LUCIDVIEW SOLUTIONS

Table of Contents

LUCIDVIEW OVERVIEW

LucidView Background

LucidView is a South African owned and based business with an international footprint that has been in the business of providing Secure, Safe, Clean and Optimised networking since 2005.

The LucidView product and solution suite is developed and designed to provide full Internet Gateway Management Solutions for Internet Service Providers (ISPs), IT Service Providers (ITSPs), large enterprises, schools and government organisations, not only in South Africa but around the world.

LucidView Capabilities Overview

The LucidView product and solution suite is developed and designed to provide full Internet Gateway Management Solutions for Internet Service Providers, IT Service Providers, large enterprises, schools and government organizations, not only in South Africa but around the world.

The LucidView product and solution suite has the following capabilities:

1. **Intrusion Detection and Prevention (IDPS)** effectively manages Internet content and provides cybersecurity by reducing the ability of remote hackers to commit data theft or plant ransomware, spyware, keyloggers, perform DDOS attacks, etc. It is extremely effective and efficient in identifying and nullifying day zero attacks. LucidView's behaviour based AI engine allows all hosts, domains and IPs that it deems legitimate and blocks anything that is considered not and is a likely threat.
2. **Content Management** provides a powerful Content Filter that allows for any organisation to define their own "Clean Internet" Policy, be it for business, children, etc.
3. **Saturation Management / Content Based Traffic Shaping** performs extremely sophisticated and effective saturation management / traffic shaping, thereby eliminating the need for costly bandwidth upgrades. It keeps your internet responsive by, for example, limiting download speed or the streaming quality of media videos to ensure that content is always available without sacrificing latency.
4. **Insights** provides the following capabilities to enable LucidView's philosophy that

"You can't manage what you can't see":

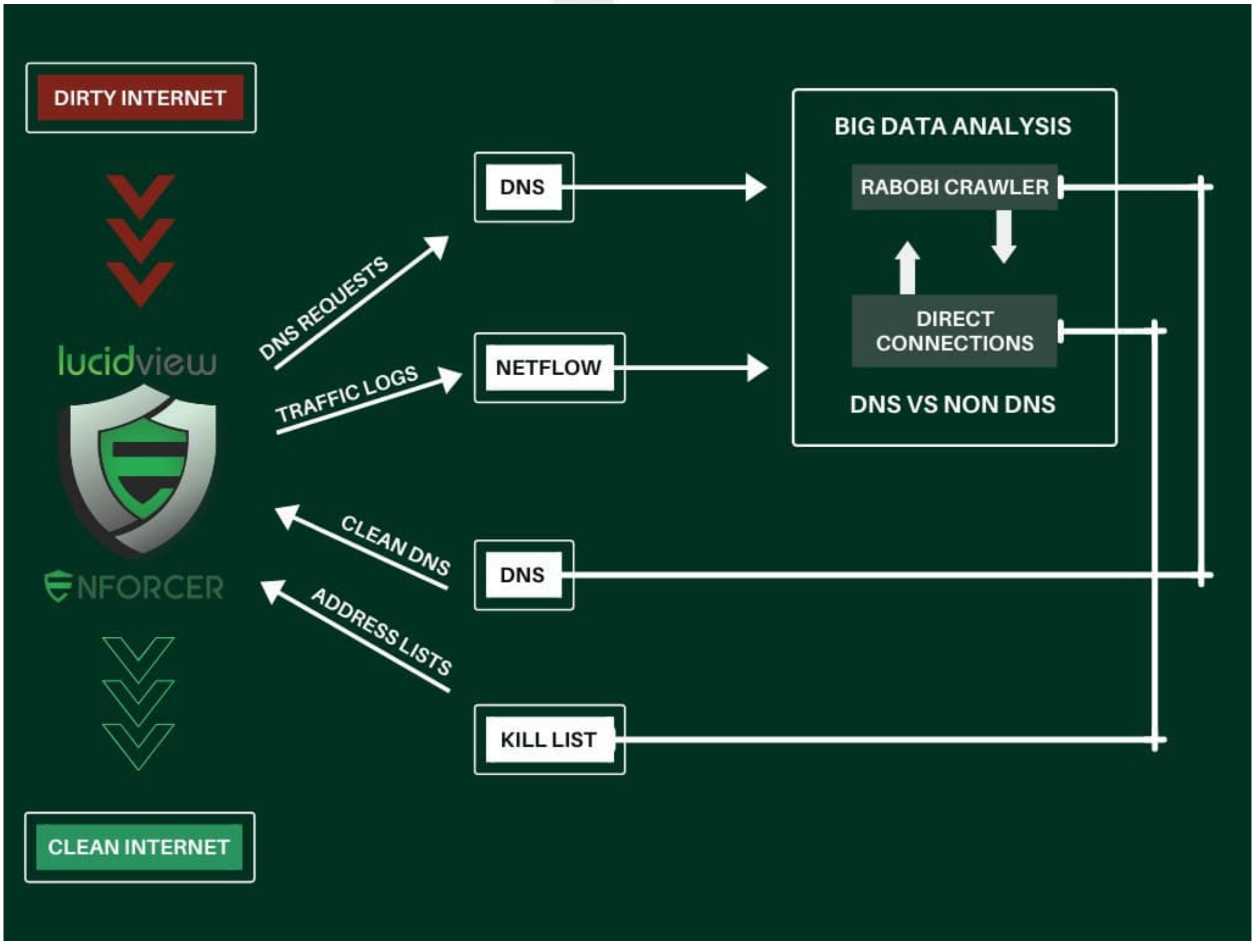
a. An extensive and flexible number of meaningful managerial style **Reports**. High level reports can be generated on demand or scheduled to be delivered on any time schedule - thereby ensuring that you always receive timely and accurate information when it is needed. The reports are extremely powerful and provide a tremendous amount of information at a glance. Network and Internet traffic information has never been so easy to discover.
b. Interactive **Dashboards** provide saved report views for up to date information - from the holistic top level view of your network, right down to individual connection inspection. The Dashboard allows you to easily save customised views and queries to make them available at a glance, which makes it perfect for use in NOCs and SOCs.
c. A powerful yet easy to use investigative **Network Traffic Analysis tool** for in depth, granular investigations.

