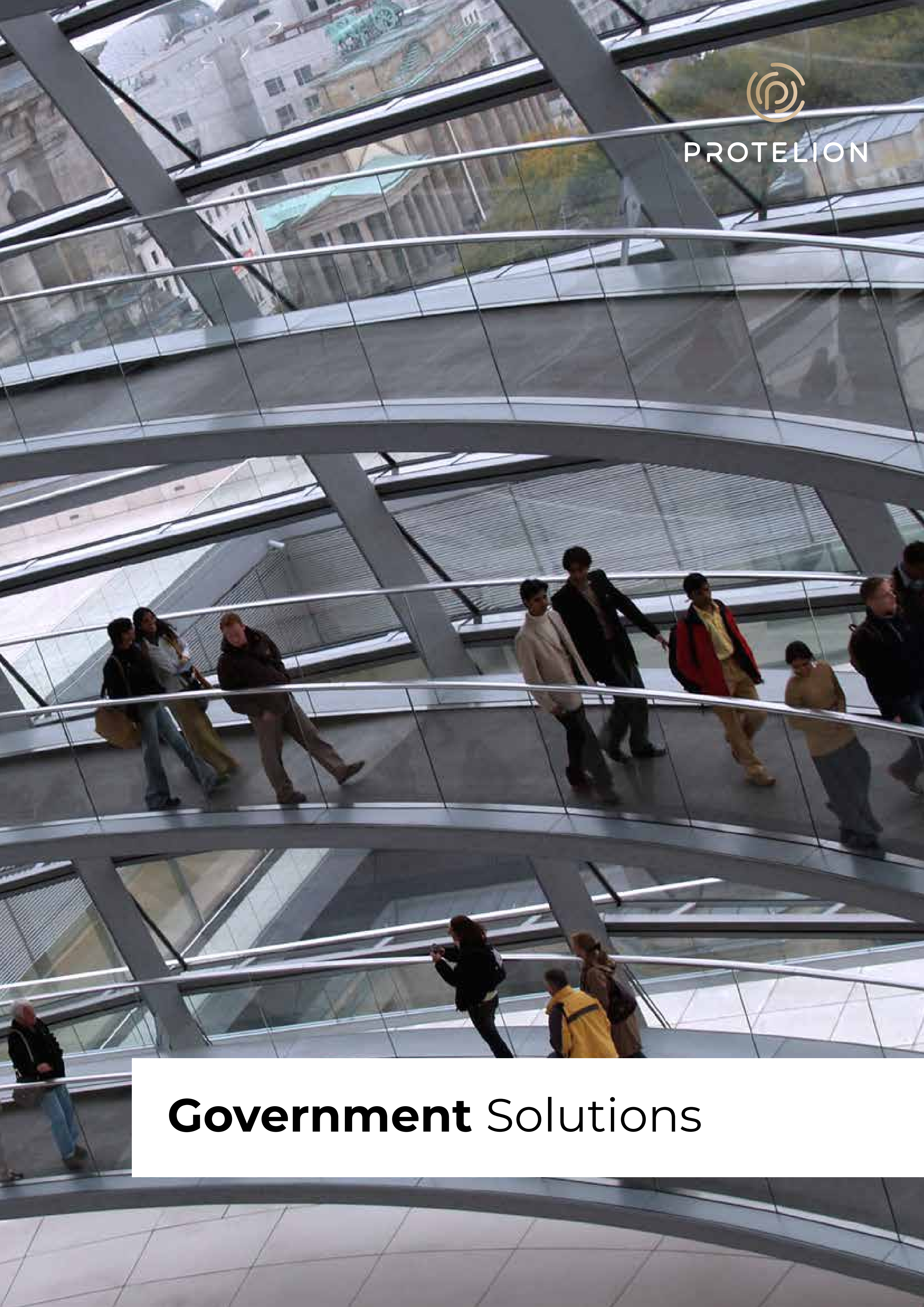
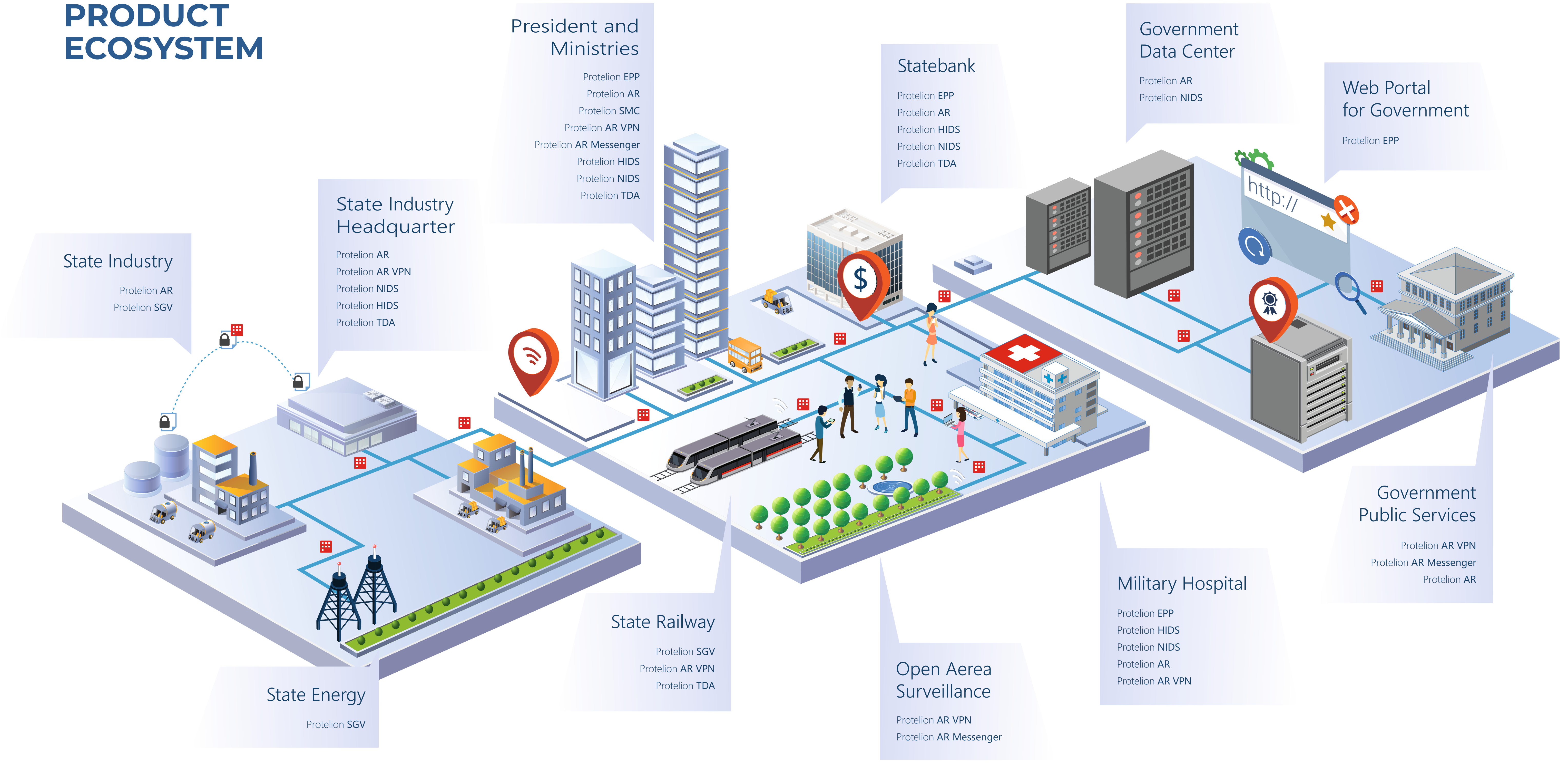


