CYBOT HUNTER

Data Sheet

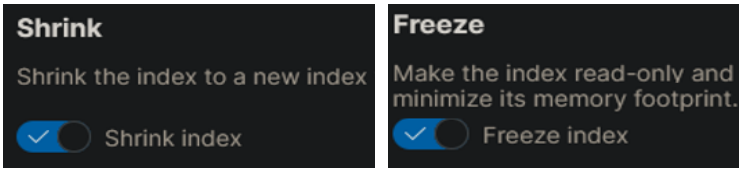
Data Lake

activebytes innovations

✓A **Big Data Analytic** Engine with best in class analytics and processing capability satisfies the organization's data analysis needs for now and future

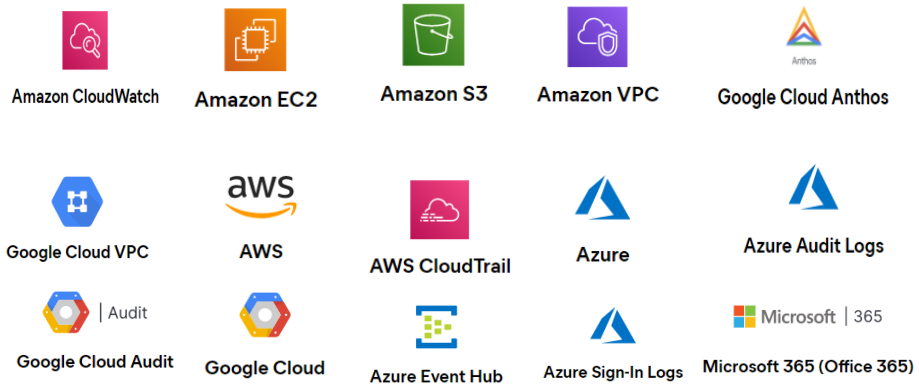
SCALE UP SIMPLY

- ❑ No limitation on size and number of instances- Just keep adding instances to the cluster for future sizing requirements
- ❑ API support for major functions – to allow seamless automation
- ❑ Can be hosted on bare metal hardware, VM or in cloud- Host the solution as per convenience
- ❑ Capable of storing the less used data with more compression ratio – Keep more data for less cost

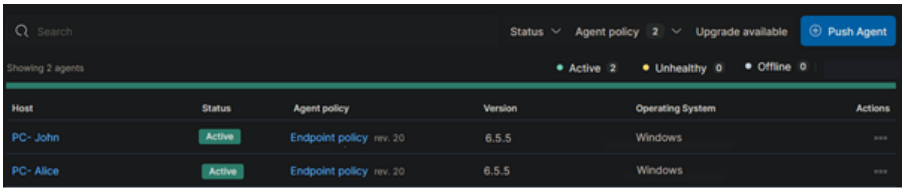


NO MORE BLIND SPOTS

- ✓ Simply collect all of your data to search, visualize, and analyze — cloud, user, endpoint or network
- ✓ Can make custom connectors or utilize community build plugins to collect remaining
- ✓ 250+ log source support out of the box
- ✓ Data extraction and correlation of major cloud service provides



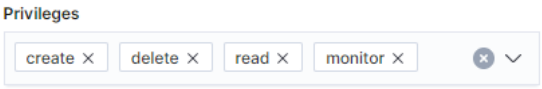
- ✓ Manage endpoints all together from a single console, whether its Windows, Linux or even Mac – Smooth way of managing rich logs being shared by host sensors



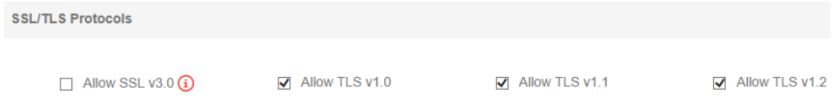
activebytes innovations

SECURITY

- ✓ Access controls based on Role(RBAC), Index, attributes (ABAC) etc.