LucidView Components Overview

A brief overview of the way in which the various LucidView components work together to provide "clean internet" by filtering the "dirty internet" is depicted in the following diagram and is further described in the following sub-paragraphs.

A more detailed capability description is provided for the technically curious in **Appendix A** to this document.

Figure 1: How LucidView works to clean the internet



LucidView Cloud and AI

The LucidView Product range makes use of LucidView's own sophisticated **Artificial Intelligence (AI) engine** that analyzes the data in a Big Data database in the **LucidView Cloud**. The success of all LucidView's solutions is the effectiveness of its web crawlers that are constantly crawling the web, analysing, identifying and categorizing domains, hosts and IPs. LucidView's own proprietary artificial intelligence ensures that the content and security rating of sites always remains up to date and that new internet sites are expeditiously and correctly categorised, thereby ensuring that LucidView's Web Identity Database stays up to date with the ever changing internet landscape.

LucidView's AI enables it to perform extremely sophisticated and effective protection against the entire range of cyber threats, whether they are socially engineered malware placed on a user's device inadvertently, ransomware connections that are installed in stealth on the network or day zero attacks.

LucidView Enforcer

The **LucidView Enforcer** is a dynamic and flexible Next Generation Firewalling solution that utilizes LucidView's powerful and dynamic information repositories that are populated and maintained in the **LucidView Cloud**. This results in meaningful additional data about connections, empowering the LucidView enforcer to continuously deliver enriched protection against sophisticated cyber threats as they evolve.

LucidView Enforcers run on MikroTik RouterOS and can run on physical or virtualized devices. By upgrading a device running MikroTik RouterOS to a LucidView Enforcer, you can enable Next Generation features not available to standard MikroTiks.

MikroTiks comprise a family of hardware appliances that differ in performance (from a device that has one CPU to a device that has 72 CPUs, up to eight 10G Ethernet SFP+ modules and dual power supplies). The various devices cater for a significant spectrum of hardware requirements, but all have identical functionality.

Architecturally LucidView Enforcers are extremely flexible. They can be installed in almost any kind of network topography, i.e they can be installed at end points on the network's edge or as a centralised solution. Whether you want centralised management (one device) for all Enforcer profiles, or Enforcers for each individual physical site location, the Enforcer can fit in and complement any network layout to ensure network integrity.

