Case Study

Baruch Pada Medical Center Secures Third-Party Activities with Ekran System

The challenge

Our customer had very limited capabilities for third-party activity monitoring and access management. When a vendor needed to connect to the organization’s network, they requested credentials from the center’s IT administrators, who had to manually create and manage these credentials. After that, the administrators had no visibility into the vendor’s actions with sensitive resources.

The need to manually provide credentials to more than 40 vendors created a huge overhead for the medical center’s IT department. Also, limited visibility into contractor actions threatened the security of patients’ medical records and left the medical center with zero capabilities to detect and respond to a security incident.

That’s why the medical center was looking for software to automate and enhance their data protection capabilities.

> As the organization's activity increased, so did the number of vendors that needed to connect to the network, and managing the allocation of users and passwords became more complicated and time-consuming than managing the computer system. In addition, we had no ability to monitor what each provider was doing on the network and make sure they weren’t connecting to servers they were not authorized to connect to or performing operations they weren’t authorized to perform. The inability to monitor and document these actions reduced the level of information security and increased the risk of data breach incidents.”

Zvika Klinger
Director of technology, Baruch Pada Medical Center

The customer

The Baruch Pada Medical Center in the Northern District of Israel provides a wide range of high-quality healthcare services to people all over the country. Today, the center has over 1,500 employees and over 40 contractors.

Baruch Pada collects lots of medical and personal records of their patients and needs to protect this data. Since all vendors have access to the center’s computer network, the customer was looking for a way to control and secure this access.

The challenge	The result	Our offer
Improve the IT management of third-party access	Centralized and quick configuration of access permissions	Automated credential management and provisioning
	Automated and convenient way to manage access rights for contractors	User groups with flexible configuration of access rights
Reduce the risk of third-party insider threats	Ability to review and investigate third-party activity with sensitive data	Continuous third-party activity monitoring
	Evidence of security incidents caused by third-party users	Detailed and searchable logs of third-party user sessions
Ensure the security of sensitive data	Possibility to detect and stop harmful activity in real time	Real-time alerts on suspicious security incidents
	Reduced risk of security-related incidents	Cybersecurity threat response and blocking capabilities

The results

Deploying Ekran System helped the customer achieve the following results:

- Centralized and quick configuration of access permissions
- Automated and convenient management of access rights for third-party users
- Ability to review and investigate third-party activity with sensitive data
- Ability to collect evidence of security incidents caused by third-party users
- Possibility to detect and stop harmful activity in real time
- Reduced chance of security-related risks

> The load on our IT team was significantly reduced immediately, as all vendors connect to a single IP point, and we can control and monitor where each user connects, as well as make sure they don’t move from there to other servers. Second, all the activities of each and every contractor are documented and recorded on video so we can watch past activities and explore and export data, which maximizes the level of information security.”

Zvika Klinger
Director of technology, Baruch Pada Medical Center

How we did it

The customer secured third-party activities and ensured the protection of sensitive data using the following Ekran System capabilities:

- ✓ **Automated credential management and provisioning.** The need to provide credentials to third-party users manually caused a lot of stress for the customer's IT administrators. With Ekran System, they now can generate, rotate, provide, and dispose of passwords automatically. This way, administrators can use their time more efficiently while ensuring that third-party users can access the required resources.
- ✓ **User groups with flexible configuration of access rights.** Each vendor that connects to the medical center's computer network must be able to access only the resources they need to work with. Ekran System helps IT administrators create groups of third-party users and define access for each group. Also, administrators can easily reconfigure user groups and limit access permissions for particular users. Using this capability, our customer can secure sensitive data from unauthorized access and reduce the risk of an insider attack.
- ✓ **Continuous third-party activity monitoring.** External connections to the organization's computer network are a constant source of security threats. That's why IT administrators have to keep a close eye on third-party sessions. With Ekran System, medical center administrators can watch third-party activity in real time and review records of past sessions. If a security incident is caused by one of the vendors, the administrators know every detail about it.
- ✓ **Detailed and searchable logs of third-party user sessions.** Knowing the details of a security incident allows IT administrators to determine the cause and impact of each user action. Ekran System provides administrators with complete records of user screens and metadata on user activity: keystrokes, opened files and URLs, connected devices, etc. The customer can also use this metadata to filter user activity records in search of particular events.
- ✓ **Real-time alerts on suspicious security incidents.** Previously, our customer had no means to detect a cybersecurity incident. And the slower threat detection and response is, the more damage may come from the threat. That's why Ekran System's ability to detect suspicious activity, alert on it, and provide the means to review third-party user sessions in real time is especially valued by the Baruch Pada Medical Center.
- ✓ **Cybersecurity threat response and blocking capabilities.** Blocking harmful third-party activity helps our customer to stop possible security violations and protect their sensitive data. They can specify which user actions Ekran System should block immediately and which they need to review before taking further actions. Combining automated and manual response capabilities allows IT administrators to quickly secure data from the most threatening actions and help out users that violate security rules by mistake.

Request an Ekran System demo to see how our platform can help secure your third-party activity!

www.ekransystem.com