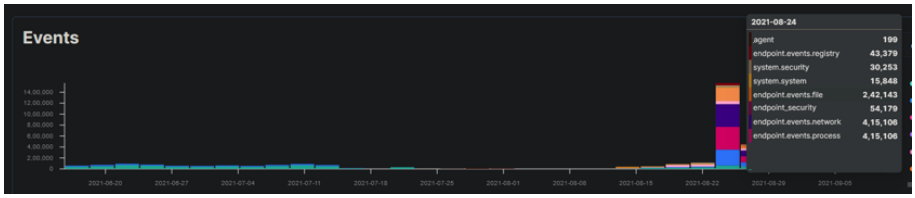


- ✓ Audit Logging
- ✓ Industry standard encryption for communication

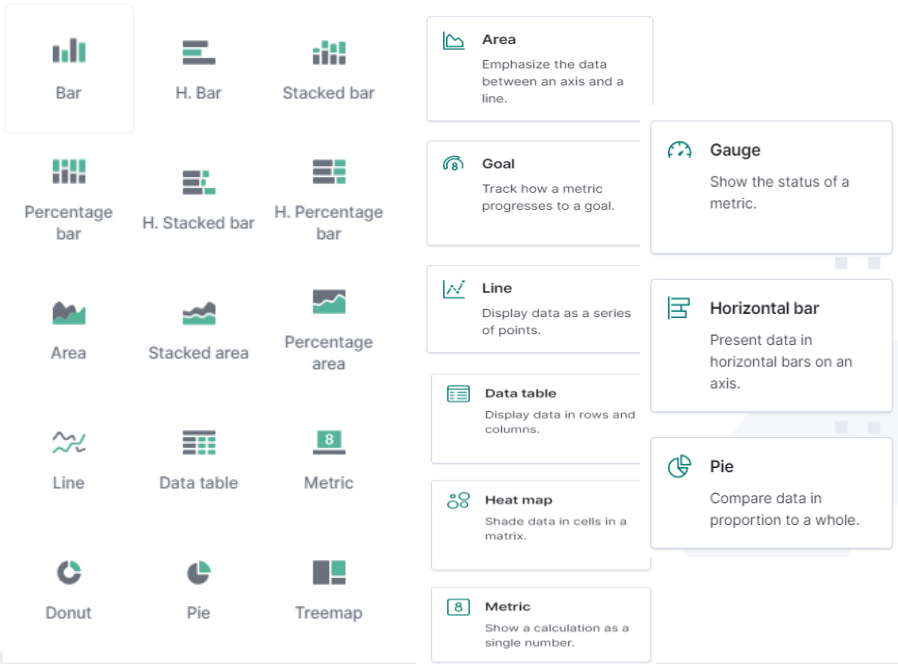


LIMITLESS DATA & VISUALIZATION OPPORTUNITIES

- ✓ Store structured/unstructured data from Endpoints, network devices, threat hunting/analytics
- ✓ Identify and correlate various data sources like logs, metrics etc.
- ✓ Get advanced insights into granular security lookup criteria



- ✓ Bunch of custom widgets to create awesome dashboards over the collected data



- ✓ Exclusive list of custom dashboards made on top of these visualization capabilities,for Compliance and Security Analytics

*** Detailed list of dashboards are available in [Dashboards Datasheet]*

activebytes innovations

List of Supported Log Sources

.NET	Abuse.ch	ActiveMQ	Aerospike
AlienVault OTX	Amazon CloudWatch	Amazon DynamoDB	Amazon EBS
Amazon EC2	Amazon RDS	Amazon S3	Amazon SNS
Amazon SQS	Amazon VPC	Amazon VPC NAT Gateway	AMQP
Anomali Limo	Anomali ThreatStream	Apache	Apache Thrift
Apache Tomcat	auditd	AWS	AWS Billing
AWS CloudTrail	AWS Elastic Load Balancing	AWS Lambda	AWS Transit Gateway
AWS Usage	AWS VPN	Azure	Azure Activity Logs
Azure Application Insights	Azure Audit Logs	Azure Billing	Azure Container Instance
Azure Container Registry	Azure Container Service	Azure Database Account	Azure Event Hub
Azure Monitor	Azure Sign-In Logs	Azure Storage	Azure VM
Azure VM Scale Sets	Barracuda	Barracuda Spam Firewall	Beats
Blue Coat Director	Box	Cassandra	Ceph
Check Point	Cisco Advanced Malware Protection (AMP)	Cisco ASA	Cisco Firepower Threat Defense
Cisco IOS	Cisco Meraki	Cisco Nexus	Cisco Umbrella
Cloud Foundry	CockroachDB	collectd	Common Event Format (CEF)
Confluence Cloud	Confluence Server	Consul	CoreDNS
Couchbase	CouchDB	CrowdStrike	Custom API sources
Cyberark Privileged Access Security	Cylance	DHCP	DNS
Docker	Dropbox	Dropbox Paper	Dropwizard
Elastic APM Server	Elastic App Search	Elasticsearch	Email
Envoy	etcd	F5 BIG-IP Access Policy Manager	F5 BIG-IP Advanced Firewall Manager
Fargate	File Integrity	Fluentd	Forcepoint
SQL	Squid Proxy Server	StatsD	Suricata
Swimlane SOAR	syslog	Sysmon	TLS
Traefik	Twitter	UDP	uWSGI
VMware vSphere	Web Crawler	Webhook	Windows
X.509 SSL/TLS Certificate Check	Zeek (Bro)	Zendesk	ZooKeeper
Zoom	ZScaler		

