Hexis Cyber Solutions

HawkEye | AP: The Data Analytics Platform

HawkEye AP

The Data Analytics Platform

When You Need

- The collection of massive amounts of data – customer proven with trillions of events per day per installation
- The highest in data access performance
- Unconstrained hosting of analysis tools
- Easy-to-use reporting, analytics modeling, installation and administration tools via a web-based GUI
- Built in connections to hundreds of network devices, machines and applications

Event Correlation

- Real-time event parsing and correlation
- Threshold-based and scenario-based correlation
- Single, multi- and cross-source event alert generation
- Contextual drill-down into events

Distributed and Parallel Data Loading

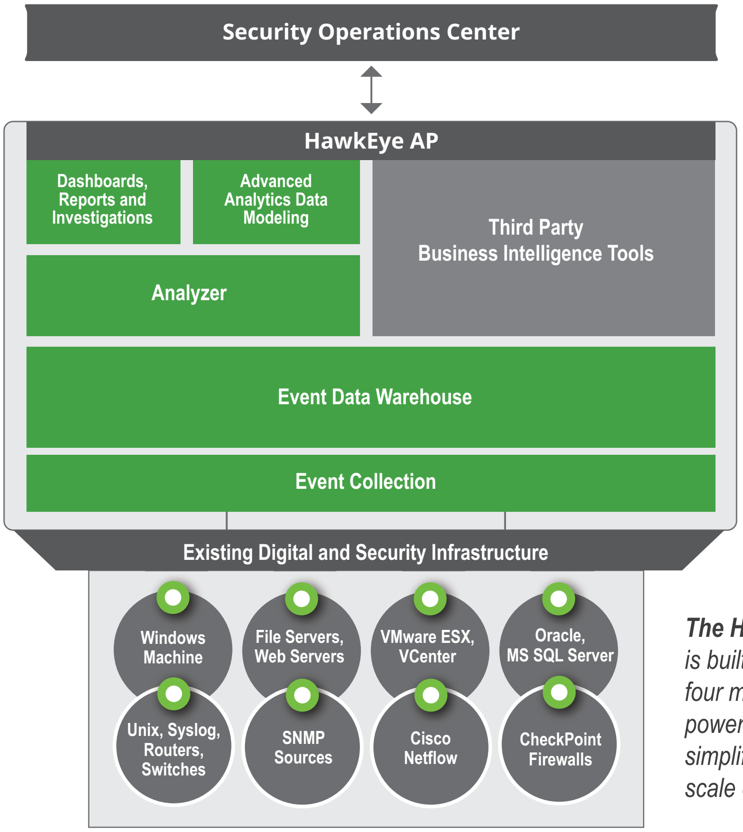
- Distributed and parallel query processing
- Compressed data retention
- Linear scalability using: Massively Parallel Processing (MPP)

Increased Visibility = Decreased Risk

The real power of big data – massively big data – is that it can be used to detect advanced cyber attacks and insider threats, diagnose service problems, assess the health of the business, detect fraudulent behavior, monitor transactions, demonstrate regulatory compliance, and provide intelligence to overcome challenges not even yet envisioned. But, to make the data valuable requires a special kind of solution. You need a platform that can readily ingest a wide scope of information, store it so it's available at lightning speed, and host and display rich visualizations and analytics via a web-based GUI. Only then can you address today's security, compliance and risk mitigation requirements.

