infotecs

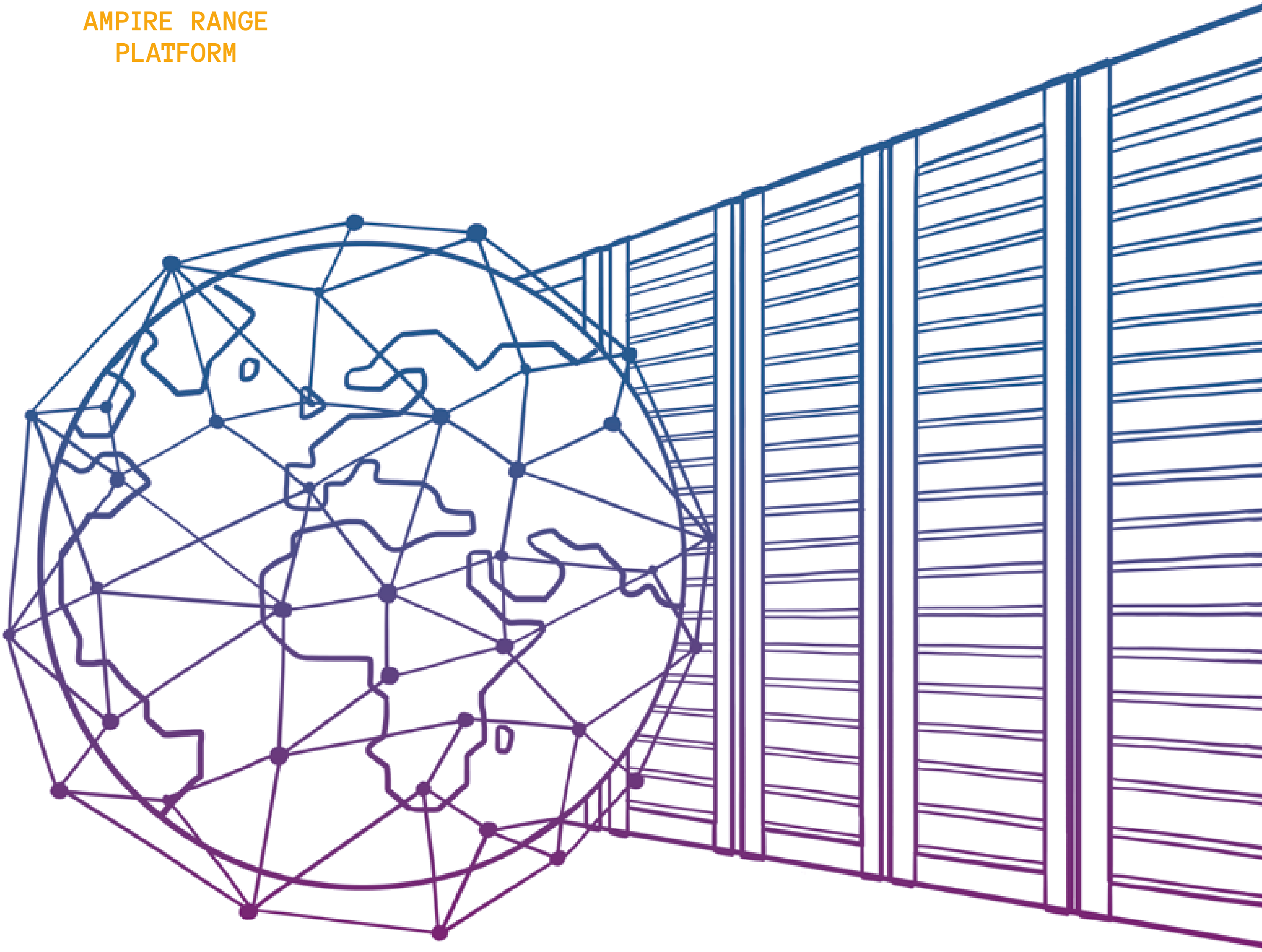
NETWORK
SECURITY

PRODUCT BROCHURE

ENDPOINT
SECURITY

INDUSTRIAL
SECURITY

AMPIRE RANGE
PLATFORM



PRODUCT ECOSYSTEM

Office

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

Factory

ViPNet Coordinator HW
ViPNet Coordinator IG
ViPNet SIES

Factory Office

ViPNet Coordinator HW
ViPNet Client
ViPNet IDS NS
ViPNet IDS HS
ViPNet TIAS

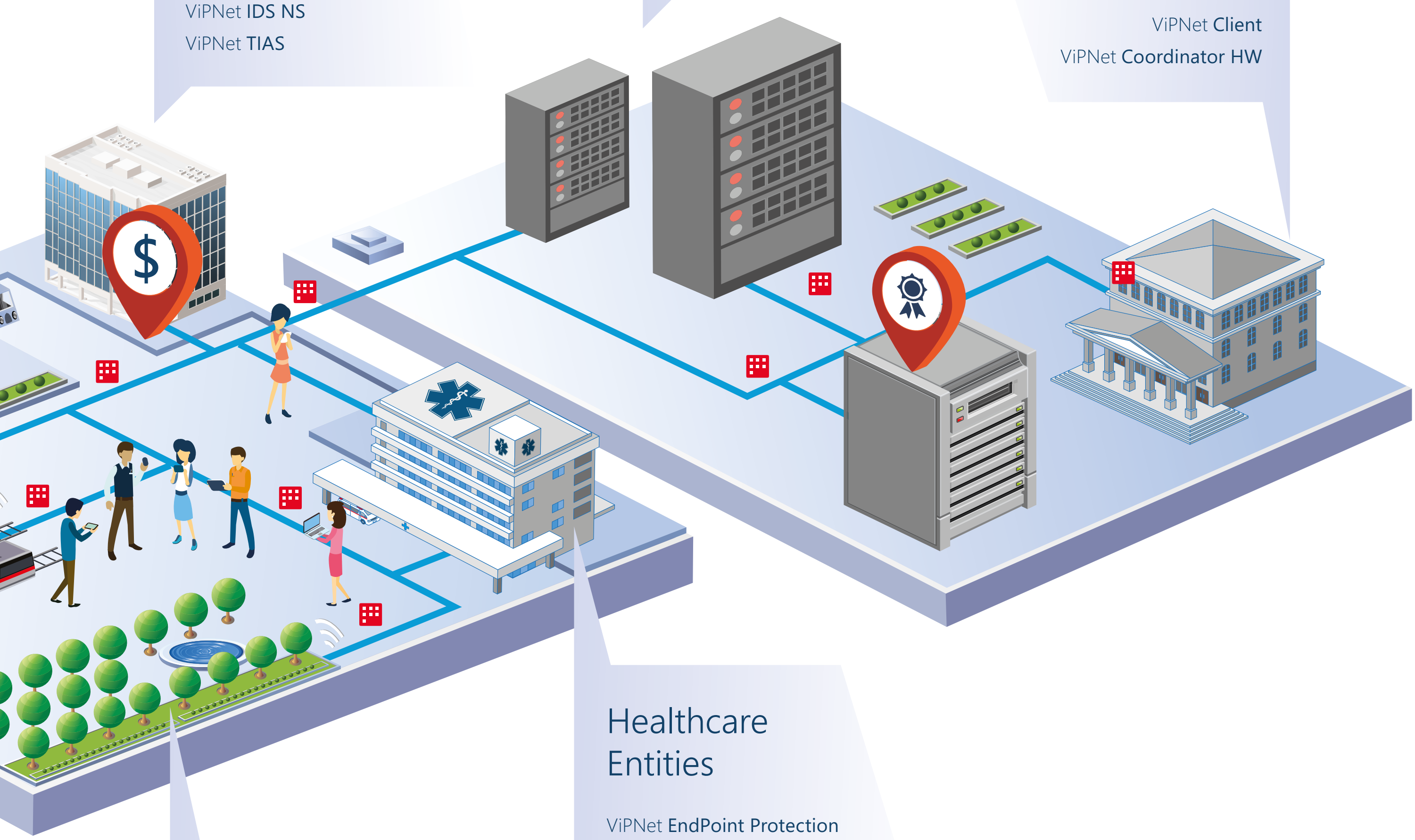
Energy

ViPNet SIES
ViPNet Coordinator IG

Transport & Logistics

ViPNet Coordinator IG
ViPNet Client
ViPNet SIES
ViPNet TIAS

CONTENT



Bank

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

Data Center

ViPNet Coordinator HW
ViPNet IDS NS

Public Services

ViPNet Connect
ViPNet Client
ViPNet Coordinator HW

Healthcare Entities

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

Public Places

ViPNet Connect
ViPNet Client

NETWORK SECURITY

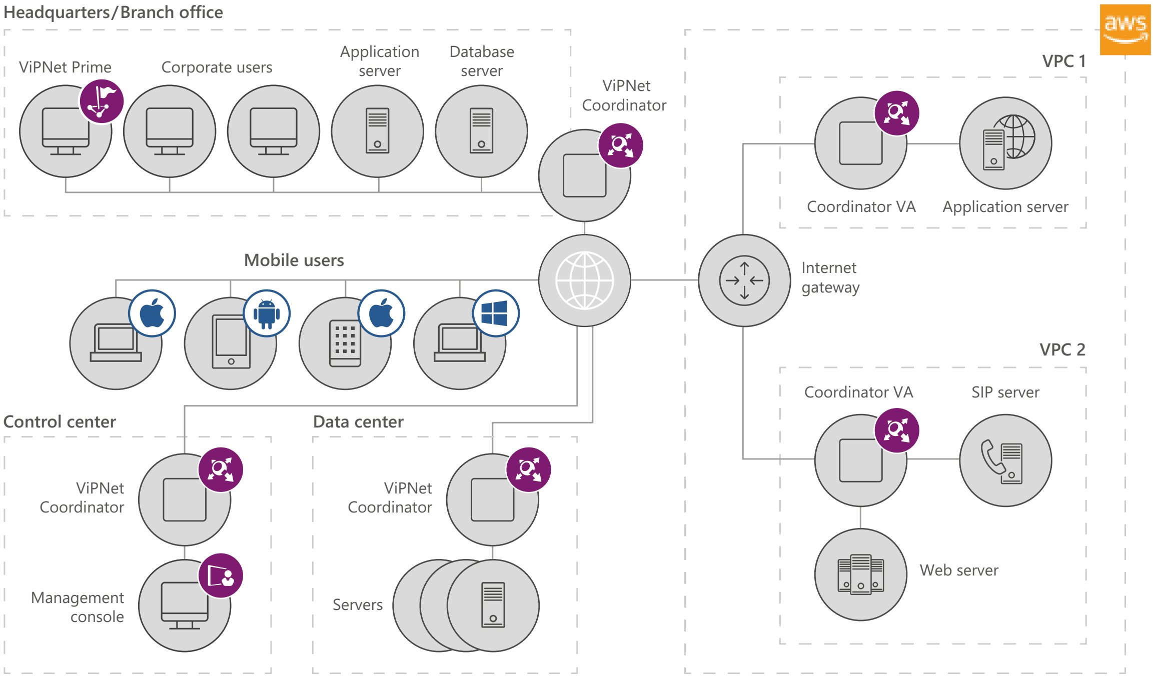
Channel Protection

Threat Detection and Responce

xFirewall

CHANNEL PROTECTION

ViPNet 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

- The solution can be supplied as a software suite, its installation and configuration do not require the purchase of specialized equipment and is interoperable with the customer’s existing IT infrastructure
- Minimum hardware requirements
- Flexible pricing, with capability 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 speeds up to 6.8 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
- 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

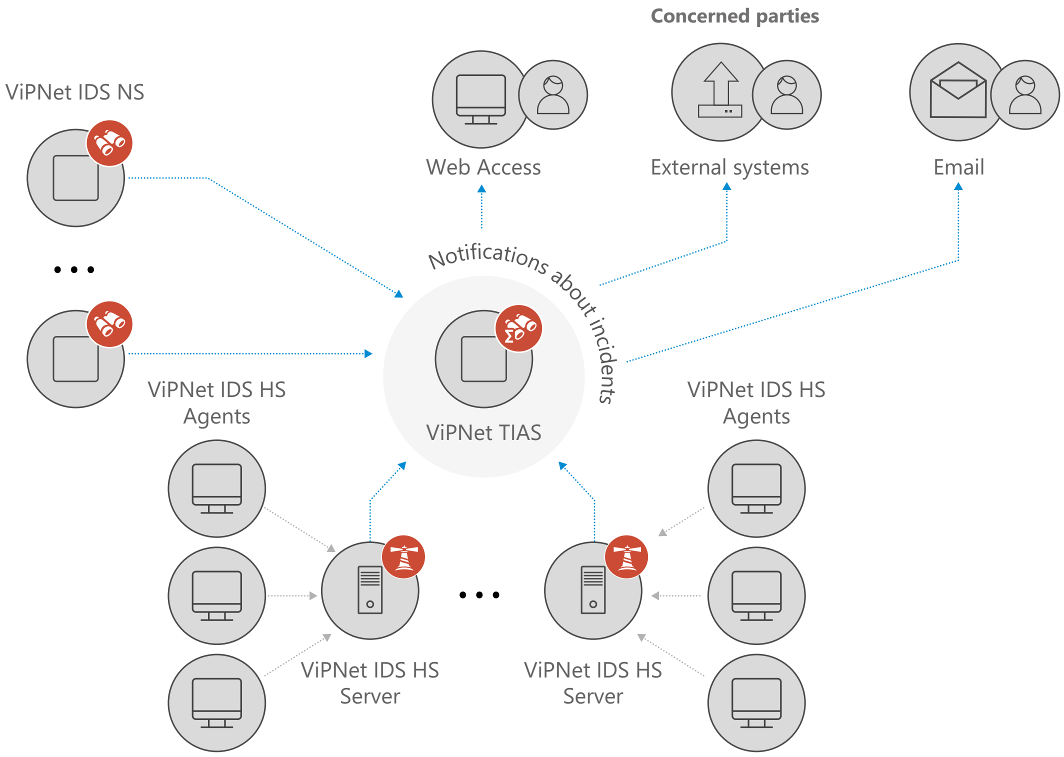
Administrative components	Server components	Client components
ViPNet Prime – security management platform to manage ViPNet products in an all-in-one scalable appliance	**ViPNet Coordinator HW** – security gate computer appliance (different throughput values available)	**ViPNet Client** – basic VPN client software. Available for Windows, MacOS and Linux