activebytes
innovations

Fortinet	Fortinet Forticlient Endpoint Protection	Fortinet FortiMail	Fortinet FortiManager
GitHub	Gmail	Go	Go Expvar
Google Cloud	Google Cloud Anthos	Google Cloud Audit	Google Cloud Billing
Google Cloud Compute	Google Cloud Firewall	Google Cloud Functions	Google Cloud Load Balancing
Google Cloud Pub/Sub	Google Cloud Stackdriver	Google Cloud Storage	Google Cloud VPC
Google Drive	Google Santa	Google Workspace	Graphite
Hadoop	HAProxy	HTTP	HTTP Check
IBM MQ	IBM Resilient	Icinga	ICMP
ICMP	Imperva Secure Sphere	Infoblox	iptables
Istio	Jaeger	Java	JavaScript
JDBC	Jira Cloud	Jira Server	JMS
JMX Jolokia	journald	Juniper Junos OS	Juniper Netscreen
Juniper SRX Series	Kafka	Kibana	Kubernetes
Kubernetes API Server	Kubernetes Controller Manager	Kubernetes Events	Kubernetes Metrics Service
Kubernetes Proxy	Kubernetes Scheduler	kvm	Linux
Linux Audit Framework	Linux systemd journals	Log files (Generic)	Logstash
Malware Information Sharing Platform (MISP)	Memcached	Microsoft 365 (Office 365)	Microsoft 365 Defender
Microsoft Defender for Endpoint	Microsoft DHCP Server	Microsoft IIS	Microsoft OneDrive
Microsoft SQL Server	Microsoft Teams	MongoDB	MQTT
Munin	MySQL	NATS	NATS Streaming
NetFlow	Netscout Arbor Sightline	Network File System	NGINX
Node.js	Okta	OpenMetrics	OpenTelemetry
OpenTracing	Oracle	Osquery	Osquery Manager
PagerDuty	Palo Alto Networks	Pensando	PHP
PHP FPM	PostgreSQL	PowerShell	Prometheus
Proofpoint Email Security	Python	RabbitMQ	Radware DefensePro
Recorded Future	Redis	Ruby	Salesforce
Salesforce Sandboxes	ServiceNow	ServiceNow SIR	SharePoint Online
Salesforce Sandboxes	ServiceNow	ServiceNow SIR	SharePoint Online
SIP	Slack	SNMP	Snort
Snyk	Sonicwall Firewalls	Sophos UTM	Sophos XG Firewall

** As the solution supports ingestion of both structured and unstructured data, Our PS team can create connectors to collect any of the solutions not listed here, based on request

activebytes innovations

DATA LAKE FULL LIST OF FEATURES

Stack Operations and Management

- Storage types
  - Inverted index (for search)
  - Evaluating calculated fields at index time
  - Runtime fields
  - Document store (for unstructured)
  - Columnar store (for analytics)
  - BKD trees (for numeric, dates, & geo)
  - Flattened field type
  - Histogram field type
  - Match only text field type
  - Shape field type
  - Vector field type
  - Version field type
  - Wildcard field type
  - Frozen indices (for long term storage)
- Data management
  - Snapshot/restore
  - Minimal snapshots
  - Snapshot lifecycle management
  - Data rollups
  - Data streams
  - Data tiers
  - Data transforms
  - Index management
  - Index lifecycle management
- Stack management
  - Data import tutorials
  - Ingest Node Pipeline Builder UI
  - Grok Debugger
  - Upgrade Assistant
  - License management
- Scalability & resiliency
  - Clustering & high availability
  - Automatic data rebalancing
  - Cross-cluster search
  - Voting-only master nodes
- Security
  - Secure settings
  - Encrypted communications
  - Role-based access control
  - Anonymous access control (public sharing)
  - File and native authentication
  - Multitenancy
  - UI feature controls
  - API keys management
- Stack monitoring
  - Full stack monitoring
  - Alerting
- Alerting
  - Alerts
  - Actions: Index and Logging
- Clients
  - REST
  - Language clients
  - Console
  - Hadoop
- Localized UI
  - English
  - Chinese (Simplified)
  - Japanese

