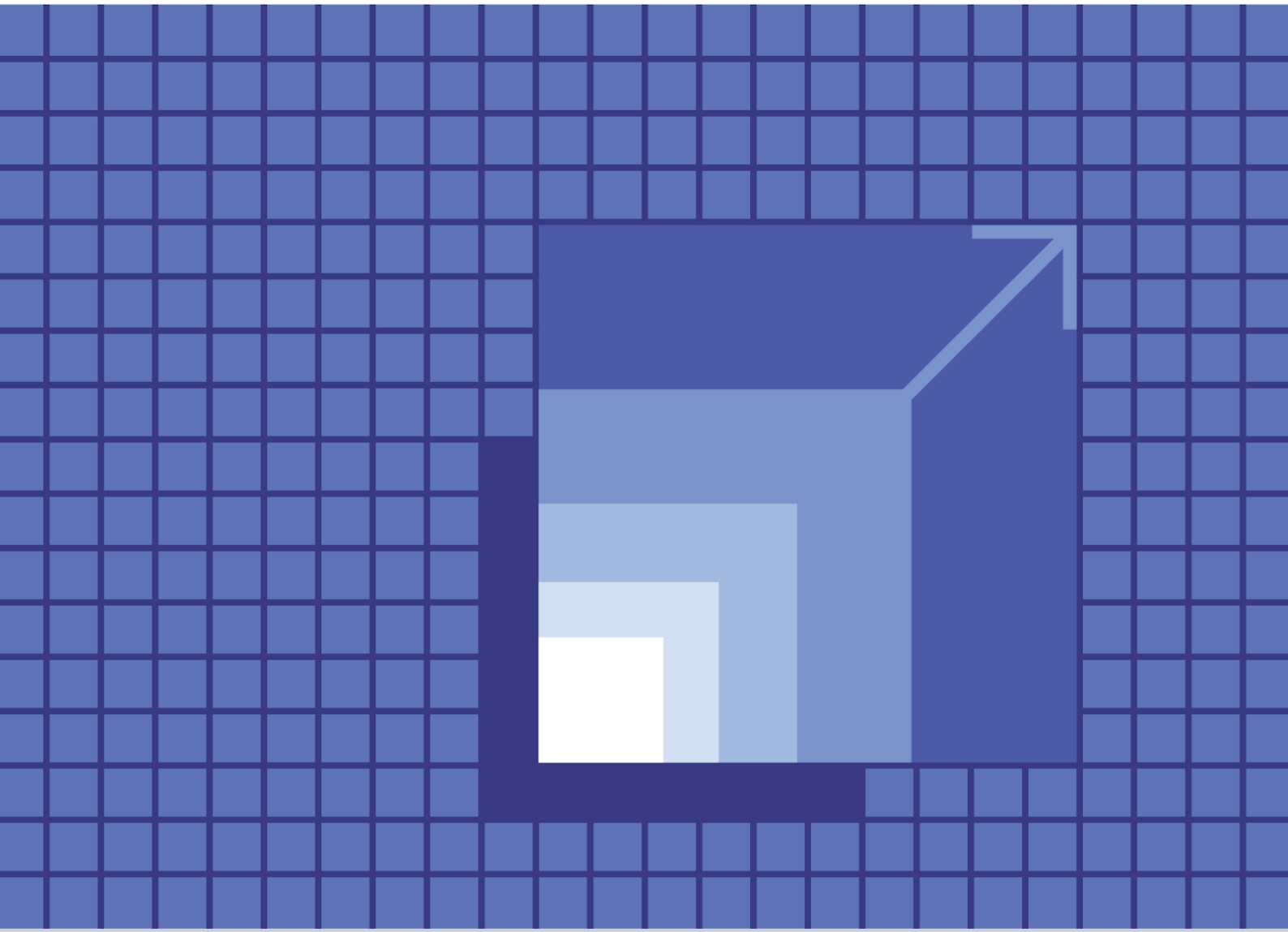
ENDPOINT PROTECTOR | by CoSoSys

Architecture, Resources and Scalability



Version 3.0

Date 15.11.2022

Table of Contents

Document Changelog

Version	Date	Notes
1.0	2017	The document was created
2.0	05.04.2022	The document was updated
3.0	15.11.2022	The document was updated with the current template

1. Introduction

This document is a brief description of the Endpoint Protector solution addressing large-scale deployments of more than 5,000 endpoints. It addresses the solution scalability (backend, administration server, etc.) and not the specific endpoints it protects or the policies and settings it can enforce.

