COMGUARD

cyber security masters

EKRAN

Jak dostat pod kontrolu aktivity nejen administrátorů?

Kamil Kosour | Senior Account Manager

18.09.2023

Co je EKRAN?


ACCESS MANAGEMENT
ACTIVITY MONITORING
Ekran
INCIDENT DETECTION AND INVESTIGATION
INCIDENT RESPONSE

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

Mentioned in NIST Special Publication

Included in **Privileged Account Management for the Financial Services Sector**, Special Publication 1800-18 by NIST (National Institute of Standards and Technology, U.S. Department of Commerce).

Microsoft Azure
Value-add Partner

Listed in approved **Partner Providers and Independent Software Vendors for Windows Virtual Desktop.**

Gartner

Included in **Market Guide for Insider Risk Management Solutions**, by Gartner

Comply with ISO 9001 and ISO 27001 for its **Quality Management System** and **Information Security Management System**

Zákazníci EKRAN

Komu je EKRAN určen?

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

Komu je EKRAN určen?

Financial services and insurance

Healthcare

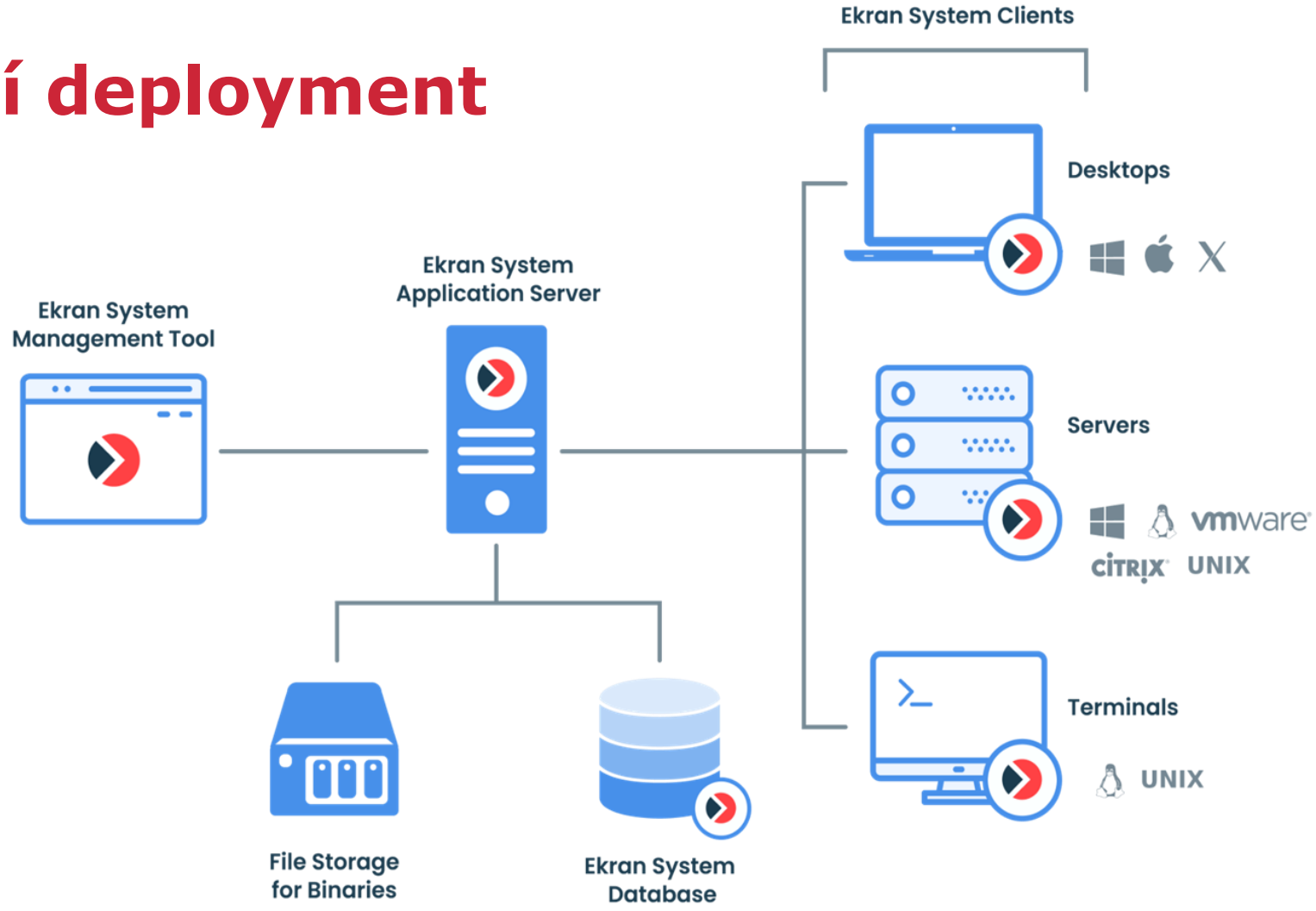
Energy

Public administration

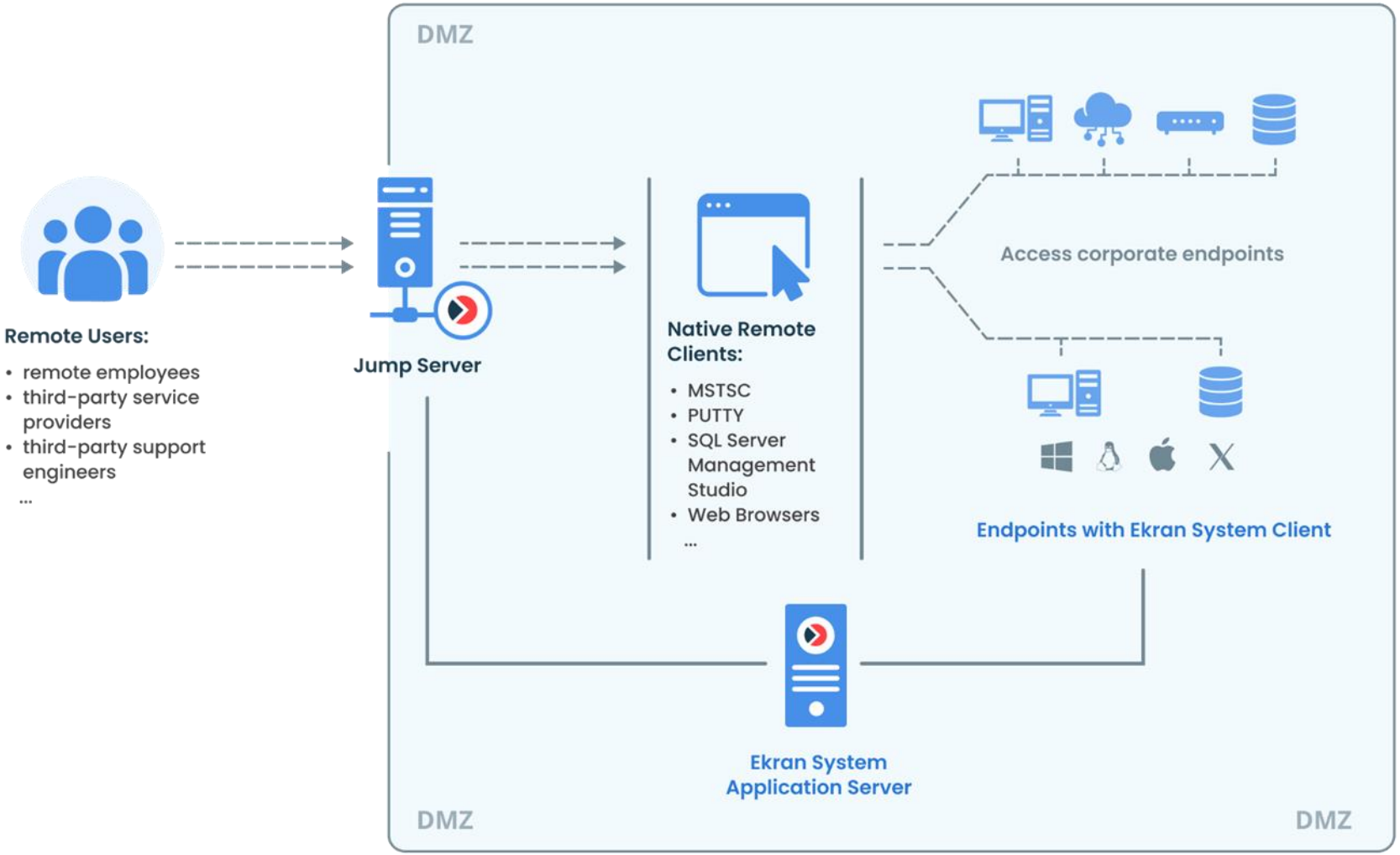
Government and military

Telecommunications

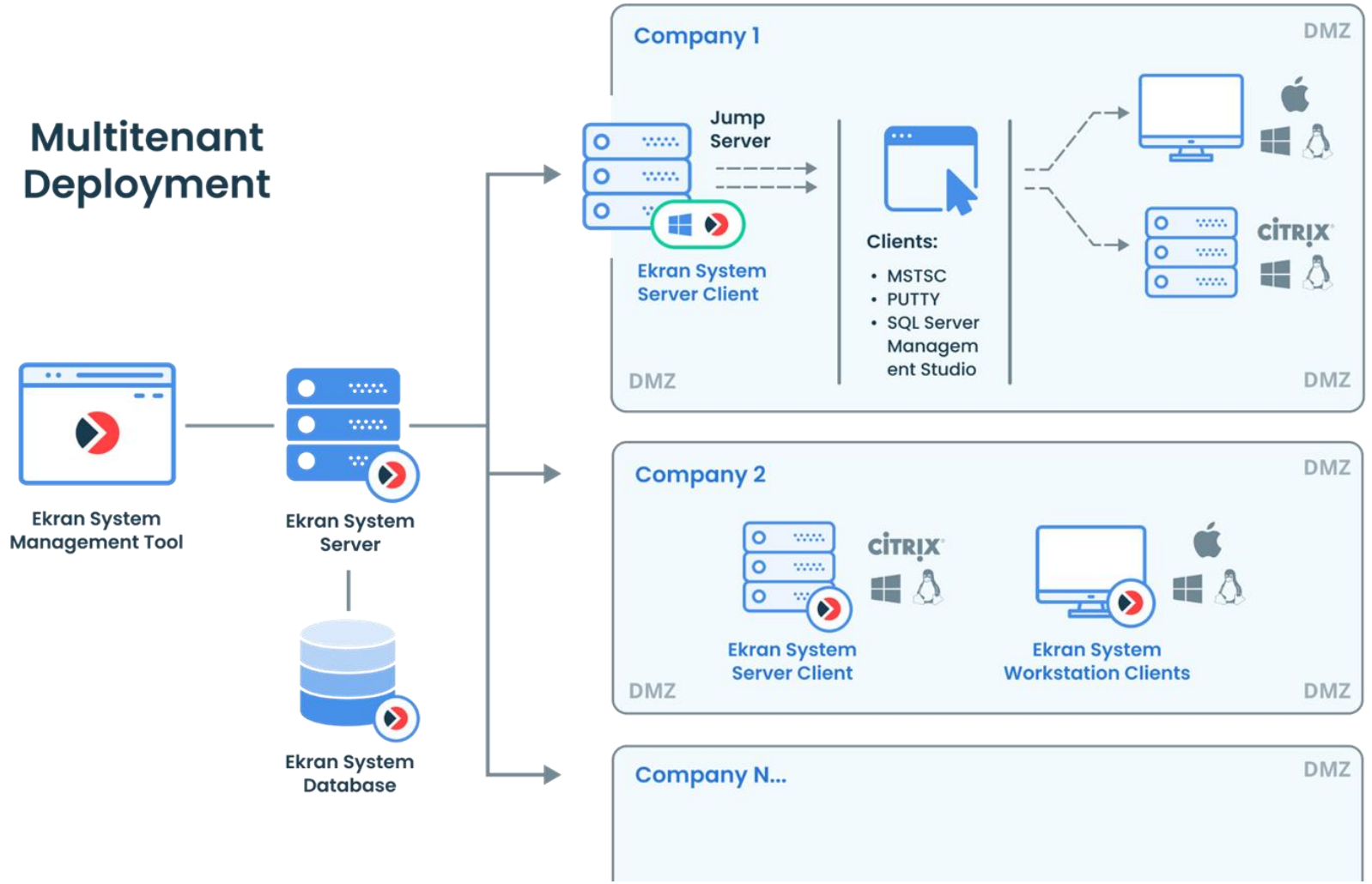
Ekran
– základní deployment



Ekran – Jump Server deployment



Ekran – podpora multitenance



COMGUARD

EKRAN - management

	Standard Edition	Enterprise Edition
Management Tool Licensing	Free, no license needed	License needed*
Session recording and viewing functionality	50 concurrent sessions	Full
Incident response functionality	Full	Full
Alerting functionality	Full	Full
Reporting functionality	Full	Full
