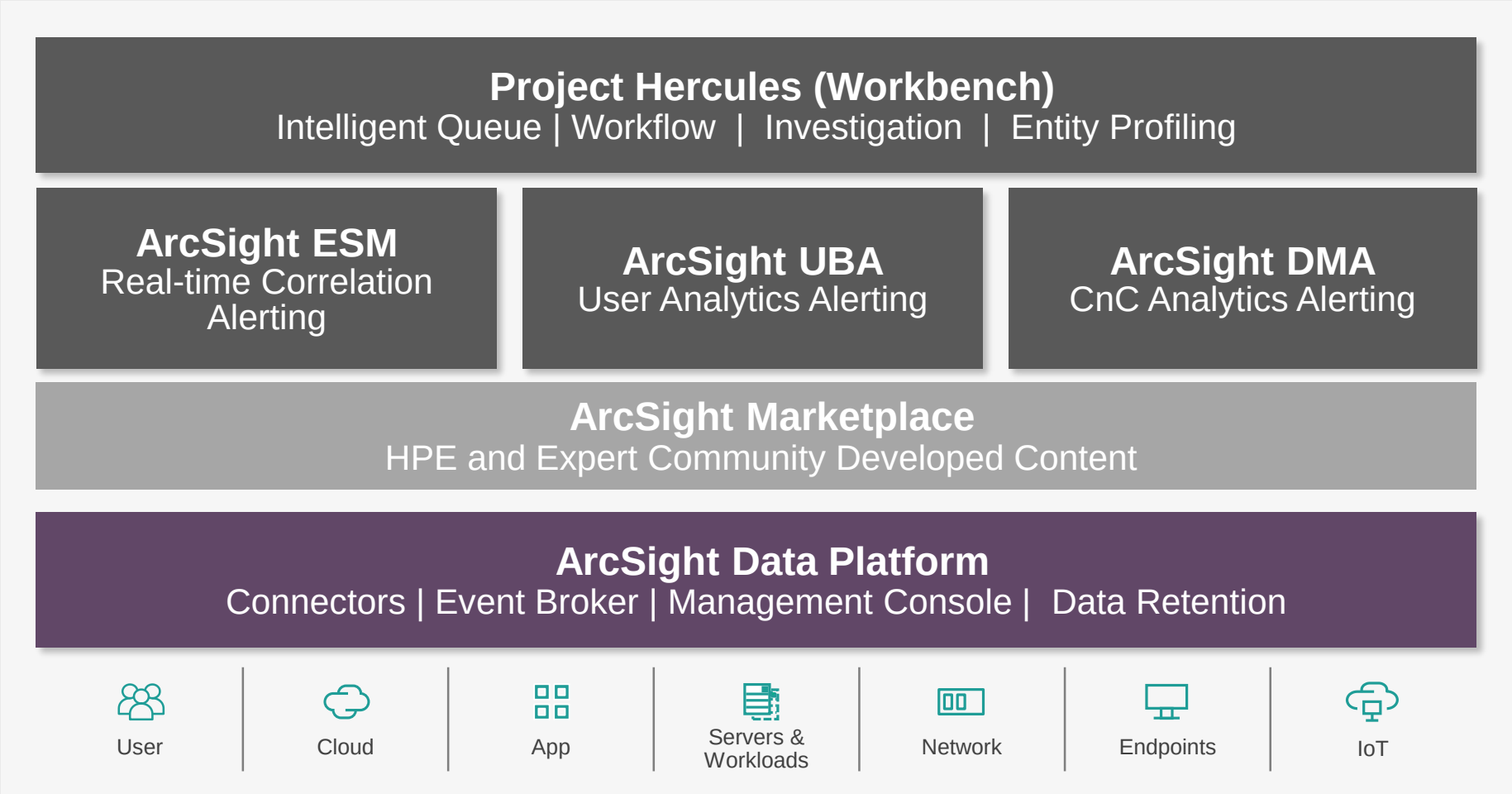
Hewlett Packard Enterprise

ArcSight Data Platform 2.0

Petr Hněvkovský, CISSP, CISA, CISM, CEH
Senior Solution Architect

Jan 2017

ArcSight Intelligent Security Operations solution



Intelligent Security Operations

Increase Speed, Simplicity and Effectiveness Across The Entire Workflow

Visibility Without Boundaries

Open platform, built for security, with massive scale and diverse log ingestion, supporting variety of operational use cases

Comprehensive Detection

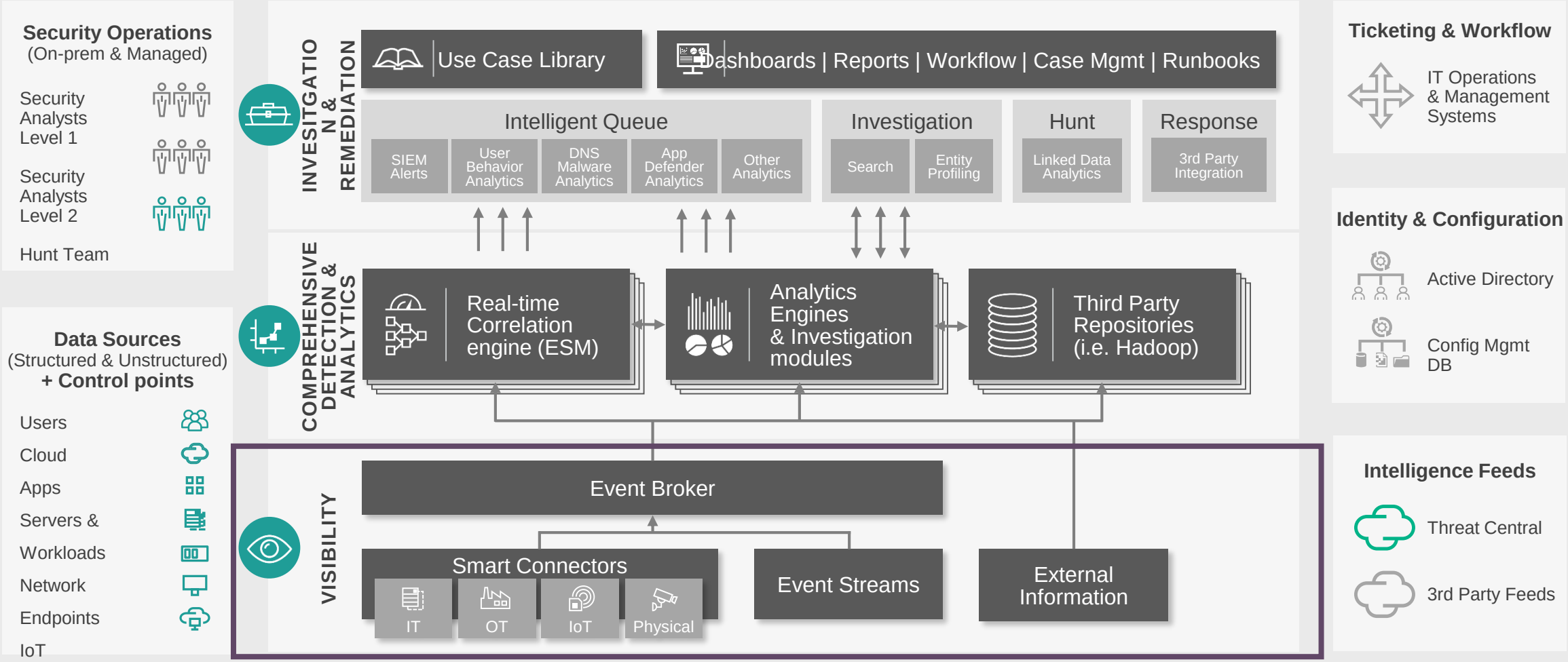
Known and unknown threats monitoring and alerting based on a seamless real-time and analytics engines built for security scale

