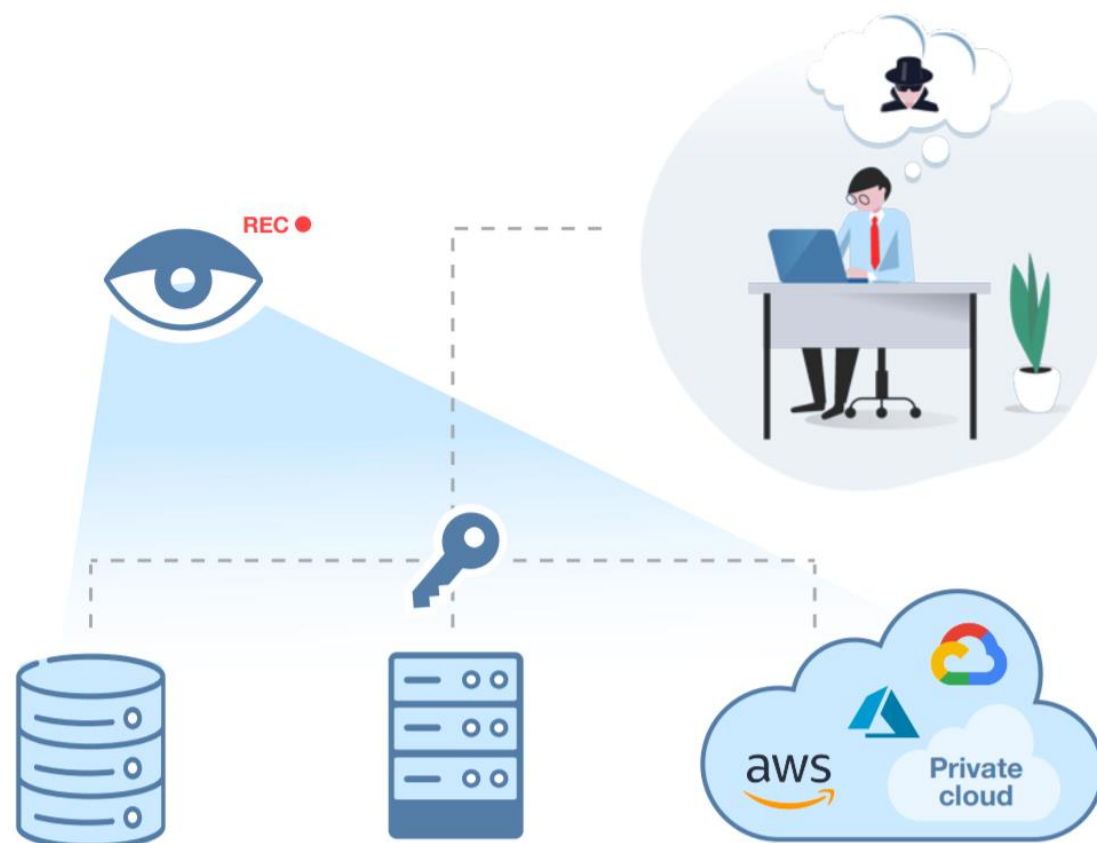




Ekran – Důvěřuj, ale prověřuj. Jak mít IT aktivity pod kontrolou

Agenda

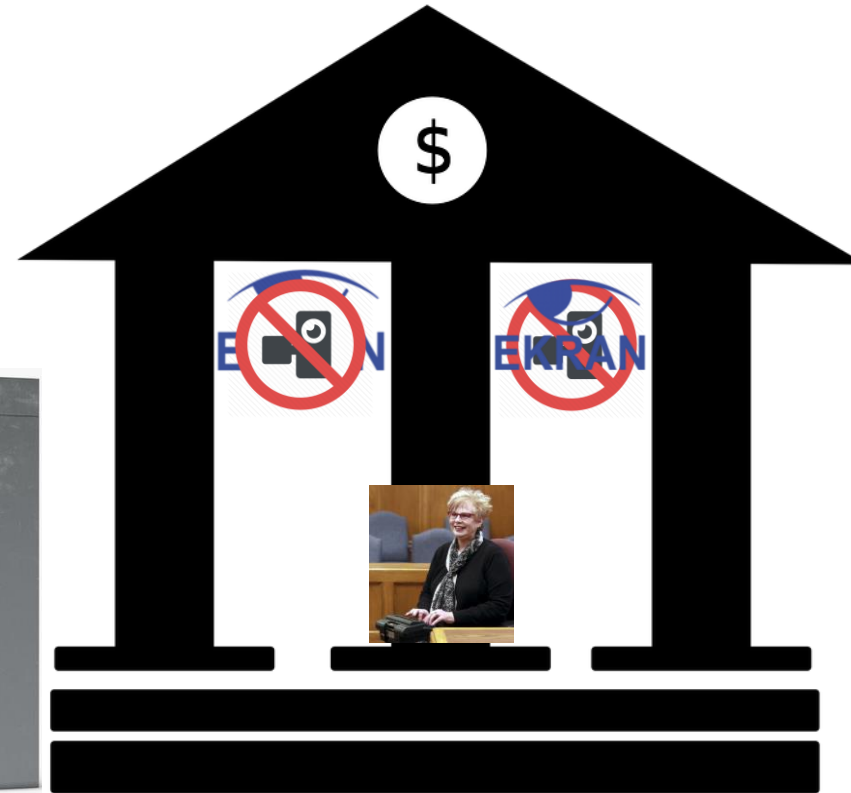
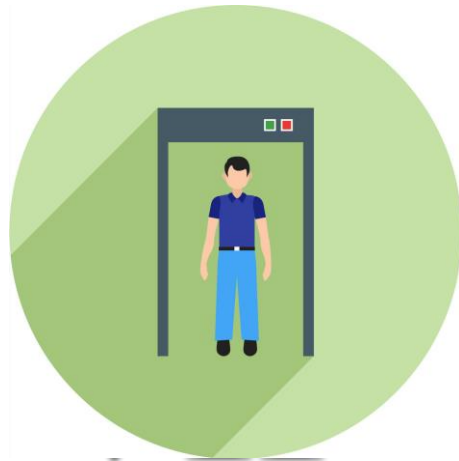
1. Komu technologie určena?
2. Architektura
3. Hlavní přínosy
4. Živá ukázka



**Implement Ekran System
to protect your environment from the inside out**



Jak si stojí Vaše servery?



Co je EKTRAN?



Co je EKTRAN?

Identity Management

- Dvoufaktorová autentizace (credentials + mobile device)
- Sekundární autentizace pro sdílené účty

Access Management

- Jednorázová hesla
- Password Management (RDP a SSH)
- Manuální schvalování přístupů
- Integrace na ticketovací systém
- USB management

Activity Control and Audit

- Session recording včetně indexace
- Pokročilé vyhledávání a reporting
- Alerting
- Manuální a automatické reakce na incidenty

Komu je EKTRAN určen?

1. Využíváte outsourcing?
2. Máte na serverech citlivá data?
3. Víte co se děje na Vašich serverech?
4. Zkoušeli jste někdy z logů vyčíst co se na serveru stalo?
5. Vyžaduje zákon nebo Vaše interní směrnice monitoring aktivit na serverech?
6. Využívají Vaši administrátoři sdílené účty?
7. Přistupují administrátoři napřímo k systémům?