PROTELION

Government Solutions

PRODUCT ECOSYSTEM



State Industry

Protelion AR
Protelion SGV

State Industry Headquarter

Protelion AR
Protelion AR VPN
Protelion NIDS
Protelion HIDS
Protelion TDA

President and Ministries

Protelion EPP
Protelion AR
Protelion SMC
Protelion AR VPN
Protelion AR Messenger
Protelion HIDS
Protelion NIDS
Protelion TDA

Statebank

Protelion EPP
Protelion AR
Protelion HIDS
Protelion NIDS
Protelion TDA

Government Data Center

Protelion AR
Protelion NIDS

Web Portal for Government

Protelion EPP

State Energy

Protelion SGV

State Railway

Protelion SGV
Protelion AR VPN
Protelion TDA

Open Aerea Surveillance

Protelion AR VPN
Protelion AR Messenger

Military Hospital

Protelion EPP
Protelion HIDS
Protelion NIDS
Protelion AR
Protelion AR VPN

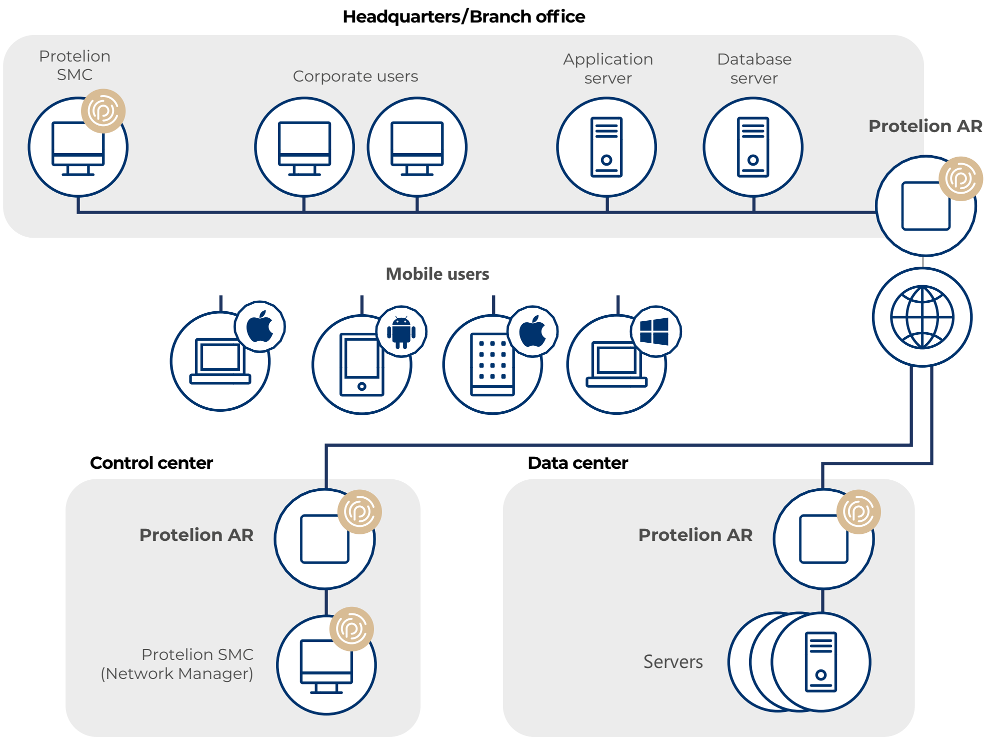
Government Public Services

Protelion AR VPN
Protelion AR Messenger
Protelion AR

CONTENT

Channel Protection

Protelion Data Channel Protection is a comprehensive solution for creating a trusted environment to enable restricted access to allow the transfer of information via public and private channels (wired and wireless communication lines). This is accomplished by organizing a centrally managed virtual private network (VPN).



SOLUTION FOR GOVERNMENT

- Protelion Security Technology solutions can be supplied as a holistic suite or as modules. Installation and configuration do not require the purchase of additional specialized equipment and can be carried out within the customer's existing IT infrastructure
- High flexibility and scalability of Protelion Security Technology make it easy to create an optimal solution for each individual customer
- High level military grade certified encryption algorithm implemented to protect top secret data and voice communication

Protelion Data Channel Protection is a unique solution that provides a set of software and computer appliance products designed to solve a wide range of information security tasks such as:

- Communication channel protection between different government organizations and their affiliated offices
- Protection of multi-data networks (voip, video conferencing)
- Secure remote access to corporate data centers and the cloud environment
- Infrastructure protection for electronic document management
- And more

Technology & functionality

- 256-bit symmetric keys at speeds up to 6.0 Gb/s traffic encryption
- Secure remote client-to-site and client-to-client connections to corporate resources and services over encrypted channels
- Split tunneling allows a user to access dissimilar security domains like a public network and LAN at the same time, using the same or different network connections. It frees the user from having to repeatedly connect and disconnect to use both networks
- Integrated Key Management System as a part of SMC, which scale to support thousands of host
- Protelion VPN Technology Components support all the services that modern IP networks offer and are indifferent to the kind of physical communication channels used to transport the data, like optical fibers, microwave, or satellite links
- Provides NAT-Translation that establishes and maintains Internet protocol connections across gateways that implement NAT. It requires many network applications, such as peer-to-peer file sharing and voice over IP (H.323, SCCP, and others)

Main components

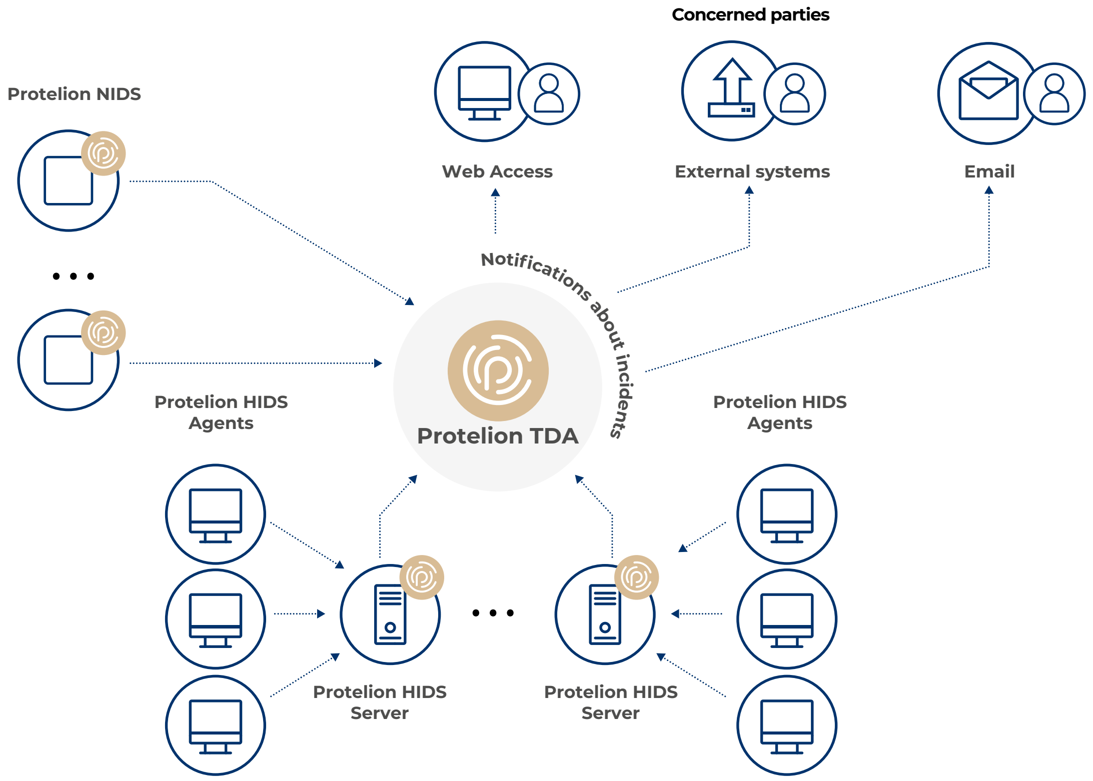
Administrative components	Server components	Client components
Protelion SMC – Security Management Center to manage Protelion products in an all-in-one scalable device	**Protelion AR –** Hardware VPN encryption device (different throughput values available)	**Protelion AR VPN –** Basic VPN client applience. Available for Windows, MacOS and Linux
Protelion SMC – Administrative tool to create Protelion network topology and generate secret keys	**Protelion SGV –** Encryption applience for deploying on a virtualization and Cloud platforms	**Protelion AR VPN** (Mobile) **–** Basic VPN client applience for Android and Apple mobile devices
Protelion SMC – Administrative tool to manage Protelion network security policies centrally	**Protelion SG RPi –** Secure encryption solution, running on a additionally protected Raspberry Pi platform	

