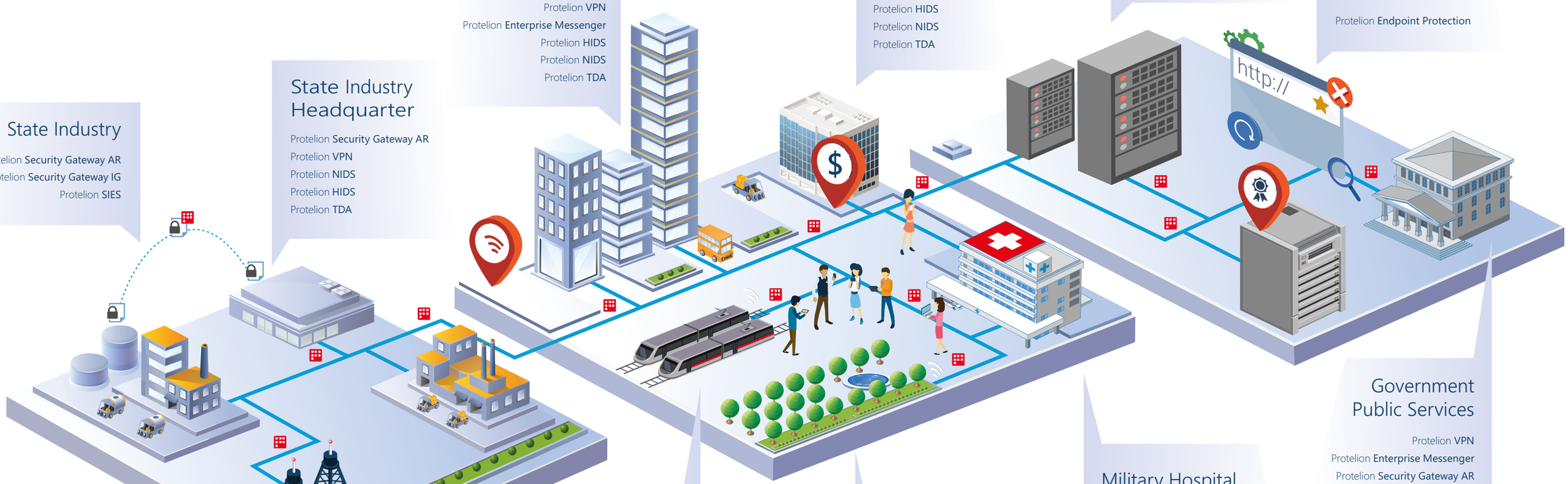
PROTELION
TECHNOLOGY MADE IN GERMANY

Government Solutions

PRODUCT ECOSYSTEM



President and Ministries

Protelion **Endpoint Protection**
Protelion **Security Gateway AR**
Protelion **SMC**
Protelion **VPN**
Protelion **Enterprise Messenger**
Protelion **HIDS**
Protelion **NIDS**
Protelion **TDA**

Statebank

Protelion **Endpoint Protection**
Protelion **Security Gateway AR**
Protelion **HIDS**
Protelion **NIDS**
Protelion **TDA**

Government Data Center

Protelion **Security Gateway AR**
Protelion **NIDS**

Web Portal for Government

Protelion **Endpoint Protection**

State Industry

Protelion **Security Gateway AR**
Protelion **Security Gateway IG**
Protelion **SIES**

State Industry Headquarter

Protelion **Security Gateway AR**
Protelion **VPN**
Protelion **NIDS**
Protelion **HIDS**
Protelion **TDA**

State Energy

Protelion **SIES**
Protelion **Security Gateway IG**

State Railway

Protelion **Security Gateway IG**
Protelion **VPN**
Protelion **SIES**
Protelion **TDA**

Open Aerea Surveillance

Protelion **VPN**
Protelion **Enterprise Messenger**

Military Hospital

Protelion **Endpoint Protection**
Protelion **HIDS**
Protelion **NIDS**
Protelion **Security Gateway AR**
Protelion **VPN**

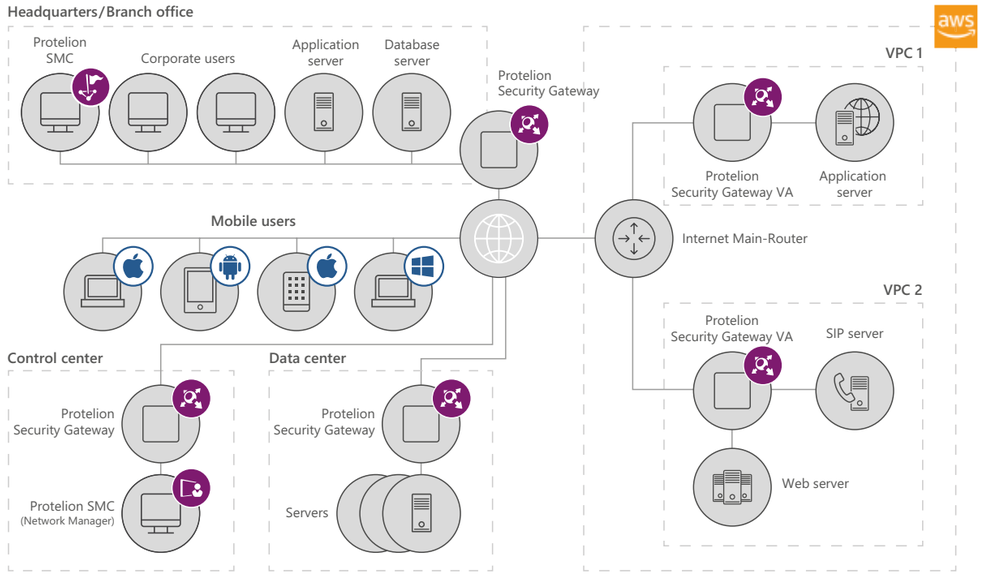
Government Public Services

Protelion **VPN**
Protelion **Enterprise Messenger**
Protelion **Security Gateway 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 BUSINESS

- 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 secrete 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 7.0 Gb/s traffic encryption
- Virtual addressing support to simplify user application configuration
- Separate unencrypted and encrypted traffic filtration to control the ability to work via unauthorized ports and protocols
- Facilitates the implementation of different scenarios of public key infrastructure (PKI) deployment
- Wide range of device types (Smartphones, Tablets, Laptops, Desktops) seamlessly connecting on different operating systems
- A variety of network hardware and software with dynamic or static network/port address translation (NAT/PAT) compatibility support
- Enables the integration of a multitude of applications and services to enable the user to work and communicate securely

