МОНИТОРИНГ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ И УПРАВЛЕНИЕ ИНСАЙДЕРСКИМИ УГРОЗАМИ

EKRAN®

ESKA

Зоны покрытия

До инцидента

После инцидента

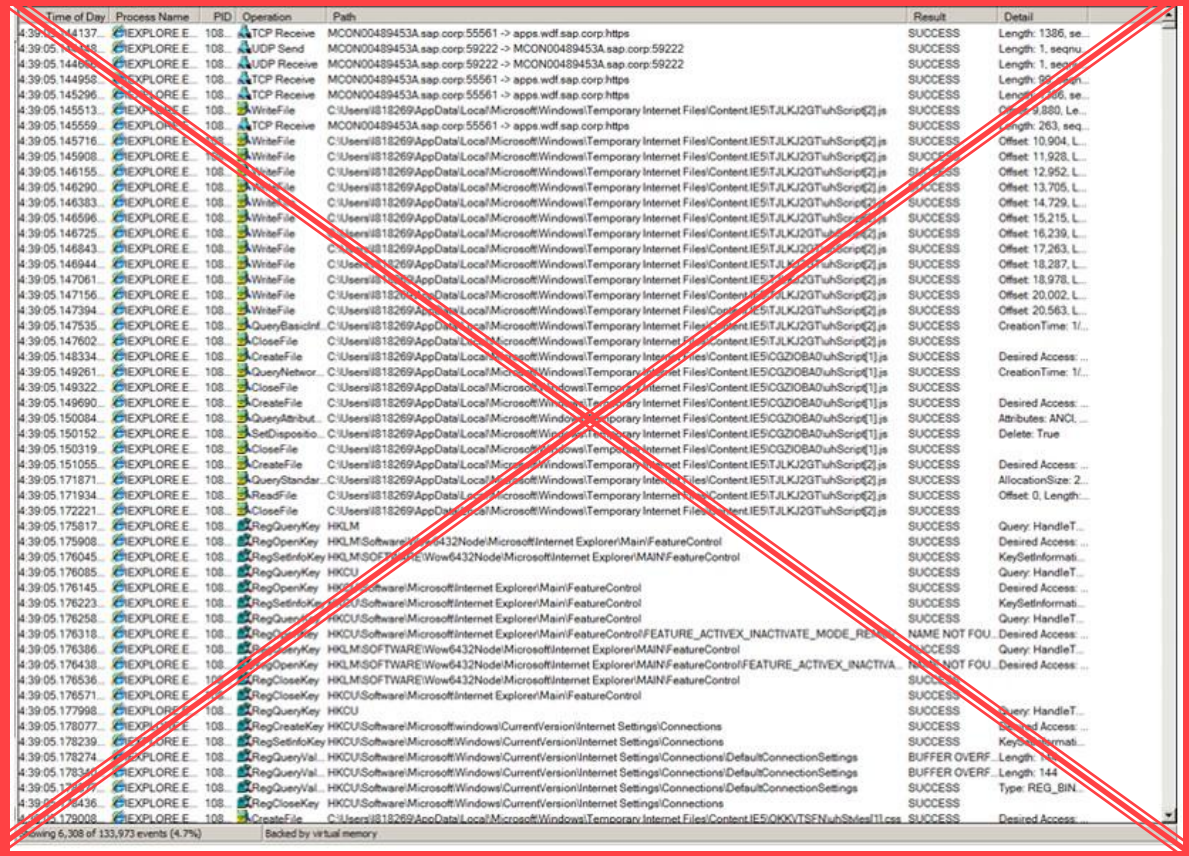
Основные составляющие защиты от инсайдерских угроз

- Управление и контроль доступа субподрядчиков к критически важной IT-инфраструктуре
- Мониторинг и аудит деятельности сотрудников
- Расследование подозрительных действий пользователя
- Соблюдение правил и стандартов безопасности