Access control	• Secondary authentication for shared logins • 2-factor authentication	• Secondary authentication for shared logins • 2-factor authentication • USB storage access approval • One-time passwords
Password Tool**	No	Yes
Integration with SIEM systems	No	Advanced (ArcSight, Splunk, IBM QRadar)
Integration with ticketing systems	No	Advanced (SysAid, ServiceNow)
Deployment	Standard	▪ Standard ▪ High availability ▪ Multi-tenant
Database Management	Managed database cleanup	Managed database archiving and cleanup
System Health Monitoring	No	Yes
Audio Recording	No	Yes
UEBA	No	Yes

EKRAN Licence

- Subscription licence
  - 2 varianty Enterprise Edition Application Server

1-50 Workstation Agents or 1-5 Server Agents	50+ Workstation Agents or 5+ Server Agents

- Perpetuální licence (1. rok support v ceně + další rok support 20% z ceny)
  - Pro větší deploymenty
  - Jedna varianta Enterprise Edition Application Server

* Nasazení HA nebo Disaster Recovery v rámci jednoho clusteru vyžadují pouze jednu licenci pro celý cluster.

EKRAN Licence

Agenti:

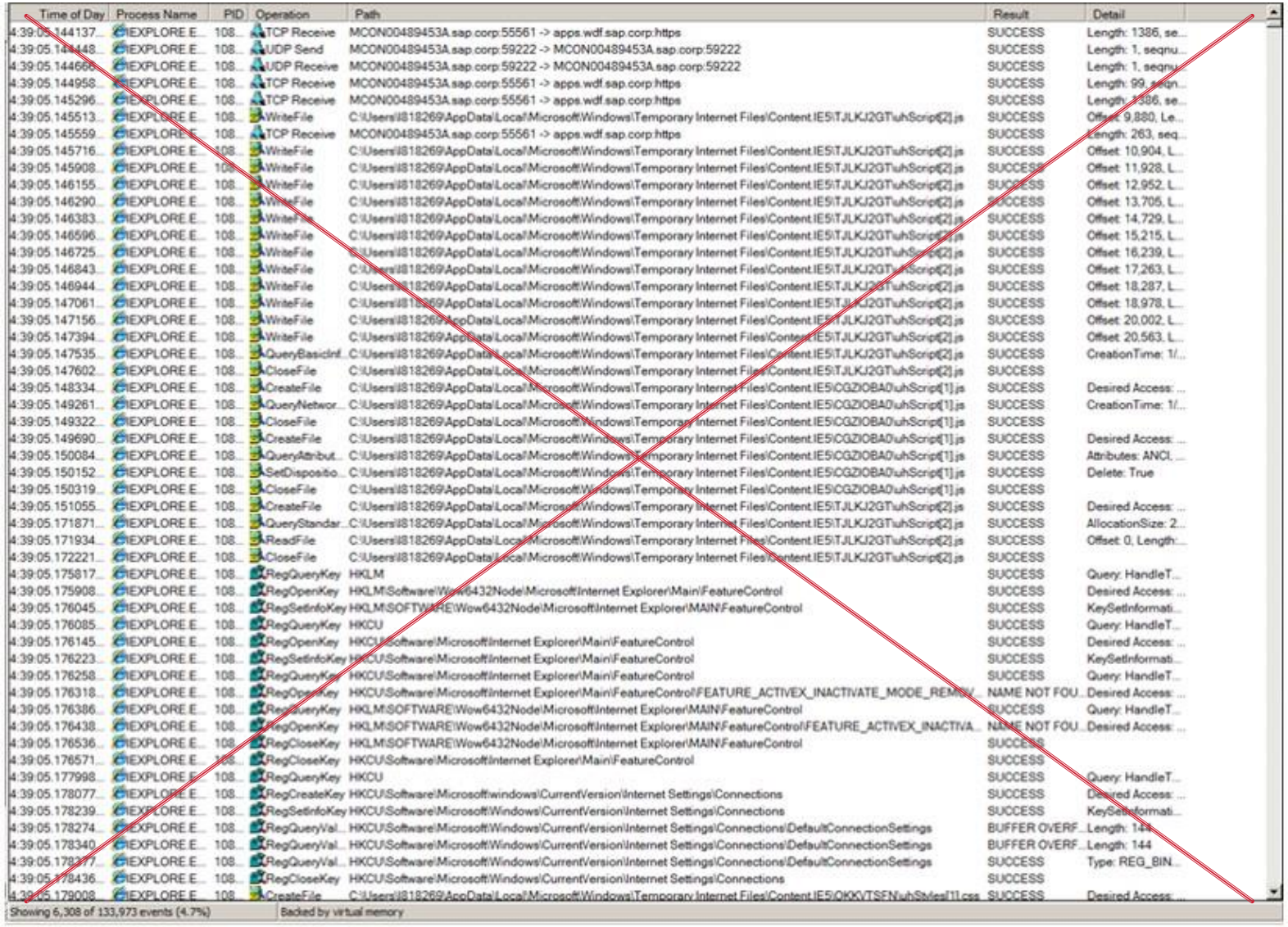
- Workstation Agent (Windows, macOS, X Window System)
- Infrastructure Server Agent (Windows Server, Linux/UNIX Server; no more than 2 concurrent sessions recording)
- Terminal Server Agent (Windows Server with Terminal Services, Linux/UNIX Server, Citrix Server, Published App Server, Jump Server, X Window System; unlimited number of concurrent sessions recording)
- Password Management Users (Password Management is available for Ekran System Terminal Server Clients installed on Windows-based jump servers under Enterprise Edition of Ekran System Application Server)
- Custom Development (100 hours minimum)

