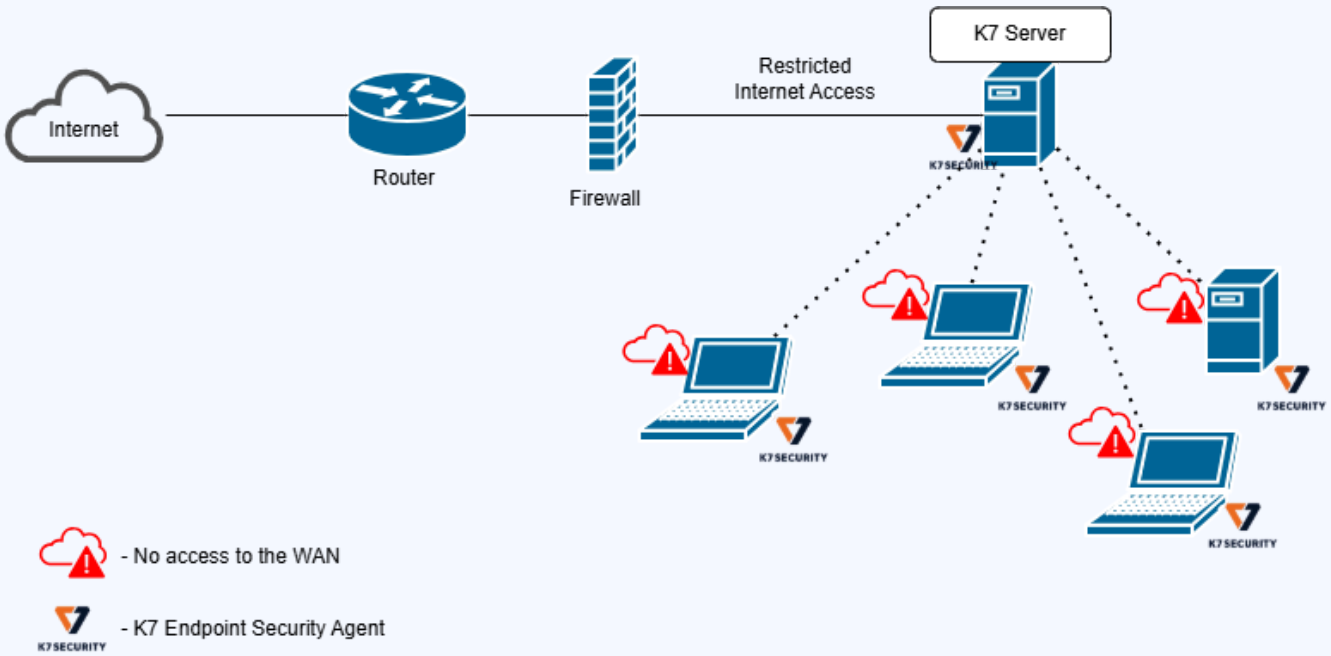
Computer and Server Protection

An engineering and automation organization with operations spread across multiple locations faced the challenge of strengthening the security of its computers and servers in a highly restricted environment with no direct internet access. The organization needed to implement a robust solution to protect against malware, ransomware, and advanced threats, while ensuring centralized control and compliance with internal security policies.

To address this challenge, an on-premises endpoint and server protection solution was implemented across two separate sites. The architecture was designed to operate on an isolated network, allowing only the WAN communications strictly necessary for security updates, through specific firewall and certificate management configurations.



The implementation included:

- ✓ Installation of K7 management consoles at each location
- ✓ Setting policies for endpoints and servers
- ✓ Creating logical groups to simplify administration
- ✓ Automated deployment of the K7 security agent
- ✓ Granular control over console access and permissions

In terms of security, the mechanisms included in the solution's default settings have been retained, which include features such as:

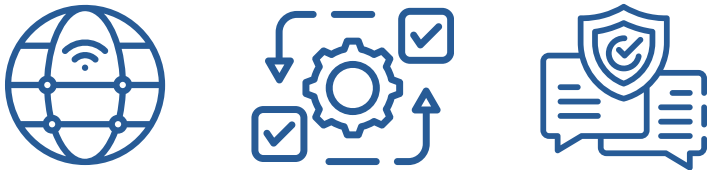
Signature-based malware detection

Firewall with integrated HIDS/HIPS systems

Ransomware protection with behavioral analysis

Web filtering and application control

During the project, significant technical challenges arose, particularly regarding system updates in an environment without internet access and compatibility with internal automation processes. These obstacles were overcome through specific adjustments, such as installing the necessary certificates for secure communication and configuring system settings to avoid conflicts with critical applications.



As a result of the implementation, the organization's security posture was significantly strengthened, accompanied by greater centralized visibility into all protected assets. In addition, it was possible to reduce the risk of malware and ransomware attacks while ensuring operational continuity, even in a restricted environment. The infrastructure was also prepared to meet audit and compliance requirements.

The project demonstrates that it is possible to implement an effective cybersecurity solution in complex and constrained environments, ensuring high levels of protection without compromising the business's specific operational requirements.

Zoom Business Park
Edifício E, Piso 1, Escritório 3
Estrada de Paço de Arcos
2735-307, Agualva-Cacém

(+351) 218 051 560

comercial@dssi.pt