A LucidView Enforcer's Content Filter and IPS both utilise specialized, dynamic firewall rule bases obtained from the LucidView Cloud to ensure that it receives regular updates to ensure all traffic is in line with the specified content and security policies.

An appropriate Enforcer can easily handle 10+Gbps while simultaneously inspecting all traffic to permit only secure and safe traffic that is in alignment with the Content Filter and Security policies. Moreover, LucidView's Content Based Saturation management has kept internet breakouts as large as 10Gbps responsive, ensuring connectivity and responsiveness for all users of the network.

LucidView Portal

LucidView Enforcer management is simplified with the **LucidView Enforcer Portal**. The Portal allows you to configure and manage all of your Enforcer profiles from one central location, anywhere, at any time.

LucidView Enforcer App

The LucidView Enforcer App is available for iOS and Android. It empowers any individual to fully manage and interact with existing Enforcer Profiles. ISPs (or Admins) can give policy, security and reporting controls to any individual, conveniently and instantly available from their favourite device.

LucidView Services

LucidView provides the following services:

1. **Licensing** of the LucidView solutions.
2. **Support** of the LucidView solutions. LucidView provides second level support for all its solutions other than to enterprises that have procured a fully managed solution.
3. **Management** of the installed Lucidview solutions for customers that have procured a fully managed solution.

LucidView’s support staff are friendly, knowledgeable and informed. This ensures rapid turnaround times for any issues or failures experienced by Clients such as NOCs or administrators. Downtime and device failures are always a possibility, and LucidView works to be proactive, efficient and swift in its responses to such events.

Further Information

More detailed information regarding LucidView’s capabilities are provided in Annexure A to this document.

APPENDIX A: DETAILED CAPABILITY DESCRIPTION

1. Intrusion Detection and Prevention

LucidView’s IDPS module primarily makes use of a behavioural approach to perform intrusion detection and prevention. The IDPS module examines each and every connection and allows those considered safe, any connection not known or part of our “white list” so to speak is immediately terminated. Our AI is designed to examine each and every connection and white list those that show no anomalous behaviour or are unknown. This all takes place in real time as the ability to analyse, identify and classify data in real time is crucial to ensuring the security of the organisation and its users.

Once LucidView identifies an intrusion attempt it proceeds to eliminate all suspicious connections, traffic and anomalies, thereby protecting the organisation from malware such as Ransomware and preventing unauthorised access into the organisation by hackers.

The LucidView IDPS solution also identifies devices on the network that have been infected with Malware, thereby ensuring that the resolution of the risk is rapid and effective.

This is a dynamic, behaviour based IDPS solution that protects your network and mitigates DDOS and other attacks as soon as they are identified, ensuring that your bandwidth is always available for business related activities.

Pull and Push Remote Protection

- **Pull Remote Protection** - These are attempted attacks into your network by a remote hacker trying to gain access to your network, The LucidView IPS module identifies these connections and eliminates them before they are able to infect the network or give a remote hacker control over the network.

- **Push Remote Protection** - This refers to remote hackers that gain access via users from within the network, e.g. via a VPN, apps like WhatsApp or Telegram and even email. The user inadvertently allows the hacker to push a remote connection into your network. The LucidView IPS module identifies these “push” remote connections and eliminates them.

Importance of Monitoring in Information Security

The importance of being able to monitor key aspects of a Network at all times cannot be over emphasised. It is essential that NOC/SOC administrators are able to tell at a glance whether or not the network has been comRisk - Known Malware or Phishing sites

Reports on intrusion attempts averted can be pulled via the dashboard data analysis tool and scheduled reports can be sent out to key administrators.

2. Content Filtering

Proper Content Filtering is necessary to protect the confidentiality, integrity and availability of your network and Internet resources. Critical business must always be prioritised and available to users. Users must not be able to circumvent security filters that have been put in place to meet the organisation's Internet Usage Policy.

Security is more than just protecting against malware, phishing, ransomware, DDOS, etc. It must also ensure that users are not able to access material considered inappropriate for the workplace, content that does not promote productivity and content that may be considered illegal such as piracy and gambling.

The LucidView Content filter includes a firewall based dynamic Content Filter that provides a clean, safe Internet by making use of both DNS and Firewall based Content Filtering (this combination ensures that the Content Filter is very difficult to circumvent). It is constantly browsing the web and adding new sites to our category lists. This AI technology ensures that when new sites on the internet are accessed, LucidView is no more than 20 minutes behind in finding them, cataloguing them, adding them to the category that they belong to and ensuring that they are in line with the Internet policy of the organisation.