Time of Day	Process Name	PID	Operation	Path	Result	Detail
4:39:05.144137	EXPLORE.E	108	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 1386, se...
4:39:05.144148	EXPLORE.E	108	UDP Send	MCON00489453A.sap.corp:59222 -> MCON00489453A.sap.corp:59222	SUCCESS	Length: 1, sequ...
4:39:05.144666	EXPLORE.E	108	UDP Receive	MCON00489453A.sap.corp:59222 -> MCON00489453A.sap.corp:59222	SUCCESS	Length: 1, sequ...
4:39:05.144958	EXPLORE.E	108	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 99, se...
4:39:05.145296	EXPLORE.E	108	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 1386, se...
4:39:05.145513	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 9,880, L...
4:39:05.145559	EXPLORE.E	108	TCP Receive	MCON00489453A.sap.corp:55561 -> apps.wdf.sap.corp:https	SUCCESS	Length: 263, seq...
4:39:05.145716	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 10,904, L...
4:39:05.145908	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 11,928, L...
4:39:05.146155	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 12,952, L...
4:39:05.146290	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 13,705, L...
4:39:05.146383	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 14,729, L...
4:39:05.146596	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 15,215, L...
4:39:05.146725	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 16,239, L...
4:39:05.146843	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 17,263, L...
4:39:05.146944	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 18,287, L...
4:39:05.147061	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 18,978, L...
4:39:05.147156	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 20,002, L...
4:39:05.147394	EXPLORE.E	108	WriteFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset: 20,563, L...
4:39:05.147535	EXPLORE.E	108	QueryBasicInf	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	CreationTime: 1/...
4:39:05.147602	EXPLORE.E	108	CloseFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	
4:39:05.148334	EXPLORE.E	108	CreateFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScrip(1).js	SUCCESS	Desired Access: ...
4:39:05.149261	EXPLORE.E	108	QueryNetwor...	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScrip(1).js	SUCCESS	CreationTime: 1/...
4:39:05.149322	EXPLORE.E	108	CloseFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScrip(1).js	SUCCESS	
4:39:05.149690	EXPLORE.E	108	CreateFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScrip(1).js	SUCCESS	Desired Access: ...
4:39:05.150084	EXPLORE.E	108	QueryAttribu...	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScrip(1).js	SUCCESS	Attributes: ANCI...
4:39:05.150152	EXPLORE.E	108	SetDisposib...	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScrip(1).js	SUCCESS	Delete: True
4:39:05.150319	EXPLORE.E	108	CloseFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\CGZIOBA0\uhScrip(1).js	SUCCESS	
4:39:05.151055	EXPLORE.E	108	CreateFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Desired Access: ...
4:39:05.171871	EXPLORE.E	108	QueryStandar...	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	AllocationSize: 2...
4:39:05.171934	EXPLORE.E	108	ReadFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	Offset 0, Length...
4:39:05.172221	EXPLORE.E	108	CloseFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\TJLKJ2GT\uhScrip(2).js	SUCCESS	
4:39:05.175817	EXPLORE.E	108	RegQueryKey	HKLM	SUCCESS	Query: HandleT...
4:39:05.175908	EXPLORE.E	108	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	Desired Access: ...
4:39:05.176045	EXPLORE.E	108	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl	SUCCESS	KeySetInformati...
4:39:05.176085	EXPLORE.E	108	RegQueryKey	HKCU	SUCCESS	Query: HandleT...
4:39:05.176145	EXPLORE.E	108	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	Desired Access: ...
4:39:05.176223	EXPLORE.E	108	RegSetInfoKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	KeySetInformati...
4:39:05.176258	EXPLORE.E	108	RegQueryKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	Query: HandleT...
4:39:05.176318	EXPLORE.E	108	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ACTIVEX_INACTIVATE_MODE_REMOVE	NAME NOT FOU...	Desired Access: ...
4:39:05.176386	EXPLORE.E	108	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl	SUCCESS	Query: HandleT...
4:39:05.176438	EXPLORE.E	108	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ACTIVEX_INACTIVA...	NAME NOT FOU...	Desired Access: ...
4:39:05.176536	EXPLORE.E	108	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl	SUCCESS	
4:39:05.176571	EXPLORE.E	108	RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl	SUCCESS	
4:39:05.177998	EXPLORE.E	108	RegQueryKey	HKCU	SUCCESS	Query: HandleT...
4:39:05.178077	EXPLORE.E	108	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS	Desired Access: ...
4:39:05.178239	EXPLORE.E	108	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS	KeySetInformati...
4:39:05.178274	EXPLORE.E	108	RegQueryVal...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings	BUFFER OVERF..._Length: 144	
4:39:05.178340	EXPLORE.E	108	RegQueryVal...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings	BUFFER OVERF..._Length: 144	
4:39:05.178377	EXPLORE.E	108	RegQueryVal...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings	SUCCESS	Type: REG_BIN...
4:39:05.178436	EXPLORE.E	108	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS	
4:39:05.179008	EXPLORE.E	108	CreateFile	C:\Users\IS18269\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QKQVTSFN\uhSmles11.css	SUCCESS	Desired Access: ...

Showing 6,308 of 133,973 events (4.7%)

Backed by virtual memory

16/07/2018 Vanessa_Mac vanessakersey **BLOCK USER** **ALERTS** **TOOLS**

Advanced Search - Monster.com(Safari) - 16/07/2018 12:22:05

Safari File Edit View History Bookmarks Window Help

Monster Worldwide Inc.