IT business and security teams select HawkEye AP when they require a single, tamper-proof repository to collect and store all massive security event data over long time horizons:

- Creating a unified version of truth for all teams doing ad-hoc analysis, activity diagnosis
- Providing historical context for real-time alert investigations
- Leveraging baselines and patterns for rapid detection of anomalies



Security Operations Center
HawkEye AP
Dashboards, Reports and Investigations
Advanced Analytics Data Modeling
Third Party Business Intelligence Tools
Analyzer
Event Data Warehouse
Event Collection
Existing Digital and Security Infrastructure
Windows Machine
File Servers, Web Servers
VMware ESX, VCenter
Oracle, MS SQL Server
Unix, Syslog, Routers, Switches
SNMP Sources
Cisco Netflow
CheckPoint Firewalls

COLLECT

STORE

ANALYZE

***The HawkEye AP architecture** is built from the ground up with four main, unique capabilities: powerful analytics, rich reporting, simplified collection and massive-scale data warehousing.*

Hexis™
CYBER SOLUTIONS
a KEYW company

Hexis Cyber Solutions, a wholly-owned subsidiary of The KEYW Holding Corporation
7740 Milestone Parkway, Suite 400 | Hanover, MD 21076 | info@hexiscyber.com | 443.733.1900

Powerful Analytics

- The core architecture maintains predefined schemas and out-of-the-box metrics, which can be used and built upon for statistics-based anomaly detection, threshold violations and more
- Web-based GUI for graphically designing advanced dataflow models
- Use ODBC/JDBC interfaces to access event data directly from preferred Business Intelligence tools
- Contextual investigation via a flexible, SQL-driven query wizard
- Access terabytes of data in real time, without the need to extract from any archive, accelerating investigations and queries

Massive-Scale Data Warehousing

- Compared to the volume of data stored in an RDBMS database, HawkEye AP achieves up to a 40 times better compression ratio
- MPP enables linear scalability in handling large data volumes – highly compressed format reduces storage requirements
- Distributed and parallel data loading and query processing

Rich Reporting

Massive volumes of data can be correlated into comprehensive, scheduled or on-demand, reports – regardless of source.

- Dashboards with web-based GUI for rapid drill-down from indicators to investigate root cause
- Predefined report templates that meet specific regulatory compliance formats such as ISO 17799, PCI, HIPAA, HITECH, Sarbanes Oxley, FISMA, DCID 6/3 and NIPSOM

Simplified Collection

Collect petabytes of data per day from any source with a time stamp.

- Agentless collection via pull methods (SCP, RCP, (S)FTP, SMB (Windows), LEA, SDEE, RDBMS tables) and push methods (SYSLOG, SNMP, HTTP(S), (S)FTP). Works in batch loads, trickle feeds, or streams. Plus special collection from Checkpoint LEA, VMware vCenter, and Audit data from Oracle and MS SQL Server
- 250+ source-specific off-the-shelf adapters for most common IT Infrastructure systems
- Ability to load and store all event data in its native form, rather than just the metadata or just aggregations and without normalizing the data, maintains the integrity of the data for audit, forensics or other future use
- Standards-based event files/names using the Common Event Expression data dictionary and taxonomy

Advanced Dataflow Models

Replace multi-step data manipulation and analytics (typically requiring third-party tools such as Microsoft Excel) with intuitive dataflow models.

- Dataflow models are represented graphically in an HTML browser and executed on the Analyzer server either interactively or on a scheduled basis
- Data can come from reports, queries or other files or systems such as LDAP lookups
- Multi-step analytic processes, analogous to functions in MS Excel, can augment, annotate, correlate, sort, filter, or further manipulate the data

About Hexis Cyber Solutions

Hexis Cyber Solutions, Inc., a wholly-owned subsidiary of The KEYW Holding Corporation (NASDAQ: KEYW), based in Hanover, Maryland, provides complete cybersecurity solutions for commercial companies, government agencies, and the Intelligence Community (IC).

Hexis Cyber Solutions' HawkEye and NetBeat families of products offer active, multi-disciplined approaches to achieve a higher standard of cybersecurity that is based on our expertise supporting our nation's cybersecurity missions to ensure that your business or organization can operate at its maximum potential. For more information contact Hexis Cyber Solutions, 7740 Milestone Parkway, Suite 400, Hanover, Maryland 21076; Phone 443-733-1900; Fax 443-733-1901; E-mail info@hexiscyber.com; or on the Web at www.hexiscyber.com.

Hexis™
CYBER SOLUTIONS
a KEYW company