Search and Analysis

- Full-text search
    - Relevance scoring
    - Highlighting
    - Type ahead
    - Corrections
    - Suggestions
    - Percolations
    - Async search
    - Results pinning
    - Dynamically updateable synonyms
    - Query profiler
    - Similarity functions for vector fields
- Analytics
    - Aggregations
    - Boxplot aggregation
    - Cumulative cardinality aggregation
    - Moving percentiles aggregation
    - Multi terms aggregation
    - Normalize aggregation
    - Range aggregation over histogram fields
    - Rate aggregation
    - String stats aggregation
    - Top metrics aggregation
    - T-test aggregation
- Query languages
    - Elasticsearch SQL APIs & CLI
    - Event Query Language (EQL)
- Machine learning
    - Data Visualizer
    - Language identification

Data ingest and Transformation

- Ingest products and features
    - Sensors for shipping Logs from Windows, Network, Uptime monitoring and Auditing.
    - Cloud services monitor
    - Real browser-based synthetic monitoring agent
    - Hadoop
    - File import wizard
- Centralized management for host sensors
    - Centralized management Server
    - Centralized management app
    - integrations
    - Host Sensors for data ingestion

activebytes
innovations

Data exploration and visualization

- Data transformation
    - Index time enrichment
    - Processors
    - Analyzers
    - Tokenizers
    - Filters
    - Grok
    - Field transformation
    - External lookup enrichment
    - Circle ingest processor
    - Match & Geo-match enrich processor
- Visualizations
    - Time series
    - Geo
    - Metrics
    - Tables
    - Tag cloud
    - Custom (Vega)
    - Lens
- Data exploration
    - Dashboards
    - Drilldown between dashboards
    - Discover
    - UI query autocomplete
    - UI runtime fields editor
    - Run search sessions in background
- Canvas
    - Canvas
    - Canvas shareables
- Share & collaborate
    - Embeddable dashboards
    - Anonymous access control (public sharing)
    - CSV exports
    - Saved queries
- Content management
    - Multitenancy UI
    - Object export UI & APIs
    - Tags
    - Navigational search

Application Performance Monitoring

- Application Performance Management Server
- Jaeger intake
- Open Telemetry intake for traces and metrics
- Application Performance Monitoring app
- Distributed tracing
- Application Performance Management agents
    - Java
    - .NET
    - Go
    - Ruby
    - RUM (JavaScript)
    - PHP
    - Python
    - Node
- Integrations
    - Logs, Metrics
    - UI alerting and actions
- Logs
- Log shipper
- Dashboards for common data sources
- Logs app
- Integrations
    - Uptime, Application Performance Management
    - alerting and actions

- Metrics
  - Metric shipper
  - Dashboards for common data sources
  - Metrics app
  - Integrations
    - Logs, Application Performance Management, Uptime
    - UI alerting and actions
- Uptime
  - Uptime monitor
  - Uptime dashboards in UI
  - Uptime app
  - Integrations
    - Logs, Metrics, Application Performance Management
    - UI alerting and actions
- Security
  - Common Schema for data
  - Extended Detection and response
  - Security information and event management
  - Host security analysis
  - Network security analysis
  - Timeline event explorer
  - Case management
  - Detection engine (e.g., correlation, indicator match, threshold)
  - Prebuilt detection rules
  - Malware prevention and data collection
  - Integrations
    - Host sensor
    - Application Performance Management
    - Maps
    - UI Alerts and Actions
    - Osquery Manager
    - Threat Intelligence feeds
- Maps
  - maps service
    - Base layer maps
  - Maps app
    - GeoJSON upload
    - Multiple layers
    - Layer-based filtering
    - Client-side styling
    - Individual points and shapes
    - Geo aggregations
    - Embed Maps in dashboard
    - Embed Maps in Canvas
    - Geo-threshold alerts
    - Display up to 24 zoom levels
    - Custom raster and vector tile service support
- App search
  - App Search Server
  - App Search UI
  - Search result curation
  - Search analytics
  - Synonyms management
  - Language-specific relevance
  - Typo-tolerant relevance model
  - Relevance model tuning
  - Index lifecycle management
  - Web crawler (beta)
  - Precision tuning (beta)
  - Clients
    - Python
    - Ruby