MONSTER Search for Jobs Location Search Account Employers Post Jobs & Find Talent

Find Jobs Career Resources Post a Resume Company Profiles

Advanced Job Search

Job Title: Accountant Companies: (e.g. Acme Computers) Add another company

Location: Nysck, NY Job Type: ☐ Full Time ☐ Contract ☐ Part Time ☐ Internship ☐ Temp ☐ Other

Posting Date: Any date

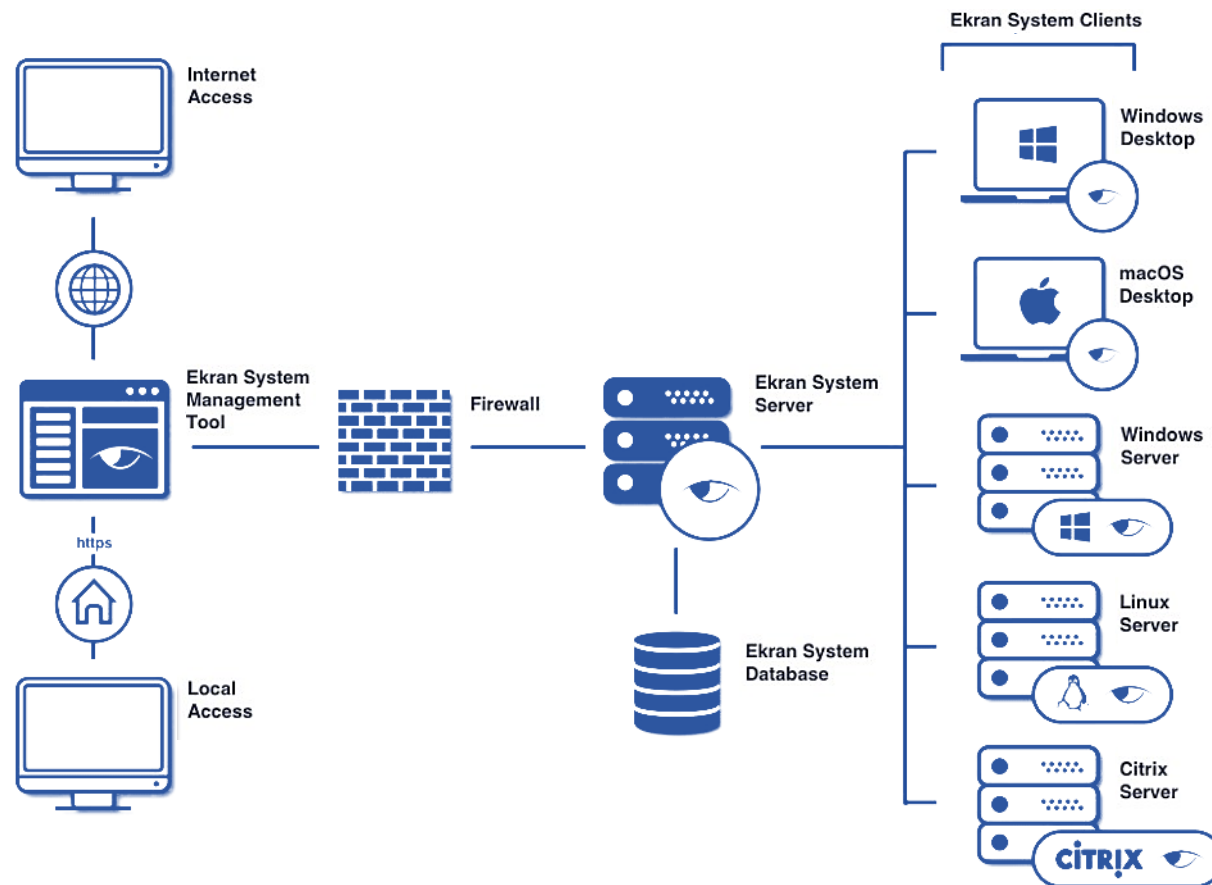
Clear Form Fields Search for Jobs

16/07/2018 12:22:05

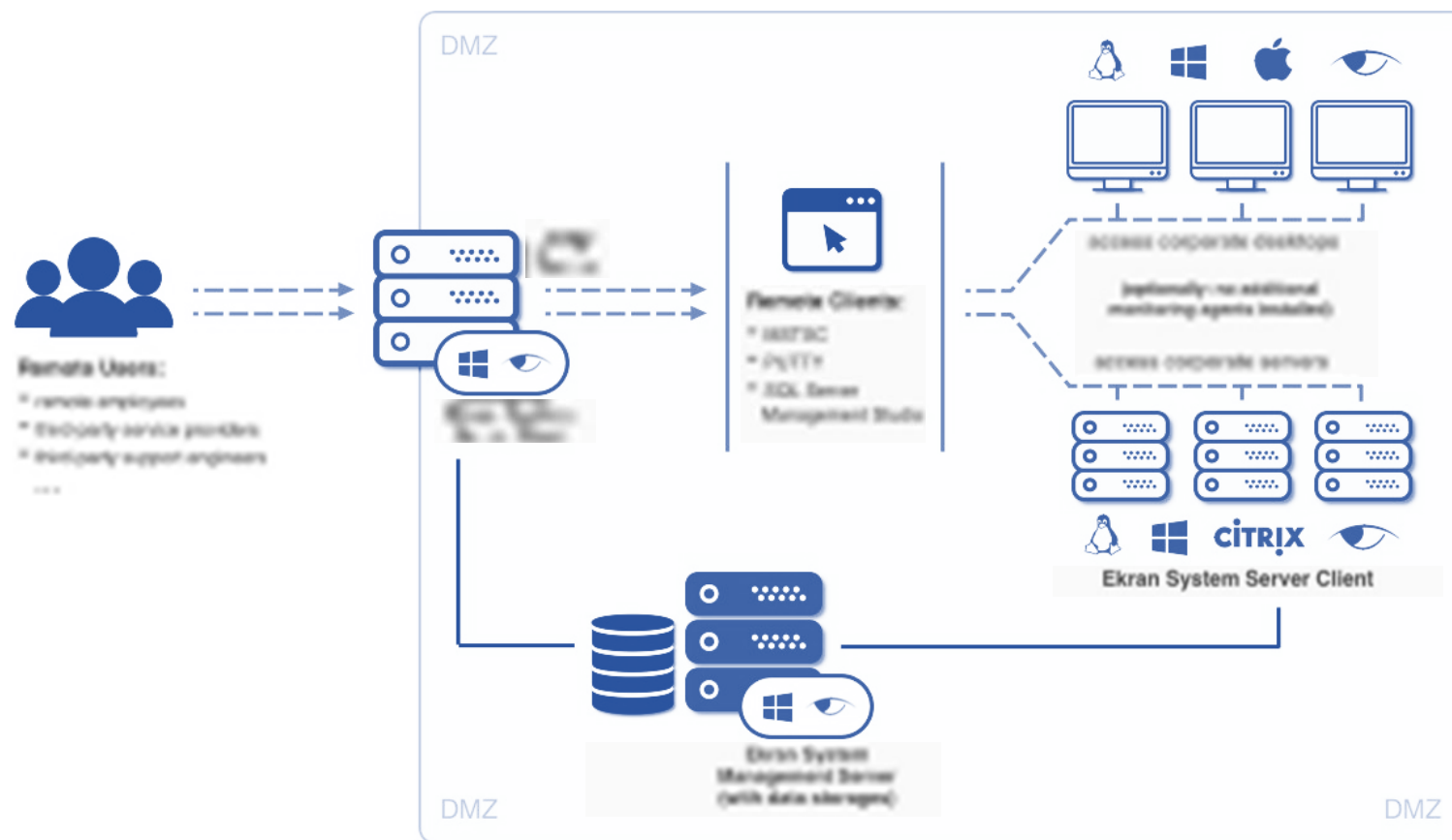
URL: www.monster.com

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...		