ViPNet Network Manager – administrative tool to create ViPNet network topology and generate secret keys	**ViPNet Coordinator VA** – security gate for deploying on a virtualization and Cloud platforms	**ViPNet Client Mobile** – basic VPN client software for Android and Apple mobile devices
ViPNet Policy Manager – administrative tool to manage ViPNet network security policies centrally	**ViPNet Coordinator Software** – security gate network server software for Windows or Linux OS **ViPNet Coordinator HW-RPi** – secure encryption solution for running on a Raspberry Pi platform	

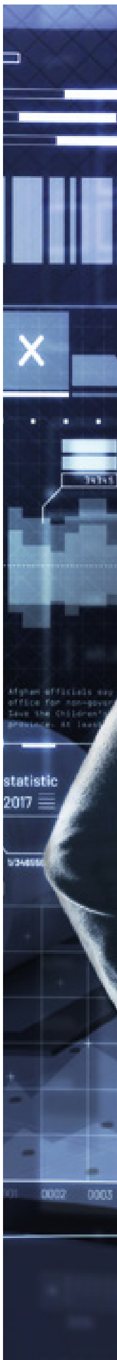
KEY BENEFITS

- Peer to peer connection technology makes it possible to build secure channels between two network nodes without using a server
- ViPNet 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
- ViPNet 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 ViPNet 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, IDS sensors capture security events and send relevant data to the ViPNet TIAS
- The ViPNet TIAS accumulates event data collected from the sensors, normalizes the data and saves it to the database
- The ViPNet TIAS 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 ViPNet TIAS 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

ViPNet TIAS – computer appliance for information security events analysis, automatic information security incidents detection and 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).

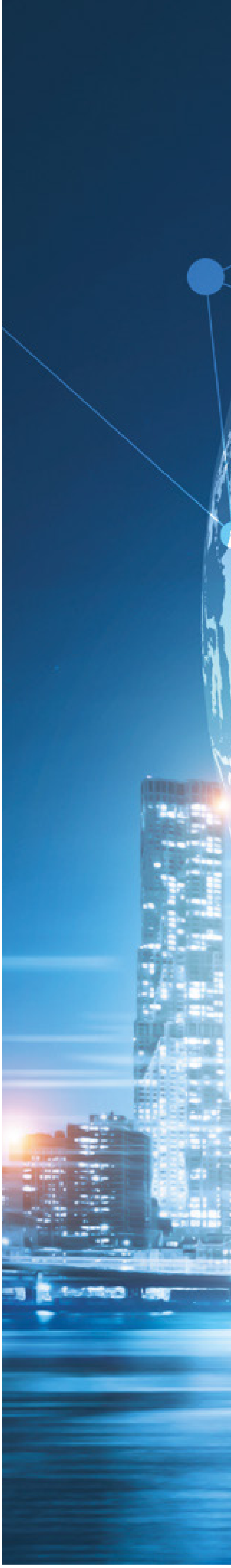
ViPNet IDS HS – Host based intrusion detection system. Enhances the security of information systems, data centers, client computers, servers and communication equipment.

