (видеоролик).  
Продукт должен иметь функционал экспорта сохранившихся графических видеоматериалов (видеороликов) во внешние видео форматы AVI, FLV, MPEG с заданной разрешающей способностью.  
Средство должно обеспечить функционал подключения к RDP сессии c возможностью перехвата управления действий привилегированных пользователей. То есть, Средство должно обеспечивать одновременную работу пользователя и администратора, который подключается к активной сессии и перехватывает управление конечной системой с фиксацией логов, кто и когда выполняет конкретные действия.  
26. Продукт должен обеспечивать контроль привилегированных пользователей, которые подключаются к целевым систем по протоколу SSH.  
Продукт должен иметь возможность работы со стандартом Х11 через протокол SSH, в том числе - возможность воспроизведения графики через Х11.  
Продукт должен иметь функционал по принудительному ограничению файловых операций (запрет протоколов файлового обмена SFTP и SCP).  
Результатом контроля привилегированных пользователей, которые подключаются к целевым системам по протоколу SSH (или X11) должен быть записан графический видеоматериал (видеоролик).  
Продукт должен иметь функционал экспорта сохранившихся графических видеоматериалов (видеороликов) во внешние видео форматы AVI, FLV, MPEG с заданной разрешающей способностью.  
27. Продукт должен обеспечивать контроль привилегированных пользователей, которые подключаются к целевым систем по протоколу Telnet.  
Результатом контроля привилегированных пользователей, которые подключаются к целевым системам по протоколу Telnet должен быть записан графический видеоматериал (видеоролик) или текстовый журнал действий (команд пользователя и ответов целевой системы на такие команды).  
28. Продукт должен иметь функционал цифровой подписи записанных сессий специальными ключами / сертификатами от доверенных поставщиков таких ключей / сертификатов с целью обеспечения неизменности данных.  
29. Продукт должен обеспечивать контроль привилегированных пользователей что подключаются к целевым систем по протоколу VNC.  
Результатом контроля привилегированных пользователей, которые подключаются к целевым систем по протоколу VNC должен быть записанный графический видеоматериал (видеоролик).  
Продукт должен иметь функционал экспорта сохранившихся графических видеоматериалов (видеороликов) во внешние видео форматы AVI, FLV, MPEG с заданной разрешающей способностью.  
30. Продукт должен поставляться в виде виртуального устройства (VA - virtual appliance), тип поставки должен быть выполнен в виде единой платформы, которая не требует использования постороннего системного или прикладного программного обеспечения (операционных систем, приложений, систем управления базами данных и т.п.) для его имплементации.  
31. Продукт должен обеспечивать контроль привилегированных пользователей, которые подключаются к целевым системам по протоколу HTTP и HTTPS (с поддержкой стандартов SSLv2 и SSLv3).  
Результатом контроля привилегированных пользователей что подключаются к целевым системам по протоколу HTTP и HTTPS (ресурсы на базе HTML) должен быть записан графический видеоматериал (видеоролик)  
Продукт должен иметь функционал экспорта сохранившихся графических видеоматериалов (видеороликов) во внешние видео форматы AVI, FLV, MPEG с заданной разрешающей способностью.  
32. Продукт должен иметь встроенный функционал оценки эффективности работы с целевыми системами как отдельных привилегированных пользователей, так и групп привилегированных пользователей. Функционал эффективности работы с целевыми системами должен предоставлять статистику активных действий привилегированных пользователей (время активной работы по отношению к общему времени работы с целевой системой) возможностью детализации и экспорта статистики во внешней отчет.  
33. Продукт должен обеспечивать контроль привилегированных пользователей, которые подключаются к целевым системам по протоколу MS SQL (с поддержкой стандартов TDS - Tabular Data Stream).  
Результатом контроля привилегированных пользователей, которые подключаются к целевым системам по протоколу MS SQL должен быть текстовый журнал действий (команд пользователя и ответов целевой системы на такие команды).  
Продукт должен иметь функционал экспорта сохранившихся текстовых журналов во внешние форматы с текстовой структурой.  
Продукт должен обеспечивать контроль привилегированных пользователей, которые подключаются к целевым систем по протоколу MySQL.  
Результатом контроля привилегированных пользователей, которые подключаются к целевым системам по протоколу MySQL должен быть текстовый журнал действий (команд пользователя и ответов целевой системы на такие команды).  
Продукт должен иметь функционал экспорта сохранившихся текстовых журналов во внешние форматы с текстовой структурой.  
34. Использование веб-консоли на базе технологий Flash или Java (JRE) не допускается.  
35. Продукт должен иметь встроенный функционал распознавания текстовой информации в записанных графических сессиях (OCR механизм или аналог), в том числе - кириллические символы, с целью дальнейшего поиска такой информации. Данный функционал должен работать как в ручном режиме, так и в автоматическом (применяться к каждой сохраненной сессии без вмешательства администратора Продукта).