Endpoint Protector with its different modules - consisting of Device Control, Content Aware Protection, eDiscovery, and Enforced Encryption - applies its policies at the endpoint level.

The number of endpoints, their geographical distribution, network bandwidth, etc., impacts the Endpoint Protector system requirements and will need to be addressed and planned for.

Deployed as a Virtual Appliance, Endpoint Protector works out of the box for approximately 1,000 endpoints. As a Hardware Appliance, different configurations are available, scaling up to 5,000 endpoints from a single appliance. All out-of-the-box versions of Endpoint Protector use MySQL as a database.

2. Main components

Endpoint Protector is designed around several physical entities:

- **Computers**
  The Windows, Mac, and Linux workstations that have the Endpoint Protector Client installed.
- **Devices**
  The devices that are currently supported by Endpoint Protector (USB devices, digital photo cameras, USB memory cards, etc).
- **Users**
  The user who will be handling the devices and the computers.

The Server side of Endpoint Protector has different parts working close together:

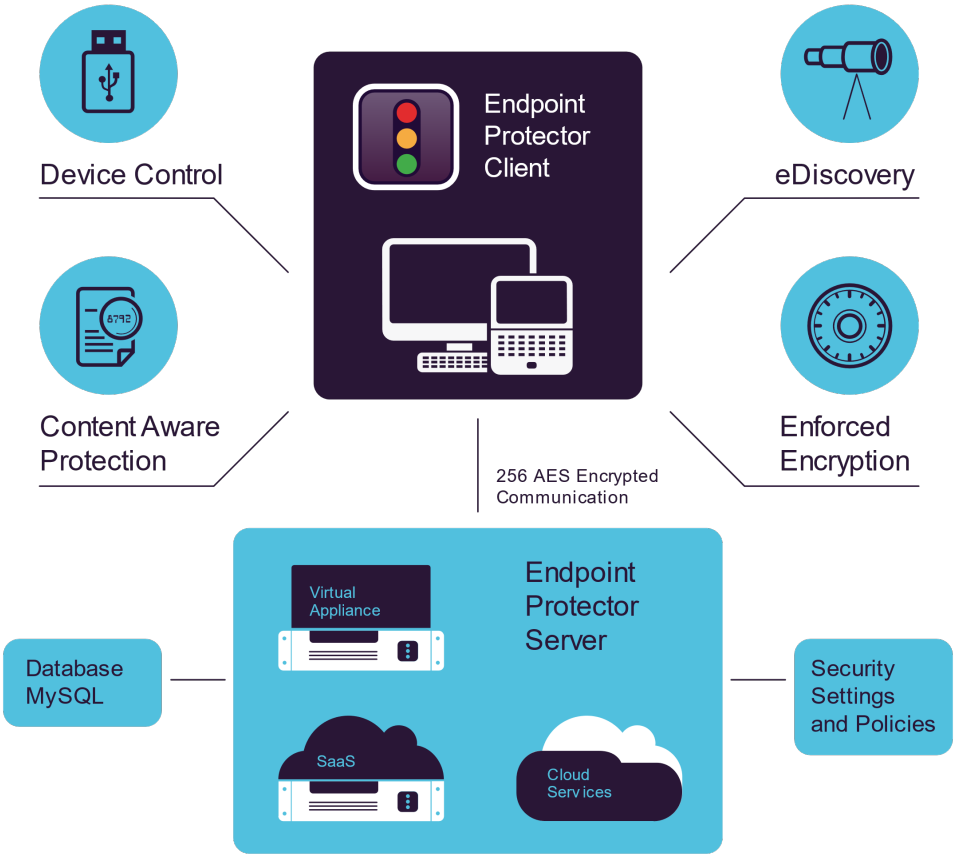
- **Endpoint Protector Hardware or Virtual Appliance** – containing Operating System, Database, etc.
- **Web Service** – communicating with the Endpoint Protector Clients and storing the information received from them.
- **Endpoint Protector User Interface** – managing the existing devices, computers, users, groups, and their behavior in the entire system.