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.

VIPNET xFIREWALL

ViPNet xFirewall – a next-generation security gateway. Placed on the network border, ViPNet xFirewall 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

- Firewall with session state control
- NAT / PAT Address Translation
- Anti-spoofing 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

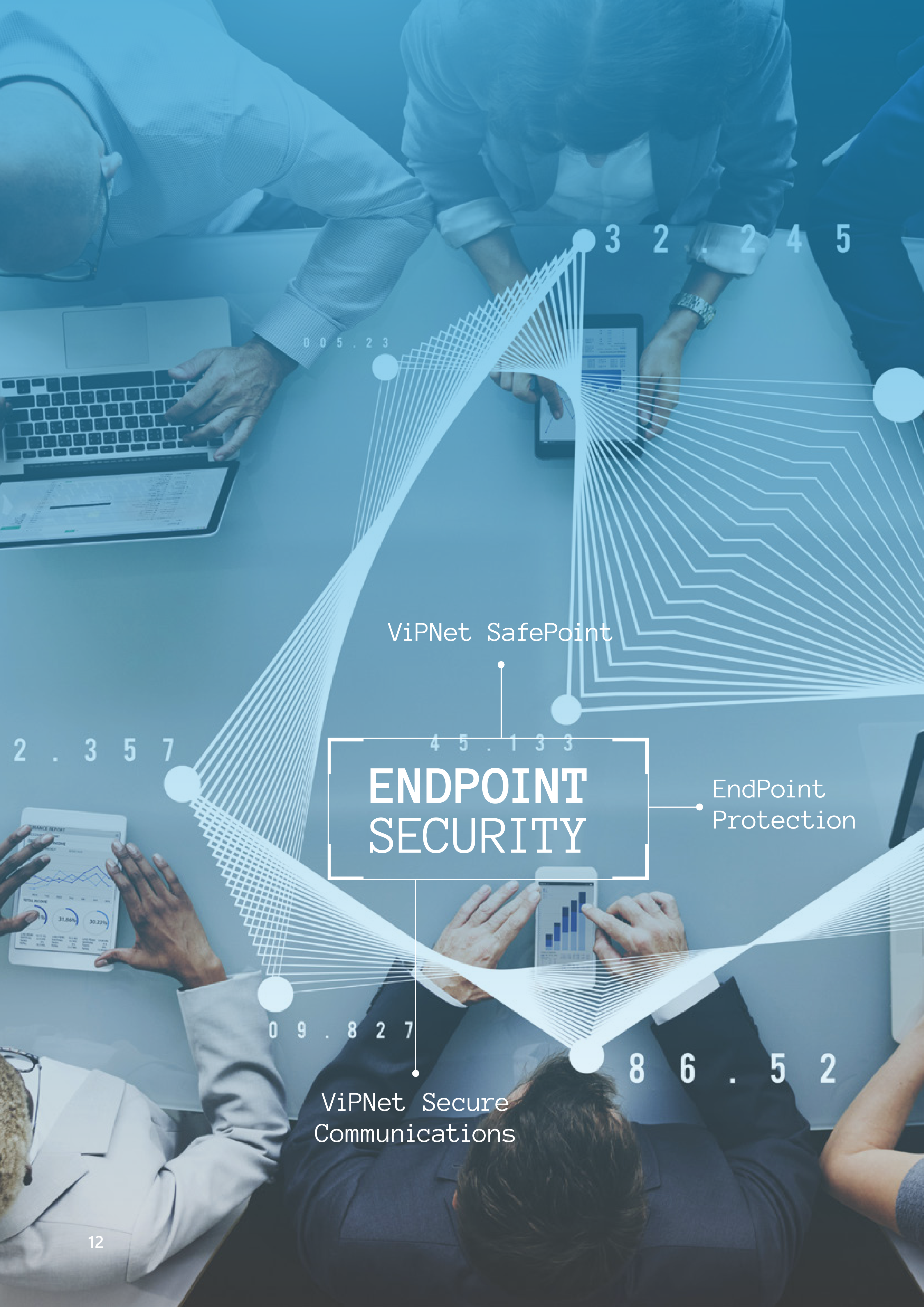
- Dynamic Routing
- VLAN support (dot1q)
- Link Aggregation (bonding (LACP), EtherChannel)
- QoS, ToS, DiffServ support

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 within full compliance of 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 Internet traffic consumption
- Minimizing the attack surface



ENDPOINT SECURITY

ViPNet SafePoint

EndPoint Protection

ViPNet Secure Communications

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.

VIPNET SAFEPOINT

Comprehensive information security system to protect from unauthorized access.

ViPNet SafePoint installed on workstations 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

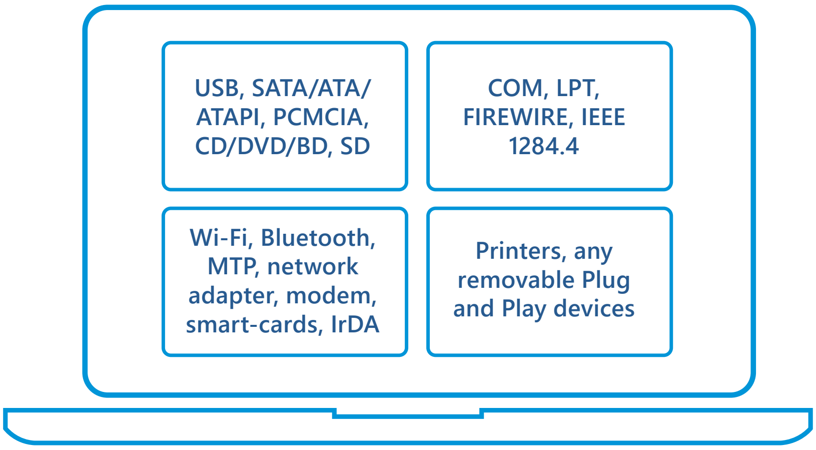
- File system
- HDD
- Registry
- Printers
- Services
- Devices
- Clipboard

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


USB, SATA/ATA/ ATAPI, PCMCIA, CD/DVD/BD, SD
COM, LPT, FIREWIRE, IEEE 1284.4
Wi-Fi, Bluetooth, MTP, network adapter, modem, smart-cards, IrDA
Printers, any removable Plug and Play devices

DEVICE CONTROL

- Mounting and unmounting control
- Event monitoring

VIPNET ENDPOINT PROTECTION

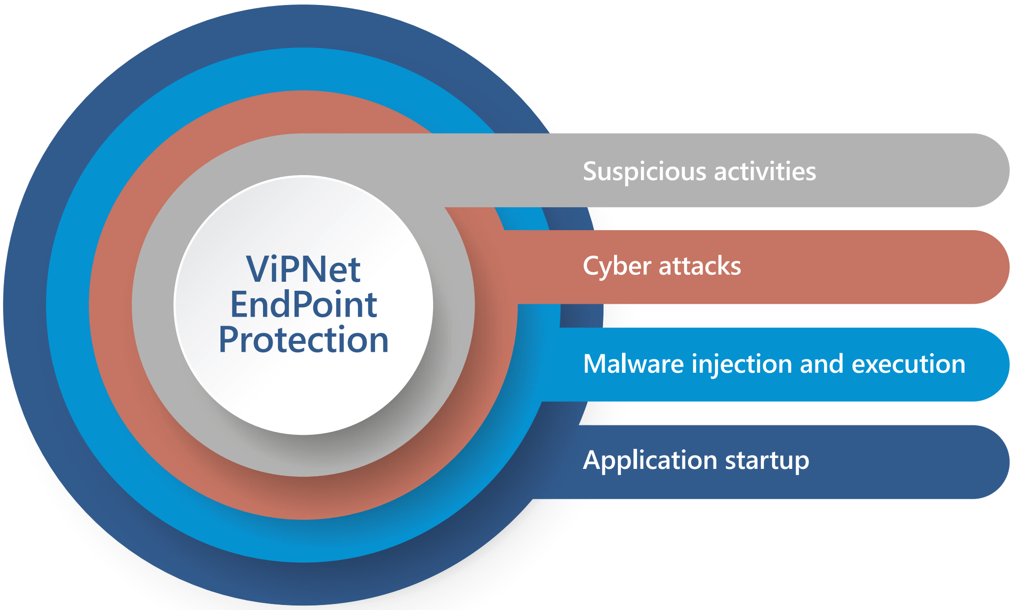
All-in-one solution to secure endpoints from zero-day exploits, unknown malware and internal or external threats. ViPNet EndPoint Protection provides high level security for desktop computers and laptops.