Intuitive Investigation

Guided, analytics empowered prioritization, investigation, entity profiling and workflow

ArcSight master architecture

Actively evolving beyond traditional SIEM to support the Intelligent SOC



Hewlett Packard Enterprise

Expand the visibility of your data

for rapid detection, investigation and response to threats

Visibility Without Boundaries

Integrating data lakes with security applications

Keeping up with scaling environments

Adding security context to data

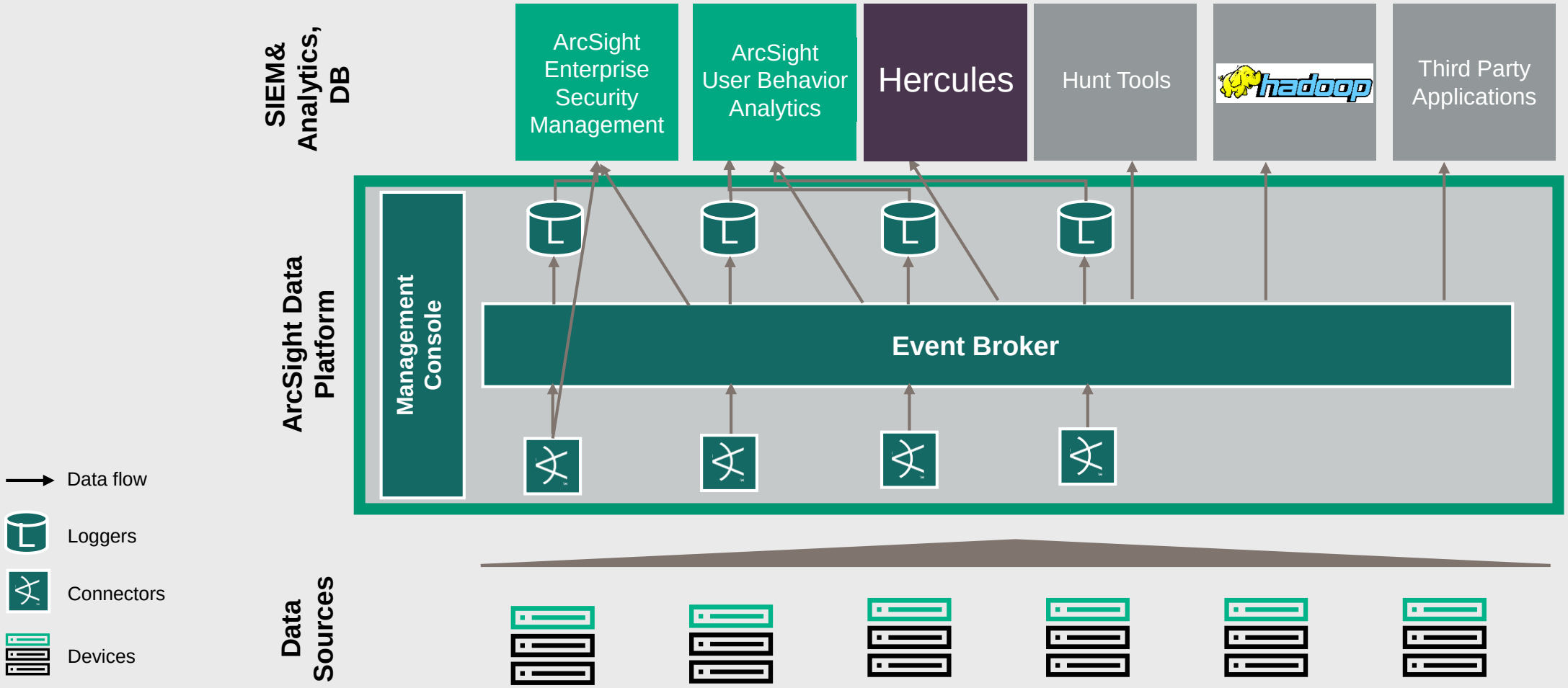
Open architecture to maximize usage	Scalability through variety and velocity	Real-time security context
Leverage data across the security posture for a wider range of applications and multiple business-specific uses	Support large environments by managing a wider variety of data at higher consumption rates	Collect data from any source and augment it with security context in real-time enabling faster threat detection

ArcSight Data Platform 2.0
Capabilities

ArcSight Data Platform summary

Platform	• Universal platform for ArcSight portfolio
Complete bundle	• Unlimited Connectors & FlexConnectors • Brand new Quick Flex parser tool • Unlimited device & Connector management ArcMC • New resilient Kafka Event Broker • Licensed Logger
Simplified Licensing	• Volume only in GB/day - pay once, consume many
HA & NP	• HA/NP does not license additional capacity
3rd party	• Support 3rd party destinations like Hadoop

Lay the Foundation for Hercules - ArcSight Data Platform 2.0

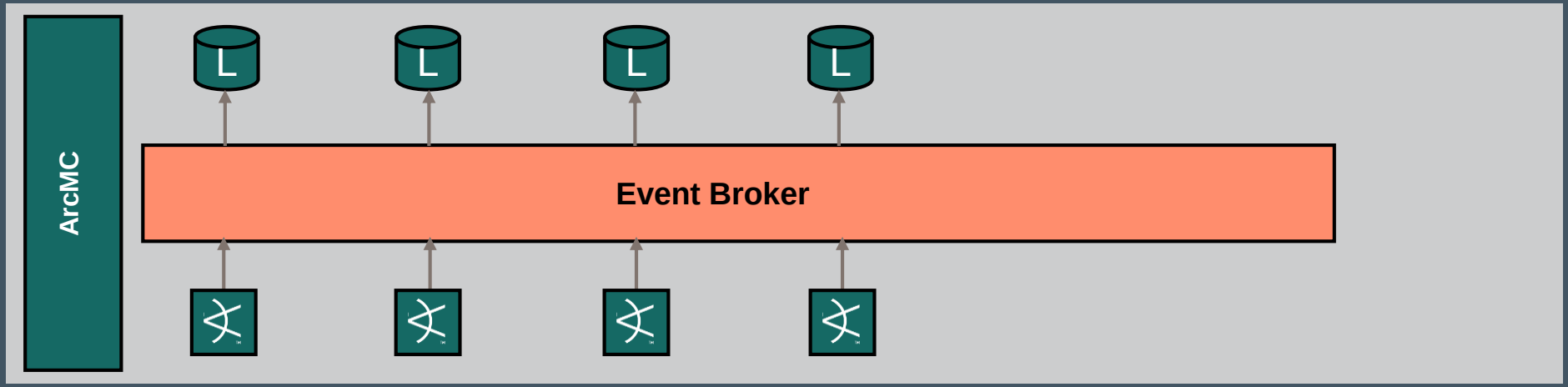


Hewlett Packard Enterprise

The ADP 2.0 Innovation

What's new?

