

MONITOR, DETECT, AND ANALYZE USER-BASED THREATS

Growing vulnerability to insider threats

The amount of **insider-based attacks** on corporate data and the resultant losses to affected businesses is continuing to rise exponentially. The negative effect on the victims makes **recovery difficult and the impact long-lasting**. In 2015, up to 90% of surveyed security specialists named “human behavior” as the biggest threat to their organizations. The insider threat landscape includes employees and third-party subcontractors accessing corporate infrastructure, users working with critical data, on-site and remote administrators.

Solution

Ekran System is an advanced software-based solution for corporate security monitoring that allows to **record and analyze** every user session on corporate servers, terminals, local PCs, and virtual machines, with support for **Windows, Citrix, and Linux** platforms.

Based on the indexed video record format, Ekran System captures any user action on corporate end-points, from server configuration changes to sensitive data access, giving you all the details necessary to **explore and document any incident**.

Captured on-screen activity makes analysis easier and saves time, while synchronized log details such as entered commands or application names enable quick search and in-depth investigation. Real-time alerts on target events and rule-based USB device management assist your incident response team with timely threat detection. Various reports improve audit capabilities and allow cross-check.

How it works

Installed on a server or a workstation, **Ekran Client records video of all logged in user sessions and accompanying metadata** such as application name, entered Linux command, URL address, keystrokes, and connected USB device details. Ekran provides full-functional playback for all session records as well as easy search by metadata – all via a Web-based panel. **Real-time alerts** with direct links to the corresponding video episode and **USB blocking** make control even more proactive.

Cost-efficient for any deployment

Ekran System is **licensed by the number of Ekran Clients** – end-points to be monitored. This transparent approach makes deployment of any size cost-efficient. The solution supports both commercial and **free embedded database**.



Ekran System

CUSTOMERS IN USA,
Europe, Middle East &
Asia.



*Privileged user
monitoring*



*Regulatory
compliance (PCI,
HIPAA, ISO, SOX)*



*The best
affordability*

DISCOVER, INVESTIGATE, AND PREVENT ALL POSSIBLE VIOLATIONS

Monitor user activity with searchable video logs

With Ekran System, you can control the work of your corporate network users, including on-site and remote system administrators. Ekran System creates **complete video records of all local, remote, and terminal sessions**. With Ekran System, nothing can hide: every user screen will be captured together with activity details. The product works for any network protocol, application, and architecture.

Analyze monitoring results – discover suspicious user behavior

Ekran System uses a combination of easy-to-analyze video record – even for Linux SSH Telnet sessions – and searchable text metadata representing activity details: application name, active window title, URL address, commands with parameters, and more. **Advanced search** across all records gives you an effective tool to perform retrospective user action analysis and incident investigation.

Enable quick incident response

Ekran System provides a rule-based alert system that will notify your security personnel about potentially dangerous actions as it occurs, including the connection of USB devices prohibited by corporate policy. Sent notifications contain a direct link to the related video enabling **quick incident investigations**. The option of viewing a currently running user session permits real-time audits and manually blocking a user if malicious activity is suspected.

Audit user activity with reports

With Ekran System you may generate a variety of reports allowing you to analyze different aspects of users' activity for a selected period of time. Scheduled reporting option insures delivery of all essential statistics right into your email box. The solution includes forensic export capabilities to create self-contained protected logs of user sessions including video, metadata, and embedded replay and navigation controls.

Get more information

Please visit our website www.ekransystem.com or contact your representative.



Ekran System



*Record terminal,
remote, and local
user sessions*



*Video-like playback and
keyword-based search*



*Real-time alerts and
“live” session view*