



CASE STUDY

International Provider of Vegetarian Food Products

Securing the network that
supports the creation of healthy,
pesticide-free food choices

The International Provider of Vegetarian Food Products has a 30-year track record of providing authentic and traditional culinary preparations. Securing their trade secrets from cyberattacks is critical to preserving their brand value, which is why they rely on K7 Security's SD-WAN solution.

Client Snapshot

- » Founded in 1987
- » 4 locations (Head Office + 3 Factories)
- » International Retail Presence

The client uses extensive inter-branch connectivity for seamless coordination of manufacturing activities and supply chain management. An open Remote Desktop Protocol (RDP) port allowed ransomware to destroy company data, following which the client approached K7 Security for a comprehensive multi-facility network security solution.

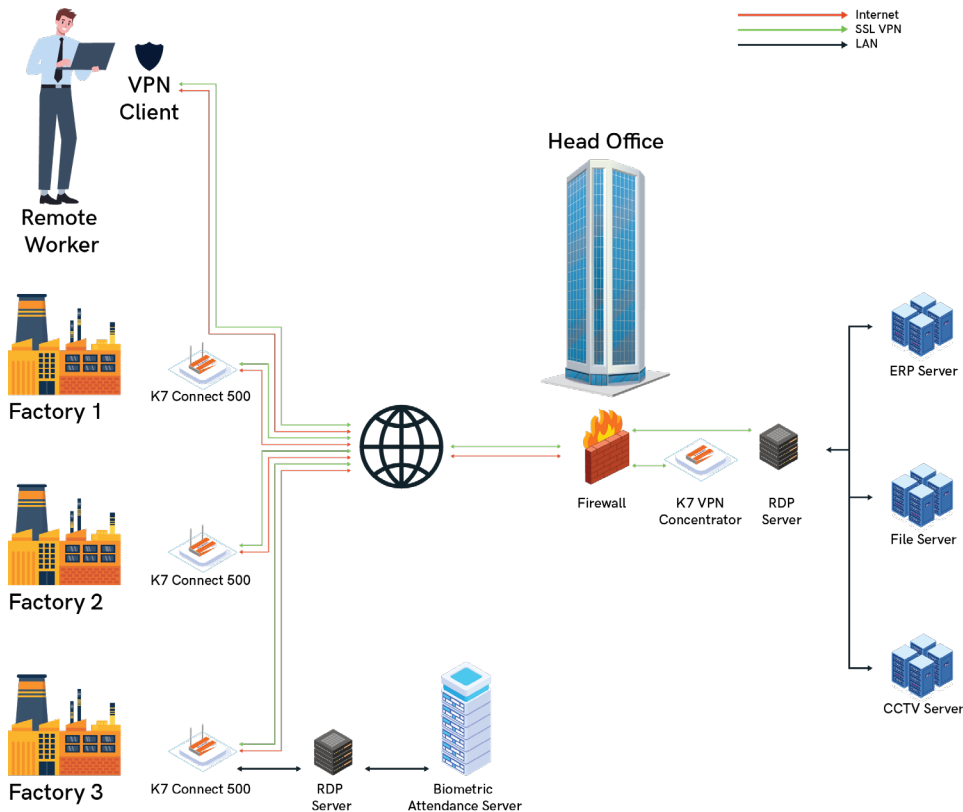
Creating Secure Inter-Branch Connectivity with K7 SD-WAN

The Client's Requirements

- Source-based RDP access
- Remote access support for
 - o Enterprise Resource Planning (ERP) software (at Head Office)
 - o CCTV access (at Head Office)
 - o Biometric attendance server (at Branch Office)
- Integration with existing firewall
- Reliable performance using inexpensive broadband
- Simple deployment and management

The K7 Solution

K7's SD-WAN creates secure connectivity between facilities using hub-and-spoke technology, allowing the client to utilise RDP safely across the organisation.



Why the Client Choose K7

- Source-based RDP access from branch offices and for remote workers
- Robust inter-branch connectivity for enterprise digital resources
- Hassle-free integration with existing firewall
- Support for multiple connectivity options
- Easy to deploy and manage

Source-based RDP Access

The client's management required RDP access to be allowed based on the source of the incoming request, limited to organisational branches and remote workers. K7's team deployed the K7 VPN Concentrator in the head office and K7 Connect 500 in each of the 3 factories to create a Software-Defined Wide Area Network (SD-WAN). VPN clients with appropriate security certificates were also configured in Remote workers' devices. The SD-WAN enabled source-restricted secure site-to-site VPN across the organisation.

Remote Access for ERP, CCTV, and Biometric Attendance

The client's IT team specified that

- The entire organisation should be able to access the ERP server located in the head office
- Security teams in the head office should be able to receive CCTV feeds from all locations
- The entire organisation should be able to register attendance by communicating with the biometric attendance server located in one of the factories
- All locations should be able to access files stored in the head office, if required in future

The client's IT team were pleased that K7's team were able to demonstrate that the K7 SD-WAN solution could provide seamless and reliable access to the specified digital resources simultaneously.

Integration with Existing Firewall

The client's IT team wished to retain their existing firewall which had been deployed at the head office to manage the organisation's internet security. The firewall had been previously configured manually to permit access to the RDP port, which allowed the ransomware attack to succeed.

K7's network security specialists worked with the client's IT team to provide appropriate configuration for and remove RDP port forwarding from the firewall. The firewall verifies if connection requests to the public VPN port are from the factories or remote workers before forwarding the requests to the K7 VPN Concentrator. The K7 VPN Concentrator verifies encryption and authenticates the connection with the K7 Connect 500 devices in the factories or the VPN clients in the remote workers' devices and then permits access to the RDP server through which other IT resources are accessed, ensuring that unauthorised users or locations are denied RDP access.

Multiple Connectivity Options

The client's management did not wish to invest in expensive private WAN or leased lines. They were delighted to see that K7 SD-WAN could enable secure and reliable communication using the residential broadband connectivity available at the factory sites. Mobile internet through cable was also configured in the K7 Connect 500 devices to provide manual failover. The client has the option to enable automatic failover through wired or wireless connectivity from a second ISP.

Easy Deployment and Management

The client did not wish to increase investment in their in-house IT team and therefore required an SD-WAN solution that could be configured, deployed, and managed easily. K7's team took just 3 hours to configure the K7 VPN Concentrator and one K7 Connect 500 to demonstrate the capabilities of the K7 SD-WAN solution across the head office and one factory. Configuring the K7 Connect 500 devices for the other two factories only required export of configuration settings from the first device to the other two devices. Configuring organisation-wide SD-WAN, therefore, only took a few hours. K7 SD-WAN also supports centralised control for easy management, allowing the client to achieve enterprise-grade cybersecurity without building a highly skilled internal IT team.

K7 Security's SD-WAN solution delivers cost-effective virtual WAN that improves security, uptime, application performance, and user productivity. [Contact Us](#) to learn more about our enterprise cybersecurity solutions and how we can help you create robust and resilient IT infrastructure.



Copyright © 2023 K7 Computing Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7computing.com