Event Broker 1.0



Event Broker

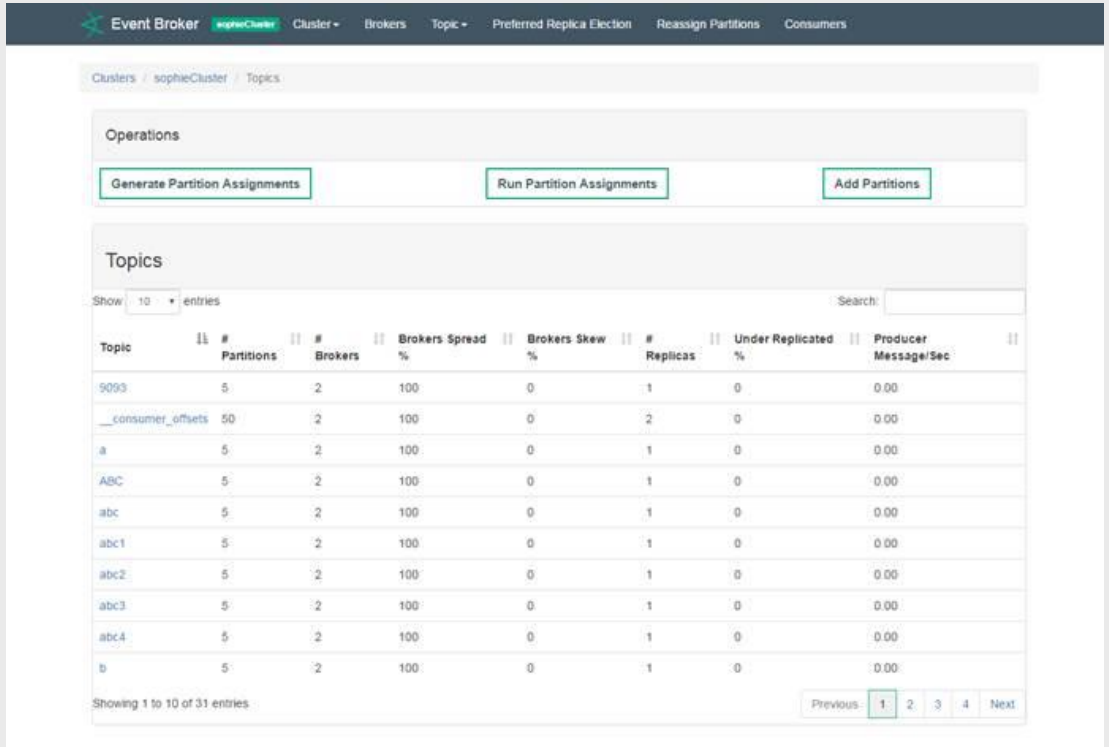
Data hub that enables getting data from aby where and send it to any destination including ArcSight applications, third party applications and in-house data lakes.

Key Attributes

– **Open**
- Documented Kafka based standard interface
- HDFS integration

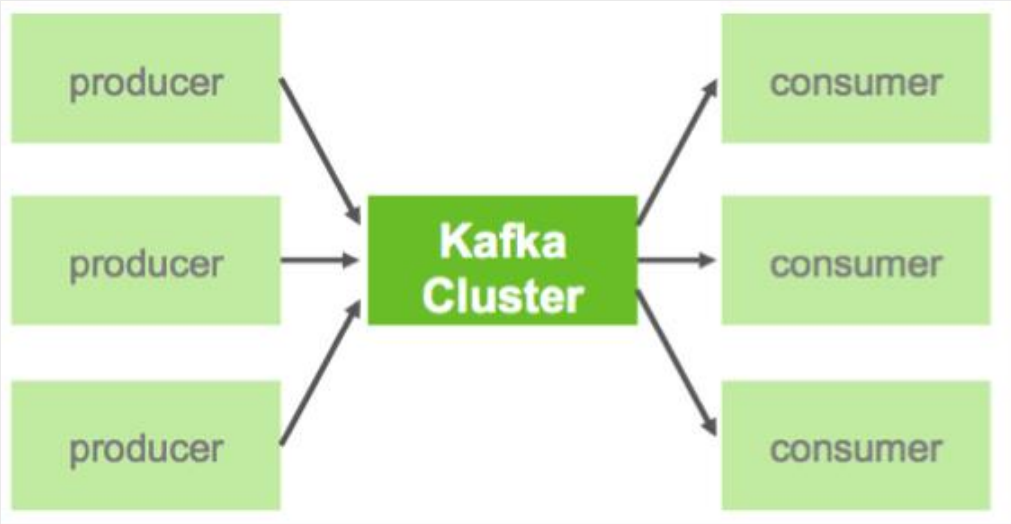
– **Scale**
- 1M EPS
- Connector scale improved, reduce dual feed impact

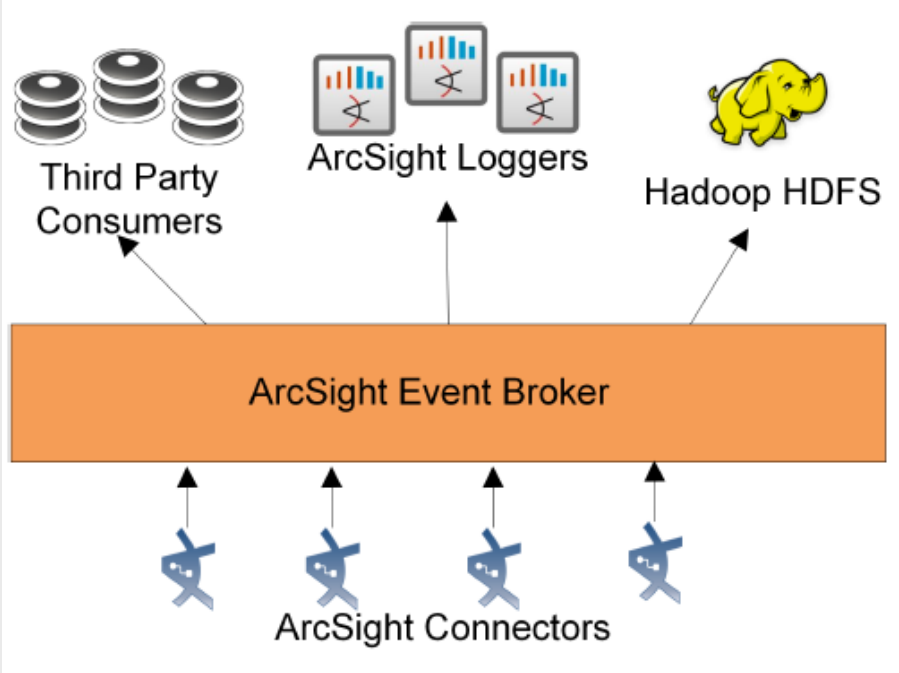
– **Security Focus**
- Built In HA reliability, 4 9’s
- TLS 1.2 encryption for data in motion



Kafka in a nutshell

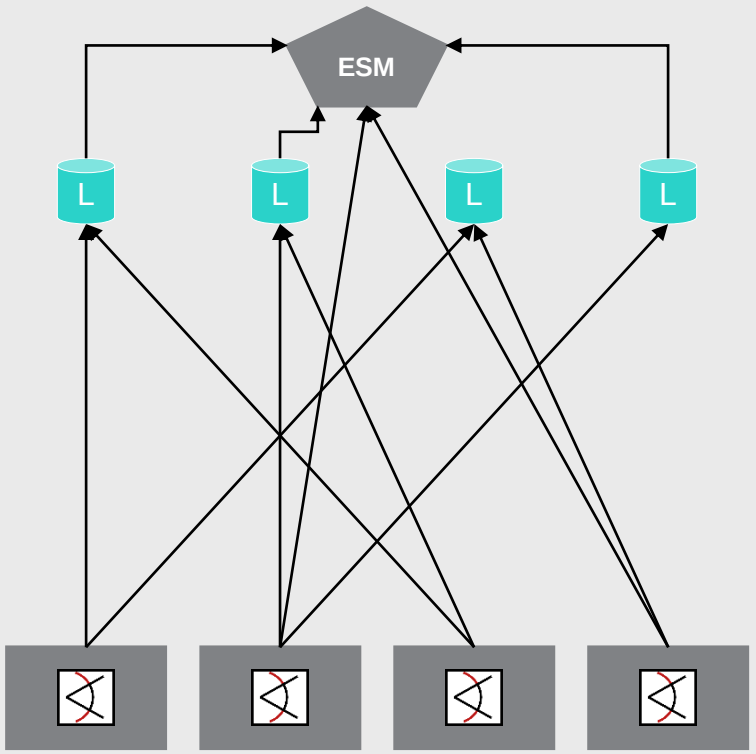
- Producer
  - Push the message into Kafka topic
- Consumer
  - subscribe to topics/s, pulls the message from Kafka
- Topics
  - messages are placed in topics
- Kafka Cluster
  - typically odd number of nodes
- Zookeeper
  - coordinate the services in Kafka
- Messages
  - pushed to kafka topics and pulled by the consumers subscribe to these topics