The Client-side of Endpoint Protector has two different components:

- **Endpoint Protector Client** – enforcing the rights and settings received from the Server on Windows, Mac, and Linux computers; it also automatically deploys EasyLock on the USB storage devices.
- **EasyLock Client** – enforcing 256 AES encryption on USB storage devices as specified from the Server; it is a stand-alone application compatible with Windows and Mac computers.

For a complete list of supported endpoint operating systems, consult the user manual(s).

3. Endpoint Protector Architecture Diagram



4. Endpoint Protector Client

The Endpoint Protector Client has one of the smallest footprints of any similar solution on the market. The resources it consumes or the bandwidth it uses is insignificant.

The processing power consumed, and bandwidth used by the Client depends on the functionalities, settings, policies used, and the endpoint's hardware configuration. In an idle state, the base requirements are:

- **CPU**: At least 1 GHz dual-core CPU
- **RAM**: 30 MB
- **Bandwidth**: Less than 1 Kbs (Kilobit per second) when idle. It can increase depending on usage when sending logs or uploading shadow files.

Note: For Content Aware Protection & eDiscovery scanning, more CPU and RAM are required.

A closer look, with all modules enabled, functionalities, and policies configured for a stress test, the average resources it consumes are:

Resources consumed in stress test conditions			
Module	**Device Control**	**Content Aware Protection**	**eDiscovery**
CPU	1 GHz	1 GHz (in general) > 1 GHz (during scanning)	1 GHz (in general) > 1 GHz (during scanning)
RAM	30 MB	30 MB (in general) > 30 MB (during scanning)	30 MB (in general) > 30 MB (during scanning)
Bandwidth	< 1 Kbs (when idle) > 1 Kbs (when sending logs or uploading shadow files)	< 1 Kbs (when idle) > 1 Kbs (when sending logs or uploading shadow files)	< 1 Kbs (when idle) > 1 Kbs (when sending logs or uploading shadow files)

5. Endpoint Protector Updates

Endpoint Protector updates are available through the Live Update or Offline Patches features.

The average size of an update is:

- **Endpoint Protector Client for Windows** ~ 50 MB
- **Endpoint Protector Client for macOS** ~ 50 MB
- **Endpoint Protector Client for Linux** ~ 15 MB (with no dependencies)
- **EasyLock Enforced Encryption Client** ~ 15 MB
- **Endpoint Protector Server** ~ 30 MB

For environments where the payload of an update is a concern, saving the bandwidth can easily be done by using Offline Patches.

Moreover, the Endpoint Protector Clients can also be deployed manually, directly on each endpoint.

6. Professional Services

For larger setups, please feel free to involve our professional services team directly, which will help tailor your deployment to your needs.

For an onsite setup, if required, we recommend two engineers and a project manager for 1 week at the customer's site. Product training can also be provided during this time.

7. Disclaimer

The information in this document is provided on an “AS IS” basis. To the maximum extent permitted by law, CoSoSys disclaims all liability, as well as any and all representations and warranties, whether express or implied, including but not limited to fitness for a particular purpose, title, non-infringement, merchantability, interoperability, and performance, in relation to this document. Nothing herein shall be deemed to constitute any warranty, representation, or commitment in addition to those expressly provided in the terms and conditions that apply to the customer’s use of Endpoint Protector.

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions, and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers’ request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

EndpointProtector.com