Key benefits

- Peer to peer connection technology makes it possible to build secure channels between two network nodes without using a server
- Protelion communication technology uses the principle of non-session connectivity, which is an important feature when connecting via poor and unstable communication channels. This feature means that a user does not need to transfer the payloads in an encrypted channel session. Data transfer starts immediately when the first IP packet is received
- Protelion communication technology employs separate open and encrypted traffic filtering algorithms. This makes it possible to apply security policies not only to open, but also to secure hosts enabling an increased information system security level
- Built-in firewall, application network activity monitoring system and ability to integrate with external firewalls
- Interworking support allows the creation of hierarchical systems and the establishment of secure communication channels between an arbitrary number of secure networks built with the Protelion communication technology
- Modern multi-service communication networks data protection (IP telephony, audio and video conferencing services). Traffic prioritization and application processing of H.323, Skinny, SIP and other protocols
- Equally suited for traditional enterprise networks as well as Cloud, Mobile, Industrial and IoT deployments

Threat Detection and Response

Fast and reliable detection of IT security incidents – even in the most complex scenarios.



How does it work?

- Based on the analysis of network traffic and events on end devices, all Protelion IDS sensors capture security events and send relevant data to the Protelion TDA
- The Protelion TDA accumulates event data collected from the sensors, normalizes the data and saves it to the database
- The Protelion TDA uses meta rules and a learned mathematical decision making model to analyze all incoming events, detecting the relevant threats most likely to be security incidents
- When the Protelion TDA suspects an incident, it behaves as follows:
    - Registers this fact in the incident details section
    - Identifies all the events related to the incident and adds them to the incident details
    - Notifies the concerned parties about the suspected incident by email
    - Provides tools and methods to investigate the incident
- The information security expert investigates the detected incidents
- The information security expert either confirms the incident or considers it a false positive
- When confirmed, the incident data is sent to external systems
- The information security expert mitigates the incident impact and prevents the incident related threats according to recommendations displayed in the incident details

Features and Components

Protelion TDA – computer appliance for information security events analysis, automatic information security incidents detection and conducting investigations on identified incidents

Protelion TDM – centralized control and monitoring of sensors. Provides the ability to manage all components of the solution

Protelion NIDS – network attacks and malware traffic detection facility. NIDS and HIDS solutions can be combined into a single Intrusion Detection and Threat Prevention System

Protelion HIDS – Host based intrusion detection system. Enhances the security of information systems, data centers, client computers, servers and communication equipment

Key benefits

- Reducing the average time of incident detection from 30 to 2 minutes when compared to a manual analysis by a qualified expert
- Reducing the cost of operating an intrusion detection system by reducing the burden on personnel and the requirements for their qualifications
- Simplify the response to information security threats using automatically generated recommendations and collection of incident related events

Firewalls

The Protelion FW – a next-generation security gateways. Placed on the network border, the Protelion FW provides traffic filtering at all network levels and supports the creation of granular security policies based on user accounts and application list.

Features and Components

Firewall

- Stateful firewall with session control
- NAT/PAT Address Translation
- Anti-spoofing protection
- Supports Protelion TDA

Proxy server

- HTTP and FTP support
- Checking and filtering traffic by MIME type and by HTTP request method type
- Traffic checking by third-party antivirus, connected via the ICAP protocol
- Integration with directory

Microsoft AD

- Captive Portal with LDAP
- Network Functions

Failover & redundancy

- Hot Standby cluster
- UPS Support

Application layer firewall with DPI (Deep Packet Inspection)

Allows to Identify and block more than 2000 application protocols and applications as:

- Games
- Social networks
- Instant messaging services
- Video Broadcasts
- P2P, torrent services
- File Hosting
- Tunneling, VPN
- Remote control
- Industrial Protocols

Advanced static routing

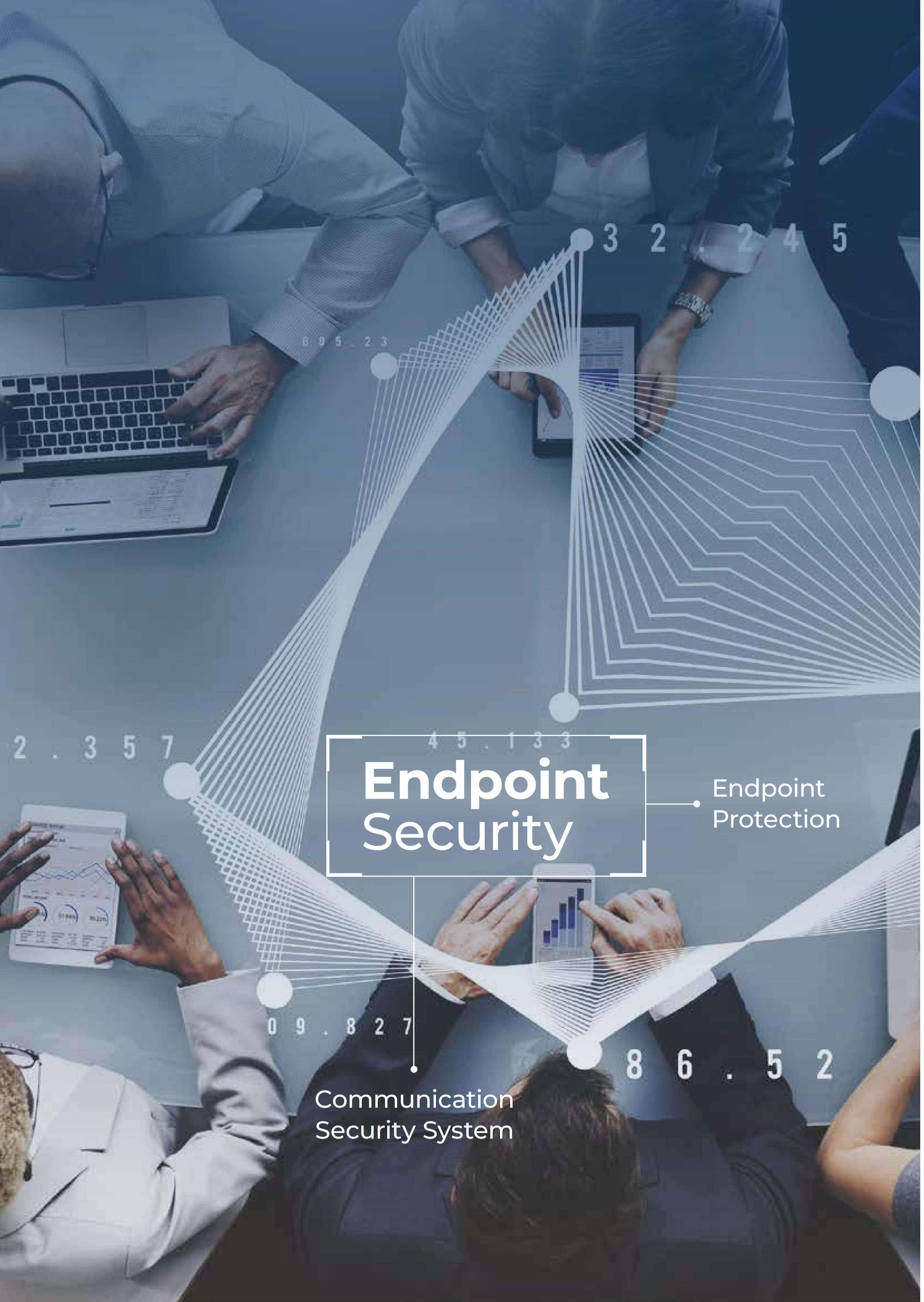
- Dynamic Routing
- VLAN support (dot1q)
- Link Aggregation (bonding LACP, EtherChannel)
- QoS, ToS, DiffServ support