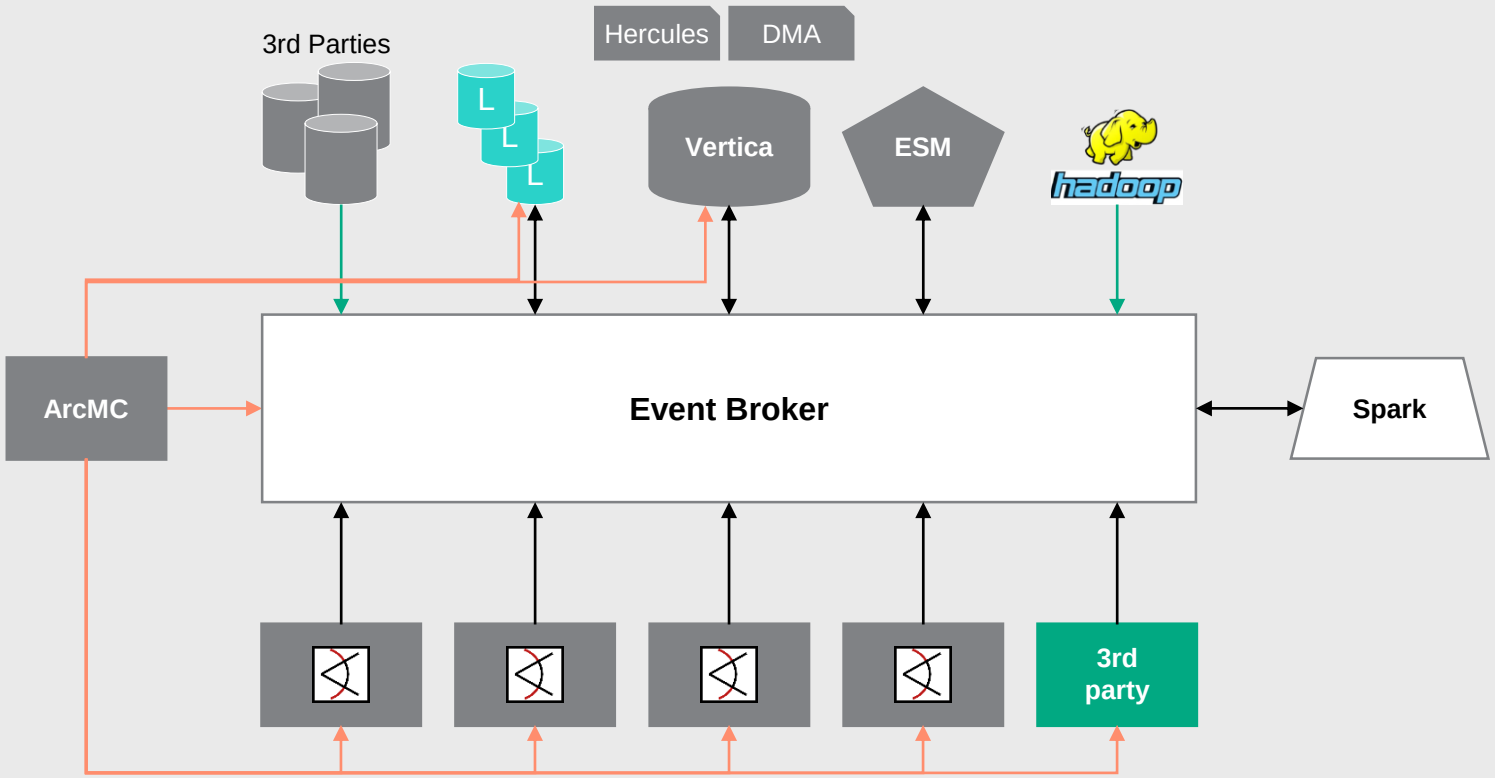


Event Broker

Without Event Broker



Future

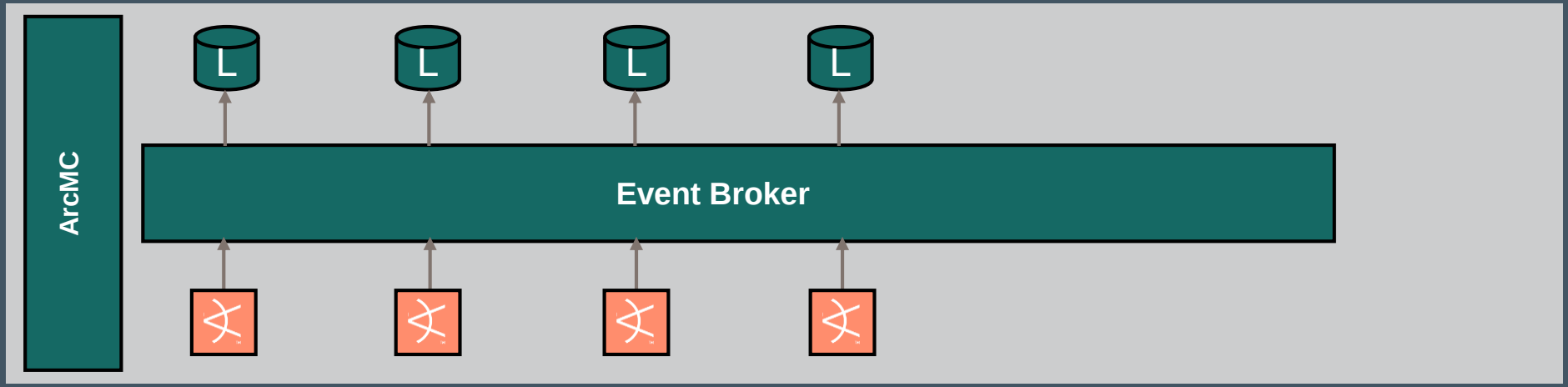


Open Architecture
Scalable – sources and destinations
Centralized data manipulation

The ADP 2.0 Innovation

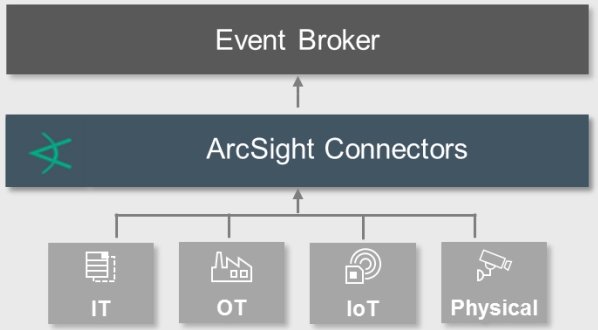
What's new?