1. **DNS based Content Filter** – While DNS is a component of Content Filtering and will protect the majority of users, when used alone it provides a false sense of security as DNS only content filtering by DNS poisoning can easily be circumvented.

2. **Firewall based Content Filter** – Adding the Firewall component to the Content Filter ensures clean, secure Internet. Each incoming and outgoing connection is analysed, classified and either blocked or allowed, depending on your needs.

The Firewall component of the LucidView Content Filter is critical in ensuring the organisation’s Internet Usage policy is enforced. Any connection in contravention is immediately “killed” via the LucidView Content Filter Firewall.

Extensive Database

LucidView does not rely only on existing databases to ensure that content is classified and categorised correctly. LucidView has its own crawlers that are constantly crawling the web looking for new sites to add to its already extensive database.

Always Learning

The LucidView Web Content Filter is constantly learning and updating every hour of every day. Thousands of new sites are added and classified every hour. Therefore, if a new unknown site is published and you or your client access it the LucidView Web Crawlers will, within an hour, have browsed, analysed and categorised the site.

Web Content Filter

Categories

The Web content filter allows you to block any or all of the of the following categories:

- Adult - Sites containing explicit content.
- Adverts - Sites hosting online adverts
- Gambling- Online gambling sites.
- Gaming - Gaming and gaming are related sites. - It is recommended that the "suspicious" also be blocked in conjunction with blocking this category to more effectively block online gaming
- Instant Messaging - Instant messaging (IM) technology is a type of online chat that offers real-time text transmission over the Internet.
- Movies - Torrent trackers and Movies/Music streaming/download sites
- Social Media - Facebook, Instagram, Twitter, Tiktok, etc

The Web content filter also allows you to:

- Enforce Search Engine Safe Search - This enforces the Google Safe Search feature on Google searches, or the equivalent for other search engines.

- Enforce YouTube Safe Search - This will force the Google safe search filter to be activated for YouTube.
- Updates - Allows you to block or schedule time for YouTube, Google Video,Android Updates as well as other updates, such as Microsoft, Apple etc.

Time Based Rules

An important feature of the LucidView Content Filter is the ability to create time based rules. For example, a company may decide that social media platforms such as Facebook are not conducive to productivity and block them during working hours. With time based rules the administrator has the power to allow social media to be accessed at specific times like lunch time.

3. Saturation Manager / Content based Traffic Shaping

This module ensures that critical data and systems are always available, even during times of peak saturation.

This feature provides administrators with the ability to manage media streaming, and other bandwidth intensive applications in such a way that it does not impact more important Internet activity. Each organisation, department or service provider can determine how much bandwidth streaming services are using during times of bandwidth saturation. Where bandwidth is unmanaged, typically one needs to increase the available bandwidth when the existing line reaches 60% to 70%, this is costly and does little to resolve the issue. Having the tools to manage saturated links is a much more effective way to deal with congestion or saturation.

Bandwidth Reservation

An example of Bandwidth Reservation is that 5% of available bandwidth can be allocated to streaming services. When the line is saturated, streaming will still function without latency, however the resolution will be automatically lowered. When the line is not being used by more critical applications, the resolution will automatically increase as more bandwidth will automatically be made available to streaming.

Categories prioritisation

With the LucidView Saturation Manager you can decide what categories are the most important and allow them to take priority during times of saturation. Using this tool, the Internet will always remain responsive, even when congested.

LucidView has a number of categories that you can select and shape, making your end-user Internet experience extremely responsive. These categories include:

- Adult - Sites containing explicit content
- Big Tech Heavy - This category contains heavy bandwidth components of Big tech companies such as Microsoft updates and Apple itunes. This category was designed to be used for lower priority shaping on congested Internet lines.
- Movies - Torrent trackers and Movies/Music streaming/download sites
- Social Media Heavy - Facebook

4. Insights: Reports, Dashboards and Traffic Analysis Tool

It goes without saying, you can’t manage what you can’t see. Without proper insight and oversight of the traffic coming in and leaving the network it is not possible to ensure its integrity. The LucidView Insights, therefore, provides the visibility necessary to ensure your Internet traffic is being used as you intended.

