SElink™ for Video Surveillance
Solution Bundle

Version 1.1

Contents

SElink™ for Video Surveillance

Solution Bundle

Introduction

SElink™ Solution Bundles, provide solution implementations of the SElink™ technology to help streamline integration and deployment into existing networks. SElink™ Solution bundles are created to assist partners in serving customers with SElink™ packaged purpose-built solutions.

The flexibility of the SElink™ architecture facilitates the gradual deployment of the solution in phases, safeguarding the investment.

IP video surveillance networks must balance efficiency, cost, bandwidth, and security to ensure performance. The exponential growth in devices and network traffic complicates this, leading to network lag. To improve communication, private connections, network segmentation, and segregation are commonly used. Segmentation and private networking involve subnets and VLANs, while segregation uses dedicated telco links, air-gaps, firewalls, bridge gateways, or data diodes. However, these methods are becoming unsustainable and increasingly difficult to implement. A deep network segmentation and data segregation solution, broadly applicable, low on network resources, efficient and secure is mandatory.

In this scenario, SElink™ can be integrated into any existing network to replace standard VPN solutions, offering virtualization, isolation, and encryption for IP video surveillance networks. SElink™ is a Zero Trust virtual networking solution designed to protect endpoints, segregate services, and create private networks without the need for costly dedicated connectivity contracts, dedicated SIM cards, or public static IP addresses. This results in a significant reduction of the attack surface and improvements in efficiency and operational costs.

In this document we focus on a case study involving the implementation of a Zero Trust model to a Construction Site Video Surveillance System to replace the VPN and reduce the running costs for public IP addresses and dedicated SIM cards.

1. SElink™ for Video Surveillance

1.1. Operational Requirements

In this specific use case scenario, the organisation's requirements are:

1. Replace VPN
2. Adopt Zero Trust access controls and continuous monitoring to prevent fake data stream
3. Lifting the requirement for Public IP address and dedicated SIM data plans
4. Remove the complexities from network segmentation
5. Enforce unidirectional simultaneous data flows at each network component
6. Guarantee isolation of each data stream at application level
7. Obtain maximum network performance, stability and availability
8. Seamless integration for easy setup, deployment
9. Improve visibility. Systematically oversee the activities conducted on the network to fulfil auditing needs, ensuring transparency and accountability in business operations and to fast-track compliance

1.2. Network Topology

The client has several construction sites with machinery equipped with cameras, as per local regulations, for site monitoring in case of accidents or damage to third-party property.

The client's network architecture presented a number of Wi-Fi cameras deployed at the construction sites on board of heavy-duty machinery. The cameras streamline live data to the HQ through a Wi-Fi LTE Router and are accessed from a remote command centre or a remote user for monitoring purposes.

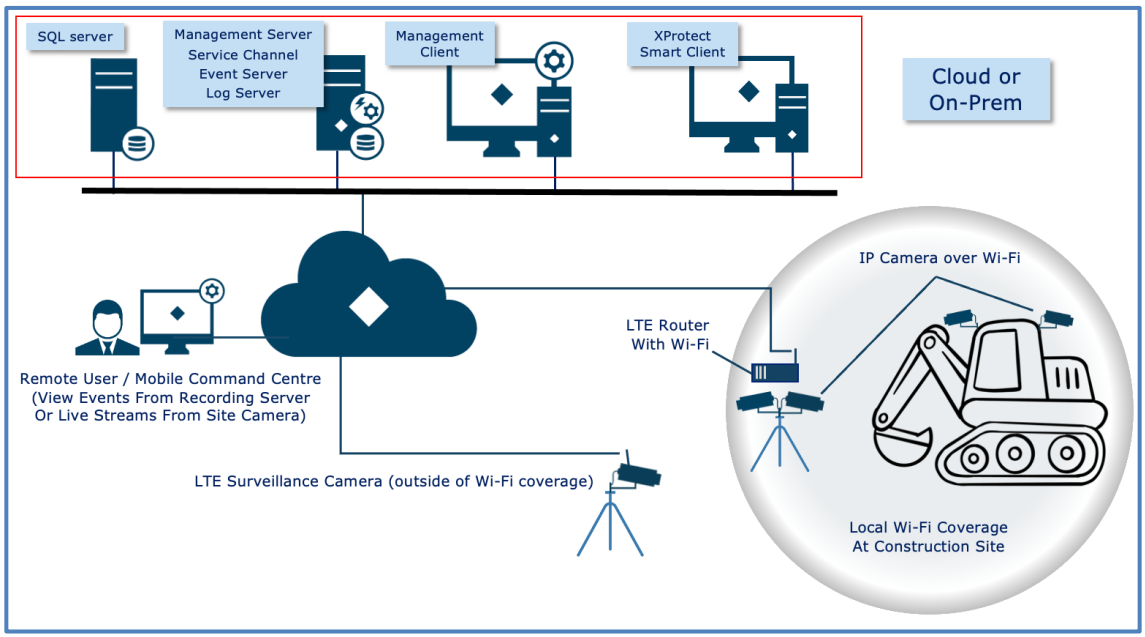

Figure 1 – Client Network Topology

The integration of SElink™ does not impact in any ways on the existing network design, which was maintained as is following client's requirement.