Connector 7.3



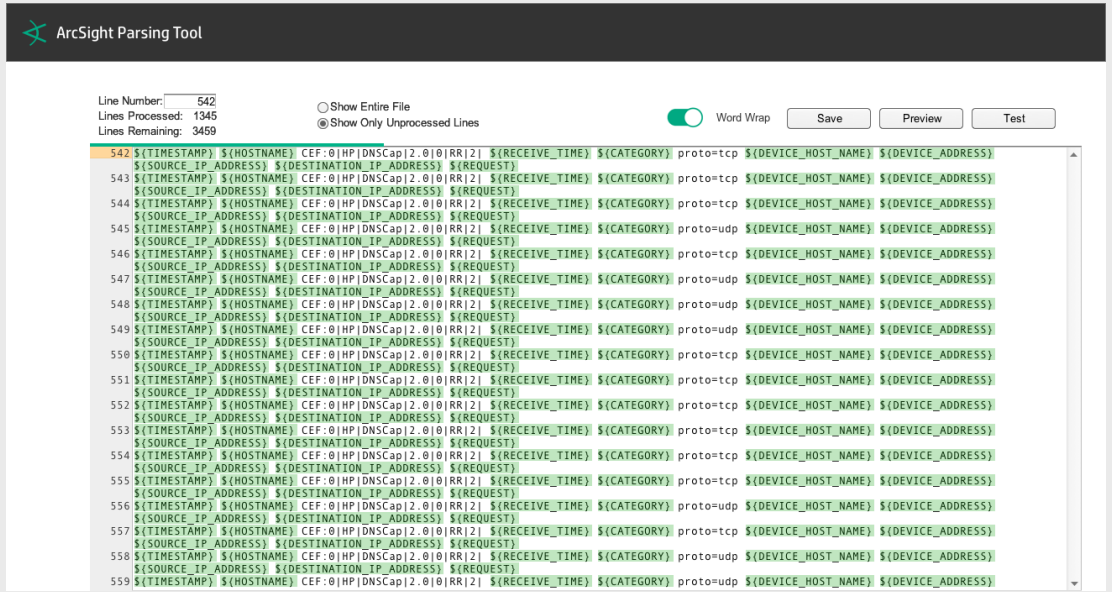
Connector

Augments data with security context to make it better suited for security application.



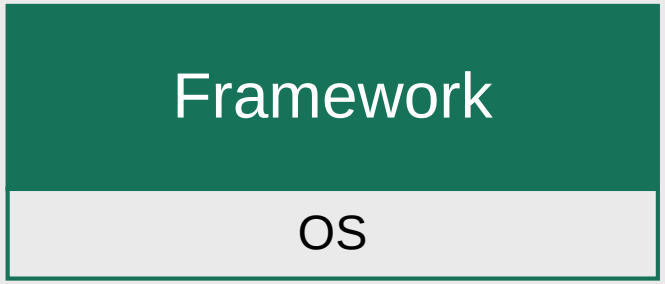
Key Attributes

- **Open**
  - Collect data from any data source and make it security relevant
  - Support new device versions by releasing parsers every 4 weeks
- **Scale**
  - Support a large variety of devices in large environments with 350+ out-of-the-box connectors
- **Security Focus**
  - Normalize, categorize and enrich data for better correlation and analytics



SmartConnector Releases cycle (7.3 and on)

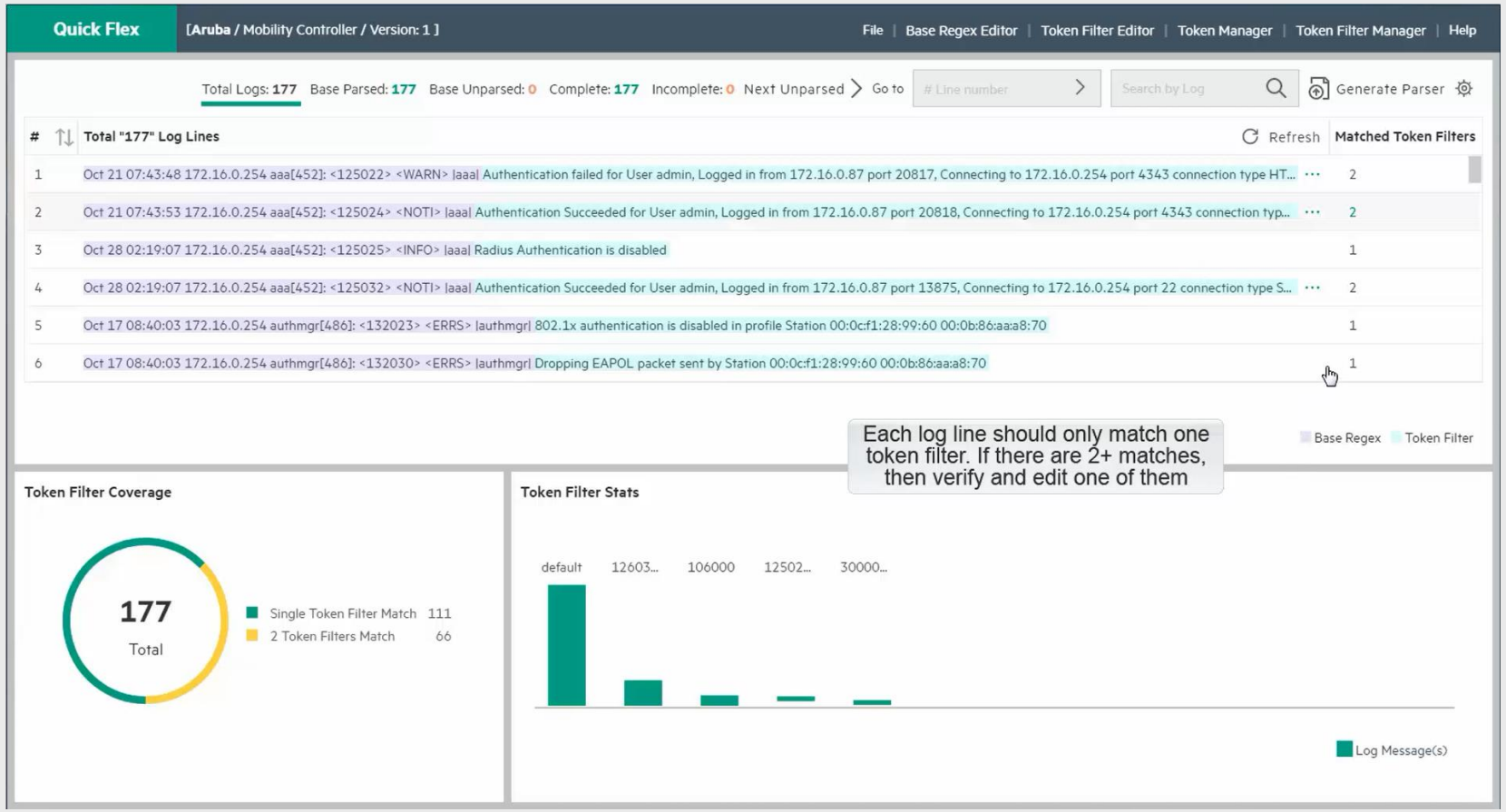
Framework every 12 weeks



Delivery every 4 weeks

- Parser Package showing on the marketplace
- Faster turnaround for parser bugs (labs, PS and Support overrides in the field) and new device version available in Market.
- Release feature rich connector framework every quarter that can be made noticeable to market(ing)

New Quick Flex tool available



Speed up flex develoment

Available free with ADP

https://www.protect724.hpe.com/groups/arcsight-product-announcements/blog/2016/12/20/quick-flex-is-now-available

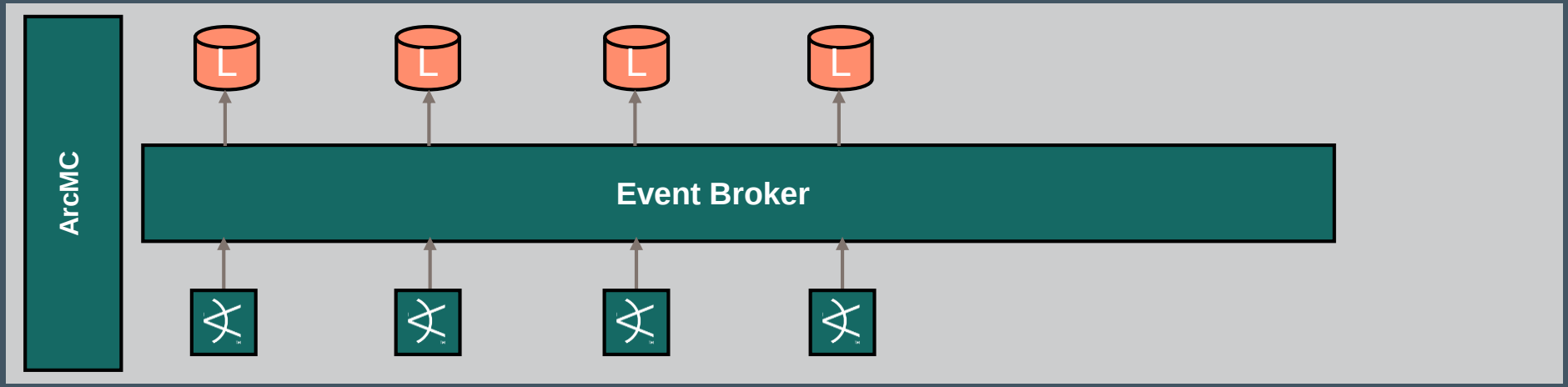
See the video tutorial on

https://www.protect724.hpe.com/docs/DOC-14871

The ADP 2.0 Innovation

What's new?

