BlackLynx High Speed Search Acceleration with Splunk

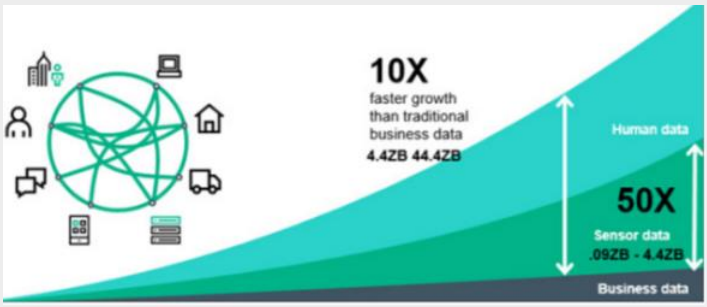
Use BlackLynx software to supercharge your current search tools like Splunk and reduce your time for getting insights from your data

- Accelerate time to extract insights from data through near real-time search performance
- Discover events significantly faster and generate alerts without the need for ETL and indexing
- Search ALL the data without increasing the Splunk Total Cost of Ownership (TCO)

BLACKLYNX

INTRODUCTION

Legacy architectures render big data useless;
There are many sources that predict exponential data growth toward 2020 and beyond. Yet they are all in broad agreement that the size of the digital universe will double every two years at least, a 50-fold growth from 2010 to 2020. Human- and machine-generated data is experiencing an overall 10x faster growth rate than traditional business data, and machine data (sensor data) is increasing even more rapidly at 50x the growth rate.



insidebigdata.com/2017/02/16/the-exponential-growth-of-data/

Threat:
Organizations are reliant upon legacy network and compute architectures that were never designed to organize, store, and process data at the rate required today. Analytics challenges are forcing new thinking in network, storage, and computing.

Opportunity:
The acquisition and analysis of data and its subsequent transformation into actionable insight is a complex workflow which extends beyond data centers, to the edge, and into the cloud in a seamless hybrid environment. The key factor driving the adoption of data-intensive computing is the need to rapidly analyze exploding volumes of data at the point of creation and at scale which is driving the need for a new technological approach.

SOLUTION OVERVIEW

BlackLynx technology combines high performance computing (accelerated CPUs and FPGAs) with standard interfaces and protocols to achieve high performance analytics.

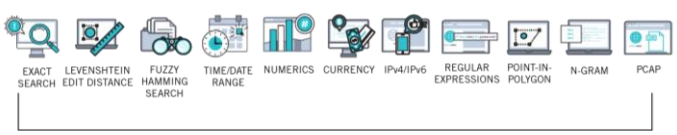
Key benefits of BlackLynx technology

Accelerate time to extract insights from data through near real-time search performance
Eliminate ETL/indexing for fast, varied data (XML, JSON, CSV, Unstructured, PCAP) providing real-time analytics performance. Accelerate various search operations through the use of parallel architectures using CPU and FPGA compute technology.

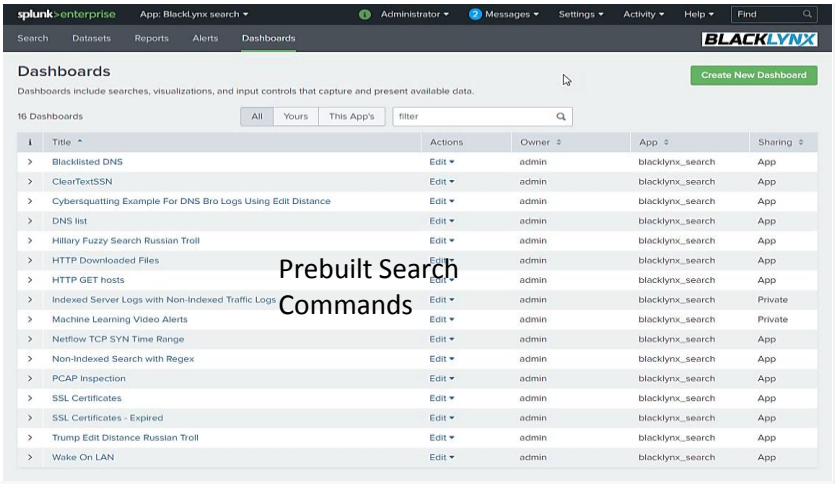
Accelerate integration efforts through an array of simple to use interfaces
Provide simple-to-use interfaces including programmatic interfaces (C, C++, Python, JAVA, etc.), command line, ODBC/JDBC, and RESTful Interfaces, enabling acceleration of existing applications and making CPU or FPGA compute transparent to the developer/user.