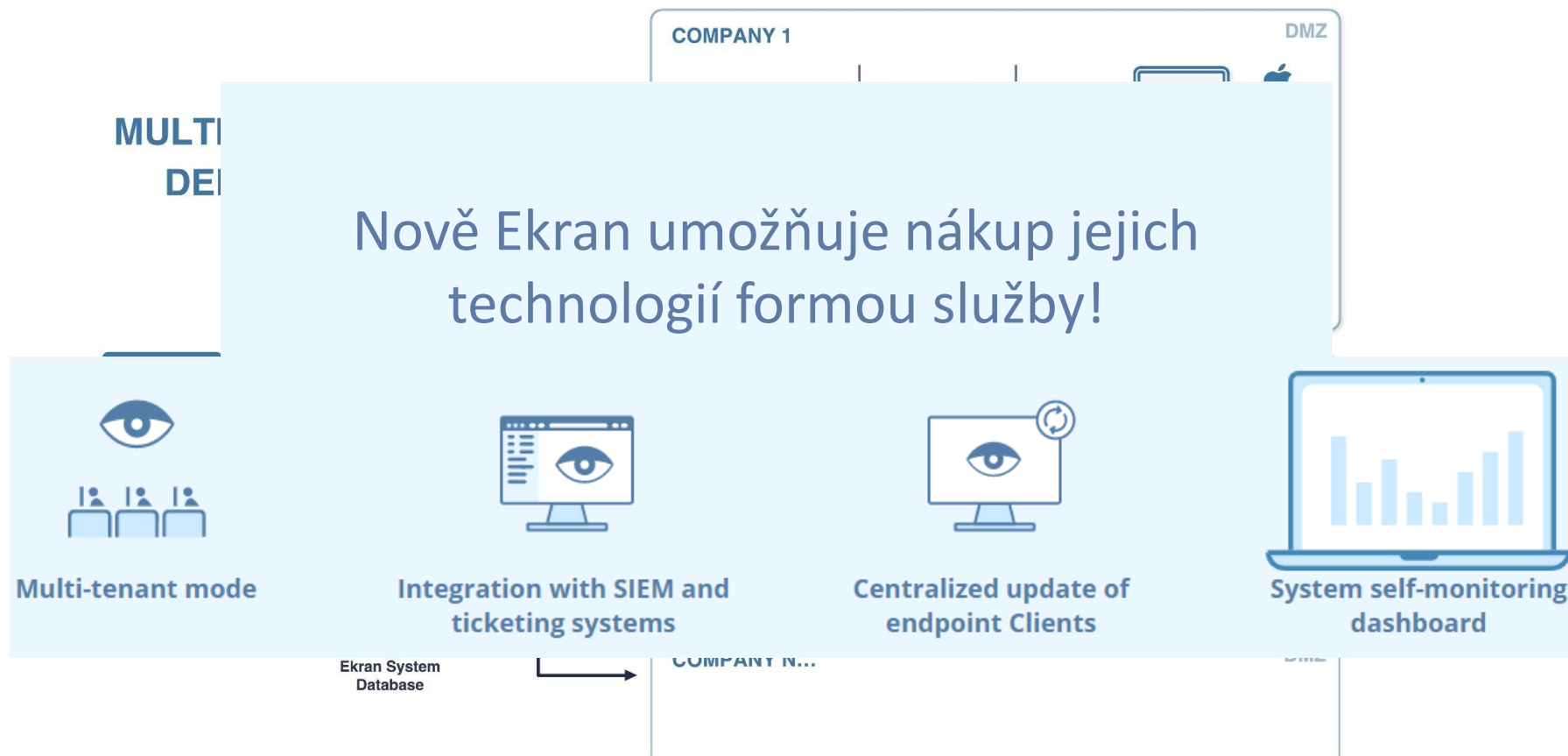
Architektura EKTRAN



Architektura EKTRAN



Architektura EKTRAN - multitenant



Hlavní přínosy

1

Záznam aktivity adminů

2

Video a přesná metadata

3

PAM + Password Management

4

Pokročilý Reporting a alerting

5

Sdílené účty již nejsou problém

6

Integrace na ticket system

7

Integrace na SIEM

8

USB management

9

Soulad se standardy a předpisy

10

System se sám zaplatí

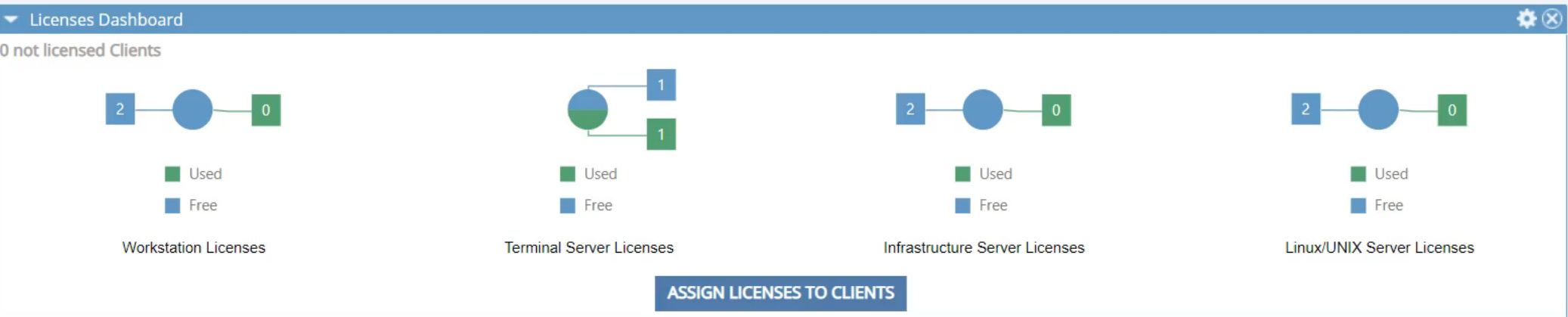
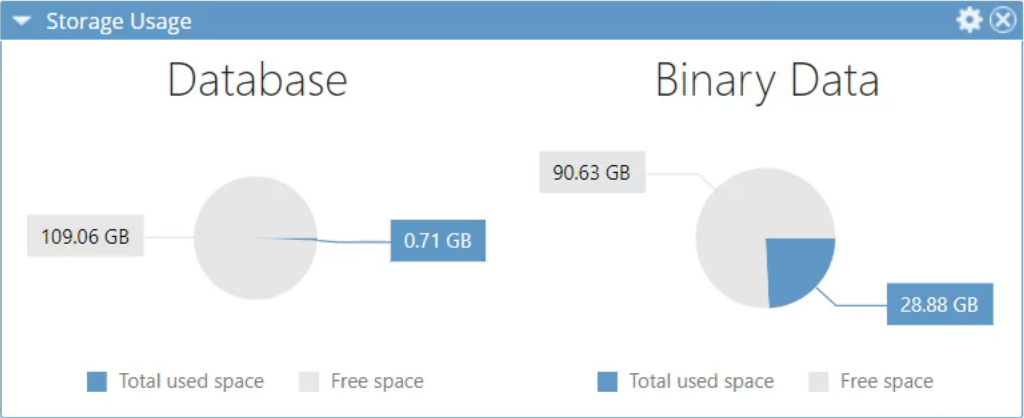
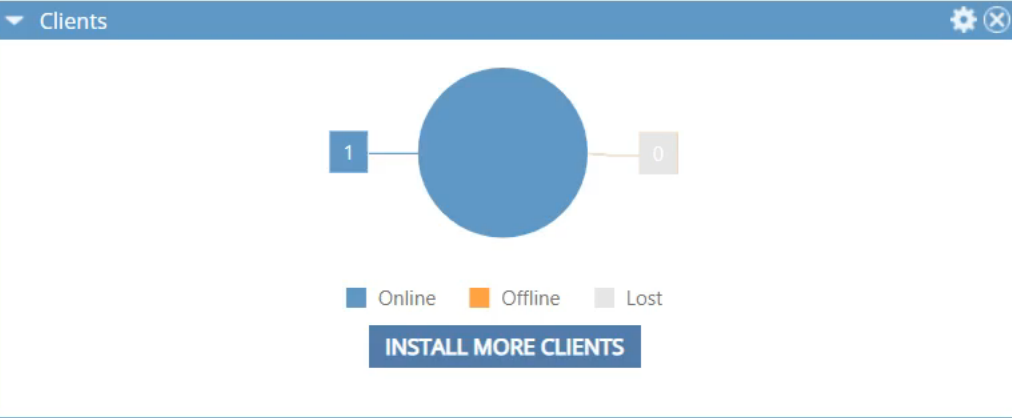
- Home
- Monitoring Results
- Forensic Export History
- Reports
- Interactive Monitoring
- Health Monitoring
- Password Management
- Client Management
- User Management
- Access Management
- Alert Management
- User Behavior Analysis
- Kernel-Level USB monitoring
- Serial Key Management
- Configuration
- Management Tool Log

EKRAN SYSTEM MANAGEMENT TOOL

Enterprise Edition v. 6.25.186.0

Update&support period end date:05/10/2023

ADD DASHBOARD





Děkuji za pozornost

martin.votava@comguard.cz
+420 734 442 468