Logger 6.3



Hewlett Packard Enterprise

Data Retention (Logger)

Cost-effective universal log management solution that unifies searching, reporting, alerting, and analysis across any type of enterprise machine data.

Key Attributes

– **Scale**

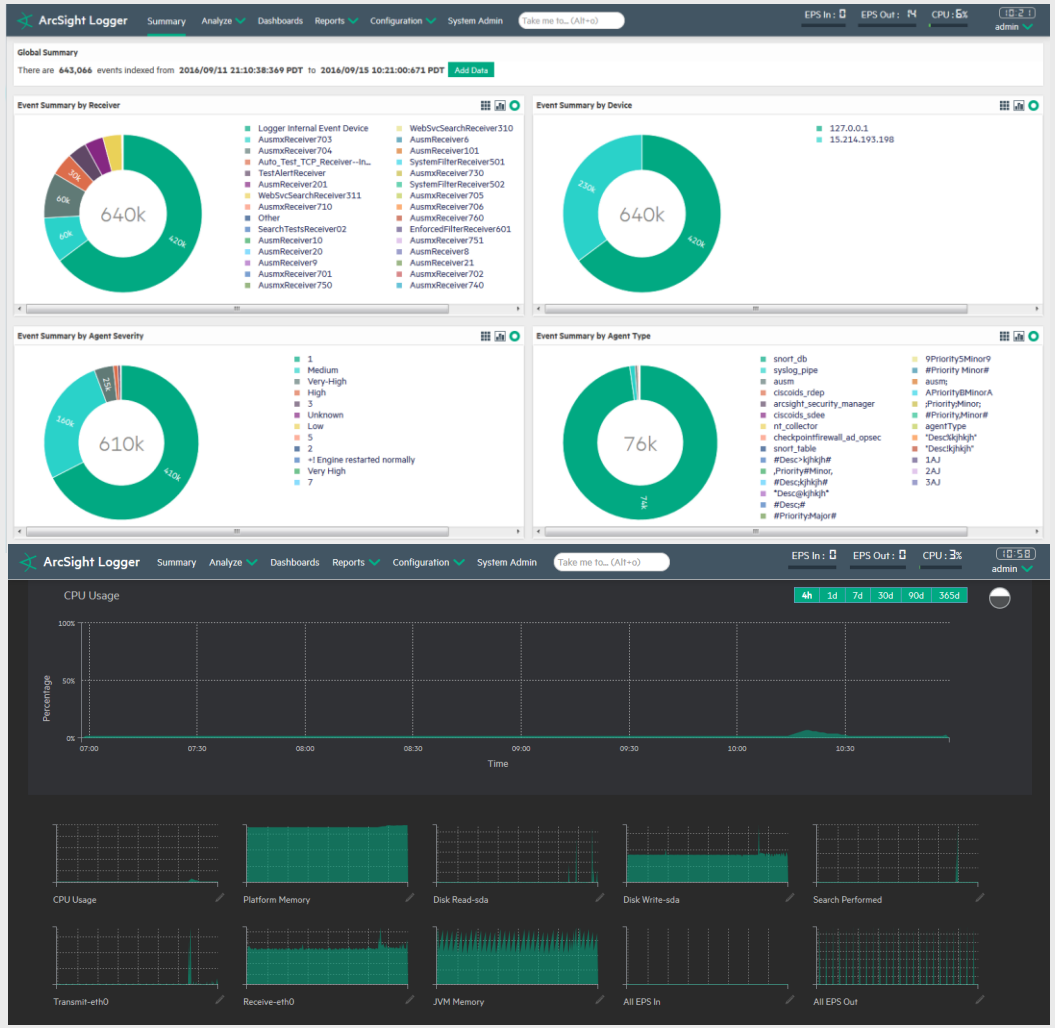
- 1M EPS in a 100 peers architecture
- 100 Concurrent search

– **Performance**

- Search speed for typical used search improved by 50%, some by X2
- 10:1 compression ration to store up to 1200 TB of data

– **Security**

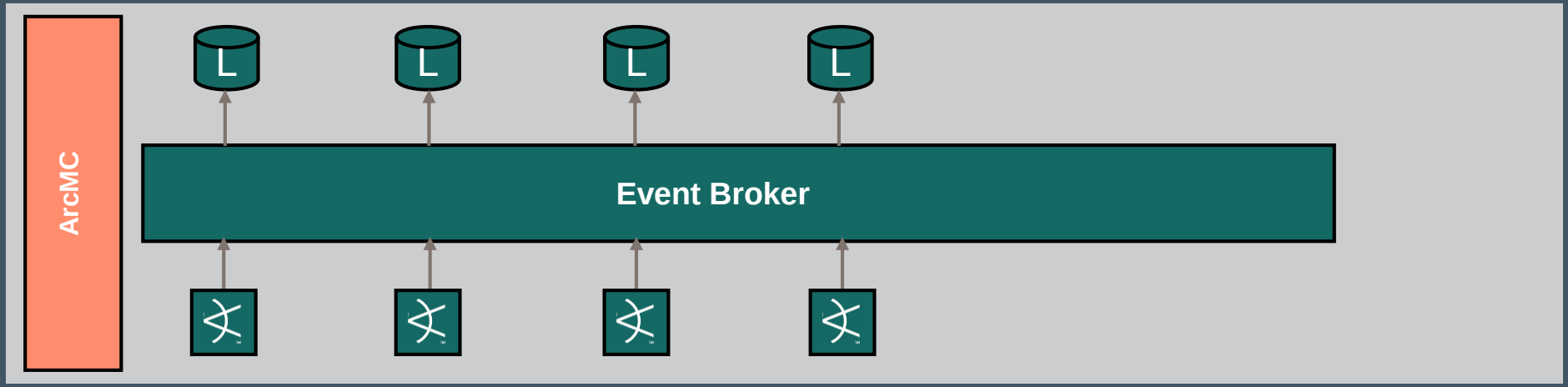
- Data at rest encryption on ADP appliances



The ADP 2.0 Innovation

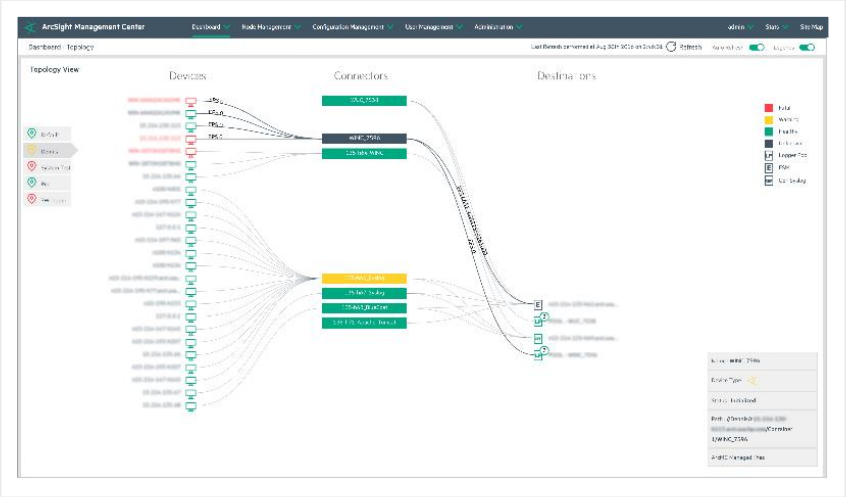
What's new?