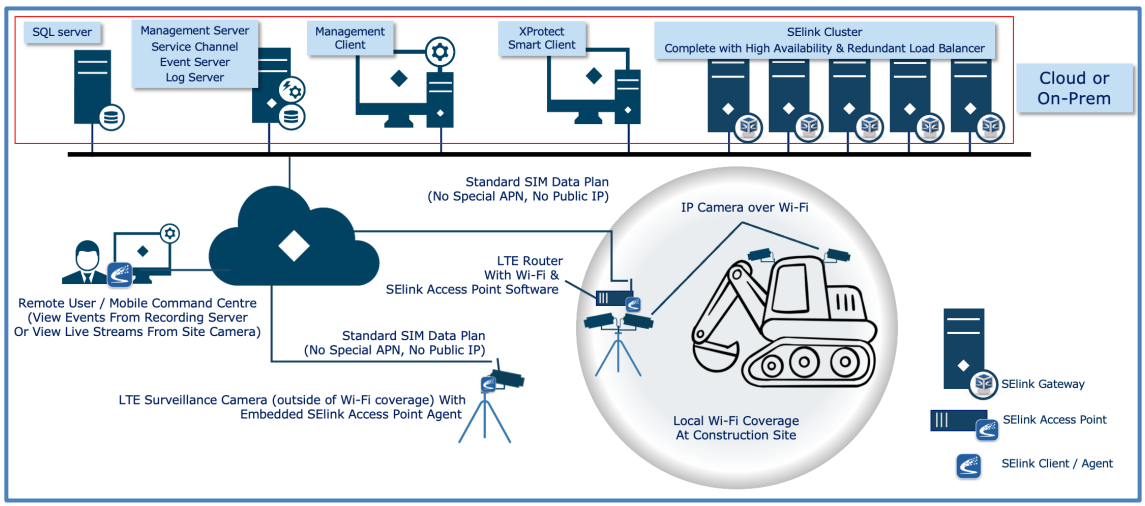

Figure 2 – SElink™ Network Topology

The SElink™ network topology comprises the following components on the server side and on the device side.

ON THE SERVER SIDE

In this example, **5 SElink™ Gateways**, featuring High Availability and load balancing, are implemented in a Cloud Data Centre. Please note that the Gateways can also be located on-premise. In any case, The SElink™ Gateways must be under the control of the client.

The SElink™ Gateways acts as a communication broker, providing software-defined connectivity links to services from any location, endpoint, making all endpoints appear as a single high-performance WAN.

The SElink™ Gateways are accessible via the Internet and/or LAN from all the network components that need to securely exchange data.

ON THE DEVICE SIDE

An **SElink™ Agent** is installed on the endpoints (cameras, LTE Router, and remote users) that need to access services from within and outside the organization.

The agent, embedded in the endpoints, enables endpoints to access authorized services and applications from any location without relying on unreliable VPN connections, Public IPs or dedicated SIM data contracts. In case integration in the device is not possible, a dedicated hardware SElink Access Point is used or, as depicted in this scenario, the SElink Access Point Agent can is on board of a standard LTE Router to manage multiple devices.

An **Endpoint License** is associated to each user/device in the network. An **Access Point License**, is installed on the LTE Router integrating the SElink Access Point Agent.

External users access the company services through simultaneous one-way SElink™ micro-links.

External users will be able to operate in various areas of the company in accordance with ZTNA security policies and their access privileges, avoiding unauthorized access to the devices.

Unlike monolithic network design, SElink™ provides a scalable cluster architecture ideal for managing distributed devices (machines, users, locations, industrial facilities) remotely, supporting a phased deployment and future network expansions. This capability extends to on-premise, cloud, and hybrid installations.

The combination of SElink with a video surveillance system establishes a cyber resilient security architecture overcoming the limitation of traditional VPN solutions while reducing the network running costs.

SElink contributes to the establishment of a resilient and secure operational environment aligned with regulatory standards and internal governance policies in hybrid network environments.

1.3. Solution Functionalities

SElink™ Secure Virtual Networking based on Zero Trust Network Access (ZTNA) is an integrated solution designed to address challenges in terms of connectivity, networking, and security.

The following functionalities are supported by SElink™:

- Stable VPN FREE connectivity
- Low on network requirements (no public IP, no open inbound Ports, no subnets)
- Maximized connectivity (supporting Client-to-Client, Client-to-Server, Server-to-Client, Site-to-Site topologies)
- Bandwidth usage efficiency (less bandwidth more data)
- Optimized data transfer speed (Anti-shaping and zero overhead in bandwidth)
- One-way micro-tunneling segmentation
- Transparent to any transport channel and operating system (supporting integration into legacy systems)
- Low on resource requirements (ideal for resource-constrained devices and poor networks)
- On-premise, Cloud (Private and Public) hosted servers accessible from the Internet
- Single point of Configuration and Management
- ZTNA Infrastructure Security (LAN and WAN)
- ZTNA Endpoint Security
- Anti-Ransomware Propagation
- Post-Quantum ready
- Crypto Agility
- Certified CC EAL5+ hardware add-ons for authentication and to secure critical processes

1.4. Solution Bill of Material

SElink™ for this purpose-built scenario requires the following components:

Description	Qty	Note
SElink™ Gateway	5	Scaled for High Availability and Load Balancing
SElink™ Agent	1 for each device in the network	
SElink™ Access Point Agent	1	Installed in the LTE Router to manage multiple IP cameras
SElink™ Access Point 300/1000	NA	The quantity of Access Points is scaled according to clients' network requirements. Available in different models for scalability up to 1Gbps data throughput and 1024 concurrent sessions
SElink™ Access Point license	1	
SElink™ Endpoint license	1 for each device in the network	
SElink™ Management Suite	1	
SElink™ Network Configurator	1	
VMS platform	1	According to client network requirements
Cloud Subscription for Cloud hosting	1	

Table 1 – Solution Elements

Description	Qty	Note
USEcube Tokens (CC EAL5+ certified)	1	Hardware USB token used for authentication purposes and to protect critical processes

Table 2 – Add-on Options