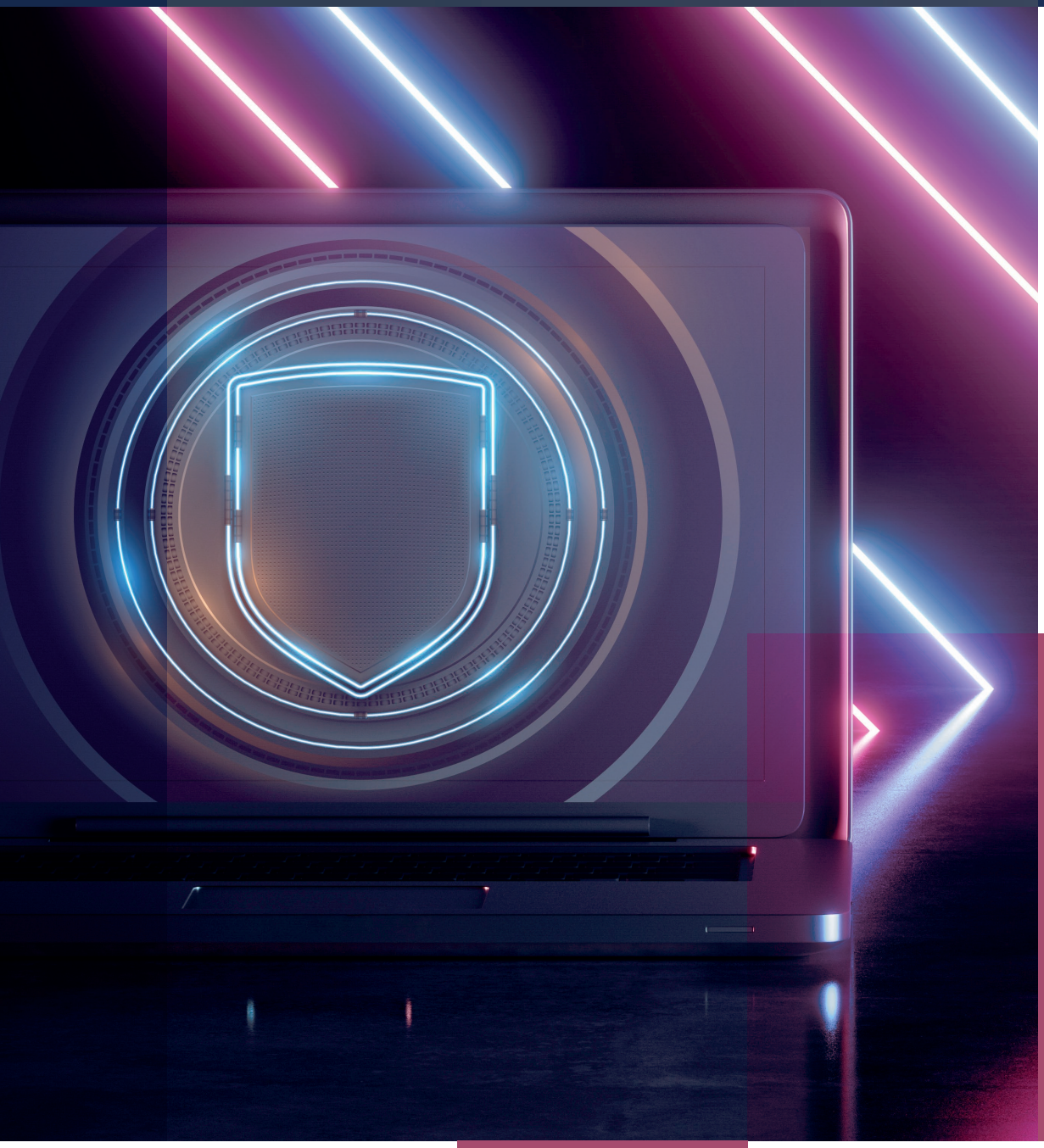
Protelion Endpoint Protection

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



PROTELION

Protelion Endpoint Protection provides high level security for desktop computers and laptops.