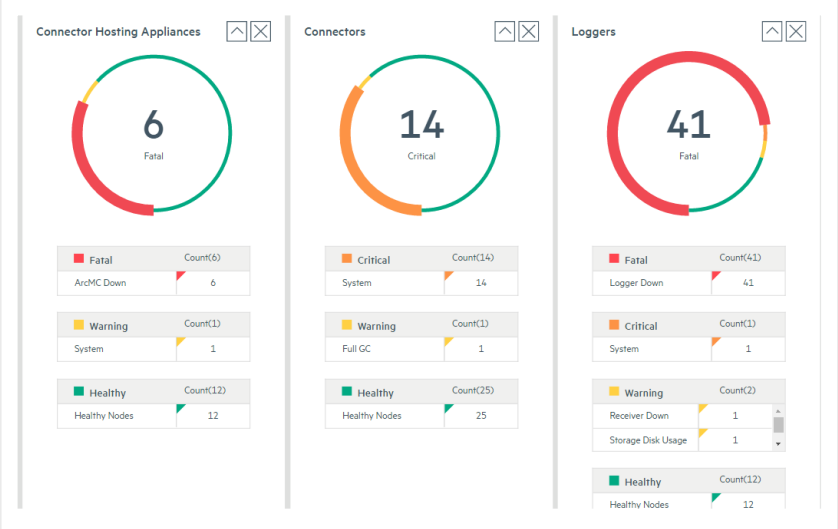
Management Console



Management Console

Centralized Management Console for end-to-end monitoring of the entire security posture.





Key Attributes

– **Ease of Management**

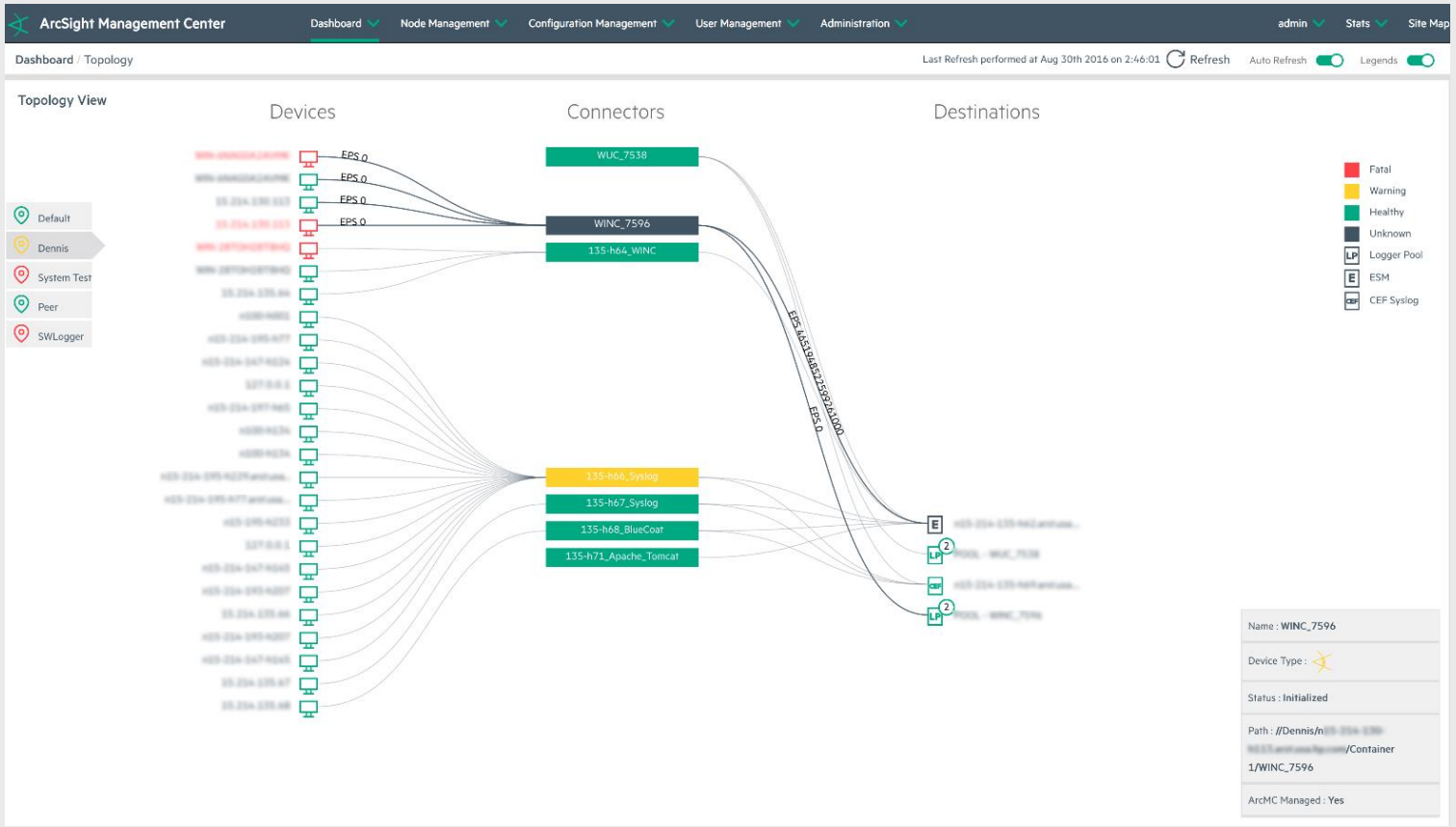
- Single-view centralized management
- Topology & System Health Monitoring
- Bulk operations for destination configuration and managing upgrades

– **Performance**

- Easily supports hundreds of connectors and entities
- Screen response time slashed by 70%

Management Console- End to end Monitoring

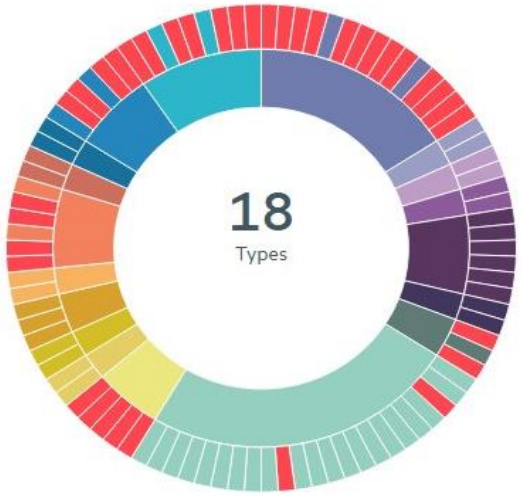
- Topology view for consolidated view
- Display device information on hover
- Sort devices by region / groups



Management Console- Device Monitoring

- Detect health related issues, like events dropping
  - Shows you which devices not sending events (inactive devices)
  - Suspicious EPS spike or drop
- Health feedback with ability to drill down
  - All devices by product type and drill down capabilities to locate specific device

