PROTELION

Use Cases

Highly Secure Communication for Data Centers

In today's rapidly evolving digital landscape, data centers and their implemented server farms face an unprecedented array of cybersecurity threats. Malware, ransomware, DDoS attacks or insider threats, constantly put the integrity of your critical data at risk. Protecting data centers is no longer optional – it's essential. That's where Protelion comes in. As a leading provider of cybersecurity solutions, Protelion specializes in strengthening data center security against these attacks. Protelion's state-of-the-art tools and expert services ensure that your digital assets remain safe. Protelion solutions protect your data center and provide the security you need in this highly sensitive environment.

Duties and As-Is Situation for Data Centers

Data Centers (DCs) are key elements of today's business infrastructure. They store and process large amounts of sensitive organizational information, including customer data, accounting information, intellectual property and more

Data Centers increase productivity and reduce data redundancy. Most often they are geographically distributed and in a single network segment

Each Data Center disposes of a security perimeter that includes video surveillance, remote and physical access and more

Project Specification

Reliable and secured data transfer between DCs or headquarters, using different communication channels, must be established

Setting up security policies that demand integration of two or several Data Centers into a single network segment (Zoning)

Security products and tools that allow a scalable solution, when expanding Data Center capacities, with minimal cost

Due to the nature of Data Center to be the storage of valuable and sensitive data assets, all activities (normal and suspicious) within the network must be recognized, registered and monitored

Protection against, cyber attacks on Data Center server farms, malicious manipulation of data assets or altering of video surveillance imagery must be put in place

Project Implementation

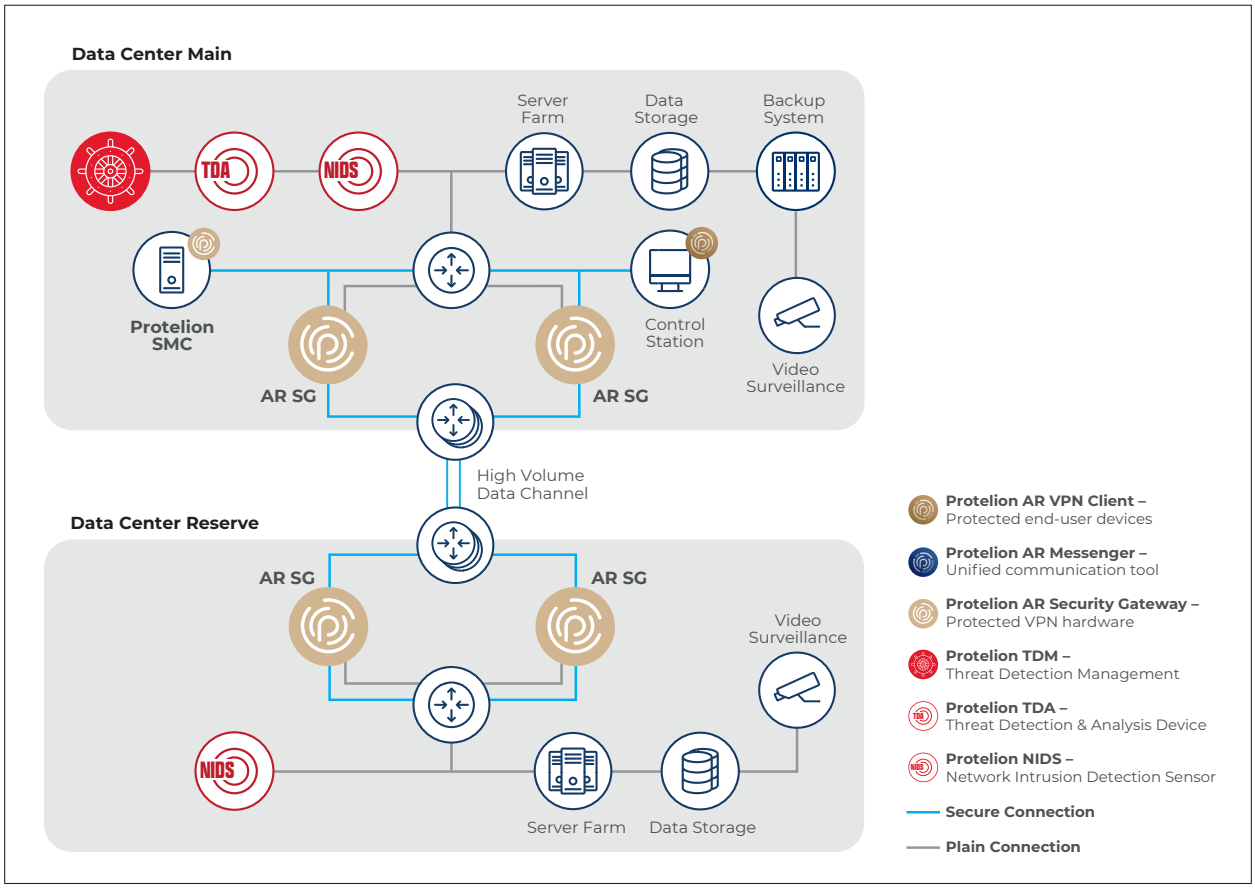
1 Protelion VPN Technology protects data centers and their IP networks from unauthorized access to data servers and critical assets and when accessed via remote connections. All data is highly secured and can be transmitted over common public channels. The implemented data encryption makes cyber attacks useless

2 IP VPN communication endpoint as well as central encryption devices are hardened and protected against various types of cyber threats such as malware, zero-day exploits, fileless attacks and malicious user behavior

3 Confidentiality and integrity of all stored, processed and transferred data between different data centers, server farms, computing centers and clouds are established as well as secure remote and direct access to and from data centers

4 The implemented Protelion TDR System provides in addition to its generic network monitoring also an increased visibility into the IT environment, allowing the authorized security administrators to identify vulnerabilities and security gaps that can be exploited by attackers and malicious software

Scheme for Data Centers



Protelion Features

Certified AES Algorithm
The implemented and certified Protelion encryption algorithm and the pre-shared symmetric key regime are designed to protect top secret and highly sensitive data and file transfers. Its security and performance features meet military grade standard and requirements

Comprehensive Protection
Protelion solutions offer comprehensive protection against a wide range of cyber threats, using advanced technologies to detect and respond in real-time and minimizing thereby the impact of cyber attacks

Operational Availability
Protelion Security Solutions provide protection and availability to IP-network infrastructures for data storage, data processing, secure remote access and monitoring sensors

Always on duty
Protelion VPN Communication Technology uses the principle of non-session connectivity, which allows the VPN services to work with acceptable performance even when connected via poor and unstable communication channels

PROTELION
Oberwallstrasse 24
D-10117 Berlin
+49 30 206 43 66-0
info@protelion.de
gov.protelion.com

GD – DKV23.1