Service functions

- DNS server
- NTP Server
- DHCP server
- DHCP -Relay

Key benefits

- Granulated security policies
- Ensuring the safe use of personal devices for work purposes within full compliance of the company's security policies – BYOD (Bring Your Own Device)
- Identify and block more than 2000 application protocols and applications like games, social networks, torrents, etc.
- Reducing the cost of Internet traffic consumption
- Minimizing the attack surface



Endpoint Security

Endpoint Protection

Communication Security System

Endpoint Protection

All-in-one solution to secure endpoints from zero-day exploits, unknown malware and internal or external threats. Protelion Endpoint Protection provides high level security for desktop computers and laptops.

Components

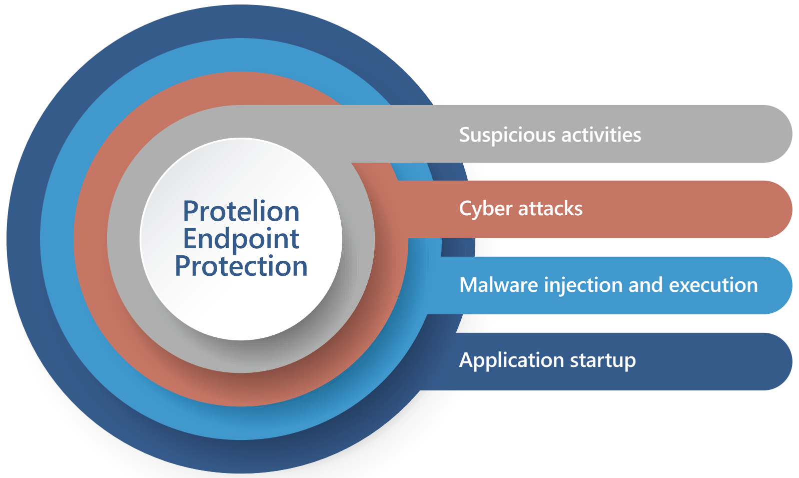
Intrusion Detection & Prevention –
protects computers from unidentified attacks and suspicious behavior

Personal Firewall –
network traffic filtering according to the predefined pack of filters

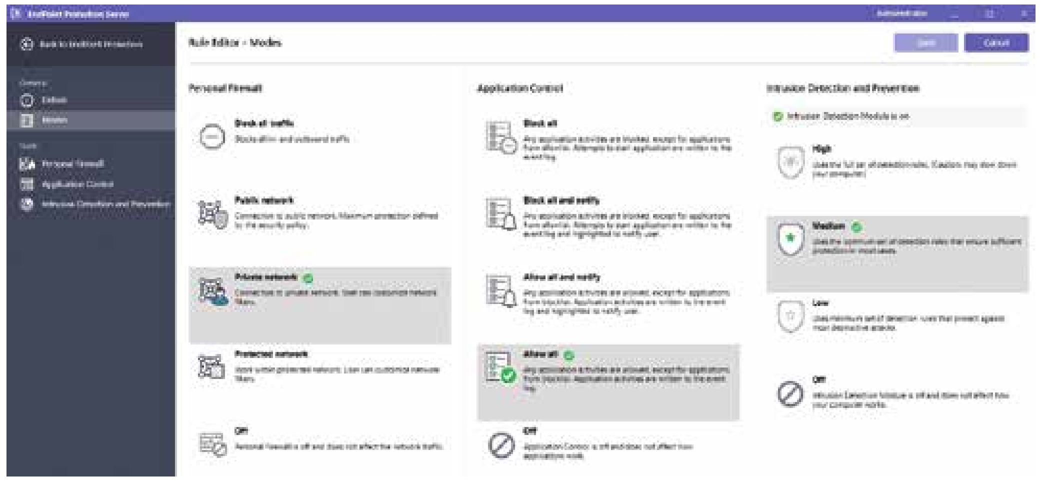
The Antimalware Module –
is a heuristic engine that uses a proprietary Malware Detection Module powered by machine learning

Application Control –
based on Allow list and Block list. Prevents unknown and unwanted applications from executing, accessing registry, processes, and command line. Blocks malware setup and startup

The Behavioral Analytics Module –
detects various anomalies in user activities and operating system behavior (running system utilities, tasks, processes, etc.)


Protelion Endpoint Protection
Suspicious activities
Cyber attacks
Malware injection and execution
Application startup

Predefined security patterns


Endpoint Protection Server
Administration
Back to Endpoint Protection
Save
Cancel
General
Defaults
Modes
Tools
Personal Firewall
Application Control
Intrusion Detection and Prevention

Rule Editor - Modes

Personal Firewall

Block all traffic
Blocks all in- and outbound traffic.

Public network
Connection to public network. Maximum protection defined by the security policy.

Private network ✓
Connection to private network. User can customize network filters.

Protected network
Work within protected network. User can customize network filters.

Off
Personal Firewall is off and does not affect the network traffic.

Application Control

Block all
Any application activities are blocked, except for applications from allowlist. Attempts to start application are written to the event log.

Block all and notify
Any application activities are blocked, except for applications from allowlist. Attempts to start application are written to the event log and highlighted to notify user.

Allow all and notify
Any application activities are allowed, except for applications from blocklist. Application activities are written to the event log and highlighted to notify user.

Allow all ✓
Any application activities are allowed, except for applications from blocklist. Application activities are written to the event log.

Off
Application Control is off and does not affect how applications work.

Intrusion Detection and Prevention

✓ Intrusion Detection Module is on

High
Uses the full set of detection rules. Caution: may slow down your computer.

Medium ✓
Uses the optimum set of detection rules that ensure sufficient protection in most cases.

Low
Uses minimum set of detection rules that protect against most destructive attacks.

Off
Intrusion Detection Module is off and does not affect how your computer works.

