Microsoft Azure

EKRAN®

Ekran System insider threat management for Windows Virtual Desktop

Record, log, and audit any Windows Virtual Desktop session

Ekran System is a Windows Virtual Desktop value-add partner that enables your IT teams to monitor all remote user activity on Windows Virtual Desktop host pools. With Ekran, you can record on-screen activity for every user session in published applications or virtual desktops while collecting a wide range of context-rich metadata including application name, active window title, visited URLs, and keystrokes. Advanced features offer in-depth visibility and quick incident response times, making Ekran System an efficient insider threat management and compliance solution. Incident response tools allow you to block users, show warnings to users, require them to acknowledge their actions, and terminate processes.

Windows Virtual Desktop session monitoring allows you to:

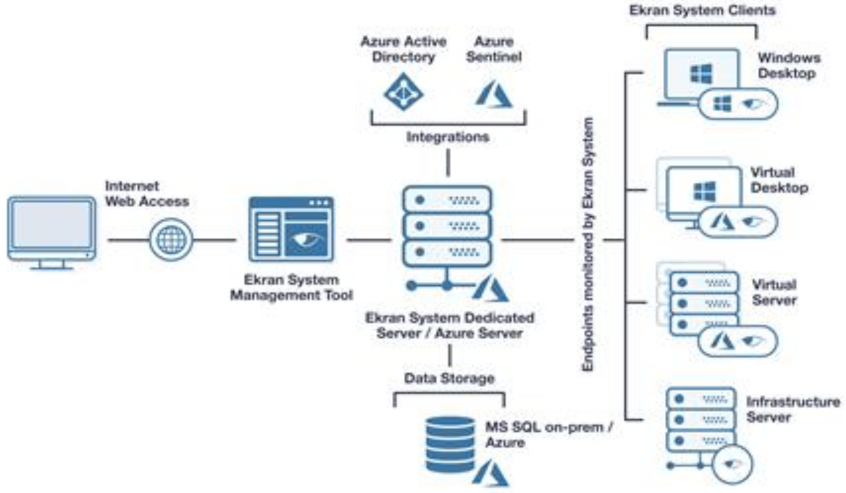
- Get notified in real time whenever an RDP connection is established
- Monitor all remote connections
- Record Windows Virtual Desktop sessions
- Configure alert notifications
- Monitor server and endpoint activity in real time
- Export sessions in encrypted formats
- Define report parameters

The Ekran System Client can record RDP sessions selectively, only recording for a range of users or host IP addresses or only recording those sessions outside of a white list.

Ekran System integrates with your existing infrastructure, including Azure Active Directory and Azure Sentinel.

> Ekran System provides a great solution for customers that need a session recording and activity audits, as well as incident response functionality to detect and prevent insider threats. Ekran System fully supports all features of Windows Virtual Desktop.
>
> **Denis Gundarev, Sr. Program Manager, Windows Virtual Desktop, Microsoft**

Deployment scheme on azure



How it works

You can achieve maximum visibility and control over any activity performed within your infrastructure by installing the Ekran System Client on each endpoint. Ekran Client software monitors user activity, manages access, and prevents malicious actions on virtual machines. Monitoring data is sent to the Ekran System Server for storage and analysis. If there is no network connection, this data is stored on the client in a protected cache until the connection is restored.

Full cycle insider threat management

Control access to deter

Ekran offers identity management and access management within a single endpoint agent. It also includes two-factor authentication, password management, one-time passwords, access request workflow, and other features.

Monitor and alert to detect

Ekran monitors, records, and audits all critical data, configurations, and user activity on Windows Virtual Desktop endpoints. Its alerting subsystem includes customizable rules and an AI-powered user-behavior analytics module.

Investigate and respond to disrupt

Ekran System delivers real-time notifications to your security team together with the full context of an event occurred on the Windows Virtual Desktop endpoint. It also provides several options for incident response.

Benefits of using Ekran System for monitoring Windows Virtual Desktop

Virtualization-ready agents

The Ekran System Workstation Client can be included in a master image to automatically monitor any new virtual desktop.

Enterprise-ready

Ekran System is easy to implement in large-scale environments due to its high availability, multi-tenancy, and ability to fill gaps in existing security solutions. Ekran provides enterprise-oriented features such as system resource and health monitoring dashboards and scheduling of automated maintenance tasks.

Major user-based risk management controls in one platform

Ekran System delivers identity and access management, session recording, and activity audits, as well as incident response functionality to detect and prevent insider threats in accordance with NIST 800-53 and most IT security standards.

Low total cost of ownership

Floating endpoint licensing enables license reassignment in a couple of clicks. For virtual environments, this process is automated to enhance your organization's agility.

Lightweight software agent and highly optimized formats for storing data

The lightweight agent works silently and isn't noticeable to users or other programs. Collected data is saved in searchable and highly optimized video, audio, and text file formats for compact log storage and easy reporting.

Visually structured evidence trail resulting in low incident response time

Context-rich recordings significantly reduce CERT and SOC response times. One-click search across suspicious activity makes investigations faster and more effective.

About Windows Virtual Desktop

Windows Virtual Desktop offers the best virtual desktop experience delivered on Azure. Windows Virtual Desktop enables organizations to deliver a virtual desktop experience and remote apps to any device. Microsoft 365 and Azure together provide users with the only multi-session Windows 10 experience — with exceptional scale and reduced IT costs.

About Ekran System

Ekran System® is a full cycle insider threat management platform that focuses on three core insider threat mitigation goals: deter, detect, and disrupt. Our mission is to provide customers with an efficient and easy-to-use tool to address all their insider threat management needs, improve their compliance, and allow them to pass security audits. Since its launch in 2013, Ekran System has been continuously gaining customers all over the world.

For more information, visit www.ekransystem.com.