Main components

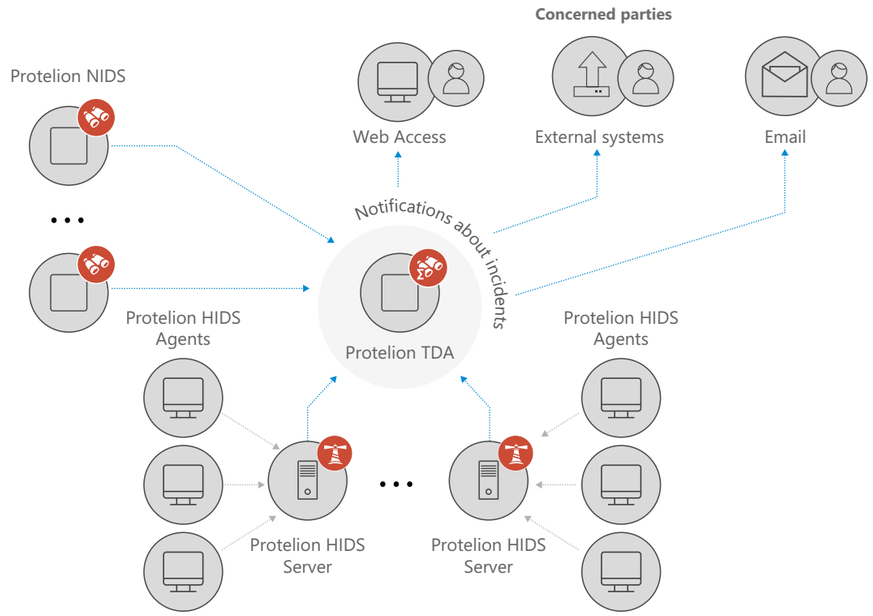
Administrative components	Server components	Client components
Protelion SMC – Security Management Center to manage Protelion products in an all-in-one scalable device	**Protelion Security Gateway AR –** Hardware VPN encryption device (different throughput values available)	**Protelion VPN –** Basic VPN client applience. Available for Windows, MacOS and Linux
Protelion SMC – Administrative tool to create Protelion network topology and generate secret keys	**Protelion Security Gateway VA –** Encryption applience for deploying on a virtualization and Cloud platforms	**Protelion VPN** (Mobile) **–** Basic VPN client applience for Android and Apple mobile devices
Protelion SMC – Administrative tool to manage Protelion network security policies centrally	**Protelion Security Gateway AR-RPi –** Secure encryption solution, running on a hardened 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
- Ready to deploy on Amazon Web Services. Functions at the cloud edge and provides secure access to resources in the Amazon Virtual Private Cloud, protecting them from attacks and unauthorized access

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

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

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

Protelion IDS HS – 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 AR Firewalls – a next-generation security gateways. Placed on the network border, the Protelion ARF 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)

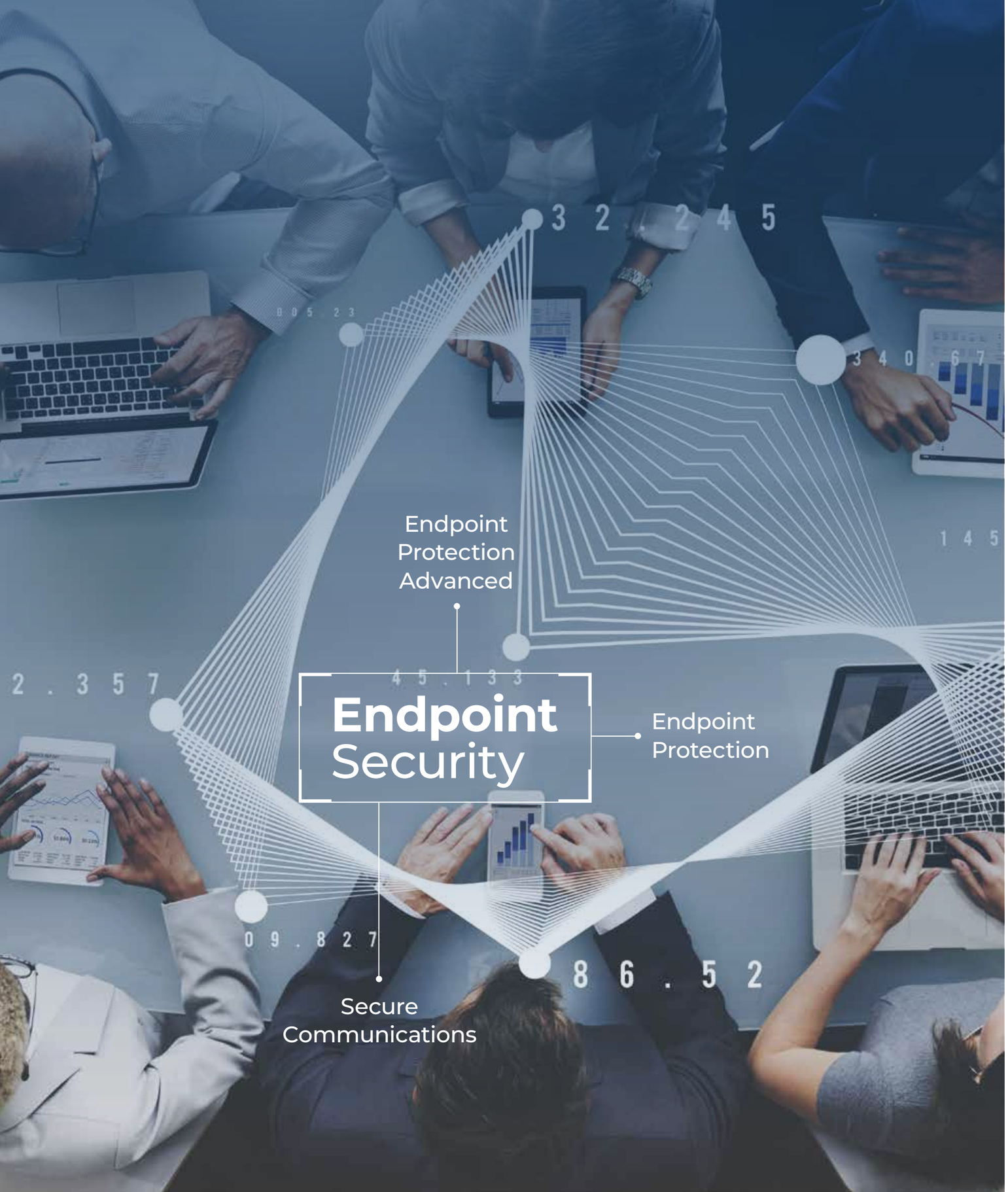
Allows to Identify and block more than 2000 application protocols and applications as:
- Games
- Social networks
- Instant messaging services
- Video Broadcasts
- P2P, torrent services
- File Hosting
- Tunneling, VPN
- Remote control
- Industrial Protocols

