infotecs

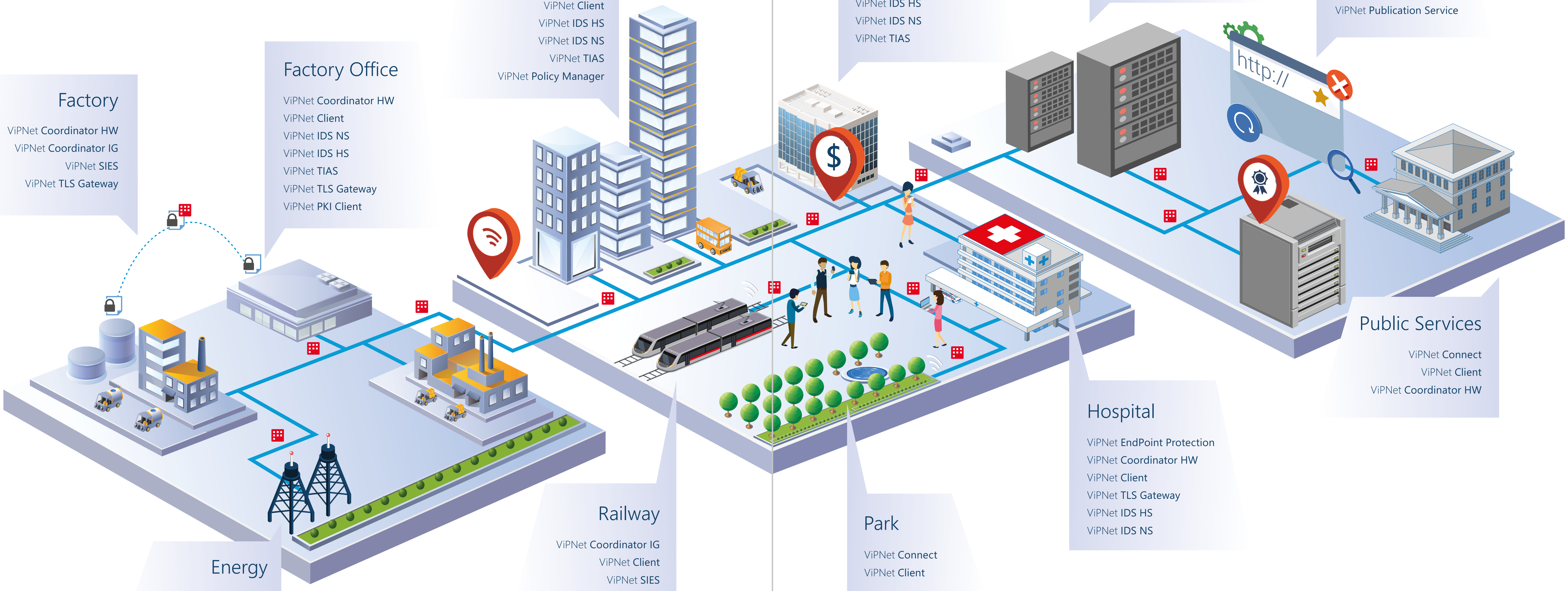
PRODUCT BROCHURE

NETWORK SECURITY

INDUSTRIAL SECURITY

ENDPOINT SECURITY

PRODUCT ECOSYSTEM



Factory

ViPNet Coordinator HW
ViPNet Coordinator IG
ViPNet SIES
ViPNet TLS Gateway

Factory Office

ViPNet Coordinator HW
ViPNet Client
ViPNet IDS NS
ViPNet IDS HS
ViPNet TIAS
ViPNet TLS Gateway
ViPNet PKI Client

Office

ViPNet EndPoint Protection
ViPNet Prime
ViPNet Coordinator HW
ViPNet Connect
ViPNet Client
ViPNet IDS HS
ViPNet IDS NS
ViPNet TIAS
ViPNet Policy Manager

Railway

ViPNet Coordinator IG
ViPNet Client
ViPNet SIES
ViPNet TIAS

Energy

ViPNet SIES
ViPNet Coordinator IG

Bank

ViPNet EndPoint Protection
ViPNet Coordinator HW
ViPNet TLS Gateway
ViPNet IDS HS
ViPNet IDS NS
ViPNet TIAS

Data Center

ViPNet Coordinator HW
ViPNet IDS NS

Web Portal

ViPNet TLS Gateway
ViPNet Registration Point
ViPNet Publication Service

Public Services

ViPNet Connect
ViPNet Client
ViPNet Coordinator HW

Hospital

ViPNet EndPoint Protection
ViPNet Coordinator HW
ViPNet Client
ViPNet TLS Gateway
ViPNet IDS HS
ViPNet IDS NS