Клиенты EKRAN SYSTEM

EKRAN®

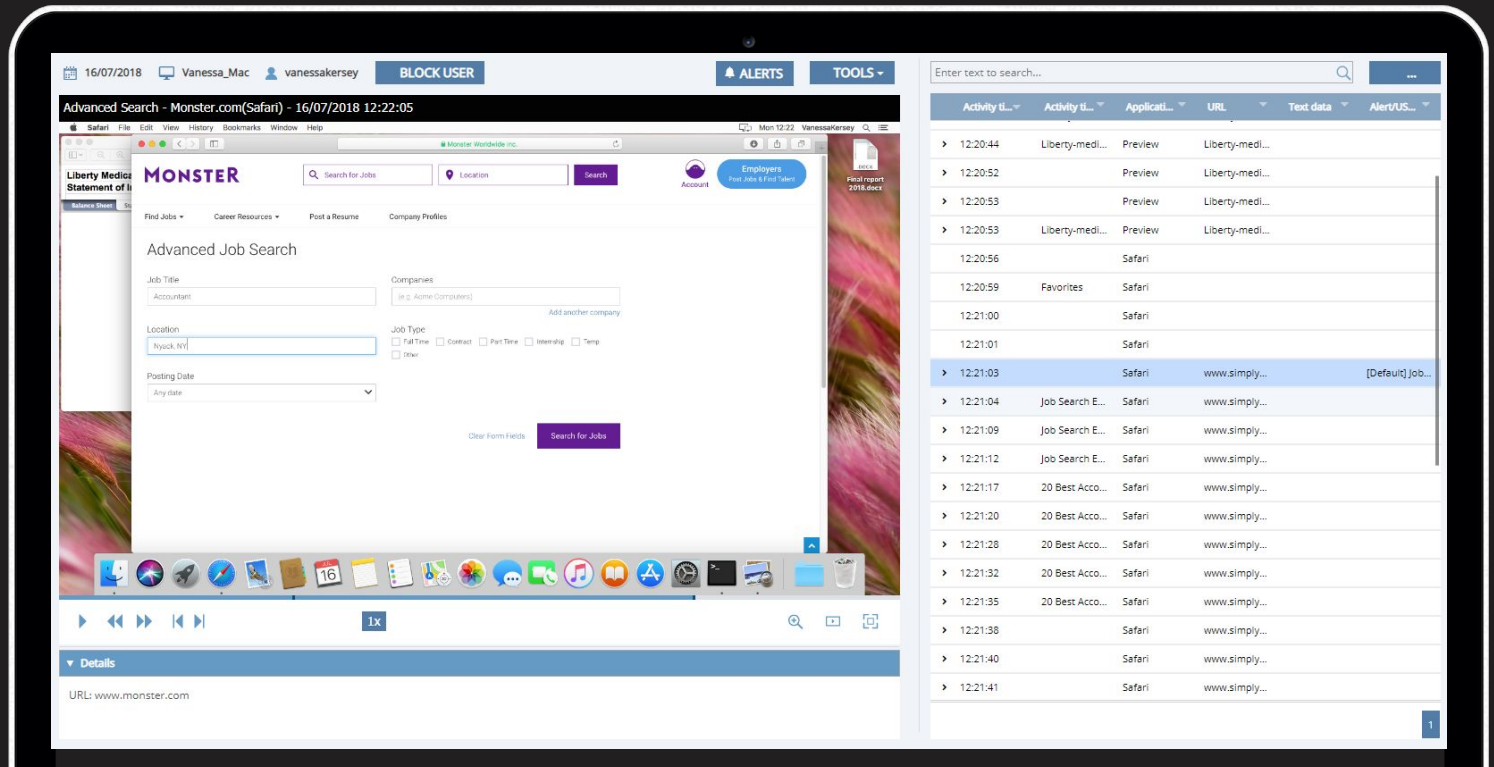
- Все сессии пользователей
  в формате индексированного видео
- Никаких сложностей
  в работе с платформой
- Инструменты защиты
  от инсайдерских угроз



