# Zecurion 12 positive criteria’s to compare with other DLP solutions

Here are some talking points how to win comparison with other DLP vendors.

We can specify the following tech potential major advantages of Zecurion DLP.

General Architecture and Deployment approaches:

1. Zecurion has several options for on-prem DLP modules deployment on customer site:

* ­Traffic interception and physical blockage on-the-fly on hosted operational gateways:
* SMTP mail servers
* SWG Proxy Server (ICAP compliant)
* Zecurion NGFW Gateway Server (ICAP compliant)
* Traffic Control endpoint module with web-traffic blockage mode.
* Ready-to-use Zecurion SWG operational web gateway and Zecurion NGFW gateway module
* MTA SMTP relay, SWG or NGFW module in-between operational Mail and Web channels
* ­Interception and also on-the-fly blockage on endpoint workstations
* DCAP modules for file monitoring and system audit in local LAN
* Several types of supported RBDMS MS SQL and PostgreSQL for system repository.

1. Zecurion endpoint agent supports all actual Windows client version releases starting from outdated Windows XPSP3 and all later releases with weak system resources (Core 2 Duo and >1 Gb RAM) and Linux Ubuntu releases.
2. Zecurion endpoint agent works successfully and perform data classification on workstations in fully-autonomous mode with no necessary direct IP connection to the central Policy Server.
3. Zecurion is able to install DLP interceptor plugin module on MS Exchange server and control all type of mail (incoming\outgoing and internal).
4. Zecurion Traffic Control module is able to capture and re-encrypt https traffic both at operational web-gateway module (i.e. Check Point, FortiGate, Cisco etc.) over ICAP protocol and at endpoint local agent module.
5. Zecurion endpoint agent is able to decrypt and capture https traffic at endpoint the following two ways:

* Using standard man in the middle (MITM) algorithm
* Extract https traffic using deep API integration with the following browsers at endpoint: Chrome, IE 8+, Firefox, Opera and Edge (web traffic can be blocked in browser level without MITM tools)

1. Zecurion endpoint agent is able to capture mail traffic at endpoint using deep API integration with the following mail clients: Outlook, Thunderbird and Lotus Notes.
2. Zecurion will fully support Active Directory domain. System officers and administrator will use AD admin account credentials from corp domain to authorize in Zecurion Management web console.
3. Also all Zecurion server modules can be installed in Linux Server environment.

Major System Capabilities and Strengths:

1. Zecurion has user-centric captured data organization and analysis method. Each monitored employee will have personal system profile with the following captured history and data lake:

* All captured data, leakages and assessments (see next points below)
* DCAP file activity audit and monitoring (see para 6-10)

DLP will create the full list of monitored employee’s profiles automatically using organization structure from corp MS AD.

1. Zecurion has advanced engines for data mining and analysis to perform the following estimation for monitored users and staff:

* User behavior analysis (UBA) model + anomalies detection
* Risk assessment model
* Staff control productivity assessment model with detailed summary of staff’s working time.

1. Zecurion is able to decrypt and trace various web IM messengers (chats, attachments and voice recordings). Zecurion supports monitoring **and blockage** for WhatsApp and Telegram thick desktop client and web-browser client for IM web service.

Zecurion supports also Skype, Viber, ICQ, Jabber, MS Teams traffic capturing on endpoints.

1. Zecurion has staff control working time analysis engine. Endpoint agent will collect and analysis employees’ working time and measure aggregated productivity for the following type of actions:

* Working time analysis and user discipline
* Time usage in certain application on PC
* Web sites and portal usages.

Detailed time sheets for the staff will be available.

1. Zecurion has more than ten data classification techniques. Those are the following:

* Dictionaries with keywords
* Regular expressions and templates
* Digital fingerprint for documents, images and source rows of target databases
* Morphology tools
* Bayesian probabilistic analysis method with dictionaries
* Machine learning algorithm (Machine Learning SVM)
* Images templates of structured objects
* OCR recognition with third party enterprise engines Abbyy OCR and Google Tesseract.

1. Zecurion is able to recognize audio files and capture voices in this files to text
2. New customizable “Data class” attribute for captured files and documents based on data classification methods. This attribute (label) can be used in Policy and Report module for report creation, policy customization.
3. Zecurion has advanced DCAP capabilities for file monitoring and system audit. In terms of architecture on the fly monitoring can be run in the following ways:

* Active server module, which can be installed on file servers and other entities
* Endpoint module to monitor file changes on workstations.

1. Zecurion DCAP has high degree of integration with DLP endpoint modules, actual DLP policies and data classification rules.
2. Zecurion DCAP module is able to monitor the following data sources:

* File servers and shared folders in corp LAN
* Local HDD drivers in PCs
* MS Active Directory and other LDAPs.