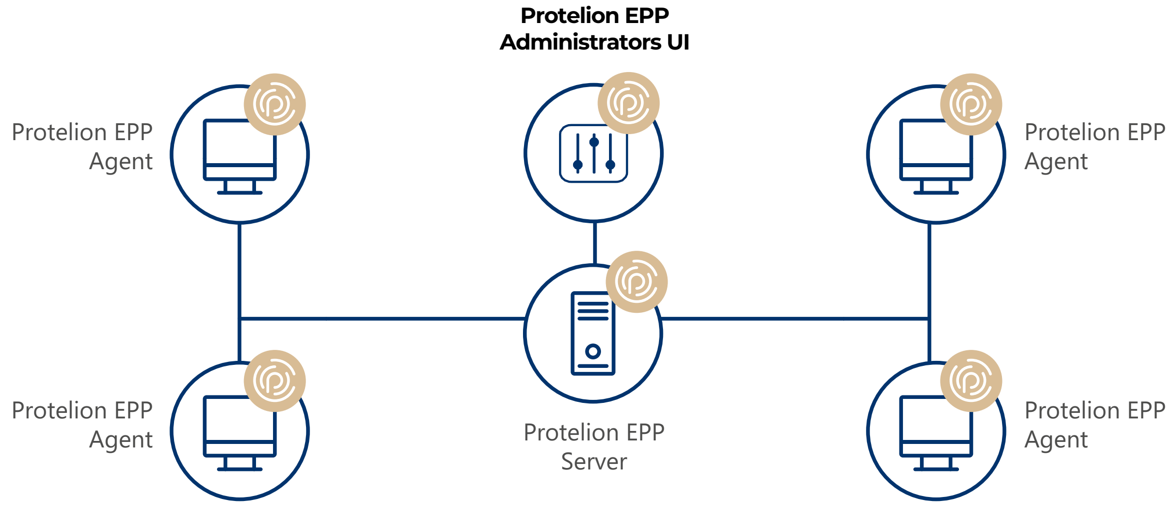
ARCHITECTURE

Protelion Endpoint Protection is a client-server software that comprises:

1 **Agent** installed on endpoints and servers to secure them from internal/external threats. Agent uses rule bases provided by the Server.

2 **Server** to manage agents for centralized rule bases and policies updates and log data collection.

3 **Administrators UI** to manage the Server and view the status of endpoints and server in real time.



Key benefits

- Monitors and blocks suspicious activities
- Secures endpoints and servers from known and unknown attacks
- Fine tuned security settings for all modules applied to both single and multiple hosts
- Predefined security patterns for all modules. Regularly updated signature bases
- Compatibility with Protelion TDA that enhances incident detection and response
- Protection from potentially unwanted applications
- Preventing malicious behaviors of applications, like a weaponized Office document that activates bad script or installs another application and runs it
- The Endpoint Detection and Response technologies, such as a host's suspicious activity, monitoring and counteracting
- Detecting and deleting malicious executables, as well as detecting and blocking fileless attacks
- Proprietary Behavioral Analysis technologies

Features

HIDS/HIPS (Host Intrusion Detection / Prevention System)
Detects and prevents attacks using signature and heuristic method.

Key areas for monitoring:
- Windows event log
- Application logs
- Command execution
- Files, folders, Windows registry
- Network traffic

Detects and prevents suspicious activities and blocks attacks based on rules and attack severity.

Personal firewall
Protects endpoints by controlling inbound and outbound traffic, uses policies to protect system from unauthorized access.

Key features:
- IPv4/IPv6 filtering
- Filter scheduling
- Predefined filters
- Blocks attacking hosts
- Network activity monitoring

Security Notifications
Notifies you about critical attacks by sending CEF messages over syslog and by email. All events and attacks are displayed in the UI.

Application Control
Application control enables an additional level of host protection against malware and targeted attacks by preventing unknown and unwanted applications from executing.

Prevents unwanted applications from accessing:
- Files
- Registry
- Processes
- Command line
- Applications Allow/Blocklists

Manage all Agents centrally
Manage all Agents, distribute policies and rule based updates from a single point.

Communication with Protelion TDA
Protelion Endpoint Protection can transfer all events to Protelion TDA, the SIEM system, and thus detect complex and unknown attacks due to mathematical model and metarules implemented in Protelion TDA. When an incident is detected, you can respond immediately and by batch adjust security settings on all hosts added to Protelion Endpoint.

Antimalware module
Detects malware signs in executables through AntiMalware scanning and blocks dangerous files.

Behavioral analytics module
Uses a protected host's normal activity model powered by machine learning.

Detects various anomalies:
- Abnormal logon to the system
- Abnormal process creation
- Abnormal scheduler task creation
- Abnormal startups of the system utilities
- Etc.

Supported operating systems
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 11
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Debian 11

Encrypted Communication

Secure mobile communication has become central to our lives. Voice and information are exchanged on an enormous scale. No type of communication is more vulnerable to interception than mobile communication. Worldwide, immense sums of money and effort are invested in order to get hold of the transmitted communication, data or information. Highly efficient trojans and spyware are wreaking mischief on supposedly well-secured mobile communication devices such as smartphones and laptops.

Communication Security System Applications for State Authorities

The CSS solution provides high eavesdropping resilience and state of the art encryption, that allows presidents, ministers and executives as well as security forces to make calls and exchange data anywhere easily and securely. This solution uses in particular specially hardened and malware proof mobile phones. These phones are hardened, pre-installed and delivered directly to the customer by Protelion.

The Protelion CSS Applications allow more over to comply with the **General Data Protection Regulation (GDPR)** and offer a highly secure replacement for WhatsApp, Viber, Signal, etc. which may no longer be used in companies that maintain customer data or customer relationships.

Protelion Security Technology

The Protelion Security Technology is based on a symmetric AES 256 encryption algorithm and offers beyond that various additional advantages.

True Point-to-Point VPN Connection
The technology features the ability to create true point-to-point VPN connections and provides therefore the capability to transmit IP packets from one end point to another directly without intermediary servers.

All communication passes through secure channels, even in the local network (LAN). It guarantees that neither internal nor external adversaries can ever eavesdrop the traffic.

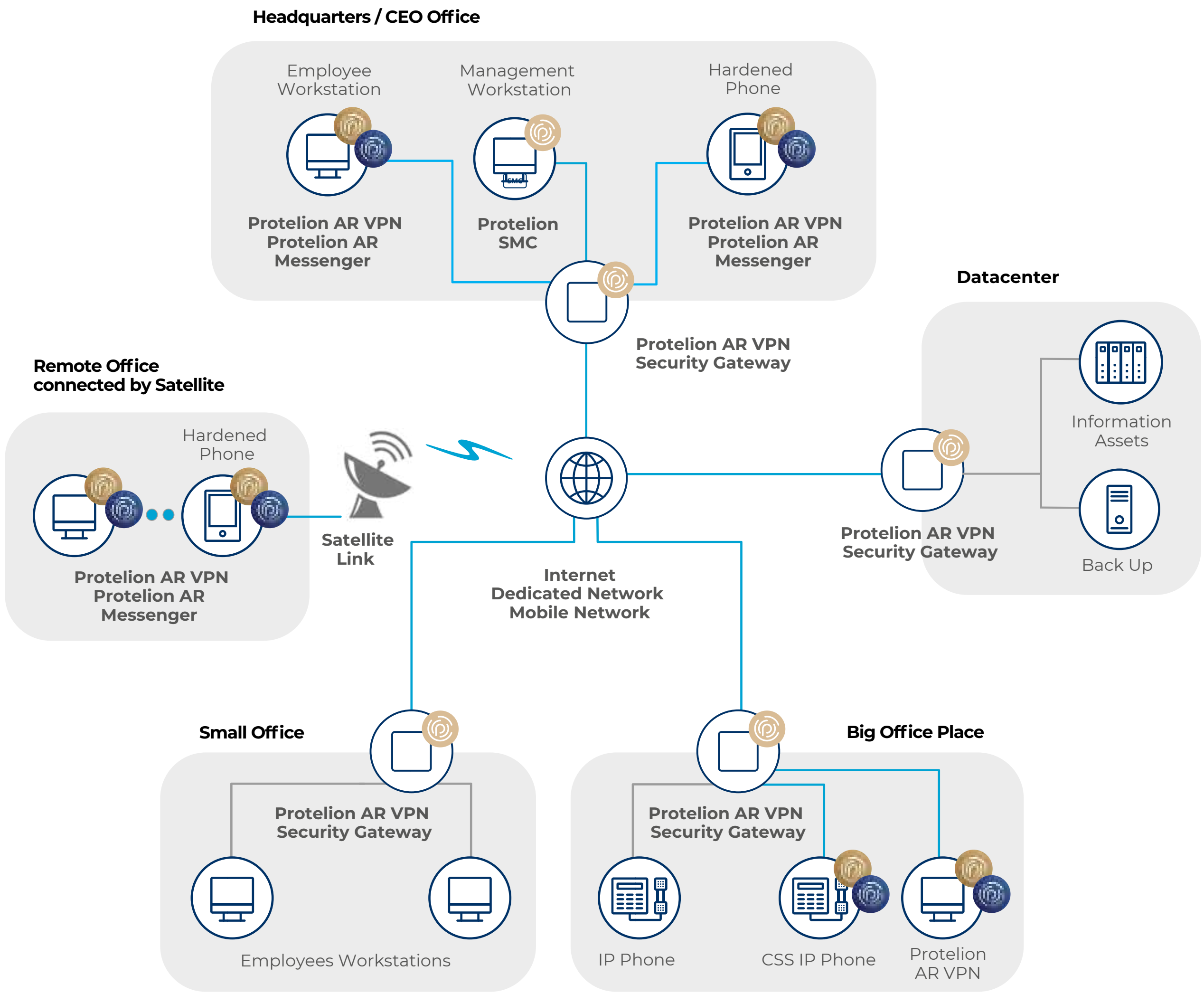
VPN without sessions
The Protelion AR VPN is a non-sessional VPN. This feature allows the VPN services to work with acceptable performance even through bad quality channels since there is no need for handshakes with servers to transmit data. The first IP packet already contains payload.