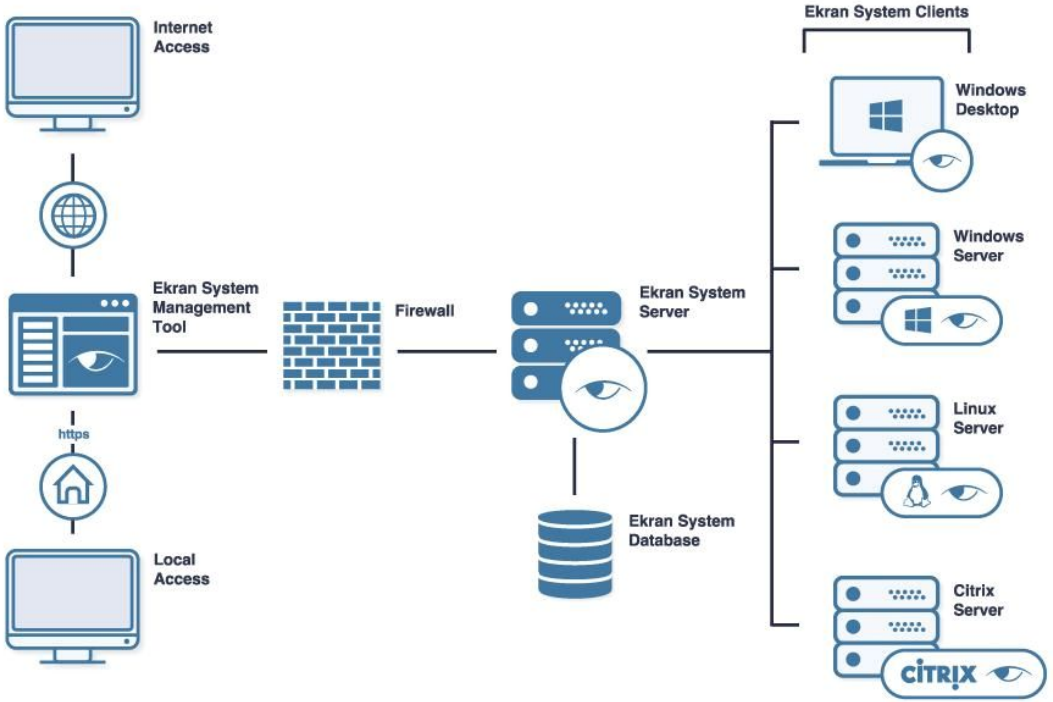
Time of Day	Process Name	PID	Operation	Path	Result	Detail
4:39:05.144137...	IEXPLORE E...	108...	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 1386, se...
4:39:05.144248...	IEXPLORE E...	108...	UDP Send	MCON00489453A.sap.corp:59222 -> MCON00489453A.sap.corp:59222	SUCCESS	Length: 1, seqnu...
4:39:05.144604...	IEXPLORE E...	108...	UDP Receive	MCON00489453A.sap.corp:59222 -> MCON00489453A.sap.corp:59222	SUCCESS	Length: 1, seqnu...
4:39:05.144958...	IEXPLORE E...	108...	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 99, seqn...
4:39:05.145296...	IEXPLORE E...	108...	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 1386, se...
4:39:05.145513...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 9,880, Le...
4:39:05.145559...	IEXPLORE E...	108...	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 263, seq...
4:39:05.145716...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 10,904, L...
4:39:05.145908...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 11,928, L...
4:39:05.146155...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 12,952, L...
4:39:05.146290...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 13,705, L...
4:39:05.146383...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 14,729, L...
4:39:05.146596...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 15,215, L...
4:39:05.146725...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 16,239, L...
4:39:05.146843...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 17,263, L...
4:39:05.146944...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 18,287, L...
4:39:05.147061...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 18,978, L...
4:39:05.147156...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 20,002, L...
4:39:05.147394...	IEXPLORE E...	108...	WriteFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 20,563, L...
4:39:05.147535...	IEXPLORE E...	108...	QueryBasicInf...	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	CreationTime: 1/...
4:39:05.147602...	IEXPLORE E...	108...	CloseFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	
4:39:05.148334...	IEXPLORE E...	108...	CreateFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScript[1].js	SUCCESS	Desired Access: ...
4:39:05.149261...	IEXPLORE E...	108...	QueryNetwor...	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScript[1].js	SUCCESS	CreationTime: 1/...
4:39:05.149322...	IEXPLORE E...	108...	CloseFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScript[1].js	SUCCESS	
4:39:05.149690...	IEXPLORE E...	108...	CreateFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScript[1].js	SUCCESS	Desired Access: ...
4:39:05.150084...	IEXPLORE E...	108...	QueryAttribut...	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScript[1].js	SUCCESS	Attributes: ANCI, ...
4:39:05.150152...	IEXPLORE E...	108...	SetDispositio...	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScript[1].js	SUCCESS	Delete: True
4:39:05.150319...	IEXPLORE E...	108...	CloseFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScript[1].js	SUCCESS	
4:39:05.151055...	IEXPLORE E...	108...	CreateFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Desired Access: ...
4:39:05.171871...	IEXPLORE E...	108...	QueryStandar...	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	AllocationSize: 2...
4:39:05.171934...	IEXPLORE E...	108...	ReadFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	Offset: 0, Length:...
4:39:05.172221...	IEXPLORE E...	108...	CloseFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScript[2].js	SUCCESS	
4:39:05.175817...	IEXPLORE E...	108...	RegQueryKey	HKLM	SUCCESS	Query: HandleT...
4:39:05.175908...	IEXPLORE E...	108...	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	Desired Access: ...
4:39:05.176045...	IEXPLORE E...	108...	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl	SUCCESS	KeySetInformati...
4:39:05.176085...	IEXPLORE E...	108...	RegQueryKey	HKCU	SUCCESS	Query: HandleT...
4:39:05.176145...	IEXPLORE E...	108...	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	Desired Access: ...
4:39:05.176223...	IEXPLORE E...	108...	RegSetInfoKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	KeySetInformati...
4:39:05.176258...	IEXPLORE E...	108...	RegQueryKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	Query: HandleT...
4:39:05.176318...	IEXPLORE E...	108...	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ACTIVEX_INACTIVATE_MODE_REM...	NAME NOT FOU...	Desired Access: ...
4:39:05.176386...	IEXPLORE E...	108...	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl	SUCCESS	Query: HandleT...
4:39:05.176438...	IEXPLORE E...	108...	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ACTIVEX_INACTIVA...	NAME NOT FOU...	Desired Access: ...
4:39:05.176536...	IEXPLORE E...	108...	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl	SUCCESS	
4:39:05.176571...	IEXPLORE E...	108...	RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	
4:39:05.177998...	IEXPLORE E...	108...	RegQueryKey	HKCU	SUCCESS	Query: HandleT...
4:39:05.178077...	IEXPLORE E...	108...	RegCreateKey	HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections	SUCCESS	Desired Access: ...
4:39:05.178239...	IEXPLORE E...	108...	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS	KeySetInformati...
4:39:05.178274...	IEXPLORE E...	108...	RegQueryVal...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings	BUFFER OVERF...	Length: 144
4:39:05.178340...	IEXPLORE E...	108...	RegQueryVal...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings	BUFFER OVERF...	Length: 144
4:39:05.178479...	IEXPLORE E...	108...	RegQueryVal...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings	SUCCESS	Type: REG_BIN...
4:39:05.178436...	IEXPLORE E...	108...	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS	
4:39:05.179008...	IEXPLORE E...	108...	CreateFile	C:\Users\I818269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\OKKVTSFN\uhStyles[1].css	SUCCESS	Desired Access: ...

