Caglayanlar, a leading automotive parts distributor, stopped critical data leakage and secured remote access with McAfee® UCE and TransientAccess

Since 1955, Caglayanlar has been distributing automotive spare parts. The company operates throughout Turkey with more than 100 partners selling their products. Caglayanlar was struggling to provide secure remote access to employees and business partners, losing critical business data to competitors.

Collecting, analyzing and prioritizing logs consumed many hours that the IT team could ill afford to spare. The team had to constantly review the security status of devices such as mobile phones and personal computers connected to the company network. In addition, the company faced a problem of password sharing by its dealers, and by extension information that was intended only for a specific dealer. This situation was a challenge for the company, bypassing many security measures and leading to data leakage to unrelated parties.

To prevent data leakage, the IT team had to manually analyze the situation, identify the resellers who provided such access and restrict their access. At that stage, it was not possible for the IT team to provide a view through a common portal to review and manage security logs. In such situations, the logs on different devices and on different days had to be examined separately. These devices included remote access VPN devices, firewalls and hardware such as switches and routers.

Such an approach both consumed a lot of time and required the technical expertise of the staff to cover all devices. This situation made it impossible to manage against such threats with limited resources and personnel for the company and left the company exposed.

Data privacy and protection regulations like GDPR and KVKK (Turkish regulations similar to GDPR) compelled Caglayanlar to review its information security practices and the importance of protecting employee and customer data. The automotive sector has become increasingly complex, and this was reflected in the security challenges faced by Caglayanlar. They elected to find a trusted partner in Turkey, DemirBT. DemirBT brought their expertise to the table in a joint consultation to create a safe end-to-end computing environment for Caglayanlar.

ÇAĞLAYANLAR
1955'ten bugüne...

Challenges

- Complex Security Environment
- No central management console
- Hard to achieve end to end protection

McAfee Solution

- McAfee Total Protection for DLP
- McAfee Disk Encryption
- McAfee MVISION Unified Panel

TransientX Solution

- TransientAccess Secure Remote Access
- TransientAccess Data Protection between client and server applications
- TransientAccess Client Device / User matching for dealers

"Easy-to-use TransientAccess integrated with McAfee UCE allows us to automate our defenses much more. We can do tasks automatically faster and easier, so we can use our team's resources where they can add the most value."

- Sinan Güner,
Deputy general manager

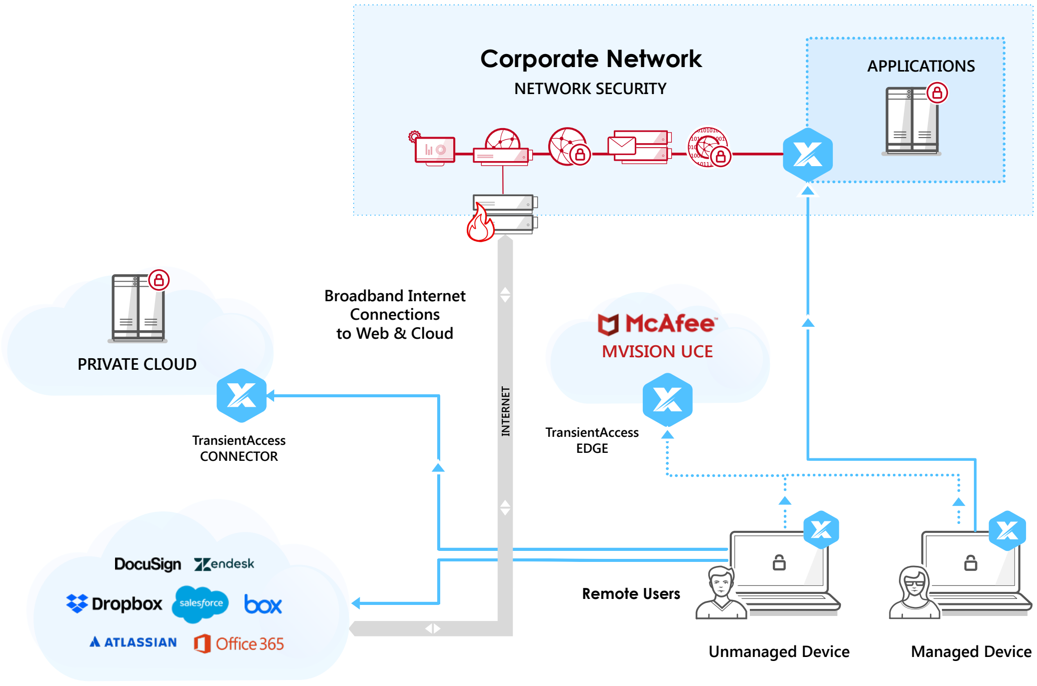
McAfee MVISION and TransientAccess resolved the company's critical infrastructure and remote access challenges.

With DemirBT, they carried out POC studies with many product alternatives and decided on **McAfee MVISION**, McAfee's Device-to-Cloud security platform, including McAfee Unified Cloud Edge (McAfee UCE) and TransientX's TransientAccess Zero Trust Network Access (ZTNA) product. With its product range, McAfee MVISION solved the problem of data leakage on end user devices with **McAfee DLP** and disk encryption products, and provided solutions to manage them on a single pane of glass. Complementing the McAfee MVISION solution, **TransientX's TransientAccess** product for remote access ensured employees, dealers and business partners could access their applications and related critical data remotely without having to expose them to the internet. They also made sure that the dealers could access their applications only from the devices defined for them by the TransientAccess policy.

Conclusion

This powerful and comprehensive suite replaced legacy manual efforts that Caglayanlar had used in the past. The combined solution used McAfee MVISION DLP with Disk Encryption and TransientAccess to defend against emerging and targeted attacks. This combination mitigates all data stealing and malware attempts as well as fraud attempts by rogue dealers.

Caglanyar network with TransientAccess ZTNA and McAfee UCE



"In the past, when a security incident involving customer data occurred, our IT teams would try to find the device logs in different networks then manually examine the source of the problem. This approach was not scalable and sustainable at all. In addition, our dealers shared their user passwords among themselves. This put us in a very difficult situation, and we had great difficulty in restricting the dealers at this point. With McAfee MVISION and TransientX TransientAccess products, we feel much more comfortable and secure. In the event of an incident, we can now control and access the source much faster, as well as managing our micro-segmented applications, making it easier to use, and maximizing security."

- Selim Çağlayan,
Vice chairman of the board.