COMPONENTS

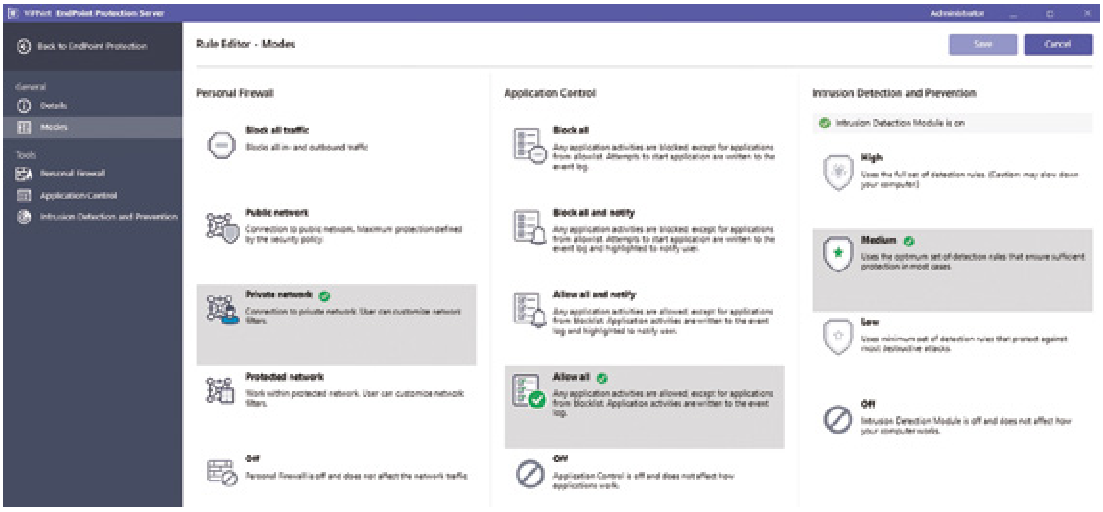
Intrusion detection & prevention – protects computers from unidentified attacks and suspicious behavior

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.

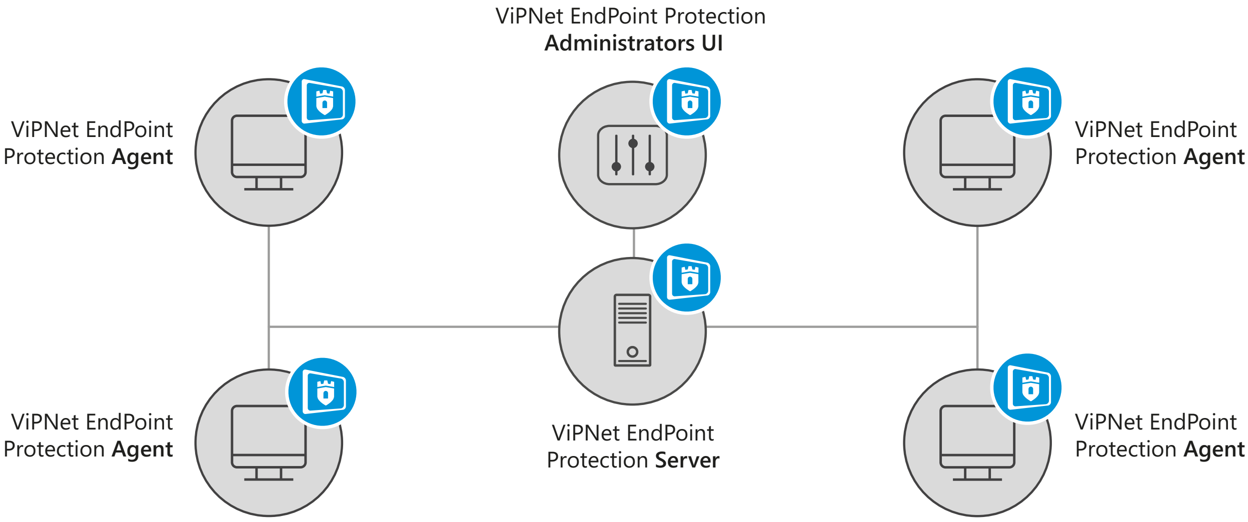
ARCHITECTURE

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 **Agent**
ViPNet EndPoint Protection **Server**

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 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 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 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 by 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 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

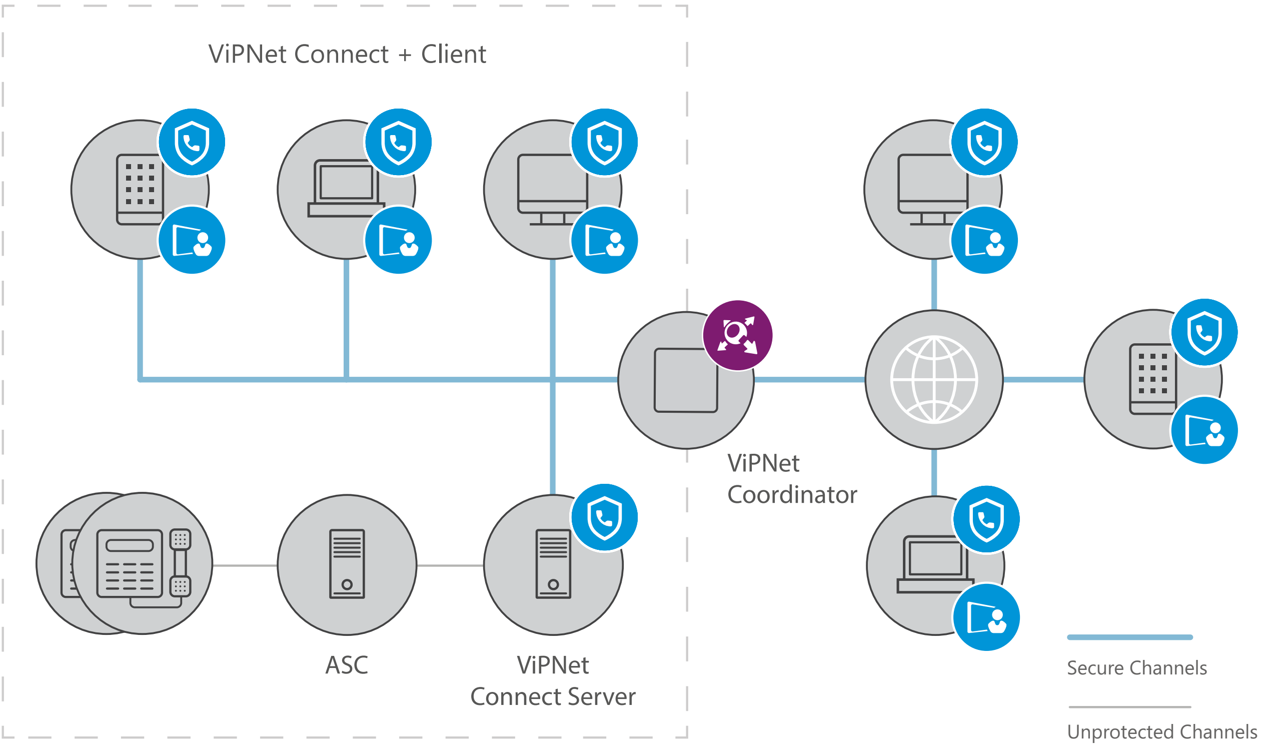
For corporate wireless communications, companies should implement a strict information security policy and user authentication / authorization mechanisms should be in place. Corporate wireless communication should be protected as a whole.

2

Mobile devices are ubiquitous. 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, Infotecs has developed a range of high security solutions based on its proprietary ViPNet technology.

ViPNet 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.



VIPNET CONNECT SOLUTION

ViPNet Connect 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 ViPNet Connect communications are protected via the company's ViPNet point-to-point encrypted network.