Park

ViPNet Connect
ViPNet Client

CONTENT

Network Intrusion Detection System

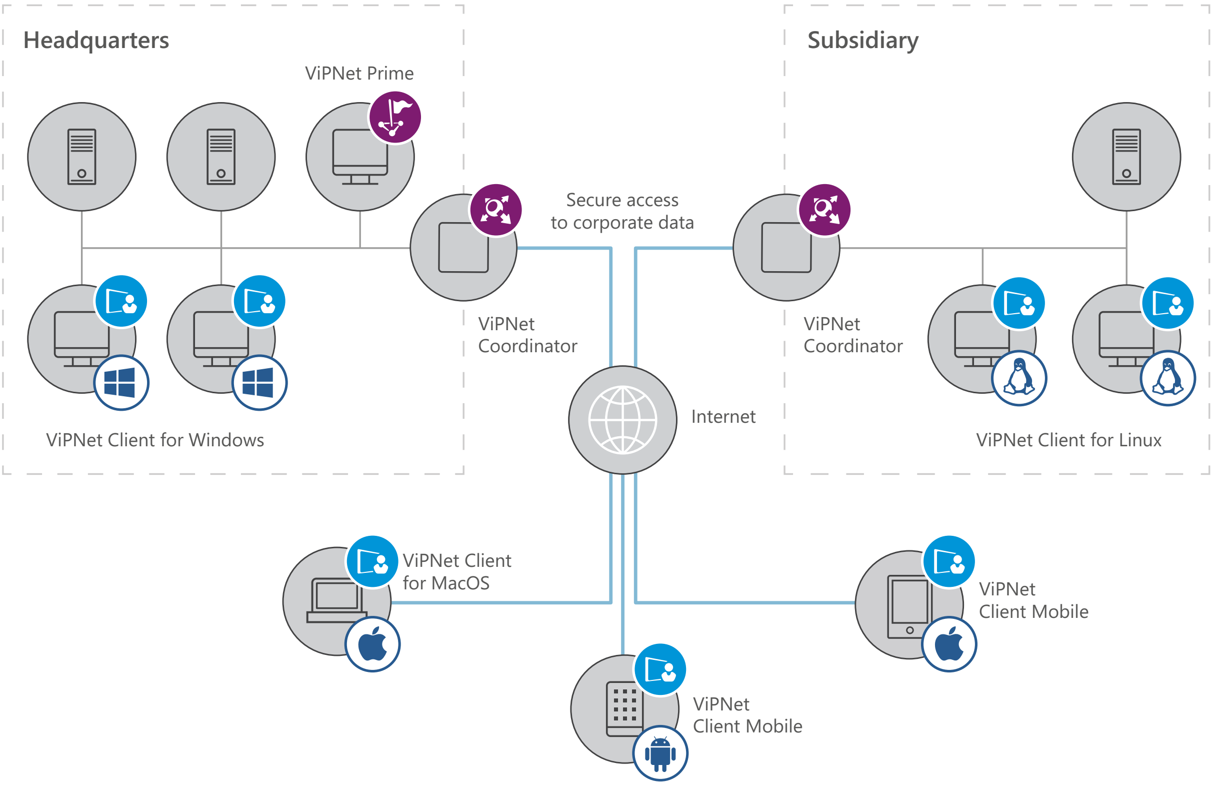
NETWORK SECURITY

xFirewall

Channel Protection

Channel Protection

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



SOLUTION FOR BUSINESS

- Solution can be supplied as a software suite, its installation and configuration do not require the purchase of specialized equipment and can be carried out within the customer’s existing IT infrastructure
- Low hardware requirements
- Flexible pricing, possible to create an optimal solution for each individual customer

ViPNet 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:

- protection of communication channels between company offices
- protection of multi-data networks (voip, video conferencing)
- secure remote access to corporate data centers and the cloud environment
- public key infrastructure for electronic document management construction
- and more...

TECHNOLOGY & FUNCTIONALITY

- 256-bit symmetric keys at speed up to 2,5 Gb/s traffic encryption
- Virtual addressing support to simplify user software application configuration
- Separate unencrypted and encrypted traffic filtration to control the ability to work via unauthorized ports and protocols
- Allows the implementation of different scenarios of public key infrastructure (PKI) deployment
- Wide range of device types (Smartphones, Tablets, Laptops, Desktops) operating under different operation systems support
- Various network hardware and software with dynamic or static network/port address translation (NAT/PAT) compatibility support
- Allows the integration of many applications and services to enable the user to work and communicate securely

MAIN COMPONENTS

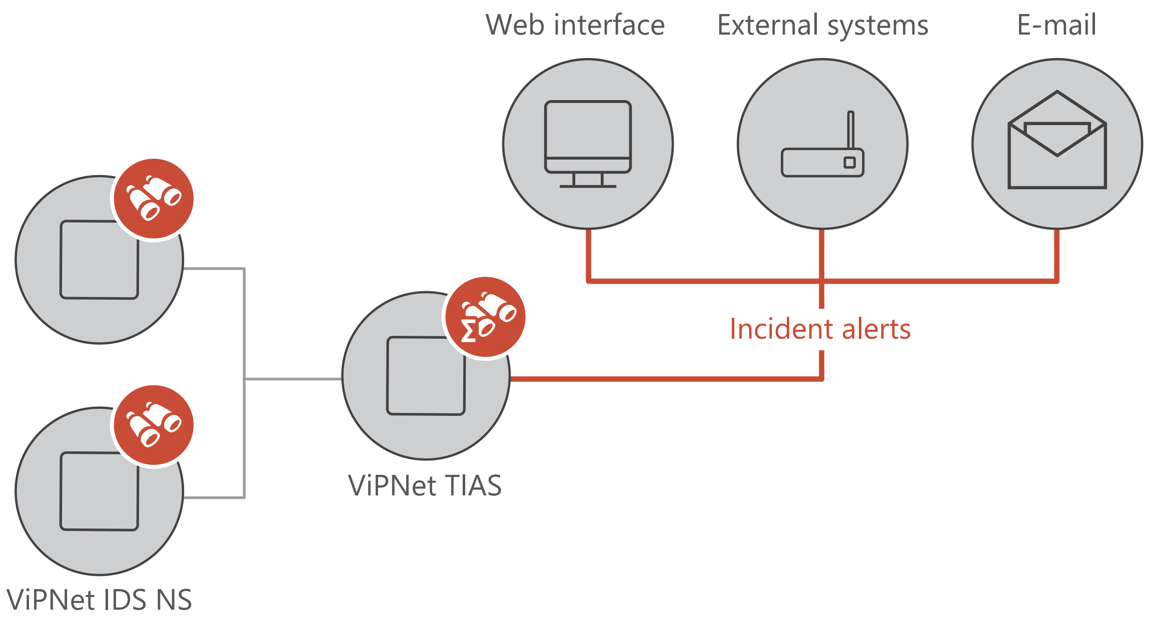
ADMINISTRATIVE COMPONENTS	SERVER COMPONENTS	CLIENT COMPONENTS
ViPNet Prime – security management platform to manage ViPNet products in an all-in-one scalable appliance	**ViPNet Coordinator HW** – security gate computer appliance (different throughput values available)	**ViPNet Client** – basic VPN client software. Available for Windows, MacOS and Linux
	ViPNet Coordinator VA – security gate for deploying on a virtualization platform	**ViPNet Client Mobile** – basic VPN client software for Android and Apple mobile devices
	ViPNet Coordinator Software – security gate network server software for Windows or Linux OS	