1. Zecurion DCAP module is able to run on-the-fly analysis and create consolidated reports for files and folders changes:

* Logging files-based events and ACL changes
* Where files and file duplicates are storied?
* Access rights summary for inspected files and folders
* On-the-fly monitoring for the selected target files or folders.

1. Zecurion DCAP identify the following events:

* Anomalies identification (massive operations with files, replacements etc)
* Files duplicates identification
* File owners. Who is the last editor? Who is the most often use this file?
* Get out of the excessive rights for files.

1. Zecurion DCAP is able to monitor and identify changes and anomalies in MS AD.
2. Zecurion has policy orientated deployment approach: **Target Channel** -> **Filtering Condition** -> **System full-auto Reaction**. Operator can create policy once and then broadcast it to selected target channels: SMTP Mail, Web channel, IM messengers, Devices, Printers, Discovery crawler etc. Policies will work on gateway server instances and workstations in fully-autonomous mode.
3. New policy creation interface in Zecurion release 12 web management console in Policy Server. This modern SWG/NGFW-like policy creation interface provides new capabilities for policy management.
4. In Zecurion it is very simple to turn on physical blockage mode for selected channels in “one click” in administrator’s GUI. Zecurion supports live-time blockage option for the following channels: SMTP mail, Web channel, Printers, Removable USB storage devices and other.
5. In Zecurion web management console in policy creation wizard in web console has simple interface with multi-level condition section to combine filtering expression with AND, OR, NOT Boolean operators.
6. Zecurion web management console also has “Dark Style” mode for operator’s eye saving.
7. In Zecurion it is very simple to setup in policy creation wizard the following verification rules:

* Incident attributes verification (User name, IP address, host name, file size, channel, recipient name, sender name, file text, body text, device name, incident type, web service, process, document metadata properties, current user’s UBA index, user status, triggered policy, amount of printed pages, user belong to specific domain etc.)
* Verification using particular digital fingerprints
* Verification using particular dictionaries
* File type verification (text, graphic, audio, video, archive, executable, encrypted data, unknown type).

1. In Zecurion administrator is able to setup and assign the following scope of auto executable system reactions in policy creation wizard:

* Create incident in system repository with the attributes
* Place and block violator object in system mail quarantine
* Send customizable notification over SMTP mail service
* Push user notification alert in Windows system tray in workstation
* Remove violator object from mail body or from user’s workstation
* Create incident in Event log or Syslog instance
* Encrypt copied file or document
* Create snapshot of user’s workspace in active OS session
* Create snapshot of web camera on user’s PC
* Assign specific status label to the user
* Active windows session logout on target PC for the user with the following options:
  + Repeated user login is impossible
  + Block user account in corp MS Active Directory.
* Screenshot making blocking in workstation for specific application launched
* Add customizable watermark on top of specific application launched.

1. Zecurion has option to activate advanced capturing on endpoints for the following channels:

* Screen photo detection module with AI capabilities. Alerting in case of making photo of the screen with a smartphone in live-mode
* Keyboard sniffing tool
* Microphones recording tool
* Screenshots and user session logs
* Web camera remote control
* Remote live monitoring session control of user’s workspace.

1. Zecurion has advanced capabilities to detect making photo of the screen with a smartphone. This feature will work on endpoint. Detecting tool are armed with Artificial Intelligent algorithm based on neural networks. It will detect image of the smartphone in live-mode with web camera snapshots.
2. Zecurion management console and reports module have the following:
   * Unified customizable homepage for operator with the set of customizable widgets, diagrams and info panels
   * Unified employee profile section in Report module web console where all incidents\leakages and key statistics regarding this user are stored (UBA and Emotional state indexes + Connection map + User’s comparisons)
   * Compare the persons and departments with unified set of parameters
   * Case management tools (incident response platform IRP)
   * Unified report creation wizard with customizable reports with filtering options based on logical operator OR, AND, NOT. Also Zecurion is able to export rows to XLSX, CSV, PST and PDF file formats
   * Unified report displaying dialogue between two sides.
3. Zecurion has case management tool in management console (incident response platform IRP) to perform investigations, assign the task for the operators and track workflow statuses and tasks.
4. Zecurion is able to setup very granular user’s access control list ACL for peripheral devices and memory removable drives at endpoint. Also Zecurion has pre-installed extended list of built-in classification of device for usage in policy creation wizard for device control channel:

* ­Typical device classes: USB devices, network devices, DVD/CD drives, removable media, printers, hard drives, PCMCAI adapters, modems, IrDA etc.
* ­Physical device classes: storage controllers, Bluetooth, portable devices, tape drives, smart card readers, IEEE devices etc.
* Black and white lists of devices.

1. Zecurion has option to perform hiding endpoint agent signs in the following in MS Windows consoles:
   * Agent processes in “Task manager” console
   * Entry in “Programs and features” console
   * Entry in “System services” console
   * File Explorer of OS.