ADVANTAGES

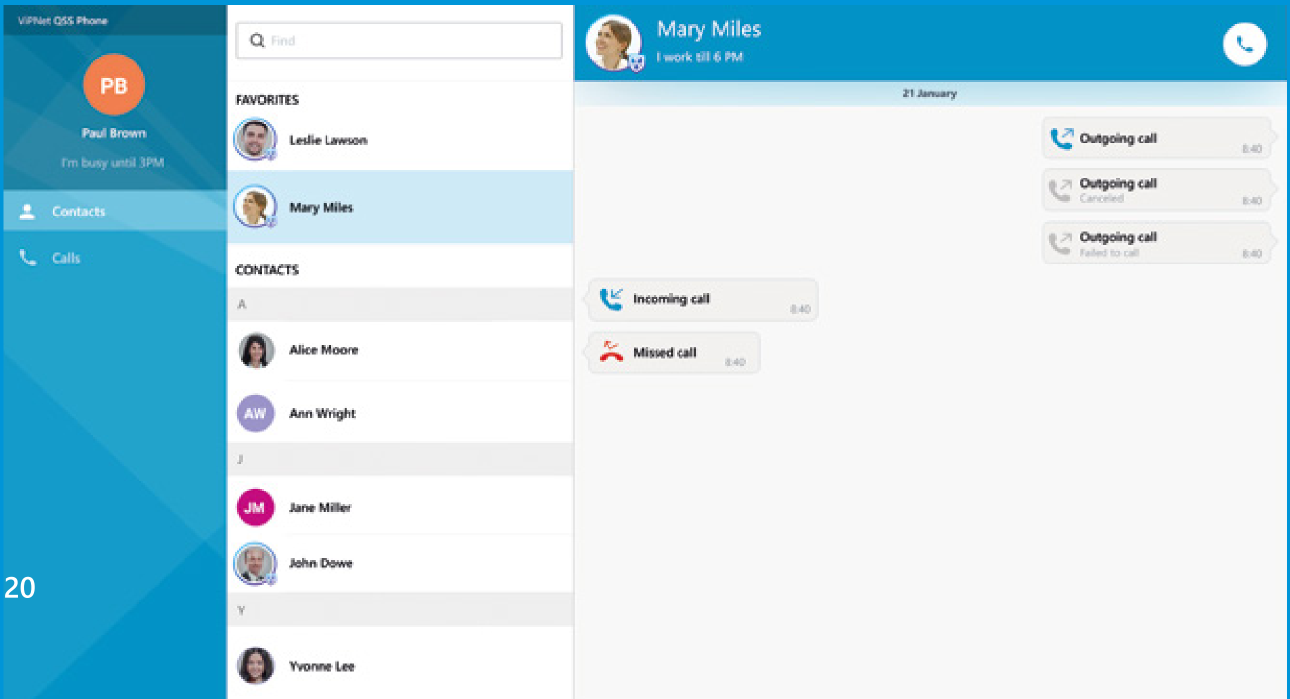
Comprehensive. ViPNet Connect unifies all corporate communications over any IP connected device.

Reliable. ViPNet Client 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.

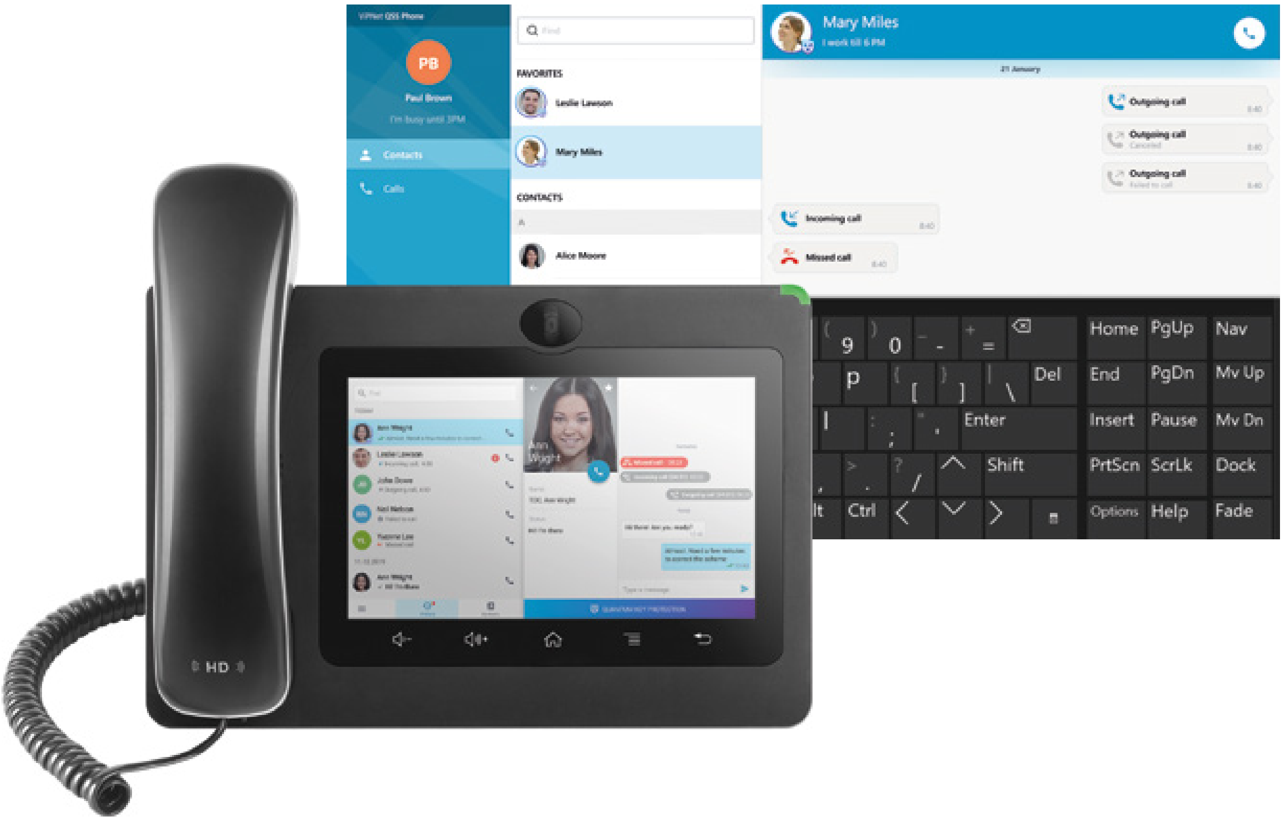
Protected contact list. The ViPNet Connect contact list is created by the ViPNet network administrator centrally and is isolated.

Secure file sharing. ViPNet Connect 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.



VIPNET CONNECT IP PHONE

A new unique device ensuring protection of business communications using ViPNet 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

VIPNET CONNECT FOR MOBILE DEVICES

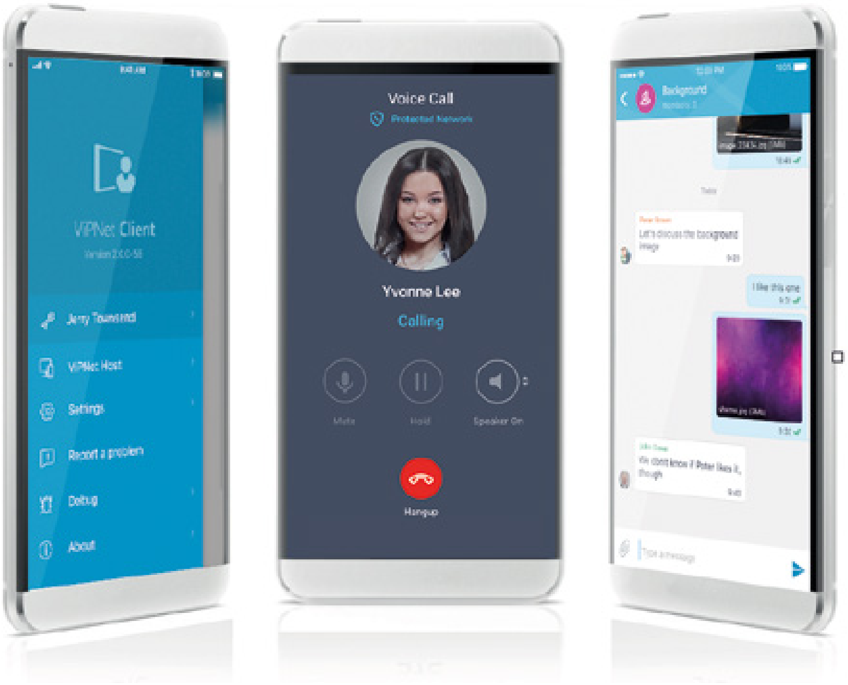
Employees are widely using WhatsApp, Viber, Telegram, Skype and other public services on their mobile devices within the corporate infrastructure. This poses significant information security risks and directly violates the GDPR requirements for the disclosure of personal data to third parties.