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



In today's world, all organizations are not only faced with the need to protect their workstations and servers. With the ascendance of mobile devices in the workplace, smartphones and tablets have actively entered companies' infrastructures, completely diffusing the traditional security perimeter. Defending this expanded threat surface is of utmost importance for companies' information security.

Endpoint Protection Advanced

Comprehensive information security system to protect from unauthorized access.

Protelion Endpoint Protection Advanced installed on work-stations and servers provides mandatory and discretionary differentiation of user access to critical information and connected devices. Realized discretionally (user to objects) and dividing (between users) access policies are based on automatic file layout and allow you to implement mechanisms of data protection against external and internal violators.

Key benefits

- Protection from intrusion and execution of malicious programs
- Protection against attacks to increase privileges
- Protection from insiders
- Protecting data from attacks on system software vulnerabilities
- Protecting data from attacks on application software vulnerabilities

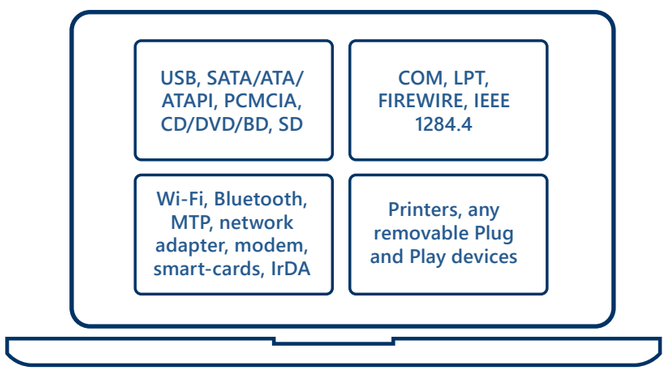
Data protection & Access Control

Discretionary
- File system
- HDD
- Registry
- Printers
- Services
- Devices
- Clipboard

Mandatory
- Files
- Folders

Features

- Access control
- Data protection
- Application Whitelisting
- Protected Software environment
- Device Control
- Data Integrity Control
- Separating roles of IT-Administrator and Security Administrator



Device control

- Mounting and unmounting control
- Event monitoring

Endpoint Protection

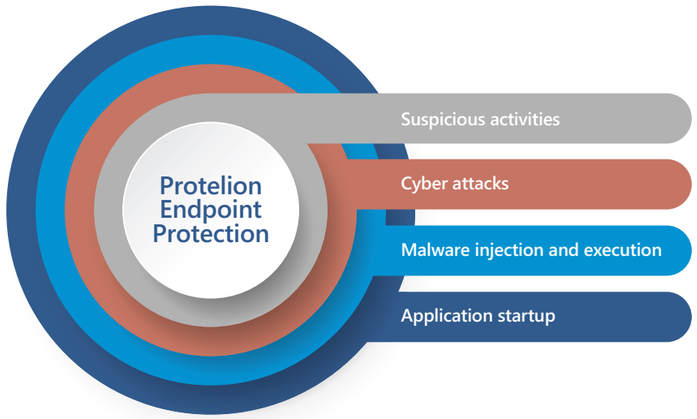
All-in-one solution to secure endpoints from zero-day exploits, unknown malware and internal or external threats. Protelion Endpoint Protection provides high level security for desktop computers and laptops.

Components

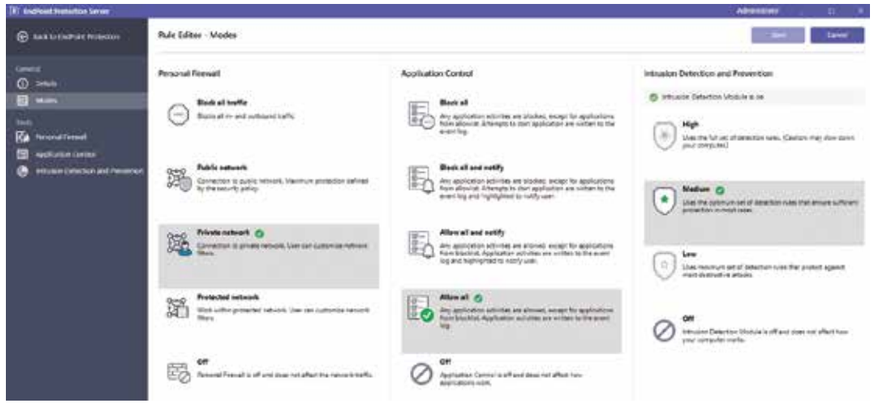
Intrusion detection & prevention – protects computers from unidentified attacks and suspicious behavior

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

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



Predefined security patterns



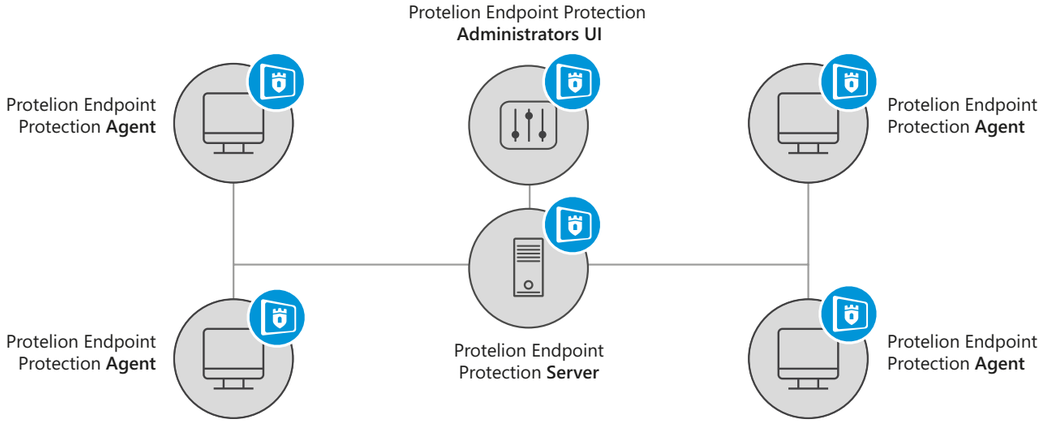
ARCHITECTURE

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

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 Protection.