* Minimum order quantity is 10 Workstation Agents or 1 Server Agent.
* Additional order quantity is 10+ Workstation Agents or 1+ Server Agent.

Co EKRAN umí a jaká rizika pokrývá?

COMGUARD

Jak to vypadá ve světě bez EKRANu?



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...
4:39:05.144448...	IEXPLORE E...	108...	UDP Send	MCON00489453A.sap.corp:59222 -> MCON00489453A.sap.corp:59222	SUCCESS	Length: 1, seqnu...
4:39:05.144660...	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_REMOV...	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
4:39:05.178377...	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\QKKVTSFN\uhStyles[1].css	SUCCESS	Desired Access: ...

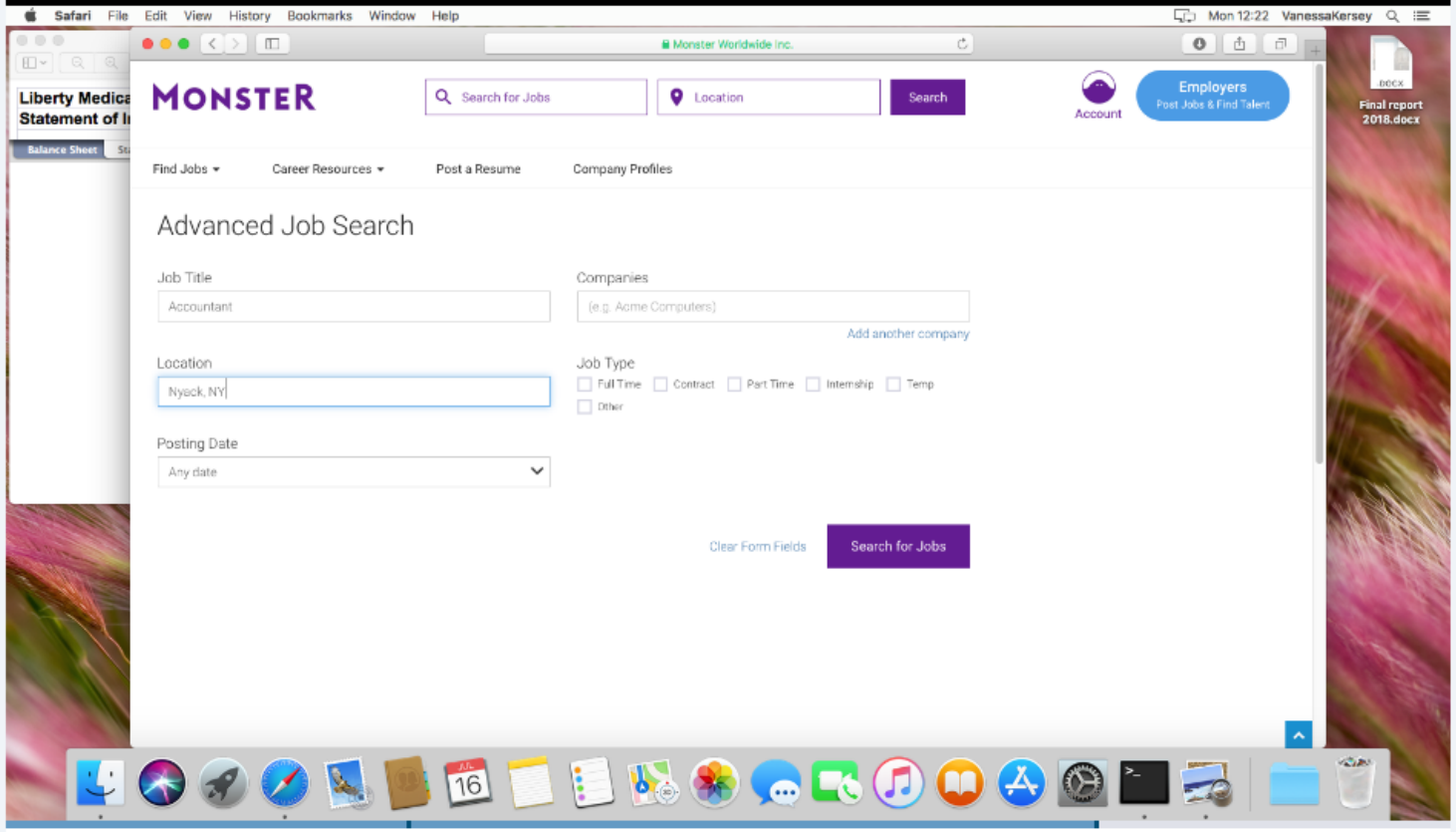
Showing 6,308 of 133,973 events (4.7%) | Backed by virtual memory