ViPNet Connect is a secure alternative to such public services. It ensures that corporate communications are protected.

ViPNet Connect encrypts voice calls, text messages, even attachments. ViPNet Connect 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 ViPNet'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 ViPNet Connect comes in.

ViPNet Connect was designed from the outset to be a secure communications app. It uses military grade point-to-point encryption, which is impervious to 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, ViPNet Connect can be deployed with accompanying ViPNet Mobile and Network security components to protect all traffic within a broader network not just data, whichgoes through the messaging application itself.

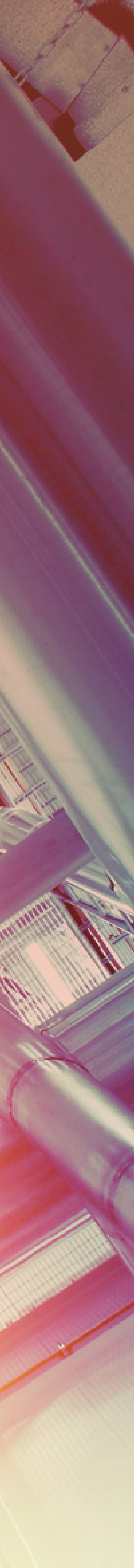
In order to be on the right side of GDPR compliance with respect to your chosen messaging app you should look for messaging applications that protect personal data from unauthorized access, use, copying, processing and storage. Moreover, you should use the strongest encryption available.

ViPNet Connect 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.

INDUSTRIAL SECURITY

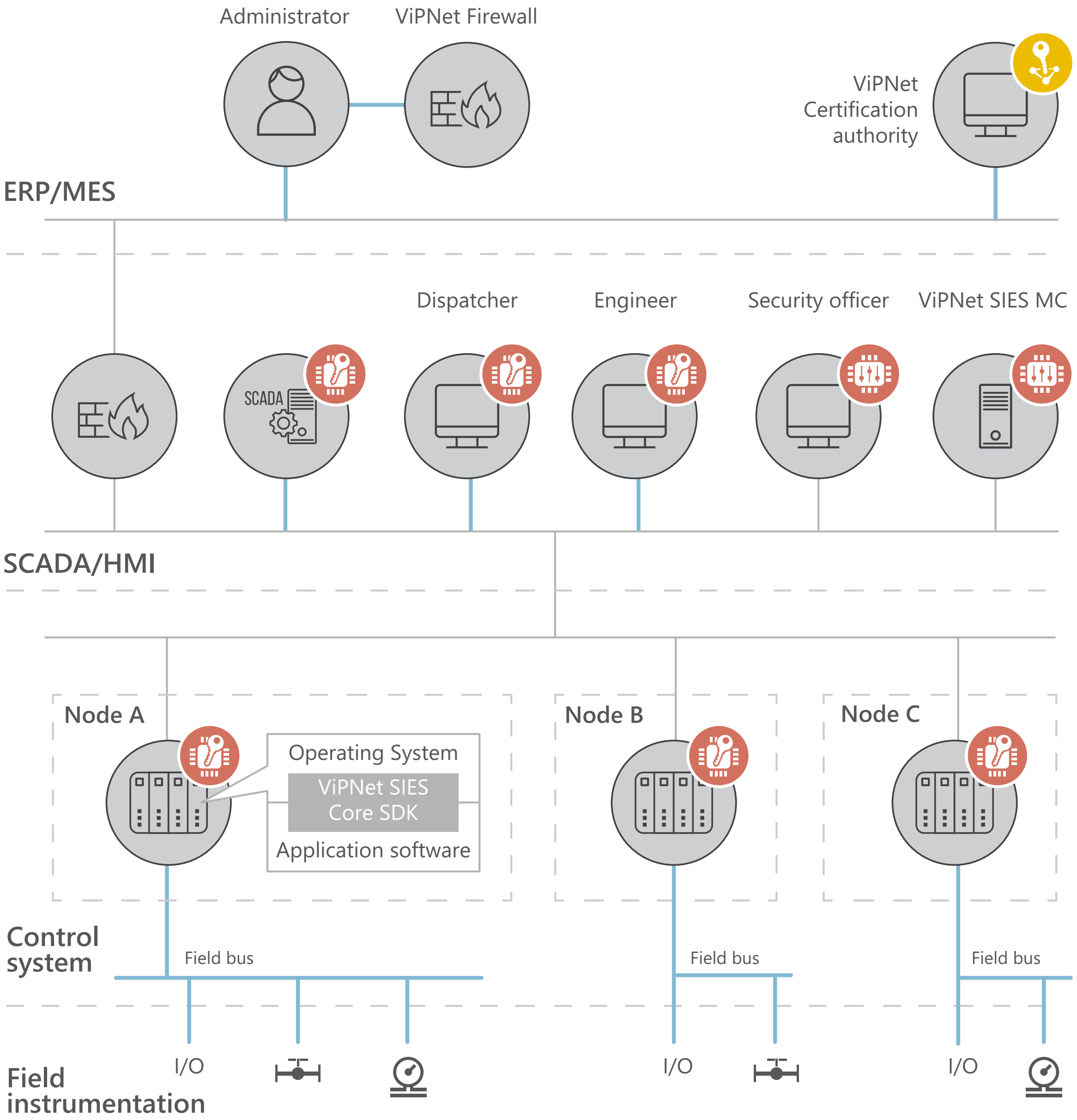
Embedded tools

Secure Industrial Gateway



EMBEDDED SECURITY TOOLS

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

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

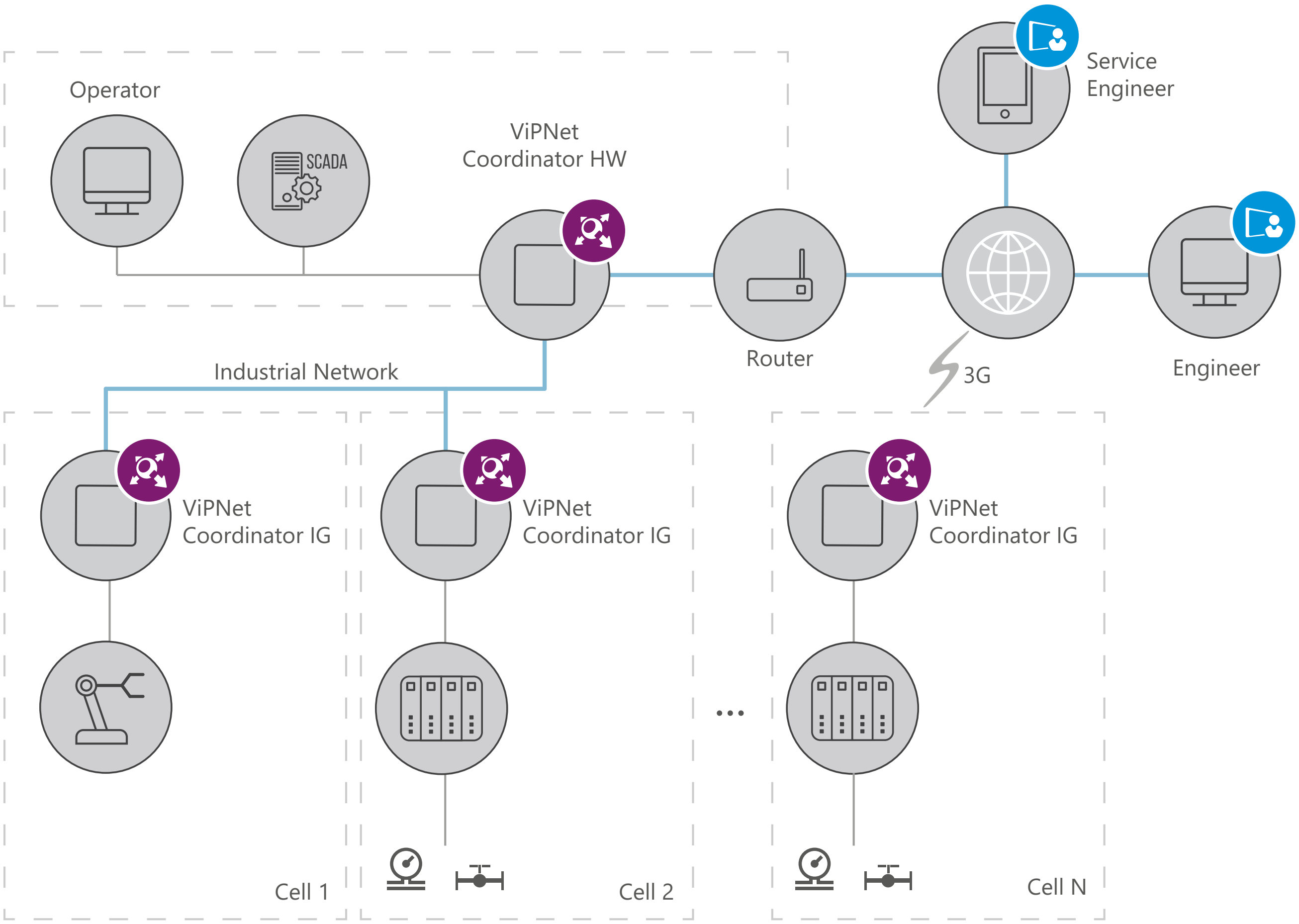
ViPNet SIES Unit software installed on the ICS dispatching level nodes such as servers and workstations and providing them basic cryptographic operations.