Supported operating systems

- Microsoft Windows 8.1 and higher
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Secure Communications

Companies depend on fast and reliable communications to conduct their business and often favor VoIP and mobile communications to reduce costs and increase efficiency.

Despite all the advantages of using VoIP and mobile communication methods they are often vulnerable in terms of security. Major threats include data interception and manipulation, user data spoofing and hacking, as well as Denial-of-Service (DoS) attacks.

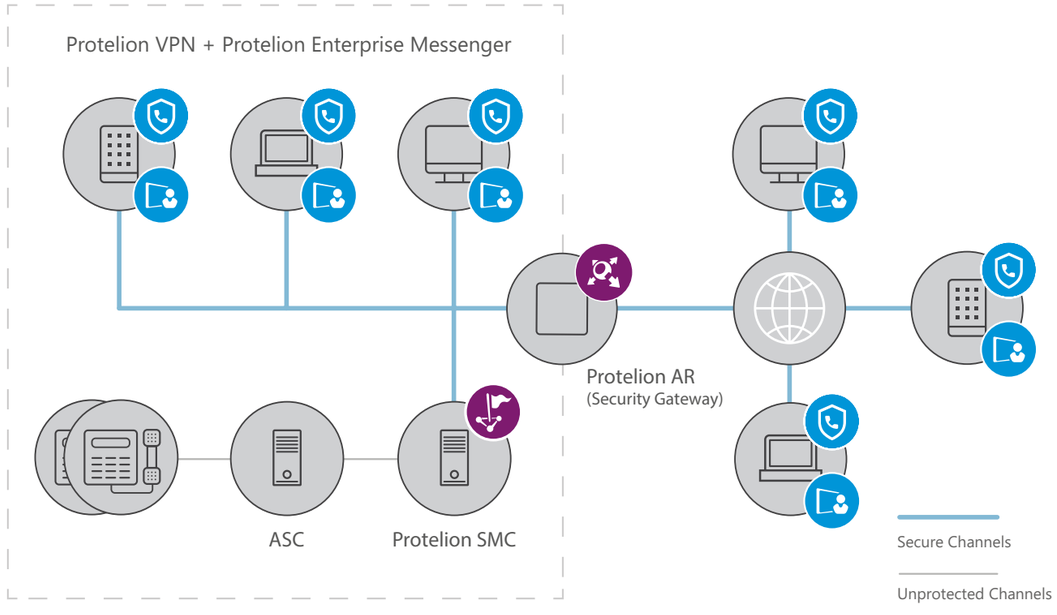
In addition to their primary function of being a mobile telephone, modern mobile devices serve as mobile terminals to access the Internet and simultaneously connect to corporate systems and sensitive data. That's why information security presents even more challenges for mobile devices than for desktop computers.

1 For corporate wireless communications, companies should implement a strict information security policy and user authentication / authorization mechanisms should be in place. Corporate wireless communication should be protected as a whole.

2 Mobile devices are omnipresent. Many of us use the same device for business and for personal use. Ensuring confidential phone calls or preventing interception of texts and files is challenging for most users.

Backed by detailed research in the field of network protection and underpinned by comprehensive analysis of vulnerabilities in corporate IT infrastructures comprising remote and mobile users, Protelion has developed a range of high security solutions based on its proprietary Protelion Security Technology.

Protelion products are designed to protect communication channels and network resources (VoIP and video communications, file sharing and texts) by way of traffic encryption and filtering.



Protelion Enterprise Messenger Solution

Protelion Enterprise Messenger organizes secure communications between multiple devices and allows security administrators to simply and efficiently manage their information security policies and infrastructure across their organization.

This unique solution supports secure voice communications, text messages, and file sharing on IP phones, desktop computers, laptops and mobile devices. All Protelion Enterprise Messenger communications are protected via the Protelion point-to-point encrypted network.

ADVANTAGES

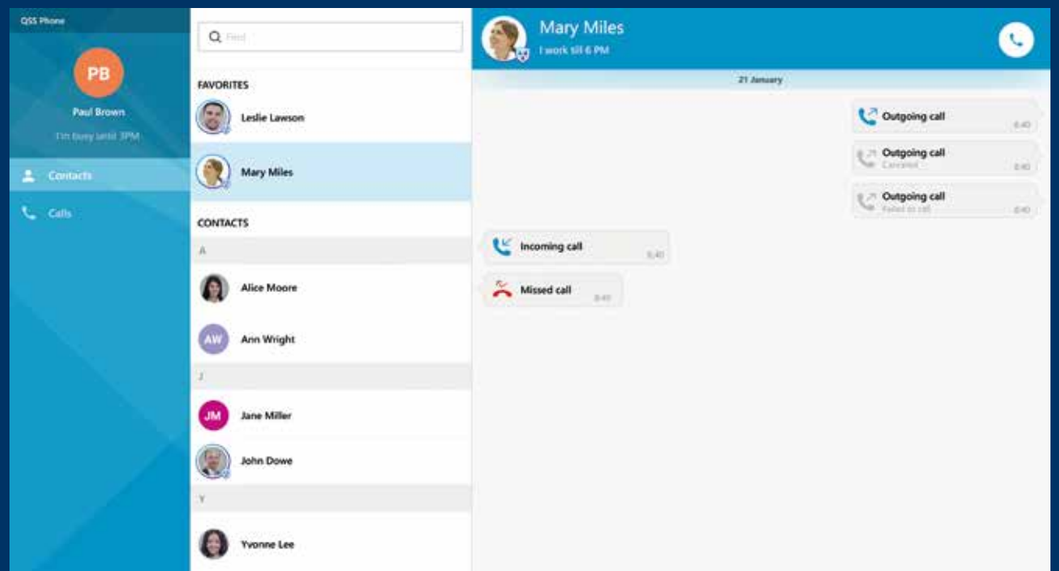
Comprehensive – Protelion Enterprise Messenger unifies all corporate communications over any IP connected device