Showing 6,308 of 133,973 events (4.7%) | Backed by virtual memory

EKRAN®


16/07/2018
Vanessa_Mac
vanessakersey
BLOCK USER
ALERTS
TOOLS
Advanced Search - Monster.com(Safari) - 16/07/2018 12:22:05
MONSTER
Search for Jobs
Location
Search
Advanced Job Search
Job Title
Companies
Location
Job Type
Posting Date
Search for Jobs
Details
URL: www.monster.com
Enter text to search...
Activity ti...
Activity ti...
Applicati...
URL
Text data
Alert/US...
12:20:44 Liberty-medi... Preview Liberty-medi...
12:20:52 Preview Liberty-medi...
12:20:53 Preview Liberty-medi...
12:20:53 Liberty-medi... Preview Liberty-medi...
12:20:56 Safari
12:20:59 Favorites Safari
12:21:00 Safari
12:21:01 Safari
12:21:03 Safari www.simply... [Default] Job...
12:21:04 Job Search E... Safari www.simply...
12:21:09 Job Search E... Safari www.simply...
12:21:12 Job Search E... Safari www.simply...
12:21:17 20 Best Acco... Safari www.simply...
12:21:20 20 Best Acco... Safari www.simply...
12:21:28 20 Best Acco... Safari www.simply...
12:21:32 20 Best Acco... Safari www.simply...
12:21:35 20 Best Acco... Safari www.simply...
12:21:38 Safari www.simply...
12:21:40 Safari www.simply...
12:21:41 Safari www.simply...

Архитектура EKRAN SYSTEM



Основной функционал EKRAN SYSTEM

Управление идентификацией

- Двухфакторная аутентификация (учетные данные + мобильное устройство)
- Вторичная аутентификация для общих учетных записей

Управление доступом

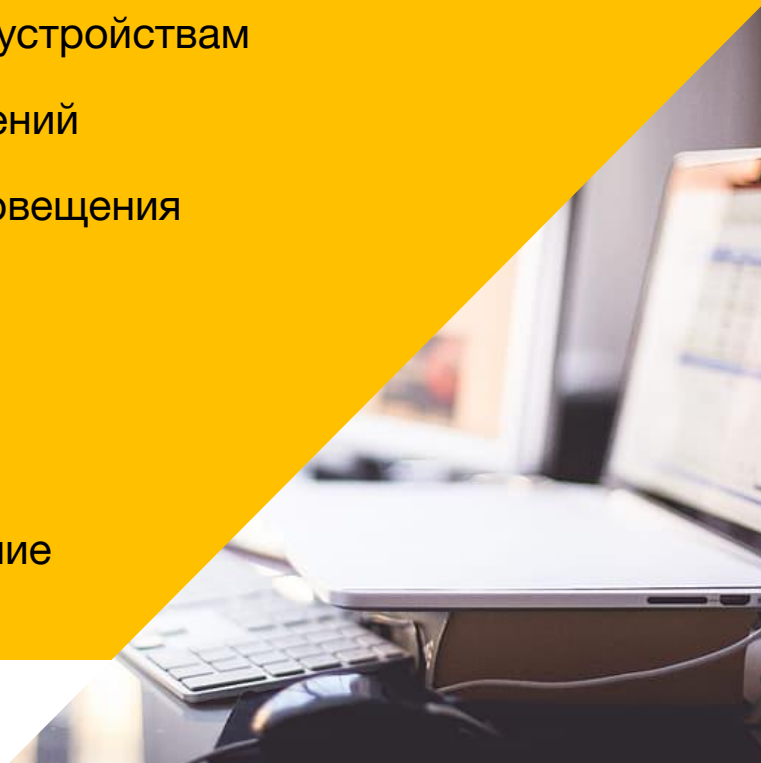
- Управление паролями (доступ по RDP и SSH)
- Одноразовые пароли
- Ручное подтверждение логина сотрудником службы безопасности
- Интеграция с тикет-системой
- Управление USB устройствами

Контроль и аудит активности

- Запись сеанса в формате индексированного видео
- Расширенный поиск и отчетность
- Стандартные и настраиваемые оповещения
- Ручное и автоматическое реагирование на инциденты

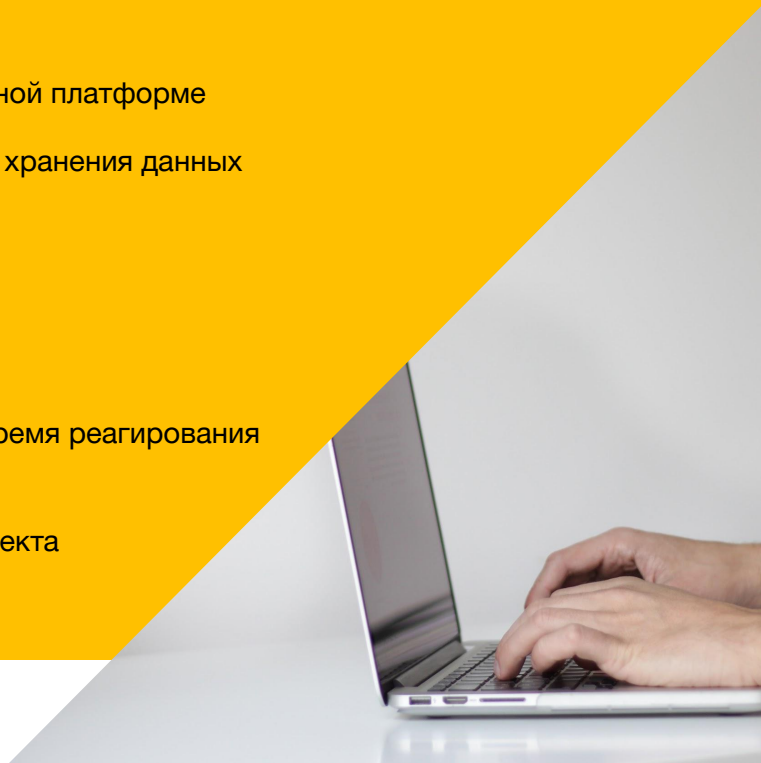
Инструменты

- Управление доступом к защищенным конечным устройствам
- Управление паролями для дальнейших подключений
- Проактивная защита и комплексная система оповещения
- Интеграция с SIEM системами
- Интеграция с тикет-системами
- Внутренний аудит
- Высокая доступность и аварийное восстановление



Преимущества

- Готов к работе в вашей среде в течение 10 минут
- Основные средства управления рисками на уровне пользователя в одной платформе
- Легкий программный агент и высоко оптимизированные форматы для хранения данных
- Полная поддержка десктопных и серверных ОС
- Отлично подходит для больших предприятий
- Низкая общая стоимость
- Визуально структурированные доказательства, которые сокращают время реагирования на инцидент
- Обнаружение взломанного аккаунт с помощью искусственного интеллекта



Влияние на конечное устройство

- Загрузка ЦП: **< 0.45%**
- Использование памяти: **21.2 MB**
- Требования к пропускной способности: **128 Kbit/S**
- Всего лишь **4 ТВ ПАМЯТИ** для записи **1’000 пользователей** в течении одного месяца