Purpose-built heterogeneous compute
Ensure the right compute architecture—CPU and/or FPGA—is used to achieve maximum performance for the desired analytics function.

Accelerated search library
An array of search capabilities is accelerated through the use of BlackLynx technology, including complex queries such as fuzzy search, PCAP analysis, and regular expression capabilities. Supports XML, JSON, CSV, unstructured and PCAP file formats.



Extend the capabilities of Splunk while reducing Total Cost of Ownership

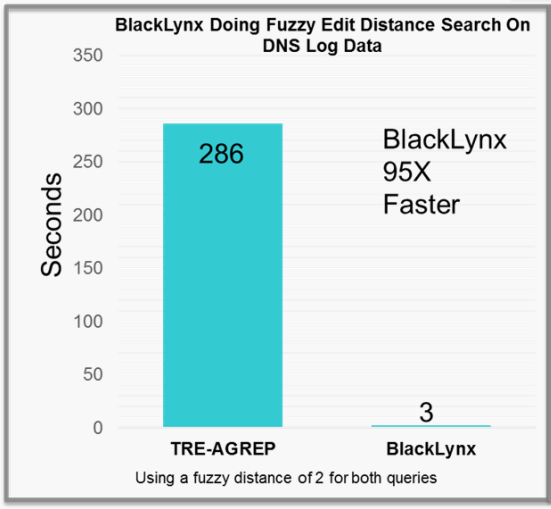


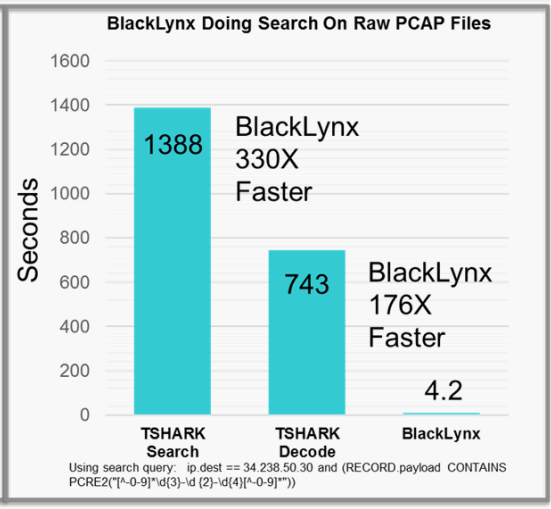
- Extend Splunk Enterprise with "Apps" to BlackLynx software technology for searching raw data for cyber, performance, and compliance purposes
- In parallel with Splunk ingest, direct all data (PCAP for example) to BlackLynx servers and provide high performance forensics while reducing Splunk storage costs
- Integrate Splunk's 24 hour real-time monitoring with BlackLynx raw data, 7 layer visibility to identify and resolve issues faster
- Create opportunities for future machine learning by fully analyzing the machine generated data

Discover events significantly faster

Search ALL the data and enable improved visibility

More Efficient Triage while reducing TCO





- The DNS log (2 GB) and the PCAP files (15.6 GB) are from the U.S. National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition (MACCDC) dataset
- The tre-agrep tool was co-authored by Udi Manber, one of the great names in contemporary Computer Science and author of the well-regarded textbook *Introduction to Algorithms: A Creative Approach*, which to this day enjoys wide use in Computer Science curricula worldwide
- TSHARK Search is doing the filter parameter(ip.dest) on 16 files (serially). The TSHARK Decode is only the time to build the decoded files (parallel processes) and does not include any filter time

Customer Benefits

- Full access and search capability to all machine generated data
- Enhanced cyber, performance, and compliance use cases
- No indexing overhead and storage costs
- Seamless transition through Splunk supported and published APIs
- Customer choices for amount of Splunk real time indexing (cost saving opportunity)
- Customer choice on long term storage and use of data (cost saving opportunity)

CONCLUSION

Use BlackLynx technology within Splunk to achieve increased visibility of machine generated data while reducing the total cost of ownership.

Get smarter insights—faster—to drive critical business decisions and next-generation innovation.

TAKE THE NEXT STEP

Please visit www.blacklynx.tech for complete details and to place an order today.