PROTELION

Use Cases

Highly Secure Communication for Lawyers and Prosecutors

Larger law firms and prosecutors' offices that provide public defenders or prosecutors to citizens usually have hundreds of employees. Many of them work in different cities and regions of the country and need to be able to access the main offices' data centers remotely for their work and research. Remote employees of these organizations access corporate resources over the public Internet. It is therefore essential that this access to sensitive data such as personal data, histories, case and evidence data, etc. is done via protected Internet access. Protelion offers solutions that provide highly secure remote access to the organization's sensitive data and ensure that data theft, loss or even disclosure over public or private communication channels is prevented.

Duties and As-Is Situation for Law Companies and Prosecutors

Country or even worldwide communication and negotiations between courts, legal entities and their clients by phone, video and conference calls is part of the daily business and is intensively used

Big amount of critical data and documents are usually transferred, nationally and globally, unsecured between different law firm headquarters, their branches and other legal entities

Client databases, server data and archived court case data are the central elements of any law firm and prosecutors. Their protection from unauthorized access is paramount

Most IT devices for remote access to the corporate data infrastructure is excessively vulnerable, making them one of the most popular attack vectors for hackers

Project Specification

Employees work with sensitive data remotely on a variety of desktops, laptops and mobile devices. All this confidential business data is transmitted over unprotected channels and needs to be protected

Data leakage and theft within companies is common since hosts are unprotected even in the local network and open for malicious party access to sensitive data, stored or when transmitted. These internal or external cyber attacks have to be prevented

Especially security systems have to be maintained and updated regularly to deliver the highest possible performance and safety. Therefore, controlled and secured update and actualization procedures need to be implemented

Project Implementation

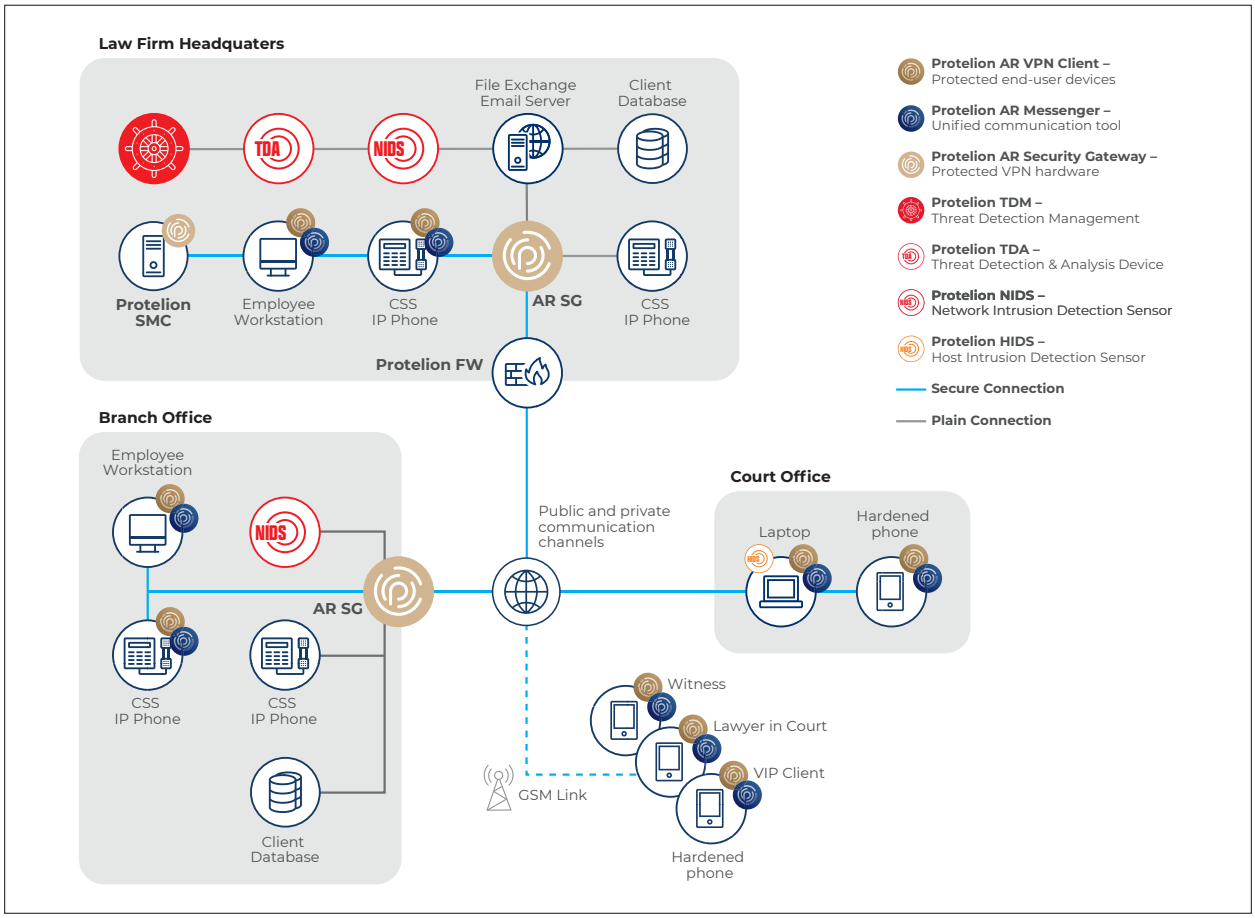
1 The deployed Security Solutions from Protelion enable multiple and discrete IT-environments of different law firms, their branches and other legal entities to be securely interconnected and protect therefore critical data from eavesdropping, theft and alteration

2 The Protelion's Security Solutions have been deployed on customer's endpoint devices, enabling securely encrypted voice and video calls, chat, email and file exchange over unsecure channels between different legal entities and their clients

3 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 and prevent vulnerabilities and security gaps that can be exploited by attackers and malicious software

4 The implementation of Protelion Security Solutions in the customer's network ensures secure access, in particular remote access, secure processing and storage of all data and brings the existing infrastructure into compliance with regulatory requirements

Scheme for Lawyers and Prosecutors



Protelion Features

Comprehensive Protection
Protelion Security 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

Customizable Solutions
High flexibility, interoperability and scalability of the Protelion Security Technology make it easy for each individual customer to create an optimal solution on top of its existing IT infrastructure

Endpoint Protection
All-in-one solution to secure endpoint devices from zero day exploits, unknown malware, ransomware, DDoS attacks and internal or external threats such as data theft, loss and alteration

Operation Security
Secured and efficient workflows for office and remote employees. Guaranteed integrity and privacy for court, process and client data through quantum computing resistant encryption while complying with today's data protection regulations

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

GD – DKV23.1