KEY BENEFITS

- When integrating the ViPNet 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 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, the ViPNet Coordinator IG supports industrial protocols and provides communication channels protection and firewall functionality.



FEATURES & COMPONENTS

- ViPNet Coordinator IG together with the ViPNet 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 (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 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

- 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

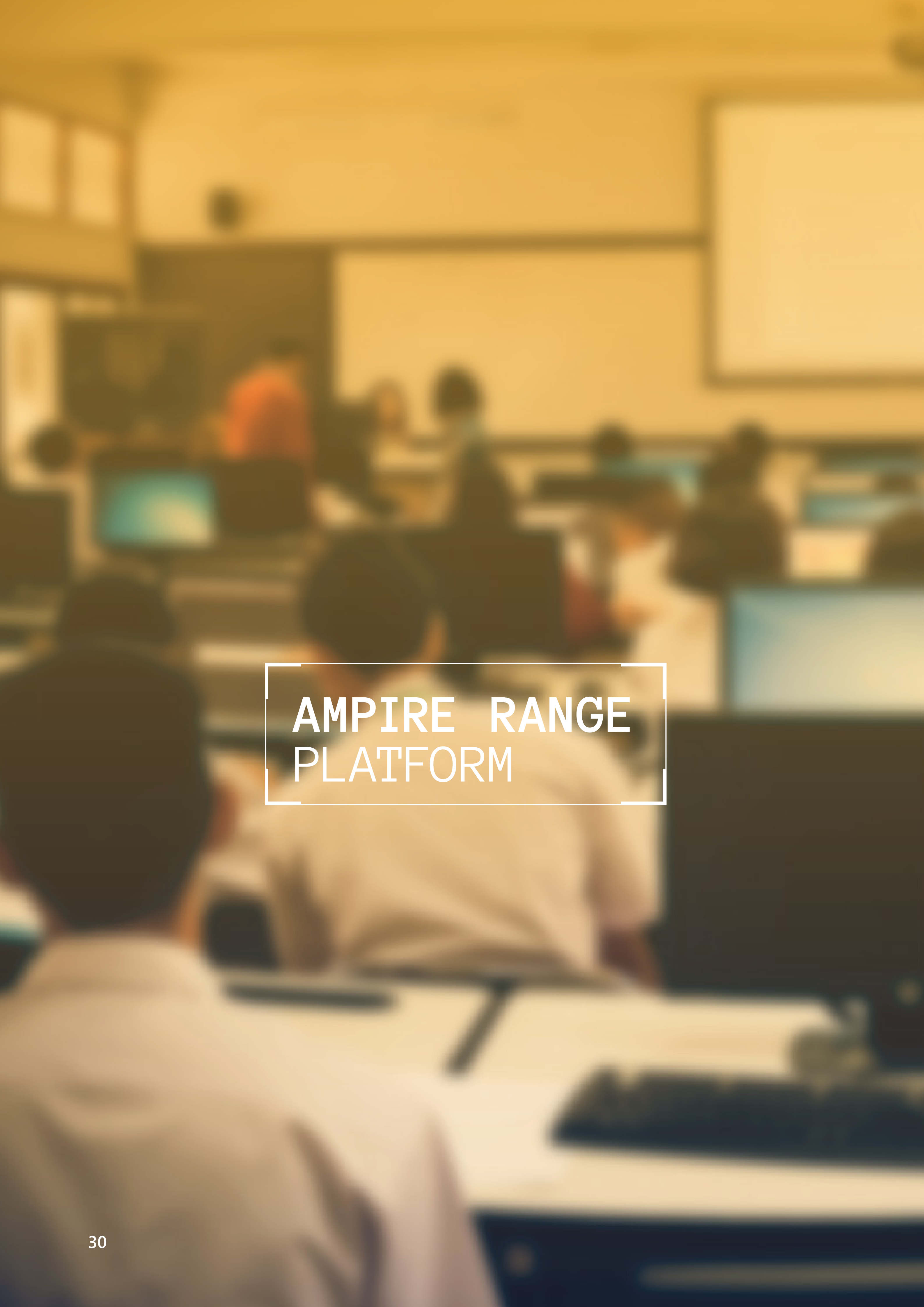
- DNS server
- NTP server
- DHCP server
- DHCP-Relay
- Hot Standby Cluster: Failover Coordinator in the ViPNet Failover Configuration

Industrial protocols support

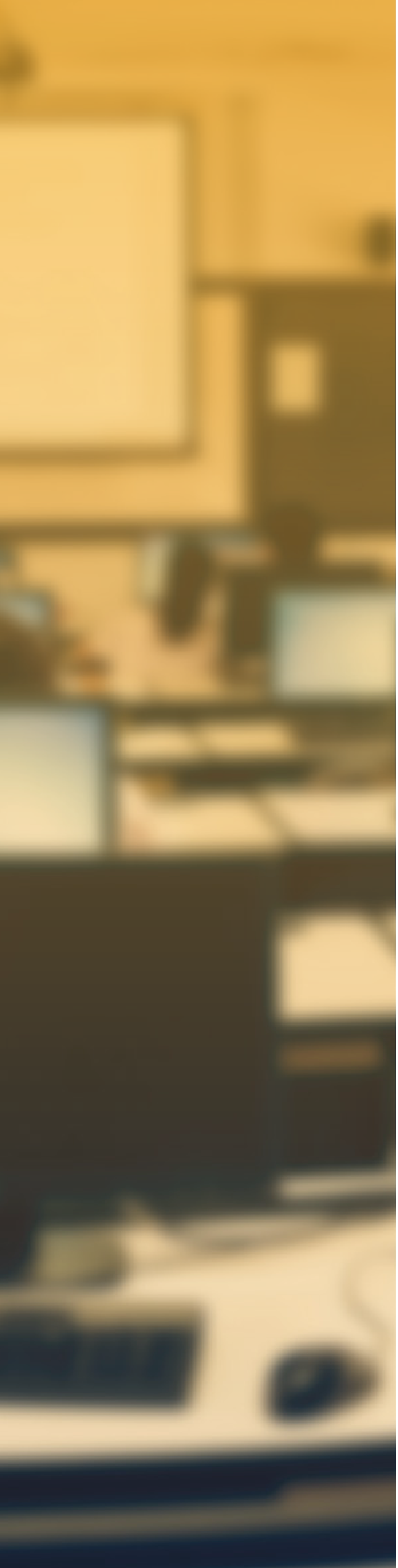
- Modbus TCP
- PROFINET
- Ethernet / IP
- DNP, IEC 60870-104, MMS
- OPC
- PTP
- LonWorks, Bacnet
- KNX, ZigBee, Z-Wave

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



AMPIRE RANGE PLATFORM



ViPNet Ampire Range – 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.

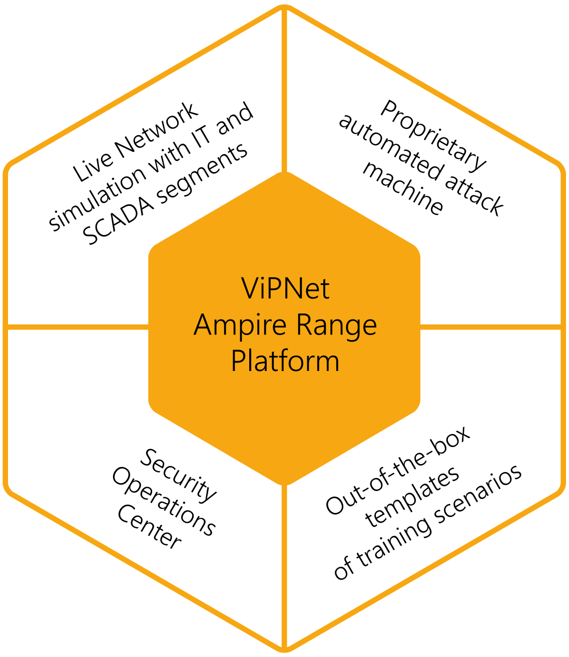
Hacking is on the rise, yet conversely, there is a global shortage of cyber experts available to help organizations counter the threat. Furthermore, many information security and network security staff have insufficient hands on experience responding to and mitigating real cyber-attacks.