KEY BENEFITS

- Peer to peer connection support allows building secure channels between two network nodes without using a server.
- ViPNet uses the principle of non-session connection, what gives an advantage when connecting via bad and unstable communication channels. It is not needed to transfer the payload to an encrypted channel session. Data transfer starts immediately in the first IP packet when a communication channel appears.
- The separate open and encrypted traffic filtering algorithm. This makes it possible to apply security policies not only to open but also to secure hosts which enables 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 using ViPNet.
- 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.
- Built-in endpoint protection services:
  - Instant messenger
  - Secure Business Mail app
  - Crypto Service Provider (CSP)
- Equally suited for traditional enterprise networks as well as Cloud, Mobile, Industrial and IoT deployments.

Network Intrusion Detection System

ViPNet Network Intrusion Detection System (NIDS) is a comprehensive solution solving the tasks of continuous monitoring and detection of information security threats and responding to these events.



HOW IT WORKS?

1 The sensors register information security events detected, based on traffic analysis, and send the information to ViPNet TIAS.

2 ViPNet TIAS aggregates information about events, stores it in the database and analyses it. In the case of a suspicious incident, the ViPNet TIAS registers this fact in the form of a card, notifies the suspicious incident to interested persons and provides tools for investigating the incident.

3 Information Security specialists investigate the incident and decide whether to confirm or reject it.

4 After confirmation, the information about the incident is transferred to external systems and Information Security specialists takes steps to eliminate the consequences of the incident in accordance to recommendations provided by ViPNet TIAS.

FEATURES AND COMPONENTS

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

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

ViPNet 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).

KEY BENEFITS

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

ViPNet xFirewall

ViPNet xFirewall – the next-generation security gateway. Placed on the network border ViPNet xFirewall provides traffic filtering at all network levels and allows the creation of granular security policies based on user accounts and application list.

FEATURES AND COMPONENTS

Firewall

- Firewall with session state control
- NAT / PAT Address Translation
- Antispoofing protection

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 (DPI)

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

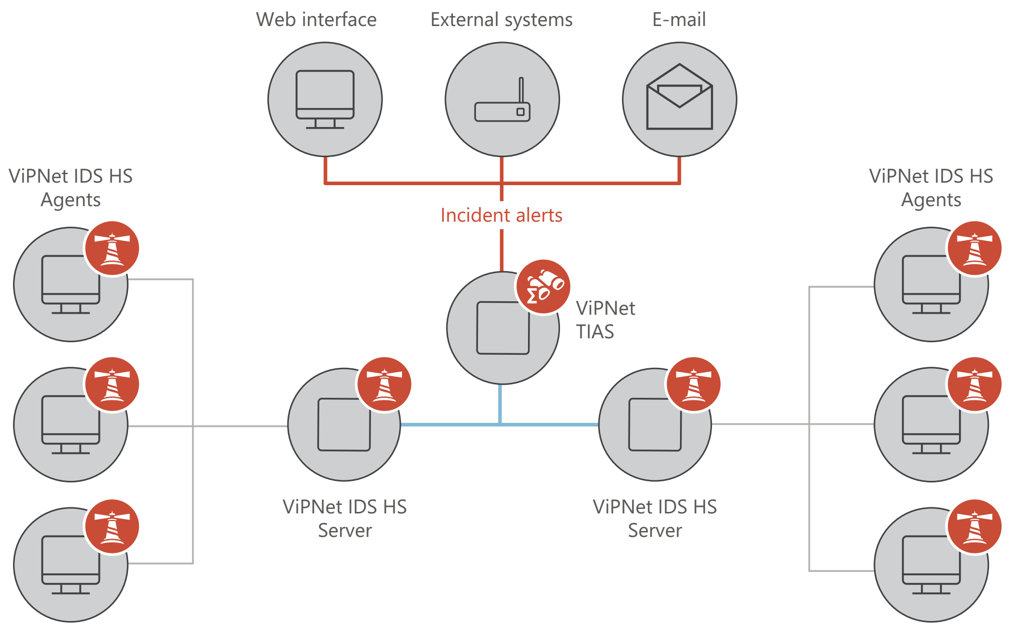
- DNS server
- NTP Server
- DHCP server
- DHCP -Relay

KEY BENEFITS

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

Host-based Intrusion Detection System

ViPNet Host-based Intrusion Detection System is a comprehensive solution solving the tasks of continuous monitoring and detection of information security threats and responding to these events.