LucidView Insights provides Reporting, Dashboards and a Traffic Flow Analyser that, together, provide comprehensive reports, at a glance custom dashboard views on all network Internet traffic as well as the ability to do comprehensive deep dive analysis on all the traffic flowing through the LucidView solution.

These Reports are powerful tools in assisting you with your Internet Management. They show you possible Malware infections and the source of these. As a result, you can quickly remedy this. They provide details such as whether your bandwidth is being used for torrents and which device is responsible.

Usage Reports

Our Reports are user friendly and easy to understand and give you complete visibility of your Internet traffic, A few examples of Internet Usage Reports available are:

- Source IP Reports
- Internet Destination Reports
- Hosts and/or Domains Report - This Report shows you which internet hosts and or domains have been accessed
- Categories Report - Adult, Gaming, Gambling, Movies, etc
- Security Reports
- Report showing Malware
- Report showing suspected unauthorised remote access which is a possible hacking attempt

Custom Internet Usage Reports

While the LucidView Reporting Module comes with many predefined Internet traffic reports covering almost every aspect of your network and Internet traffic we also cater for customised reports. If you can think of any aspect regarding your Internet traffic you would wish to report on and there is not an existing report for it, one can easily be created to meet your needs.

Scheduled Reports

Using LucidView's Reporting Module's scheduling feature, scheduled reports can be emailed to your clients or users as often as you like, whether it be daily, weekly, monthly or whatever your requirements are.

LucidView's reports show you exactly which device on your network is visiting what websites, when and for how long. You can use them to measure your quality of service ensuring that you are getting the bandwidth you are paying for.

The value of visibility via detailed reports from our Reports & Dashboards is invaluable in ensuring that your network and Internet resources are being used in line with your policy.

Traffic Flow Analyzer

The Reporting Module’s Traffic Flow Analyzer provides extensive tools to drill down and identify key areas of concern or interest and provides for customised reporting and scheduled reports. The dashboard feature provides a completely customisable oversight feature that is perfect for any SOC or

NOC. The Traffic-flow analyser allows you to investigate every aspect of your Internet traffic and identify an anomaly - no matter how small. This feature allows you to find the proverbial needle in a haystack, so to speak.

For example: You notice on your dashboard that an excessive amount of connections are being made to one site - this immediately indicates a potential Malware infection. Using the LucidView Traffic-Flow Analyser you are able to rapidly identify the offending PC and remove the Malware.

5. LucidView Enforcer Portal

The LucidView Enforcer Portal facilitates the centralised management of numerous Enforcer profiles, each with their own configurations. It allows the administration of the Enforcer feature set and allows a user to easily configure policy around content filtering and security (e.g. it can enable individual modules, such as the IPS, to be disabled and enabled as required), as well as easily generate managerial style reports.

Very detailed logs are stored for months (client dependent) and can be interrogated on the live dashboard or by generated predefined reports. Portal logs are extremely useful for log analysis as they contain enriched information.

The powerful LucidView Enforcer Management system enables rules to be added as disabled (or inactivated) by a user with the requisite access control (this requires the additional step of enabling the rule in order for it to be in effect). In addition, a “Safe mode” option is available that not only rolls back the last change but any change since the last saved point. This allows seamless rollback to a working state in the event that connectivity is lost.

Portal Management activity is logged online and LucidView Enforcer activity audit logs are available as Syslog and can be sent to any logging server. Additionally, an Enforcer contains a native method for notification and alert for configurable actions and events.

Log information can be exported via Syslog, JSON, or downloaded as a CSV file enabling seamless integration with many available event logging and notification providers.

LucidView products are highly flexible and support multiple means of integration through many different processes and mechanisms.

6. LucidView Enforcer APP

The LucidView Enforcer App provides an easier way to interact and configure Enforcer Profiles.

Enforcer Profiles are created on the LucidView Administration Portal and are then linked, with a QR scan, to the LucidView Enforcer App.

This allows you to manage your LucidView Enforcer Content filter, IPS, Saturation manager and/or pull reports and much more from the comfort of your favourite Android or Apple device.

As an Enforcer Administrator the active modules for an enforcer can be chosen as desired. This means the app can be recommended to your clients, with the ability to manage all the features or limited features like, for example, just being able to generate reports.

For more information on the LucidView, please visit www.lucidview.net.