TransientAccess delivers true Zero Trust Network Access for the Fenerbahce Sports Club

With over 5000 employees and more than 300,000 members, Fenerbahce is one of the largest multi-sport clubs in Turkey and is a major retailer in its own right.

With their dedicated fan bases, legal and illegal betting riding on game results and big revenue streams, professional sports clubs are among the most targeted companies by hackers. Successful attacks can have devastating effects on company operations and reputation. Damage caused by IP loss can imperil an organization's viability.

For an organization like Fenerbahçe, SAP is the most important digital asset to defend. Protecting such a high value asset means going beyond traditional security paradigms.

Most organizations deploy multiple security layers to protect SAP data, such as NGFWs, AV, MFA along with robust IT security policies. Yet all these steps can still leave holes that need to be closed.

FC Fenerbahce relies heavily on SAP to carry out product lifecycle, finance, customer relationships, human resources and many other processes, all involving business-critical information. The executives and security teams are responsible for carrying out this process knowing that their business revolves around this information. However, they are also aware of hidden dangers such as user accesses, file downloads, and data leaks that can occur due to data streaming. It therefore became critical to implement solutions that monitor and prevent such leaks.

SAP data is the digital lifeblood of the organization

At Fenerbahce, Financial, Sales, Product Planning, Materials Management, Quality Management and Human Capital Management modules are all business-critical applications that need to be protected.

How does a company protect its highly sensitive data while sharing it with partners? By controlling the export and processing of sensitive SAP data.

A **TransientAccess** management console is provided to the required SAP modules with micro-segmentation. Thanks to TransientX's disposable network technology, SAP is available within the internal network of the company without any openings in the firewall. Access is allowed only for authorized users via TransientAccess.

By using **TransientAccess**, daily audit access logs can be monitored and the threats analyzed for data loss. In addition, for partners granted access, the data is accessible only in a secure environment via the **TransientAccess** workspace. Documents are encrypted to prevent them from being displayed outside of the secure environment. Access to SAP in the internal network is limited by the Firewall, and only the patented technology of **TransientAccess** allows access to externally authorized users without being exposed to the Internet. In this way effective protection mechanisms have been created to secure data.

FC Fenerbahçe, a global brand with a history dating back more than a century, relies on SAP ERP and shares access with key business partners. Therefore, ensuring the security of the shared data is mission-critical.

Authorized SAP users, especially external users who are in constant contact with the club, must access relevant critical data continuously and externally, and the data must be exported for various operational and commercial purposes.

Despite strict controls around required authorization and firewall policies, there is still potential risks such as theft of critical data, access to SAP directly by attackers, and accessing the internal network to breach more applications and data. By opening up to the Internet in order to enable sharing and integration with external parties and remote workforces, many internal controls are rendered ineffective.

The TransientX Value Proposition

TransientAccess is able to proactively eliminate threats such as data loss and ransomware attacks by providing users with an operational convenience they have not experienced before.

It provides proactive protection against commercial damage by ensuring data protection and facilitating secure operational processes. Thanks to the micro-segmentation feature of **TransientAccess**, only relevant users are authorized to access company data in the relevant SAP modules. IT Managers can now see 'who' can access 'which' data from the SAP system and make sure that this data is securely encrypted, even outside the company.

The result: Unparalleled effective data security and operational flexibility
In addition, **TransientAccess** automatically prevents unauthorized people from accessing SAP.

Benefits

- Improved User Experience
- Quick and Easy Installation
- Micro-level user segmentation in minutes
- Total visibility into system access and usage logs
- Critical application security for managed and unmanaged devices
- Encrypted data in non-secure environment
- No cloud-in-the-middle solution needed for data transmission

"After a detailed product assessment, in-depth presentations and a pilot project to measure performance in our company's environment, TransientAccess demonstrated reliability and effectively demonstrated its value in providing SAP access and data security."

Bülent Kaçmaz, CTO, FC Fenerbahçe

*"We work in a security-sensitive environment in the football industry and other sports fields.
Of course, we take extremely strict measures to protect our data inside and outside our systems."*

Fatih Yildirim, IT Manager, FC Fenerbahçe