Customers can also change or move between channels/antennas and mobile providers without interruptions.

Protelion Communication Security System (CSS)

The **Protelion AR VPN Technology** protects user devices against internal and external attacks and provides secure access to corporate resources over the Internet and LAN networks by deploying a virtual private network (VPN). It supports all modern IP services and any kind of physical communication channels (optical fibers, microwave or satellite links).

Protelion Communication Security System Scenario


Headquarters / CEO Office
Employee Workstation
Management Workstation
Hardened Phone
Protelion AR VPN Protelion AR Messenger
Protelion SMC
Protelion AR VPN Protelion AR Messenger
Protelion AR VPN Security Gateway
Datacenter
Information Assets
Back Up
Protelion AR VPN Security Gateway
Remote Office connected by Satellite
Hardened Phone
Protelion AR VPN Protelion AR Messenger
Satellite Link
Internet Dedicated Network Mobile Network
Small Office
Protelion AR VPN Security Gateway
Employees Workstations
Big Office Place
Protelion AR VPN Security Gateway
IP Phone
CSS IP Phone
Protelion AR VPN

Protelion AR VPN Client – Protect user devices against intruders

Protelion AR Messenger – Unified communication tool

Protelion AR Mobile – Encrypted communication solution with protected and hardened cell phones

Protelion SMC – Secure key and network management center

Protelion AR Security Gateway Protected VPN hardware

Secure Connection

Plain Connection

Protelion AR Messenger

The Protelion AR Messenger is an alternative to unsafe public messenger applications and allows users to communicate securely and easily due to its implemented Protelion Security Technology.

Customers can install the Android Package Files (APKs), Protelion AR Messenger and Protelion AR VPN Client, on their devices running under Android, Windows and Linux.

Protelion AR Messenger on CSS IP Phones

The Protelion CSS IP Phone is compatible with various enterprise SIP servers and ensures communication confidentiality due to preimplemented Protelion AR VPN and Protelion AR Messenger Applications.

Protelion AR Messenger on Notebooks and Desktops

The Protelion AR Messenger Application converts laptops or desktop computers in a fully integrated and protected part of the client's secured communication system.

Protelion AR VPN Client **Protelion AR Messenger**

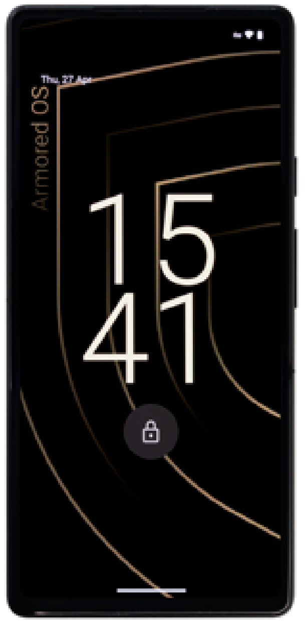
Protelion AR Messenger on Mobile Phones

The Protelion AR Messenger allows employees to securely communicate by voice calls, video calls, chat-messages and supports file exchange.

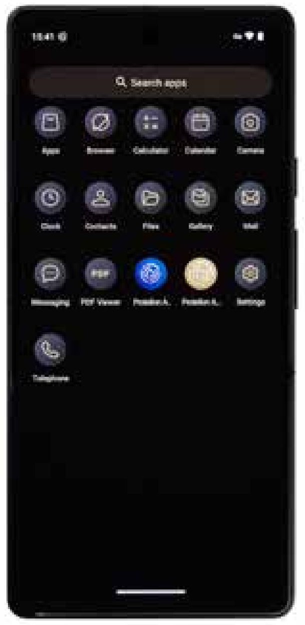
The application can be installed manually on any private Android phone.

Protelion Hardened AR Mobile Phone

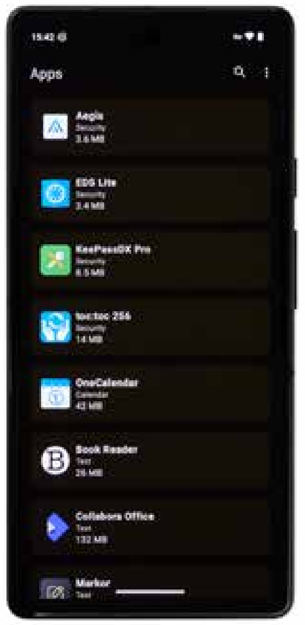
The Protelion AR Mobile Security Solution is the answer to government's need for secure and reliable mobile communication. The solution provides highly protected communication capabilities with secure and verified content.



Protelion AR Mobile
Main screen of Protelion AR Mobile Phone



Protelion Standard Applications
Lists of available applications for users



Protelion Proprietary AppStore
The AppStore offers verified applications to download by the users

SERVICES BLOCKED ON THE PROTELION AR MOBILE

- Protelion fixes, in agreement with the customer, a list of restrictions and preinstalled applications
- It restricts access to the Google Play Market App-Store
- It blocks the installation of not verified and signed applications on the device
- It offers a Kernel Level Firewall
- It prohibits the possibility of flashing the device or accessing the operation system Bootloader
- It provides Bootloader Locking, which prevents installation of modified Recovery Partition and reflashing
- It denies any connection bypassing VPN
- It denies the ability to reset the device to factory settings
- It prohibits any uncontrolled updating of the operation system version
- It blocks GSM services. All communication is conducted only through protected IP VPN channels

Protelion SMC

The Security Management Center – Protelion SMC is an all-in-one management platform that serves to manage and control different Protelion products and solutions.

It supports web graphic user interfaces and allows to:

- Facilitate Protelion security products deployment, management, key generation/delivery and license management
- Distribute/Manage licenses for Protelion products to organizations

- Divide Protelion AR Messenger users into groups depending on their profile by establish specific links between them
- Manage Protelion networks for each organization, user accounts, devices etc.
- Manage the AR Messenger Address Book in the Protelion SMC platform. Any alteration can only be done, internally or remotely, by the organization's assigned security administrator

Protelion SMC –
On-premise or Cloud based

Protelion SMC can be deployed On-Premise, Remote in a secure environment (Bunker) or in a Cloud. The latter options can be used for customer organizations that don't want to install any management components on their premises. In any case, customers will always be able to operate their management centers through highly secured remote access channels.

