infotecs

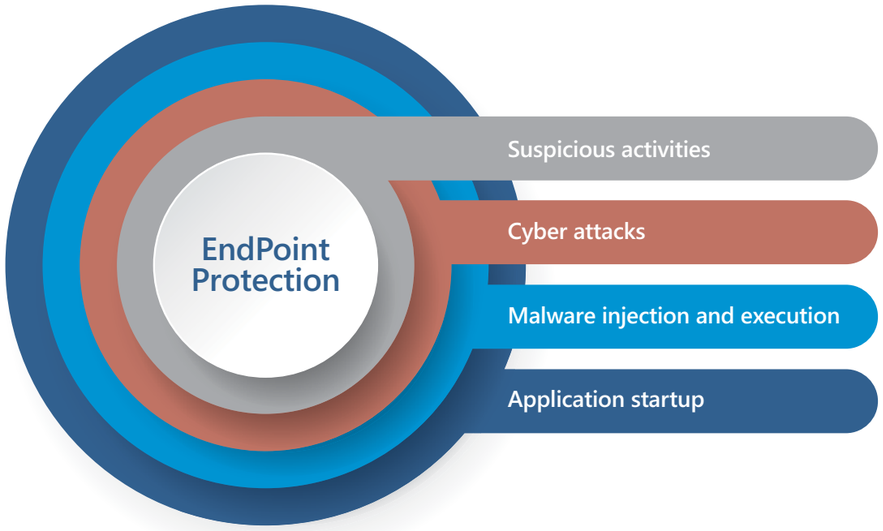
ViPNet
EndPoint Protection

All-in-one solution to secure endpoints from zero-day exploits, unknown malware and internal or external threats

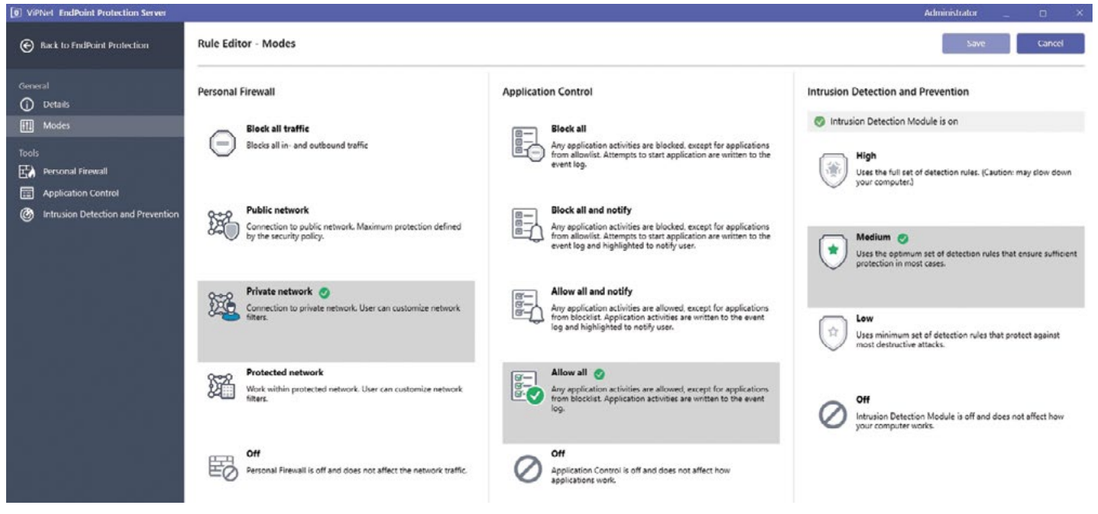
ViPNet EndPoint Protection provides high level security for desktop computers and laptops

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



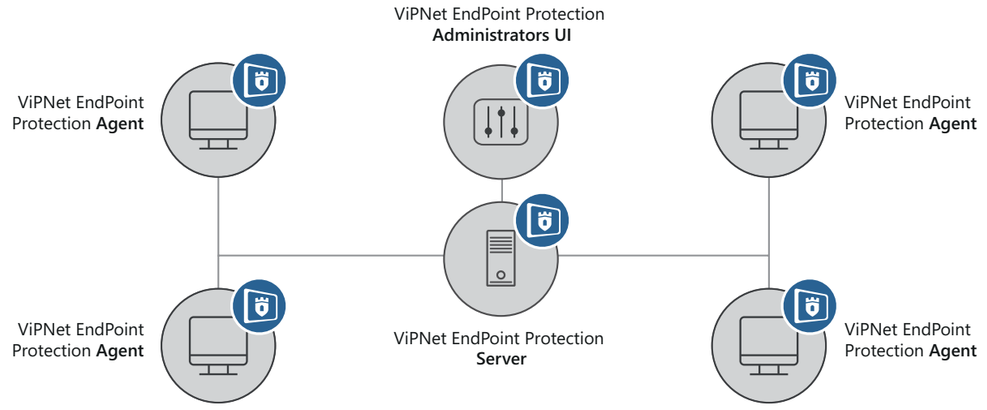
ARCHITECTURE

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



ADVANTAGES

- 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:

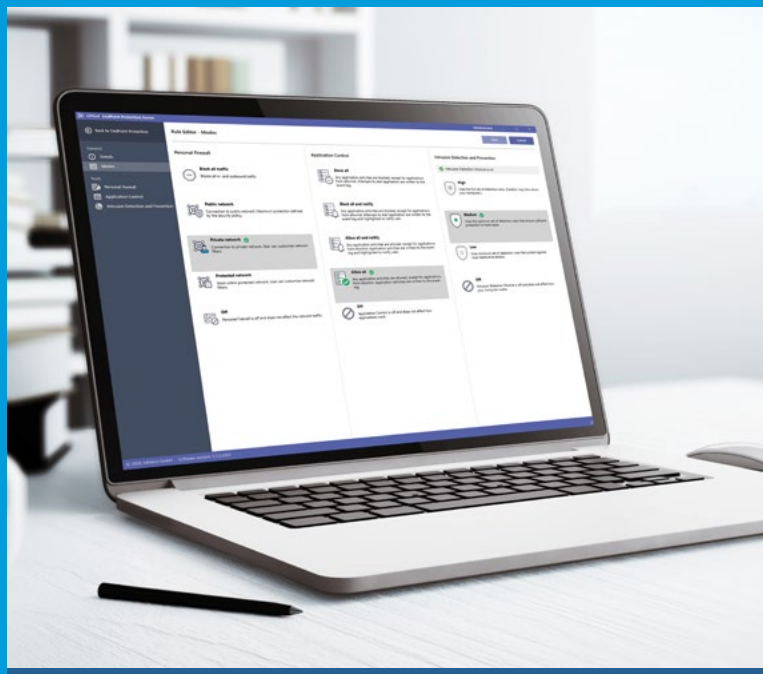
- Files
- Registry
- Processes
- Command line
- Applications Allow/Blocklists

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

infotecs

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

+49 30 206 43 66-0

info@infotecs.de

www.infotecs.de

EPP21_00EN

ViPNet Virtual Private Network