COMGUARD

Jak to vypadá ve světě s EKRANem?

16/07/2018 Vanessa_Mac vanessakersey BLOCK USER ALERTS TOOLS

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



1x

▼ 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...		

1

Proč zvolit právě EKRAN?

- Rychlost nasazení
- Nízké celkové náklady na vlastnictví
- Jednoduchý softwarový agent a vysoce optimalizované formáty pro ukládání dat
- Kontrola uživatelských rizik pod jednou platformou
- Plná podpora desktopových a serverových OS
- Krátká doba odezvy na incident díky vizuálně strukturované stopě
- Enterprise-ready, dostupný ale i pro menší a střední společnosti
- Detekce kompromitovaných účtů na základě AI

Jak to vidí Gartner Peer Insights?

Ekran

5.0 ★★★★★ Overall User Rating

Product(s): Ekran System

"Excellent IRM Solution"

Submitted Jul 11, 2023

Overall Comment:"Optimal Insider Risk Management tool, with broad functionalities; a very efficient and cost-effective solution"

5 ●●●●●	Evaluation & Contracting	5 ●●●●●	Integration & Deployment
5 ●●●●●	Service & Support	5 ●●●●●	Product Capabilities

Lessons Learned

What do you like most about the product or service?

- Complete control on risk activities - Comprehensive overview of risky hosts and accounts - Intuitive user-experience interface - Excellent customer service - Cost-effective solutions and fair princing plans

What do you dislike most about the product or service?

- They need to work more on brand awareness and recognition

What do you like most about the product or service?

1. convenient tool for viewing important events 2. convenient mechanism for setting the trigger rules 3. convenient user interface

What do you dislike most about the product or service?

Nothing

Evaluation & Contracting

Why did you purchase this product or service?

Improve compliance & risk management
Create internal/operational efficiencies
Enhance decision making
Cost management

What were the key factors that drove your decision?

Strong services expertise
Product functionality and performance
Breadth of services
Product roadmap and future vision
Overall cost

Evaluation & Contracting

Why did you purchase this product or service?

Create internal/operational efficiencies
Improve compliance & risk management
Improve supplier or partner relationships
Improve business process outcomes

What were the key factors that drove your decision?

Strong services expertise
Strong consulting partnership
Product functionality and performance

Ekran

Ekran System Reviews

by Ekran System in Insider Risk Management Solutions

5.0 ★★★★★ 3 Ratings

Related markets: Ekran System in Privileged Access Management (9 Reviews)

COMGUARD

cyber security masters

Děkujeme za pozornost!

kamil.kosour@comguard.cz
+420 602 129 569