CSS KEY BENEFITS

- Protelion Communication Security System provides a highly secure protected communication system for everyday use by means of a military standard AES encryption
- Protelion Communication Security System users exchange encrypted traffic directly between devices (point-to-point)
- Protelion Communication Security System is made for voice- and video calls, group chat and file exchange
- Protelion Communication Security System is easy to use through a modern and intuitive UI design that requires no special skills from users
- Protelion Communication Security System contact list is created by the Protelion SMC centrally. It is isolated and protected
- Protelion Communication Security System is the ultimate mobile communication protection for government and business use

Cyber Range Platform

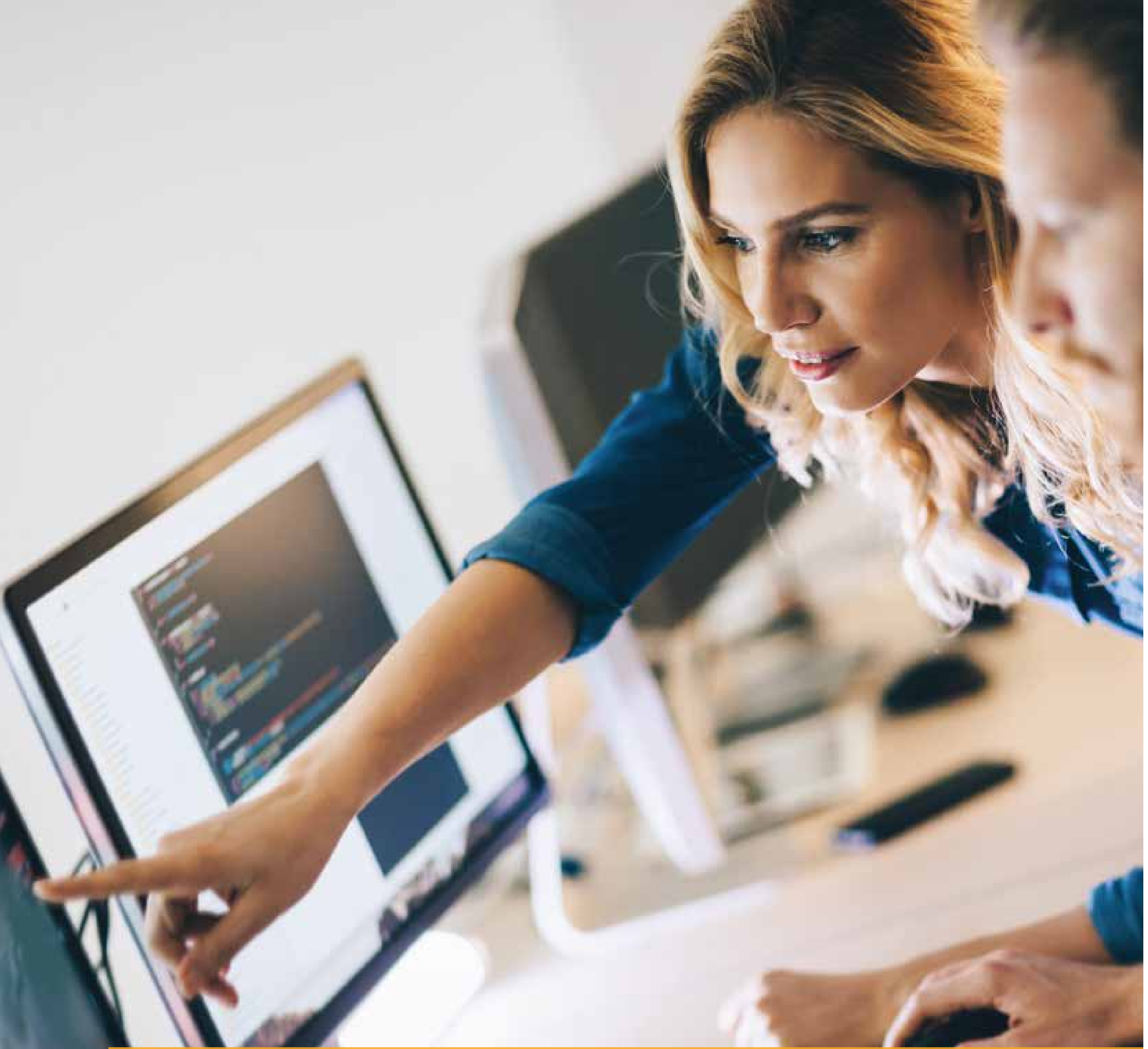
Protelion Cyber Range Platform – training and simulation platform enables organizations to provide training for cybersecurity and IT security specialists or students in the methods of detecting, investigating and responding to cyber-attacks. Participants work in a simulated hyper-realistic IT infrastructure to develop practical skills in investigating cybersecurity incidents, as well as hands on experience in implementing response measures to close gaps and vulnerabilities in their cyber defenses.

Challenge

The growth of digitalization has created a wealth of new possibilities as well as exponentially increased cyber risks. The dramatic shift to remote working in response to the Coronavirus has compounded the risk by exposing a host of new vulnerabilities.

Hacking is on the rise, yet conversely, there is a global shortage of cyber experts available to help organizations counter the threat. Furthermore, many information security and network security staff have insufficient hands on experience responding to and mitigating real cyber-attacks.

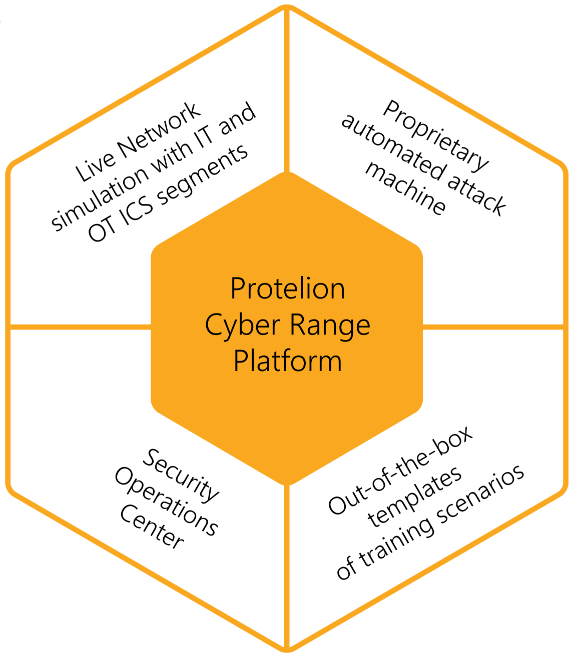
To bridge this gap in qualified cybersecurity expertise, smart companies are turning to immersive training in virtual environments to ensure their teams stay up to date. Cyber Range Platform allow teams to train in a simulated hyper-realistic environment and build practical hands on experience responding to real world attacks ensuring that you are able to defend your network when the time comes.