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.

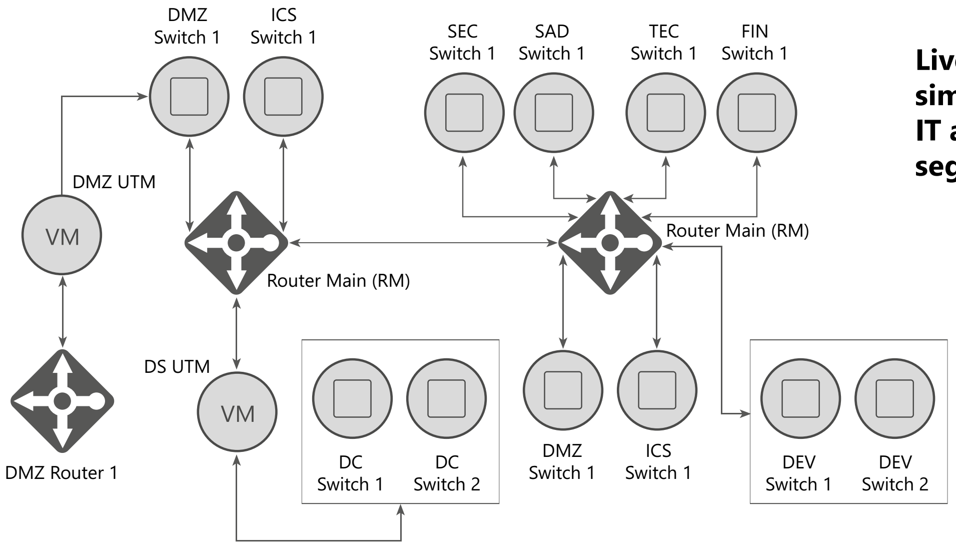
ViPNet Ampire Range Platform Provides Flexible Components Continuously Improved to Keep Pace with New Methods and Tactics:

- New templates and scenarios delivered monthly
- 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

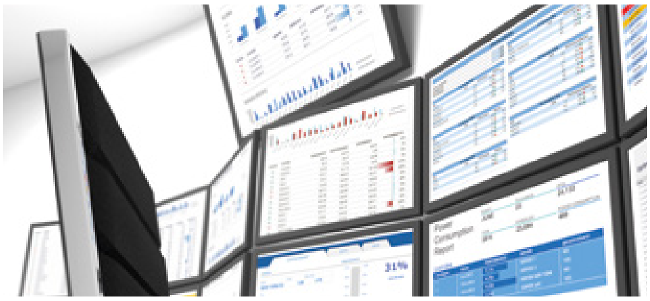
PLATFORM ARCHITECTURE


ViPNet Ampire Range Platform
Live Network simulation with IT and SCADA segments
Proprietary automated attack machine
Security Operations Center
Out-of-the-box templates of training scenarios

Live Network simulation with IT and SCADA segments

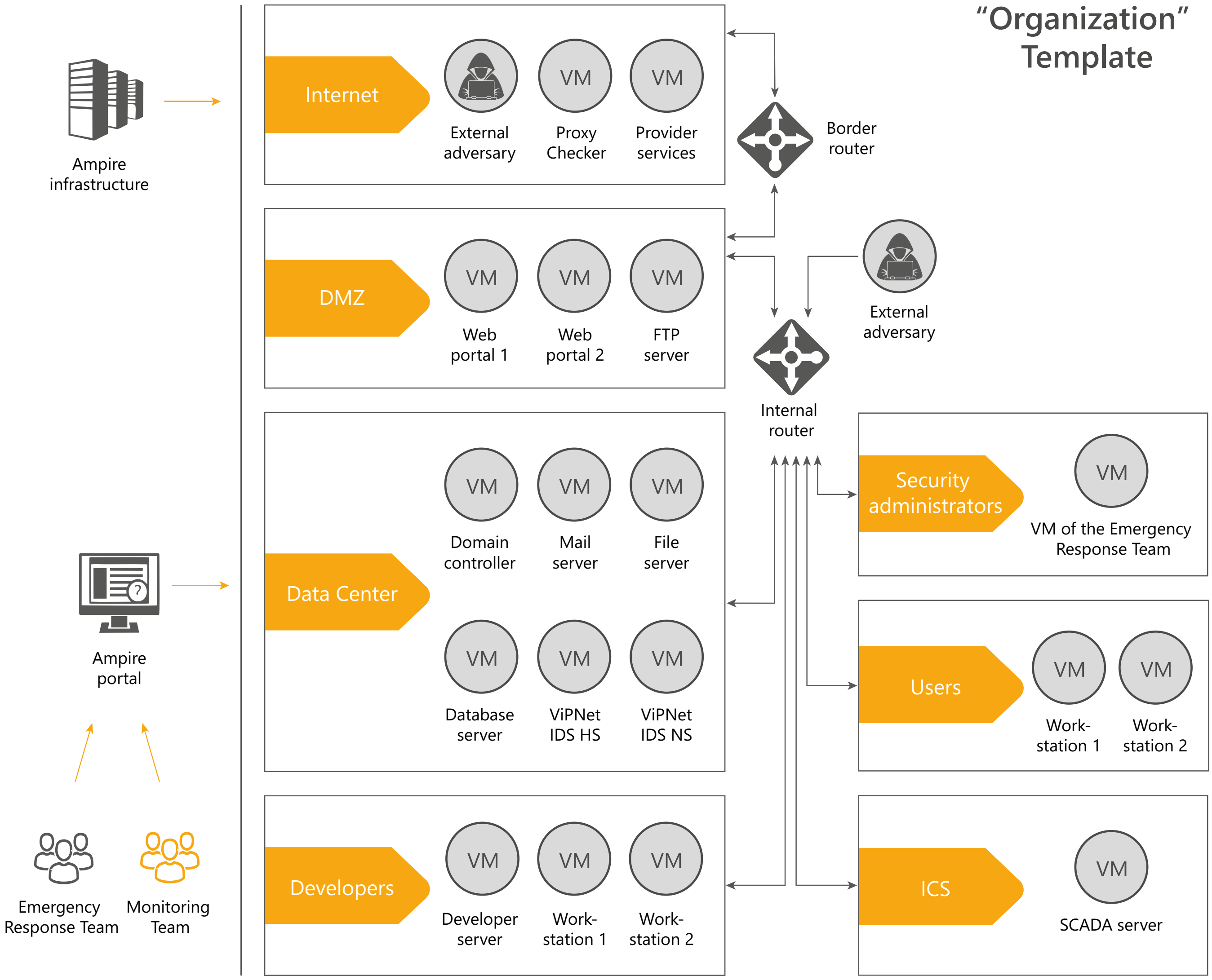


Security Operations Center



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 ViPNet Ampire Range 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
testbed, internal SOC team, training services for education, SMB, financial services

Cyber Range Platform as defined by the European Cyber Security Organization (ECS) consists of "interactive, simulated representations of an organization's local network, system, tools and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer."

Source: NIST (2018), Cyber Ranges, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

ABOUT US

Infotecs is a leading security software and solutions provider and has developed the ViPNet Ampire Range Platform on the basis of our extensive experience in helping organizations identify and thwart cyber attacks. Infotecs delivers security solutions, which are suitable for a broad range of applications and business processes and are used across clients in a variety of industries. Infotecs products are backed up by an unparalleled world-class support, development and technical team as well as a strong network of partners. Our channel-only sales model makes us committed to building a long-term, successful and profitable relationship together with Resellers and MSPs.

CONTACT US FOR DEMO OF OUR LIVE ENVIRONMENT TO EXPERIENCE HOW THE VIPNET AMPIRE RANGE PLATFORM WILL HELP YOU:

1. Increase Cyber Competence
2. Improve Preparedness
3. Acquire Practical Skills & Experience to Defend Your Network

Infotecs GmbH, Germany
Potsdamer Strasse 182, D-10783 Berlin
+49 30 206 43 66-0
info@infotecs.de
www.infotecs.de

Membership: