KONTROLA PRIVILEGOVANÝCH PŘÍSTUPŮ NAHRÁVÁNÍM RELACÍ

DATA SYS

EKRAN

Privilegovaní uživatelé, **zaměstnanci i pracovníci třetích stran,** hrají klíčovou roli při provozování jakéhokoli informačního systému. Účty s eskalovanými oprávněními nebo správci systému a databází mívají neomezený přístup nejen ke konfiguraci systému, ale i k datům. Mohou spravovat účty jiných uživatelů a jejich oprávnění.

NÁSTROJ PRO ZAZNAMENÁVÁNÍ UŽIVATELSKÝCH RELACÍ

NÍZKONÁKLADOVÉ A VELMI PŘÍMOČARÉ ŘEŠENÍ

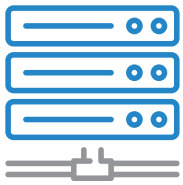
NEVYŽADUJE ŽÁDNOU ZMĚNU V POSTUPECH SPRÁVY SYSTÉMŮ

Srozumitelná kontrola činností privilegovaných uživatelů je jednou z nejdůležitějších součástí firemních bezpečnostních opatření a auditování privilegovaného přístupu uživatelů je vyžadováno mnoha různými průmyslovými předpisy.

Nástroj **Ekran System** naplňuje tyto potřeby tím, že v informačním systému ustavuje proces trvalého průběžného monitorování činností administrátorů. Řešení může být snadno nasazeno na kritických serverech a od té chvíle **poskytne detailní videozáznam** všech nebo jen vyjmenovaných uživatelských relací.

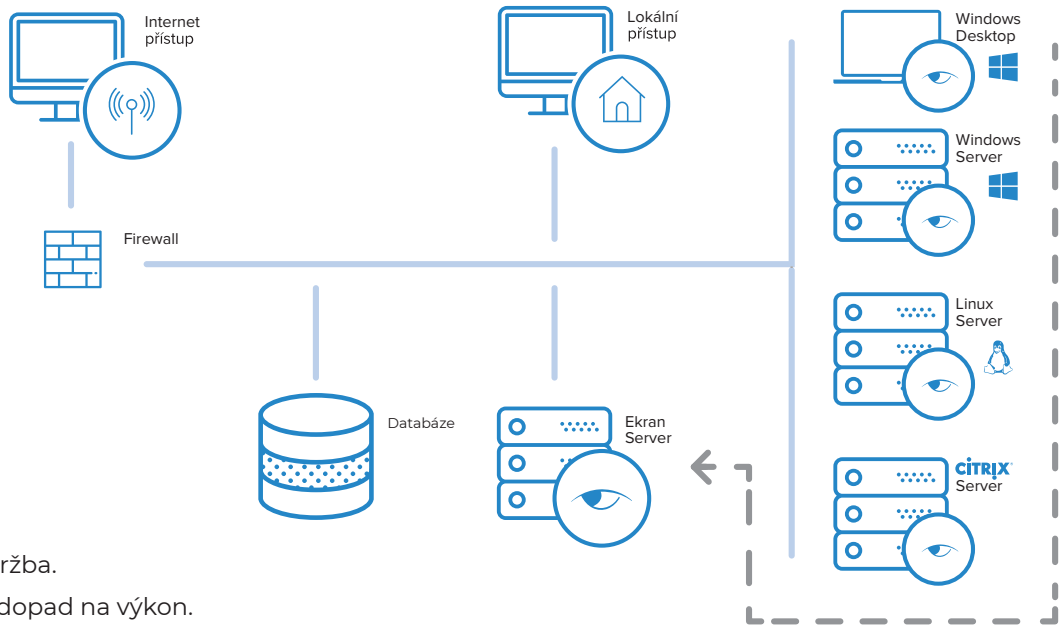
Video formát je indexován a díky metadatům o aktivním okně, spuštěném systémovém procesu či o administrátorem provedeném příkazu supervizor rychle vykoná rámcovou analýzu i několikahodinové relace. Nástroj podporuje **sledování aktuálního průběhu živé relace** a notifikace podezřelých činností. Pokročilý režim **ochrany agenta** zabrání neoprávněným pokusům o jeho zastavení nebo odinstalaci. Nástroj může též vynutit **druhou úroveň ověření uživatele** při přihlášení sdílenými systémovými účty, jako jsou např. „admin“ nebo „root”.

PODPOROVANÉ PLATFORMY:



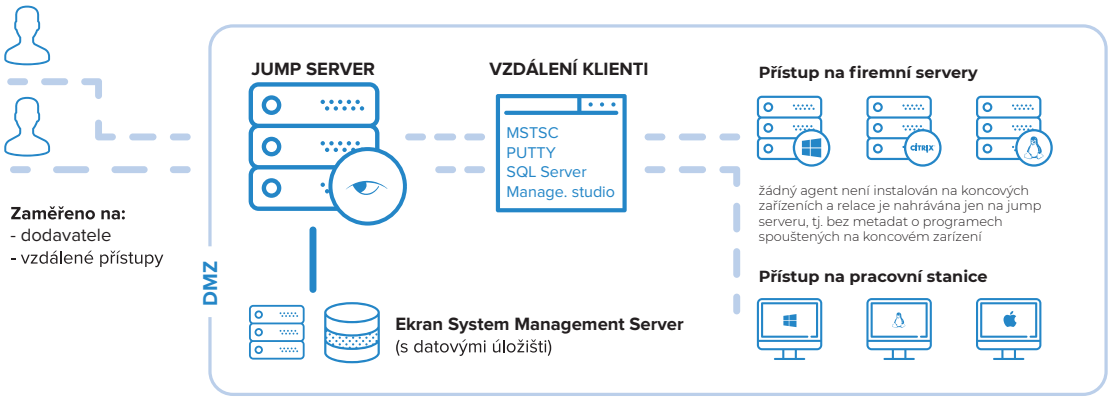
- **Microsoft Windows** s nahráváním místních, vzdálených i terminálových relací. Nástroj umožňuje též monitorovat aktivitu uživatelů v aplikacích publikovaných v **Citrix XenApp** a virtuální desktopy **XenDesktop.**
- **Linux and Unix** servery, na kterých jsou zaznamenávány Telnet a SSH relace, včetně všech uživatelem spuštěných příkazů.

OBVYKLÝ ZPŮSOB NASAZENÍ



- Snadná údržba.
- Minimální dopad na výkon.
- Shromažďuje podrobná metadata o aktivitách uživatele.
- Nevyžaduje žádné změny postupu správy technické infrastruktury.

NAHRÁVÁNÍ JEN NA PŘÍSTUPOVÉM SERVERU



Chráněný okruh

- K dispozici je i "multi-tenant" instalace.
- Jedná se o bezagentský režim, agent je instalován jen na přístupovém, tzv. jump serveru.
- Centrální Ekran server může být provozován v clusteru, tj. v režimu vysoké dostupnosti.