Reliable – Protelion VPN encrypts and protects all the data (including traffic encapsulation in a local network)

Easy to use – A modern and intuitive UI design requires no special skills from users. Contact lists are centrally managed and updated

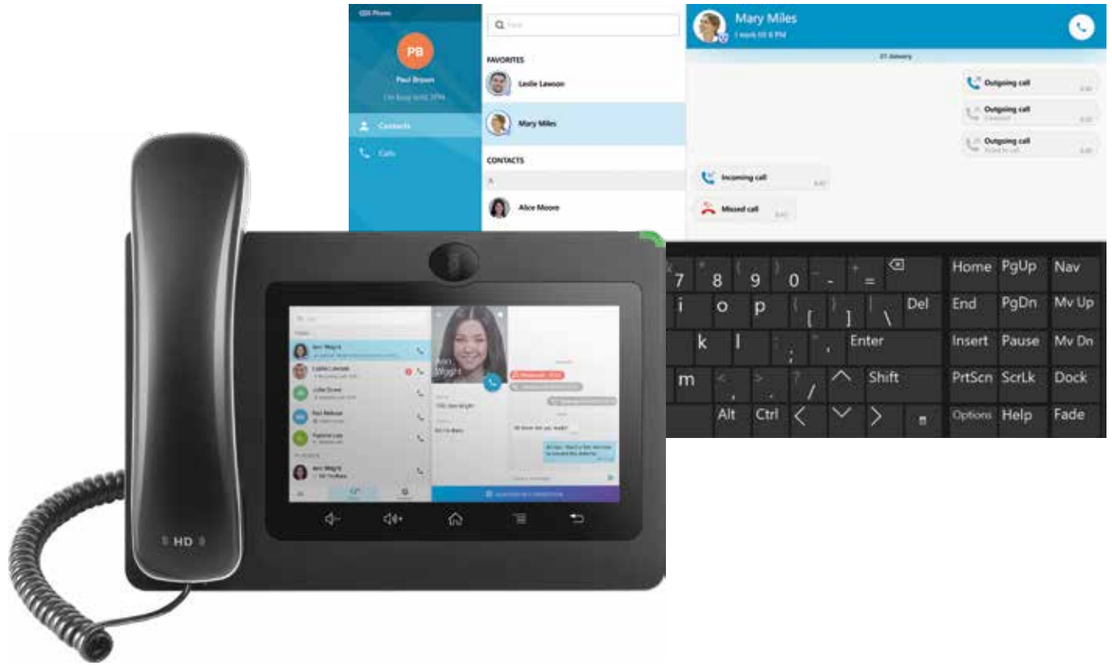
Protected contact list – The Protelion Enterprise Messenger contact list is created by the Protelion SMC (Administrator) centrally and is isolated

Secure file sharing – Protelion Enterprise Messenger users exchange traffic directly between devices; there are no servers to decrypt data at intermediate stages. Thus, the data is protected against decryption even by an insider



Protelion Enterprise Messenger IP Phone

A new unique device ensuring protection of business communications using Protelion Security Technology.



SOLUTION ADVANTAGES

- Easy to use, with a user-friendly and intuitive UI, no tricky buttons or confusing search and call algorithms
- Encrypts and filters the signaling and voice traffic for all parties in the VoIP network
- Ensures that the VoIP traffic passes through NAT devices smoothly
- Supports virtual addresses, particularly in application protocols, resolving often met conflicting IP address issues for remote offices

SPECIFICATIONS

- 7'' sensor display with an intuitive UI
- Wire phone, left- or right-hand holder design
- Built-in camera
- Built-in WiFi adapter
- 2-port Gigabit Ethernet (10/100/1000) switch
- Integrated PoE

Protelion Enterprise Messenger for Mobile Devices

Employees are widely using WhatsApp, Viber, Telegram, Skype and other public services on their mobile devices within the corporate infrastructure. This poses significant information security risks and directly violates the GDPR requirements for the disclosure of personal data to third parties.

Protelion Enterprise Messenger is a secure alternative to such public services. It ensures that corporate communications are protected.

Protelion Enterprise Messenger encrypts voice calls, text messages, even attachments. Protelion Enterprise Messenger users exchange data directly (using point-to-point encryption). There are no intermediate servers to store or decrypt the data. This prevents third-party access to the data.

Since Protelion's point-to-point encryption functions without a central routing server, all communications are fast, efficient and do not require dedicated high-bandwidth channels.

ADVANTAGES

- All traffic is protected even including traffic within the local network
- Easy to use, intuitive UI
- Secure communication within the corporate network and with partner networks
- Centrally configured

Messaging App

With the advent of GDPR many businesses have understood that their preferred mobile messaging app WhatsApp is not compliant and theymay need to stop using it or potentially face serious fines and financial penalties.

Since WhatsApp sends every single address book entry of their users to their servers located in the US. This means that data from people who never wanted nor intended to use the messenger app will find their way to WhatsApp. This doesn't comply with GDPR use of personal data. How can businesses and organizations both large and small take advantage of convenient and effective messaging, chat and VoIP calling while remaining GDPR compliant?

That is where Protelion Enterprise Messenger comes in.

Protelion Enterprise Messenger was designed from the outset to be a secure communications app. It uses military grade point-to-point encryption, which impedes man-in-the-middle attacks.

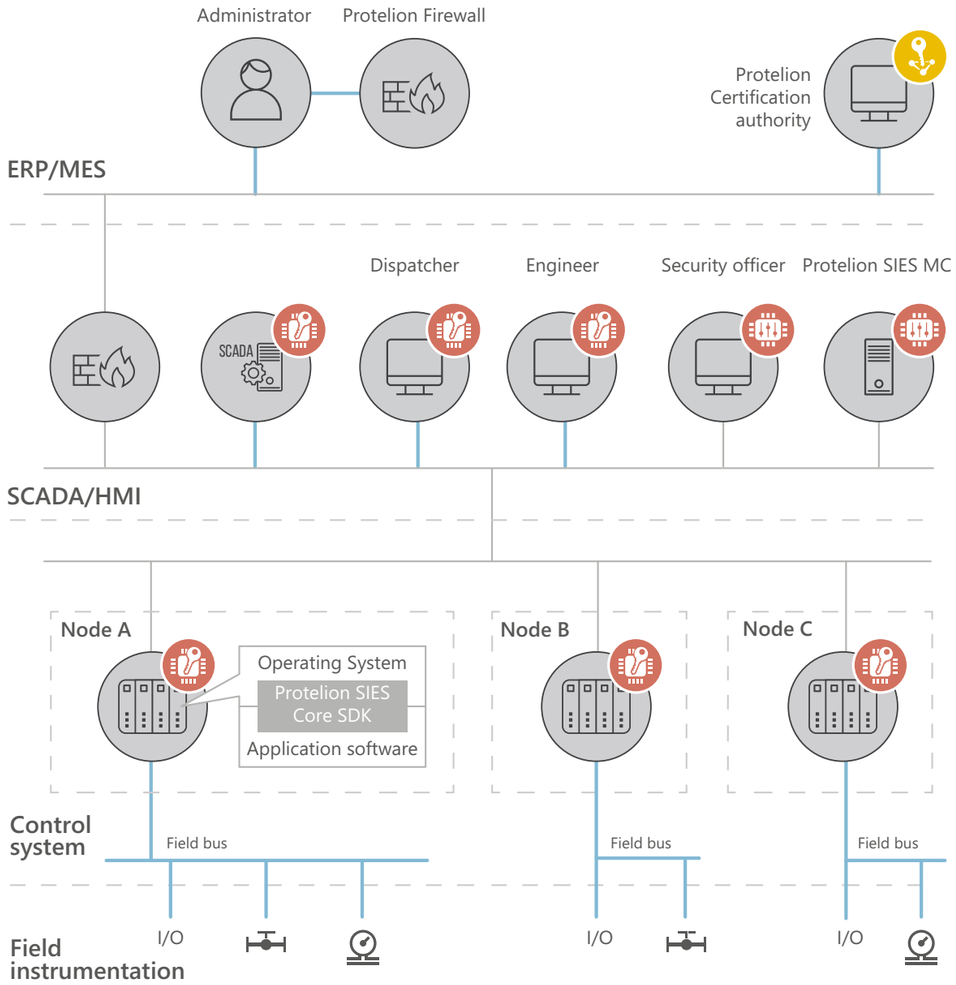
It seamlessly combines GDPR compliant secure VoIP, Chat, Group Chat and Text in one easy to use app. Moreover, it is multi- platform letting you move from your mobile to your tablet or your desktop for maximum convenience and productivity. In addition, Protelion Enterprise Messenger can be deployed with accompanying Protelion Mobile and Network security components to protect all traffic within a broader network not just data, whichgoes through the messaging application itself.

In order to be on the right side of GDPR compliance with respect to your chosen messaging app you should look for messaging applications that protect personal data from unauthorized access, use, copying, processing and storage. Moreover, you should use the strongest encryption available.

Protelion Enterprise Messenger answers all of these concerns to give you a GDPR compliant messaging App with the strongest available encryption combined with maximum convenience, functionality and usability.

Embedded security tools

Protelion Security for Industrial and Embedded Solutions (Protelion SIES) is a solution for cryptographic data protection to be used for integration into industrial control systems (ICS) and machine-to-machine interaction systems (M2M).



Protelion SIES solution is a set of embedded security tools that creates a root of trust for the elements of the ICS and M2M systems. Based on the trust and basic cryptographic operations, Protelion SIES can provide the following information security features:

- identification (crypto-resistant) of the protected node
- authentication of the protected node by other protected nodes
- authentication of the ICS users by the protected nodes
- ensuring the integrity of information transmitted between the protected nodes
- encryption of the data transferred between the protected nodes
- authentication of commands and data transmitted between the protected nodes
- non-repudiation of information
- trusted loading of protected device
- trusted software update for protected device

Protelion SIES solution includes

Protelion SIES – Management Center managing all Protelion SIES components and providing complete lifecycle of the key information and certificates

Protelion SIES – Core Crypto Modules providing basic cryptographic operations for the end nodes of the ICS automated and field level devices

Protelion SIES – Workstation Software for initializing and local maintenance of the Protelion SIES Core crypto modules

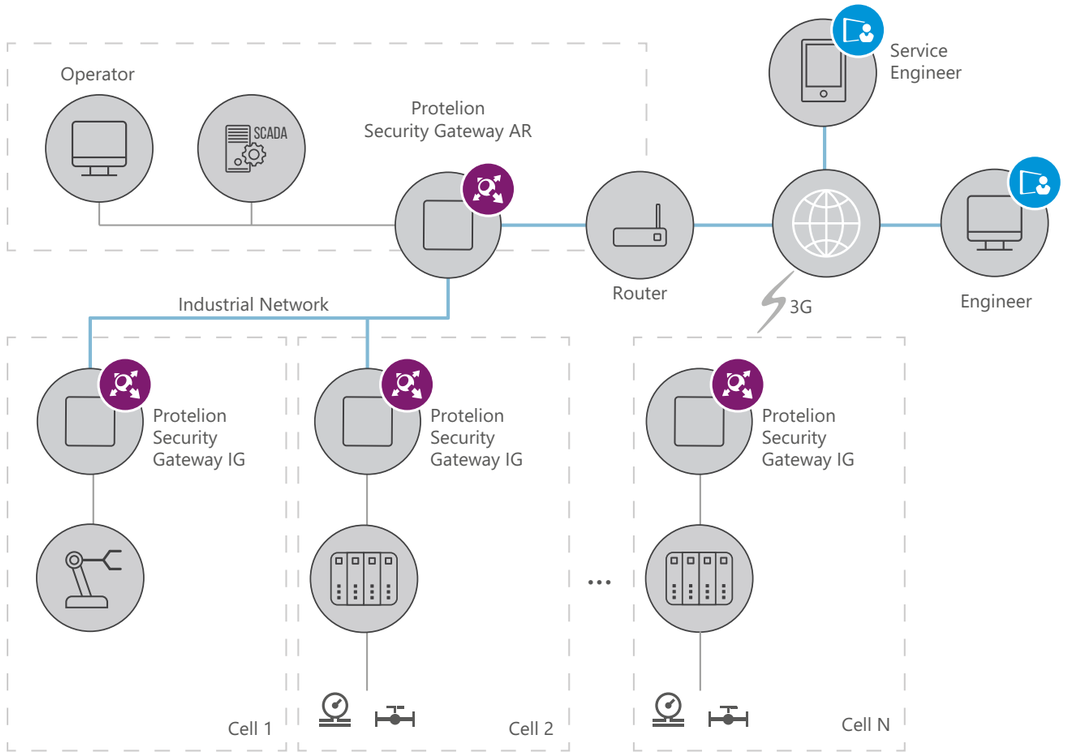
Protelion SIES – Unit Software installed on the ICS dispatching level nodes such as servers and workstations and providing them basic cryptographic operations

Key benefits

- When integrating the Protelion SIES solution into ICS, the information security is provided at the data level. Therefore, the ICS developer can determine the amount of protected data
- The ICS developer determines the logic of processing the protected information and the ICS reaction to the information security breach
- A large number of business scenarios of data protection for implementation into ICS
- Industrial interfaces support allows integrating the Protelion SIES solution into the control system without modifying the information flow topology
- The tasks of cryptography initialization, key information security, and ensuring and maintaining the appropriate infrastructure for cryptographic information protection are not assigned to the ICS

Secure Industrial Gateway

Protelion Security Gateway IG supports industrial protocols and provides trusted data and communication channel protection and firewall functionality.



Features & Components

- Protelion Security Gateway IG together with the Protelion Network Security suite can be used in the following ICS and IIoT infrastructure protection scenarios: Industrial network and industrial wireless local area network (WLAN) protection
- Defense in Depth (Protelion Security Gateway IG can be used together with application level data protection tools)
- Network segmentation and perimeter protection, access delimitation
- Secure remote monitoring
- Access from the industrial network to the Internet control center
- Secure remote access to the industrial network, to the operator's or engineer's workstations as well as to the equipment. Notably it is possible to provide mobile remote access
- Communication gateway for interaction with industrial equipment via serial interfaces

Features

Secure channel establishing

- Protelion network and channel layers gateway (L2 & L3): connection protection by encryption and authentication
- 256-bit symmetric keys at speed up to 10 Mbit/s traffic encryption
- Masking the structure of traffic due to encapsulation in UDP, TCP

Traffic filtering (firewall)

- Firewall with state control session and application protocol inspection. Separate filtering settings for open and encrypted IP traffic
- NAT / PAT
- Anti-spoofing
- Proxy server

Setting up and management

- Remote configuration by Protelion Administrator, web interface, remote management via the SSH protocol, the system console
- Local configuration by the console
- Remote monitoring by Protelion StateWatcher and SNMP protocol
- Group security policies by Protelion SMC (Policy Manager)

Network Functions

- Static Routing
- Dynamic routing
- VLAN support

Service functions

- DNS server
- NTP server
- DHCP server
- DHCP-Relay
- Hot Standby Cluster: Failover Gateway in the Protelion Failover Configuration

Industrial protocols support

- Modbus TCP
- PROFINET
- Ethernet / IP
- DNP, IEC 60870-104, MMS
- OPC
- PTP
- LonWorks, Bacnet
- KNX, ZigBee, Z-Wave

Key benefits

- Industrial Control system (ICS) protection by VPN and traffic filtering (firewall)
- Both wired (Ethernet) and wireless (Wi-Fi, GSM) control channels for ICS protection
- High-energy efficiency
- Industrial devices with RS-232/422/485 interfaces support, functioning as a Modbus TCP-Modbus RTU gateway
- Work at temperatures from -40 to +60 °C
- Industrial design

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 cyber security incidents, as well as hands on experience in implementing protective 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.

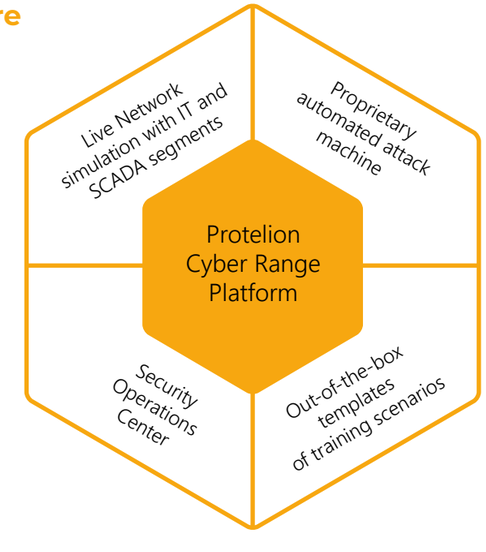
Hacking is on the rise, yet conversely, there is a global shortage of cyber experts available to help organizations counter the threat. Furthermore, many information security and network security staff have insufficient hands on experience responding to and mitigating real cyber-attacks.

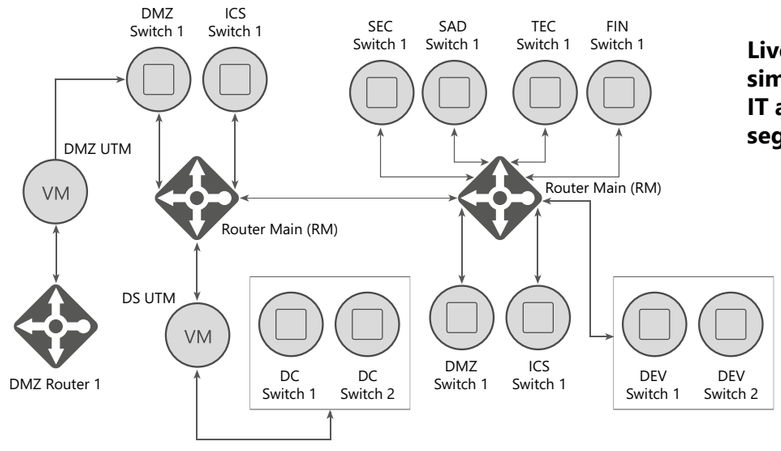
To bridge this gap in qualified cybersecurity expertise, smart companies are turning to immersive training in virtual environments to ensure their teams stay up to date. Cyber Range platforms allow teams to train in a simulated hyper-realistic environment and build practical hands on experience responding 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



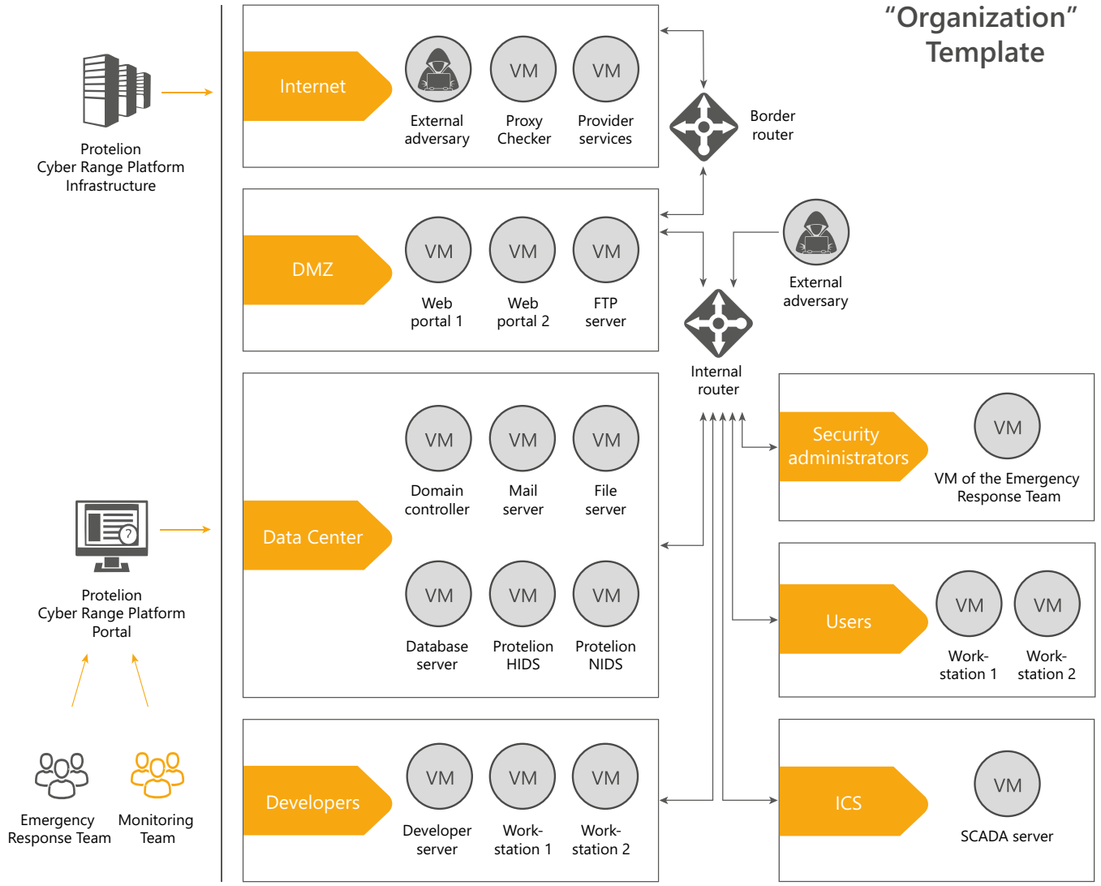


Live Network simulation with IT and SCADA segments

Security Operations Center

Proprietary automated attack machine

Out-of-the-box templates of training scenarios



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

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.

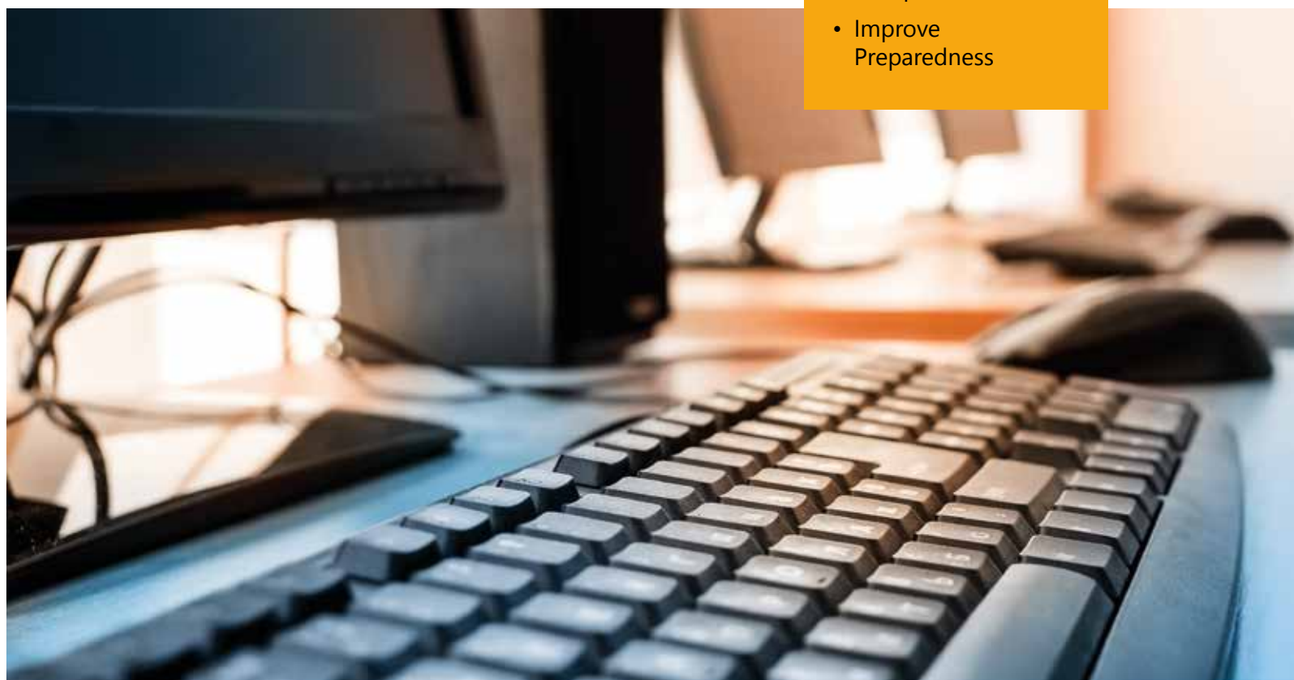
Banks – testbed, SOC teams, information security specialists, decision makers

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
TECHNOLOGY MADE IN GERMANY

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