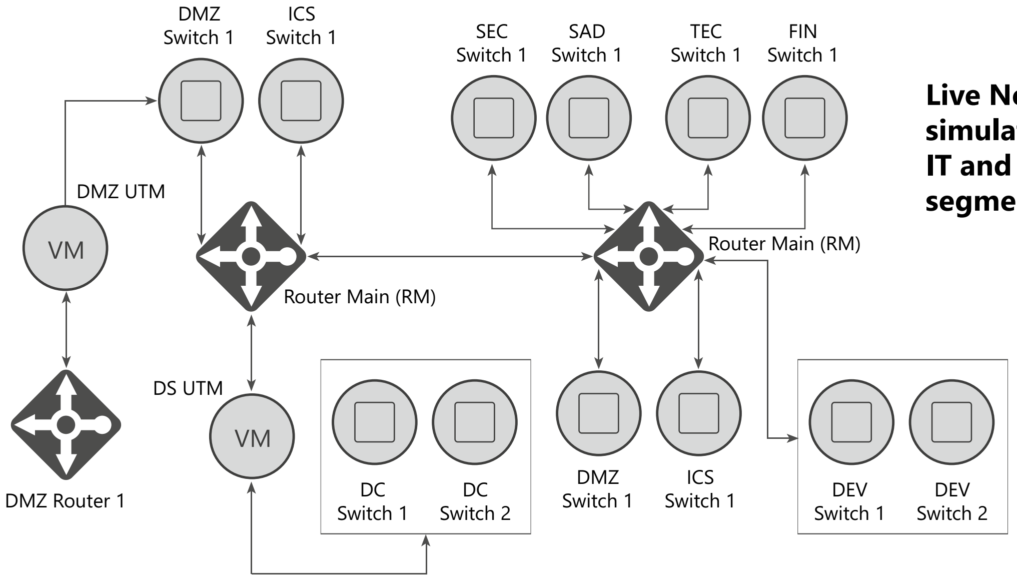


Protelion Cyber Range Platform Provides Flexible Components Continuously Improved to Keep Pace with New Methods and Tactics

- New templates and scenarios delivered on a regular basis
- Lessons include step-by-step guidance, hints and support
- All modules include hands-on simulation and practice
- Out of the box components to provide training for different skill levels from beginner to expert
- Practical, role-based learning
- On premise or cloud deployment model

Platform Architecture


Protelion Cyber Range Platform
Live Network simulation with IT and OT ICS segments
Proprietary automated attack machine
Security Operations Center
Out-of-the-box templates of training scenarios

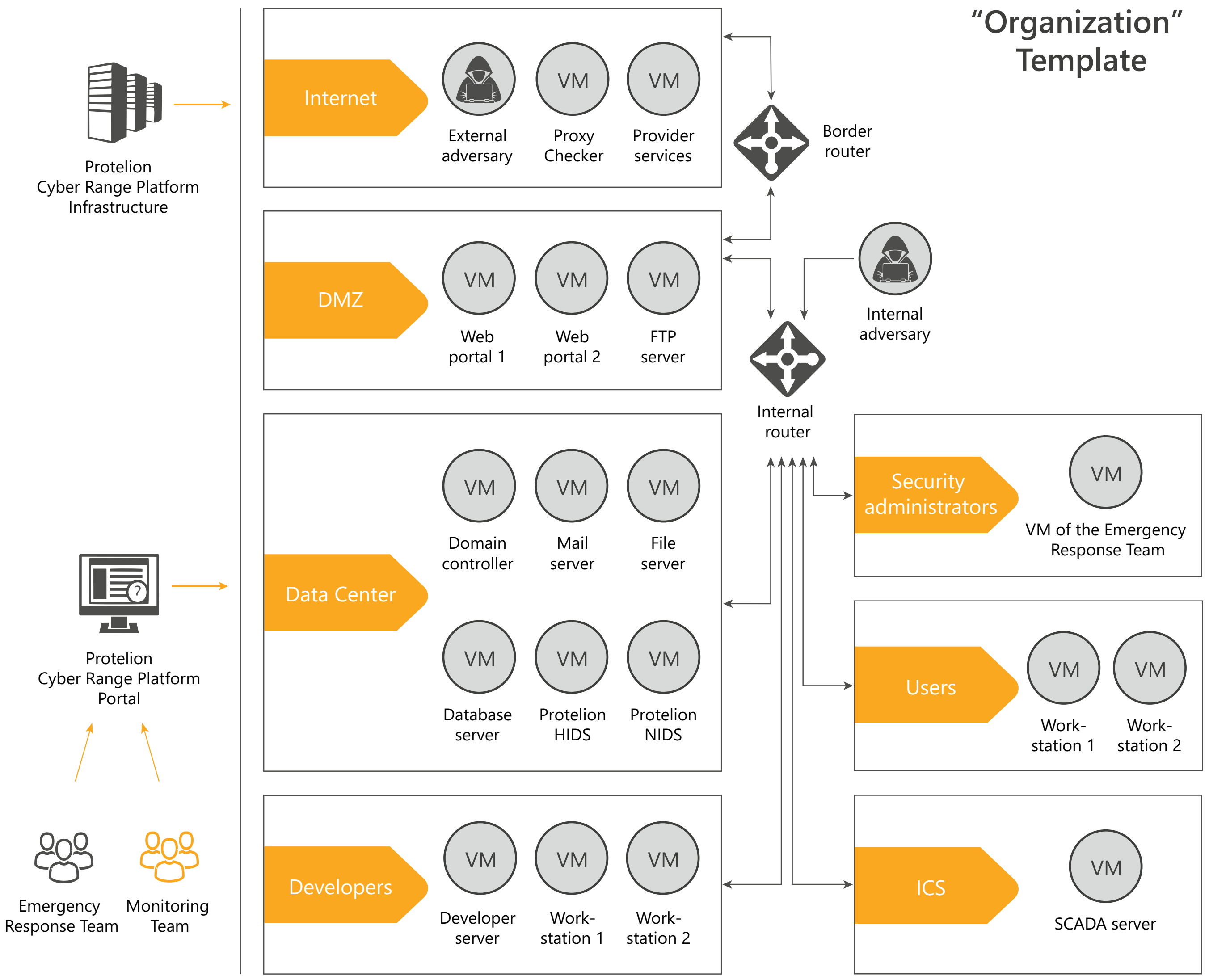


Live Network simulation with IT and OT ICS segments

Security Operations Center

Proprietary automated attack machine

Out-of-the-box templates of training scenarios



“Organization” Template

Developed by a team of international cyber experts with extensive experience in cyber defense, the highly configurable platform consists of components containing multiple templates and scenarios. The flexible component based architecture enables instructors to build a wide range of courses encompassing security operations, DevOps, Applications Security AppSec or ICS / OT that can be set for variable skill levels from basic to advanced. Implementing a Training Center using the Protelion Cyber Range Platform will not only improve your team’s overall threat detection and response effectiveness but will also help you to understand strengths, weaknesses, progress and skills development for individuals and the team as a whole.

Advantages

Configurable –
Easily develop your own customized courses for a variety of roles, skill levels and activities (workshops, training courses or certification tests)

Easy to Use –
Point-and-click to launch pre-built components, and the training is automatically evaluated

Flexible –
Use as a training platform, a simulation tool or a testbed. Simulate multiple environments in the same platform:
IT, OT, Medical devices, IIoT, etc.

Realistic –
Advanced attack scenarios designed by cyber experts based on real world incidents

Suitable for Use By

Government – CERT Teams, national SOCs, military cyber experts etc.

Education – universities, colleges, commercial training centers, etc.

Banks – testbed, SOC teams, information security specialists, decision makers

Enterprises – testbed, SOC teams, information security specialists, decision makers

MSSP (Managed Security Service Provider) **–** testbed, internal SOC team, training services for education, SMB, financial services

Contact us for demo of our live environment to experience how the Protelion Cyber Range Platform will help you:

- Increase Cyber Competence
- Improve Preparedness

PROTELION

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

Disclaimer. The information contained herein has been prepared solely for the purpose of providing general information about Protelion and its products. Protelion has taken care in the preparation of the content of these materials. Such information presented is believed to be reliable but is subject to change at any time without notice Protelion disclaims all warranties, express and implied, with respect to such content. Protelion does not represent that the information contained herein is accurate or comprehensive and shall accept no liability for the information contained herein or for any reliance placed by any person on the information. All brands and product names that are trademarks or registered trademarks are the property of their owners. The ™ and ® symbols are omitted in this document.