COMPONENTS

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

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

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

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

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

PROTELION ENDPOINT PROTECTION

PREDEFINED SECURITY PATTERNS

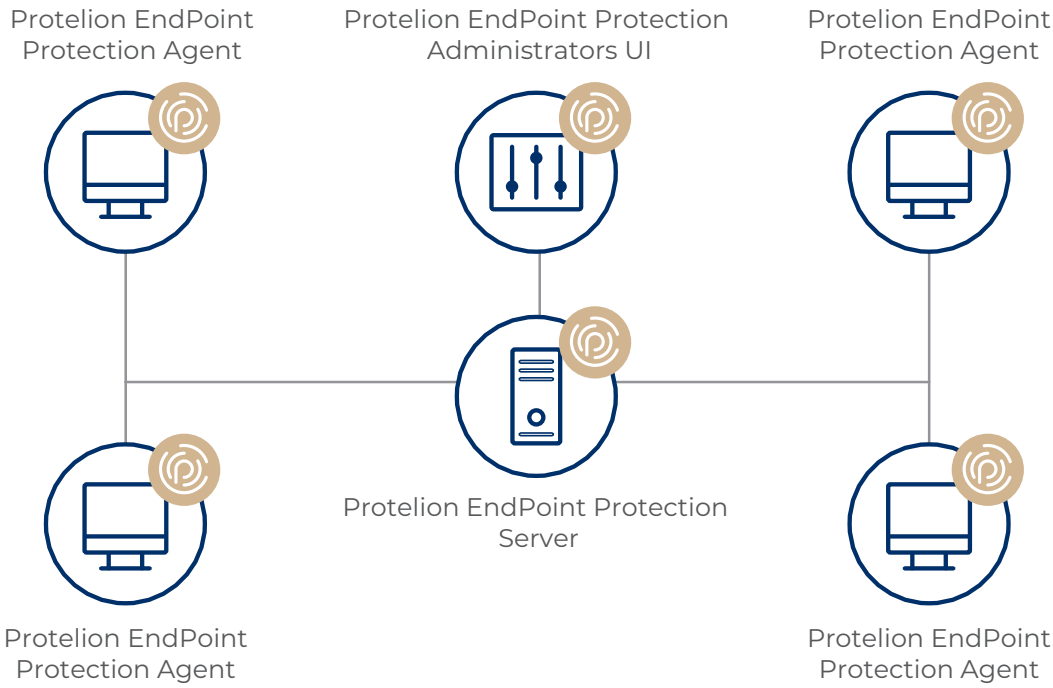
ARCHITECTURE

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

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

02 Administrator's UI to manage the Server and view the status of endpoints and server in real time.

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



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.
- Preventing malicious behaviors of applications, like a weaponized Office document that activates bad script or installs another application and runs it.
- Compatibility with Protelion TDA enhances incident detection and response.
- Protection from potentially unwanted applications.
- The Endpoint Detection and Response technologies, such as a host's suspicious activity, monitoring and counteracting.
- Detecting and deleting malicious executables, as well as detecting and blocking fileless attacks.
- Proprietary Behavioral Analysis technologies.

FEATURES

HIDS/HIPS (HOST INTRUSION DETECTION/PREVENTION SYSTEM)

Detects and prevents attacks using signature and heuristic method.

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

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

PERSONAL FIREWALL

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

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

SECURITY NOTIFICATIONS

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

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 batch adjust security settings on all hosts added to Protelion Endpoint Protection.

SUPPORTED OPERATING SYSTEMS

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

BEHAVIORAL ANALYTICS MODULE

Uses a protected host's normal activity model powered by machine learning. Detects various anomalies:
- Abnormal logon to the system
- Abnormal process creation
- Abnormal scheduler task creation
- Abnormal startups of the system utilities
- Etc.

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.

ANTIMALWARE MODULE

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

PROTELION

Protelion
Oberwallstr. 24
D-10117 Berlin

info@protelion.com

+49 30 206 43 66-0