KEY BENEFITS

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

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

ViPNet IDS HS – software package that is intended to detect intrusions on a node based on signature and heuristic methods of information analysis.HIDS and NIDS solutions can be combined into single Intrusion Detection System.

EndPoint Protection

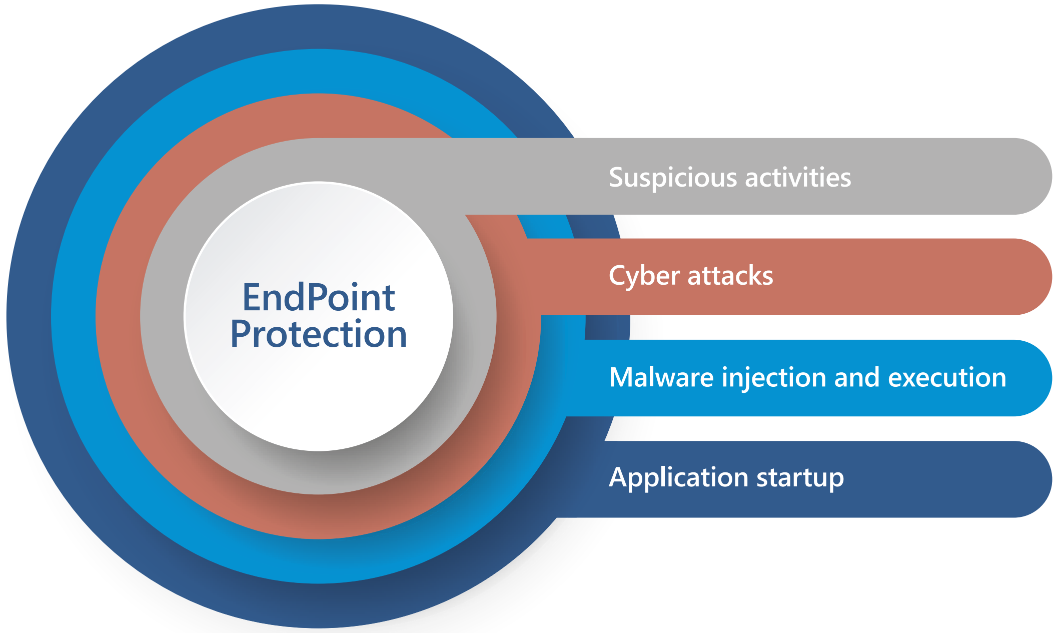
All-in-one solution to secure endpoints from zero-day exploits, unknown malware and internal or external threats. ViPNet EndPoint Protection provides high level security for desktop computers and laptops.

COMPONENTS

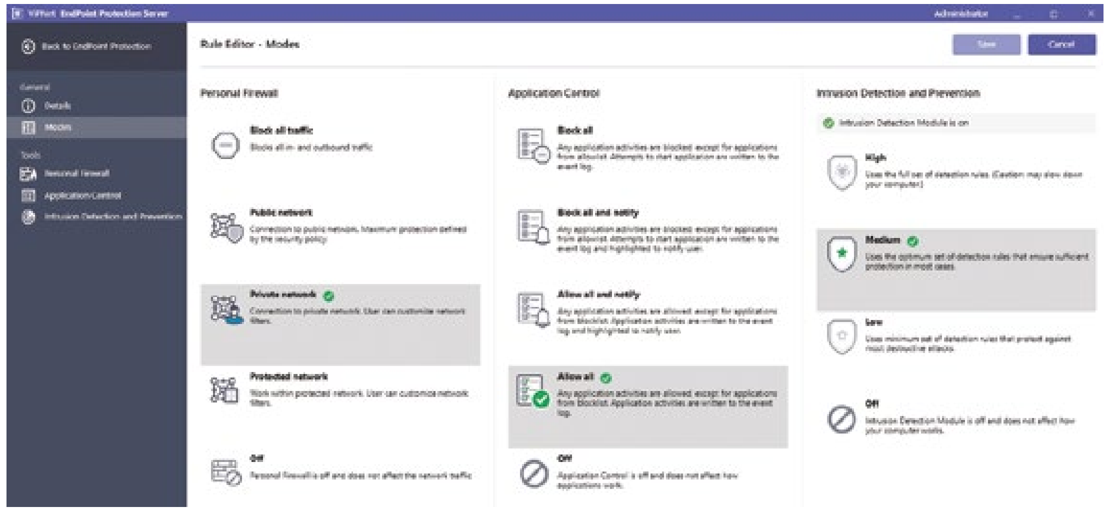
Intrusion detection & prevention - protects computers from unidentified attacks and suspicious behavior

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


ViPNet EndPoint Protection Server
Administrator
Back to EndPoint Protection
General
Details
Modes
Tools
Personal Firewall
Application Control
Intrusion Detection and Prevention
Save
Cancel

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.

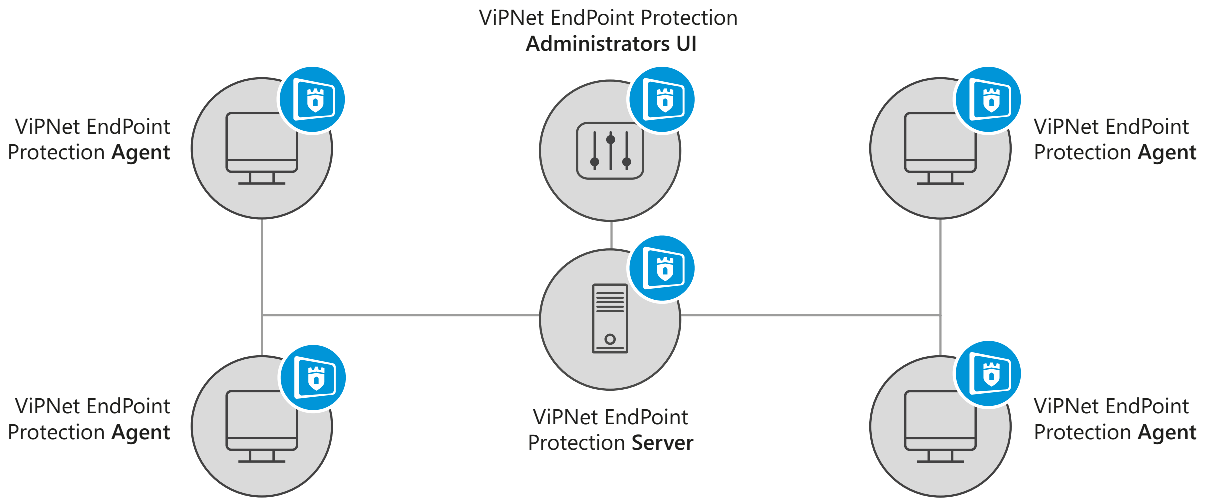
ARCHITECTURE

ViPNet 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


ViPNet EndPoint Protection Administrators UI
ViPNet EndPoint Protection Agent
ViPNet EndPoint Protection Agent
ViPNet EndPoint Protection Agent
ViPNet EndPoint Protection Server
ViPNet EndPoint Protection Agent

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. Regulary updated signature bases
- Compatibility with ViPNet TIAS 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 makes 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 base updates from a single point.

Communication with ViPNet TIAS

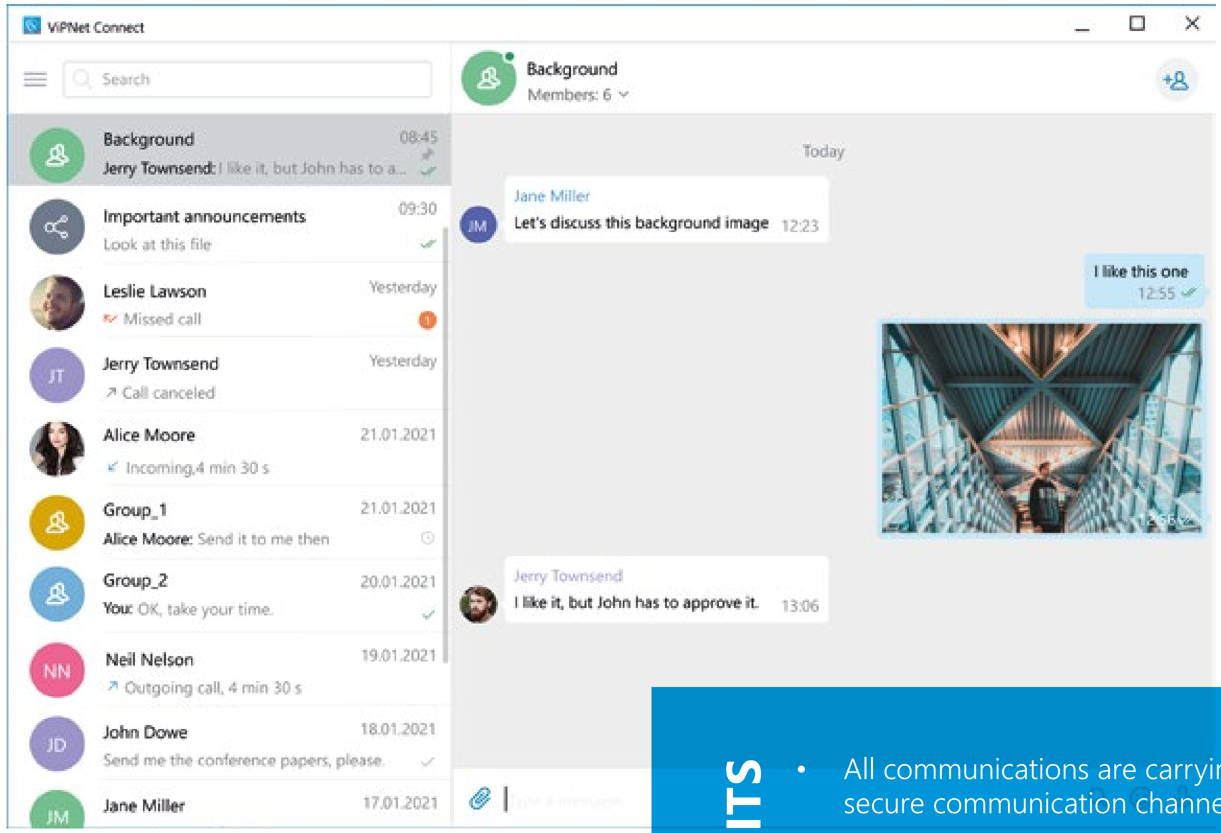
ViPNet EndPoint Protection can transfer all events to ViPNet TIAS, the SIEM system, and thus detect complex and unknown attacks due to mathematical model and metarules implemented in ViPNet TIAS. When an incident is detected, you can respond immediately and batch adjust security settings on all hosts added to ViPNet EPP.

Supported operating systems

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Secure IM

ViPNet Connect is an alternative to public instant messengers for establishing secure communication of corporate users. ViPNet Connect application provides voice communications, text messages and files exchange between computers, laptops and mobile devices. ViPNet Connect users can communicate confidentially using ViPNet secure network with point-to-point encryption.



Background 08:45
Jerry Townsend: I like it, but John has to a...

Important announcements 09:30
Look at this file

Leslie Lawson Yesterday
Missed call

Jerry Townsend Yesterday
Call canceled

Alice Moore 21.01.2021
Incoming,4 min 30 s

Group_1 21.01.2021
Alice Moore: Send it to me then

Group_2 20.01.2021
You: OK, take your time.

Neil Nelson 19.01.2021
Outgoing call, 4 min 30 s

John Dowe 18.01.2021
Send me the conference papers, please.

Jane Miller 17.01.2021

Jane Miller
Let's discuss this background image 12:23

I like this one 12:55

Jerry Townsend
I like it, but John has to approve it. 13:06

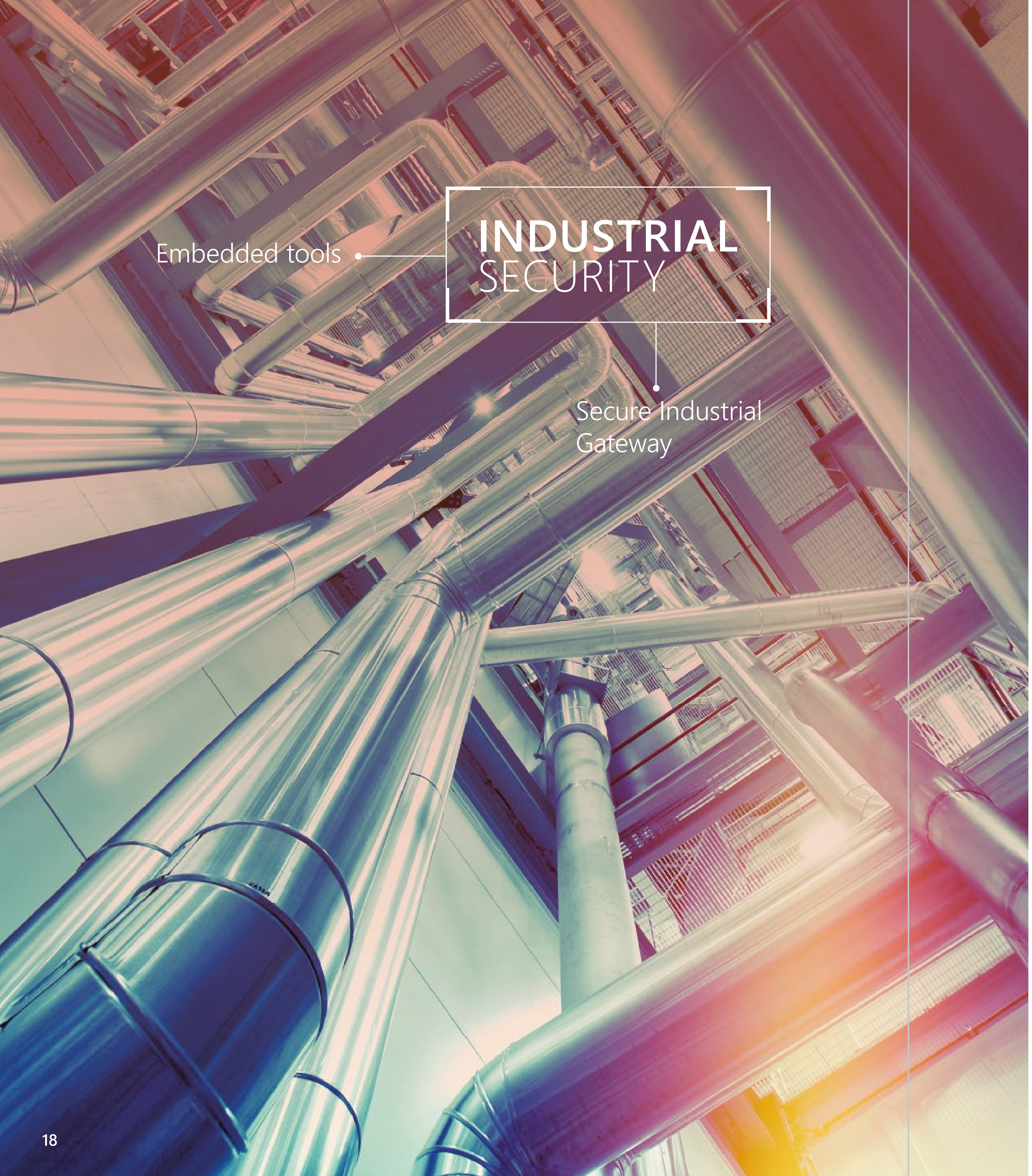
FEATURES AND COMPONENTS

Connection between ViPNet Connect users is organized directly (point-to-point encryption). The absence of intermediate servers which would store or decrypt the data solves the problem of access to information by unauthorized persons.

Work in the "point-to-point" mode does not require to use routing server. It allows not to provide a high-speed communication channel.

KEY BENEFITS

- All communications are carrying using secure communication channels
- An intuitive interface allows to users use the application easily
- The address book of ViPNet Connect forms centrally and cannot be changed by a user (it is set by the administrator of ViPNet network)
- Ability to communicate both with users within their own ViPNet network, and with users in the networks of partner organizations
- Point-to-point communication



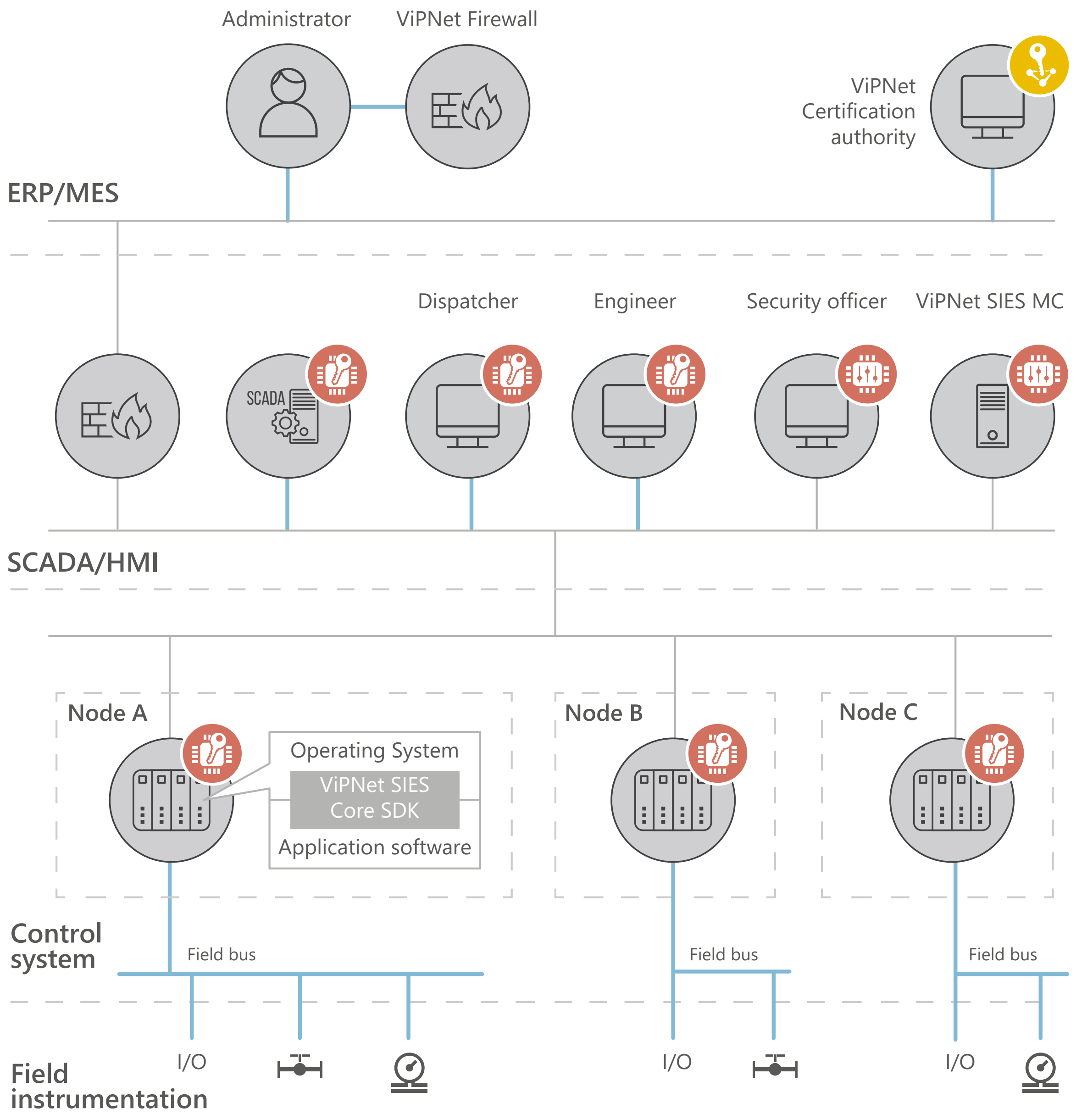
INDUSTRIAL SECURITY

Embedded tools

Secure Industrial Gateway

Embedded security tool

ViPNet Security for Industrial and Embedded Solutions (ViPNet 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).



ViPNet 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, ViPNet 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

THE VIPNET SIES SOLUTION INCLUDES

ViPNet SIES Management Center managing all ViPNet SIES components and providing complete lifecycle of the key information and certificates.

ViPNet SIES Workstation software for initializing and local maintenance of the ViPNet SIES Core crypto modules.

ViPNet SIES Core crypto modules, providing basic cryptographic operations for the end nodes of the ICS automated and field level devices.

