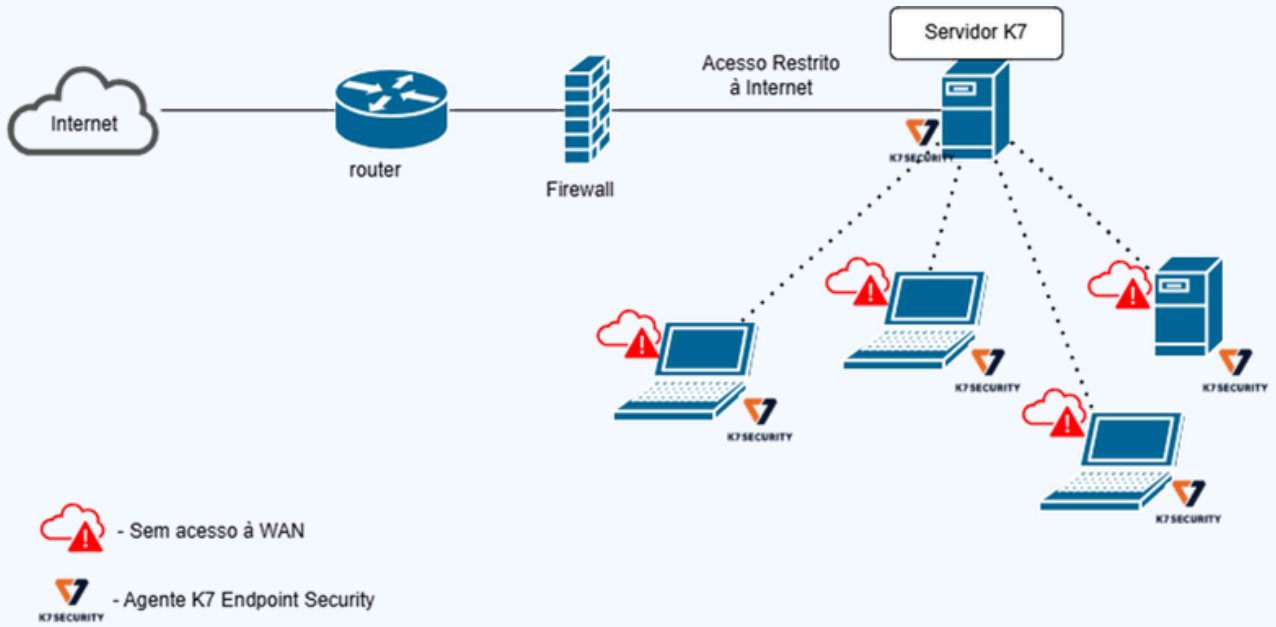
Proteção de Computadores e servidores

Uma organização de engenharia e automação com operação distribuída por múltiplos locais enfrentava o desafio de reforçar a segurança dos seus computadores e servidores num ambiente altamente restrito, sem acesso direto à internet. A necessidade passava por implementar uma solução robusta de proteção contra malware, ransomware e ameaças avançadas, garantindo simultaneamente controlo centralizado e conformidade com políticas internas de segurança.

Para responder a este desafio, foi implementada uma solução de proteção de endpoints e servidores, on-premises, distribuída por dois sites distintos. A arquitetura foi desenhada para funcionar numa rede isolada, permitindo apenas comunicações com a WAN estritamente necessárias para atualizações de segurança, através de configurações específicas ao nível da firewall e da gestão de certificados.



A implementação incluiu:

- Instalação de consolas de gestão K7 em cada localização
- Definição de políticas para endpoints e servidores
- Criação de grupos lógicos para facilitar a administração
- Distribuição automatizada do agente de segurança K7
- Controlo granular de acessos e permissões à consola

Ao nível da proteção, foram mantidos os mecanismos incluídos nas configurações padrão da solução, que contemplam funcionalidades como:

Deteção de malware baseada em assinaturas

Firewall com sistemas HIDS/HIPS integrados

Proteção contra ransomware com análise comportamental

Filtragem web e controlo de aplicações

Durante o projeto, surgiram desafios técnicos relevantes, nomeadamente na atualização dos sistemas num ambiente sem internet e na compatibilidade com processos de automação interna. Estes obstáculos foram ultrapassados através de ajustes específicos, como a instalação de certificados necessários para comunicação segura e a parametrização de configurações de sistema para evitar conflitos com aplicações críticas.

Como resultado da implementação, verificou-se um reforço significativo da postura de segurança da organização, acompanhado por uma maior visibilidade centralizada sobre todos os ativos protegidos. Adicionalmente, foi possível reduzir o risco de ataques contra malware e ransomware, garantindo simultaneamente a continuidade operacional, mesmo num ambiente restrito. A infraestrutura ficou ainda preparada para responder a requisitos de auditoria e conformidade.

O projeto demonstra que é possível implementar uma solução de cibersegurança eficaz em cenários complexos e limitados, assegurando elevados níveis de proteção sem comprometer os requisitos operacionais específicos do negócio.

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