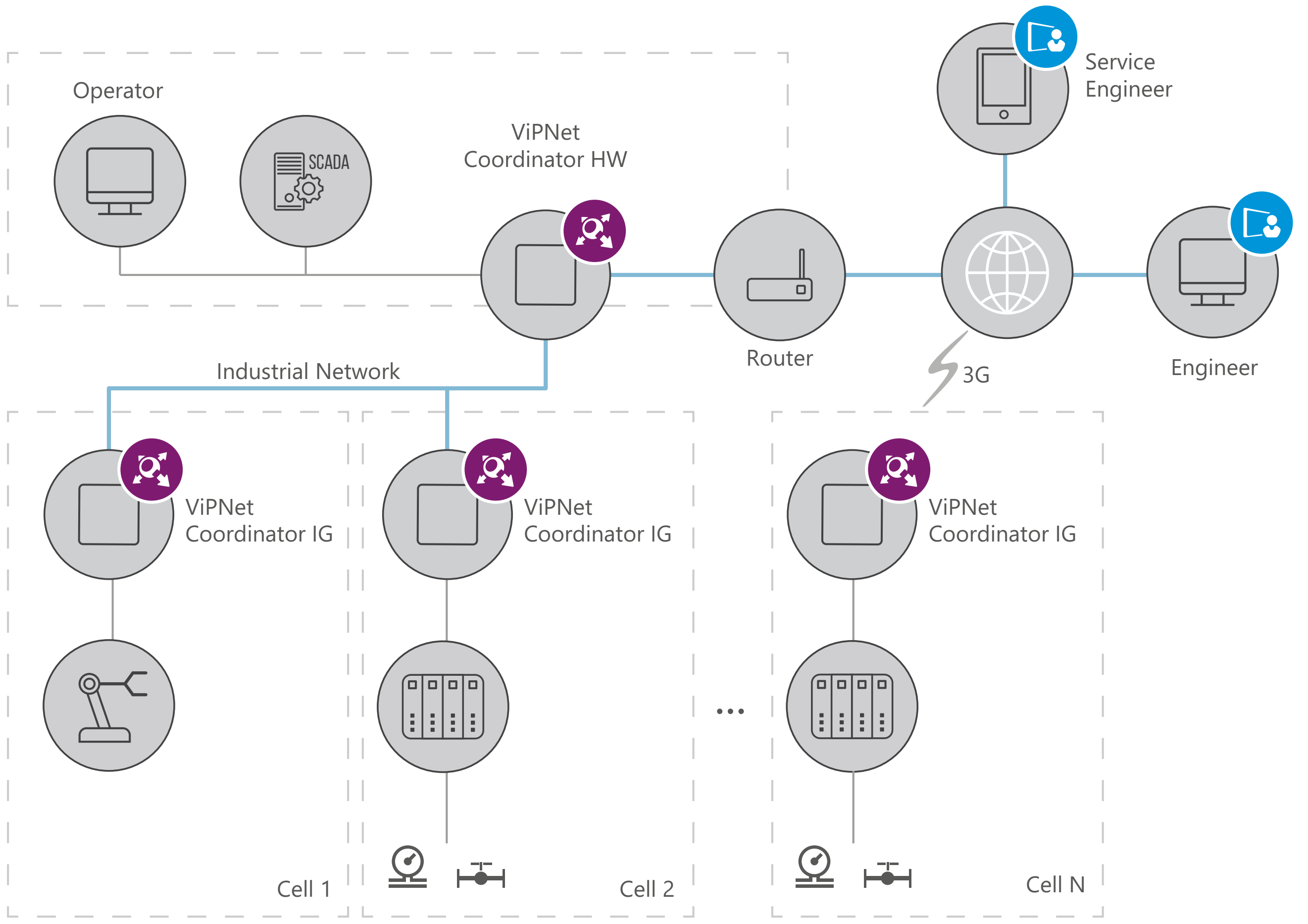
ViPNet SIES Unit software installing on the ICS dispatching level nodes such as servers and workstations and providing for them basic cryptographic operations.

KEY BENEFITS

- When integrating the ViPNet SIES solution into ICS, the information security is provided at the data level. Therefore, the ICS developer can determine 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 are supported
- Industrial interfaces support allows integrating the ViPNet 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

Secure and trusted data transmission environment by security gateways (ViPNet Coordinator IG) supporting industrial protocols and providing communication channels protection and firewall functionality.



FEATURES & COMPONENTS

- ViPNet Coordinator IG together with the ViPNet Network Security lineup can be used in the following ICS and IIoT infrastructure protection scenarios: Industrial network, industrial wireless local area network (WLAN) protection
- Defense in Depth (ViPNet Coordinator 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
- Secure remote access to the industrial network, to the operator's or engineer's workstations, as well as to the equipment. Moreover, it is possible to provide mobile remote access
- Communication gateway for interaction with industrial equipment via serial interfaces

FEATURES

Secure channel establishing

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

Network Functions

- Static Routing
- Dynamic routing
- VLAN support

Service functions

- DNS server
- NTP server
- DHCP server
- DHCP-Relay
- Hot Standby Cluster: Failover Coordinator in the ViPNet 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

Infotecs GmbH, Germany
Potsdamer Strasse 182, D-10783 Berlin

info@infotecs.de

+49 30 206 43 66-0

www.infotecs.de

COM21_00EN

Disclaimer. The information contained herein has been prepared solely for the purpose of providing general information about Infotecs and its products. Infotecs 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. Infotecs disclaims all warranties, express and implied, with respect to such content. Infotecs 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 TM and ® symbols are omitted in this document.