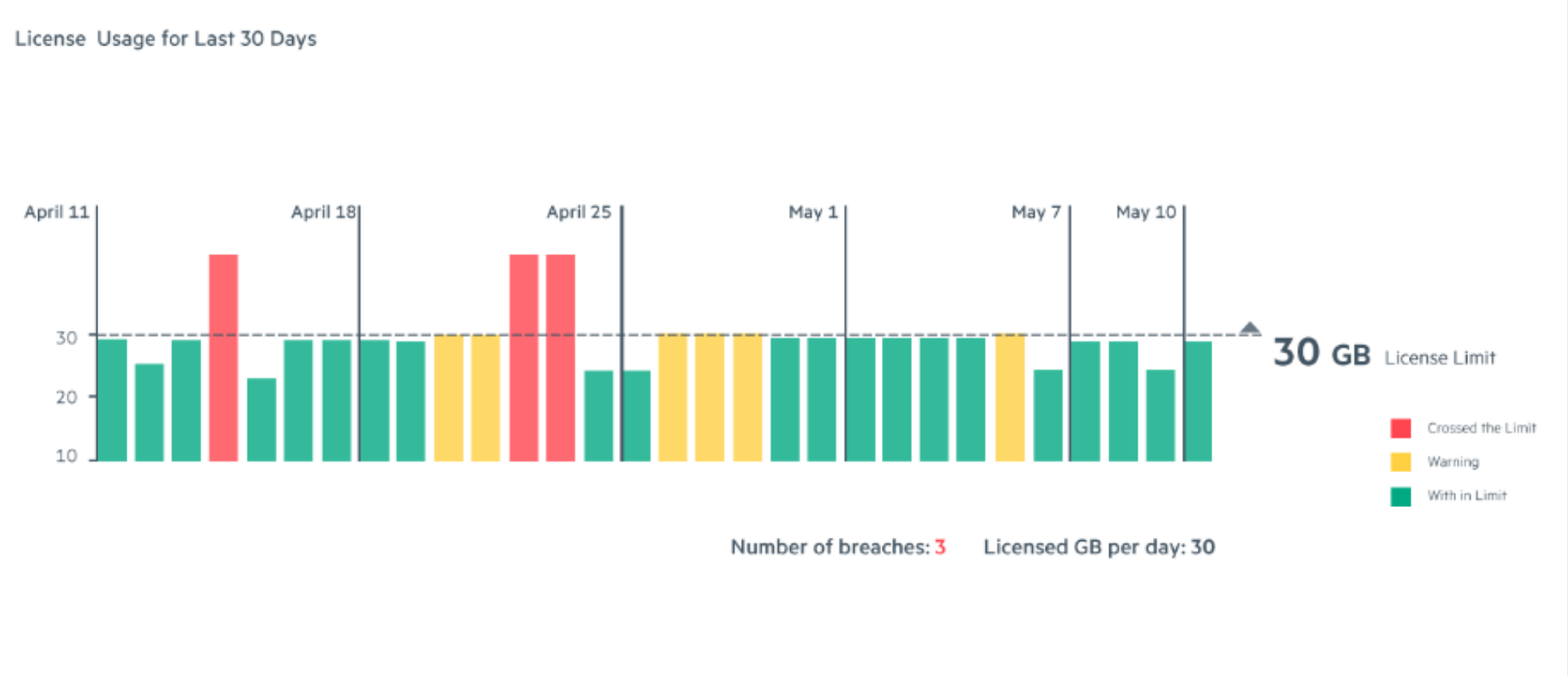
Devices by Product Type



Device Type	Total Devices	Inactive Devices
Unix	15	13
Peakflow	2	0
CiscoRouter	2	0
PacketAlarm	2	0
NSM	6	0
DefensePro	2	0
System or Application Event	3	2
ArcSight	23	2
ASA	5	5
Total	94	37

Management Console- Centralized ADP license tracking

– Track ADP licenses in one place



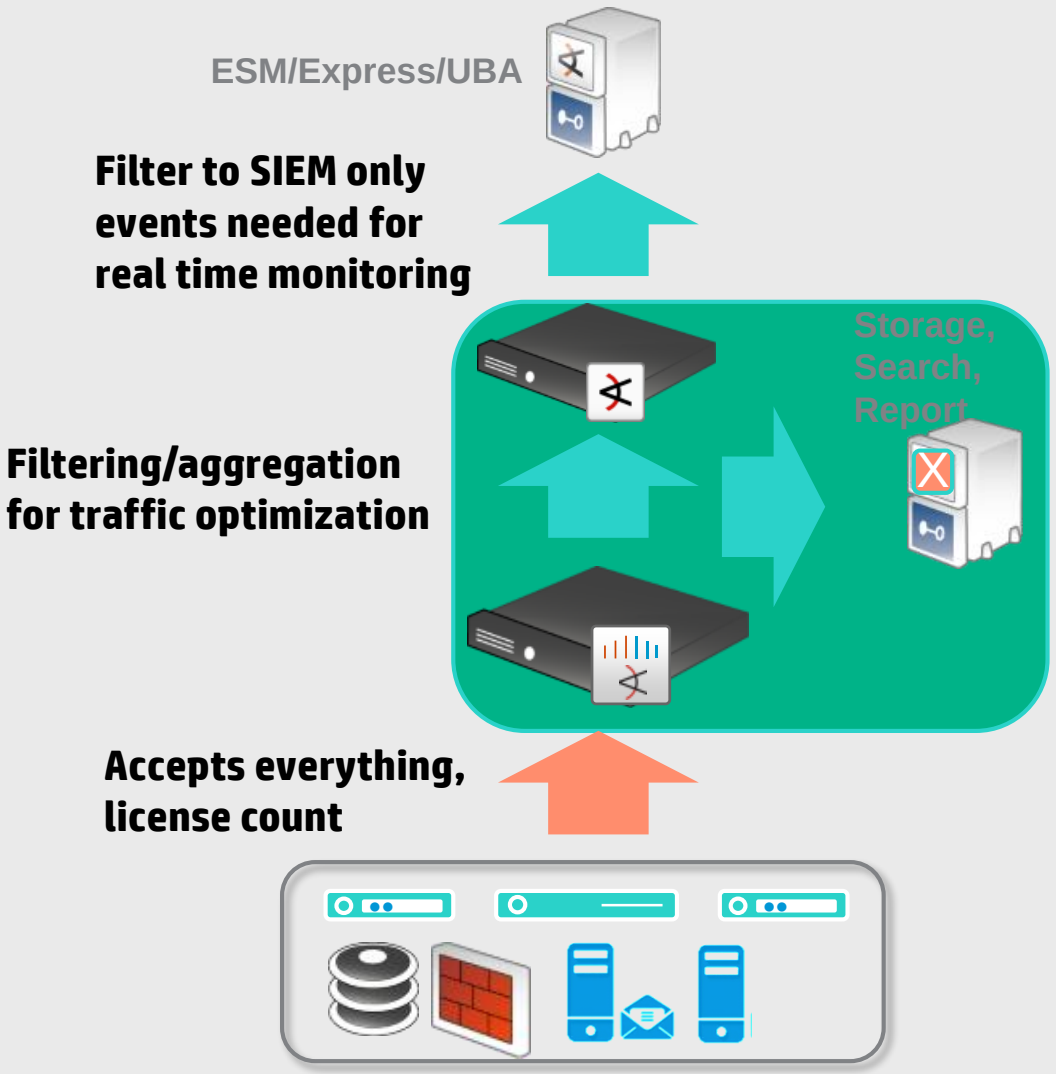
ADP Licensing

ADP 2.0 Entitlements

What do I get from the move to ADP license?
One **single SKU** for Logger + Event Broker + ArcMC + Connectors + Flex
Rights for **unlimited** Devices, Consoles, Web users, Scanned assets on ESM
Unlimited centralized **management** function for the whole environment - centralized user management, archives, nodes of logger and/or connectors, devices monitoring
Rights for **Flex** toolkit & Quick Flex wizard
Only path to get the new modern collection architecture with **Event Broker**
Gb/d **ingestion based pricing** to be used on any destination, no double counting of capacity for non-production and high availability systems
Rights to feed into **3rd party** data lake from the ArcSight CEF connectors

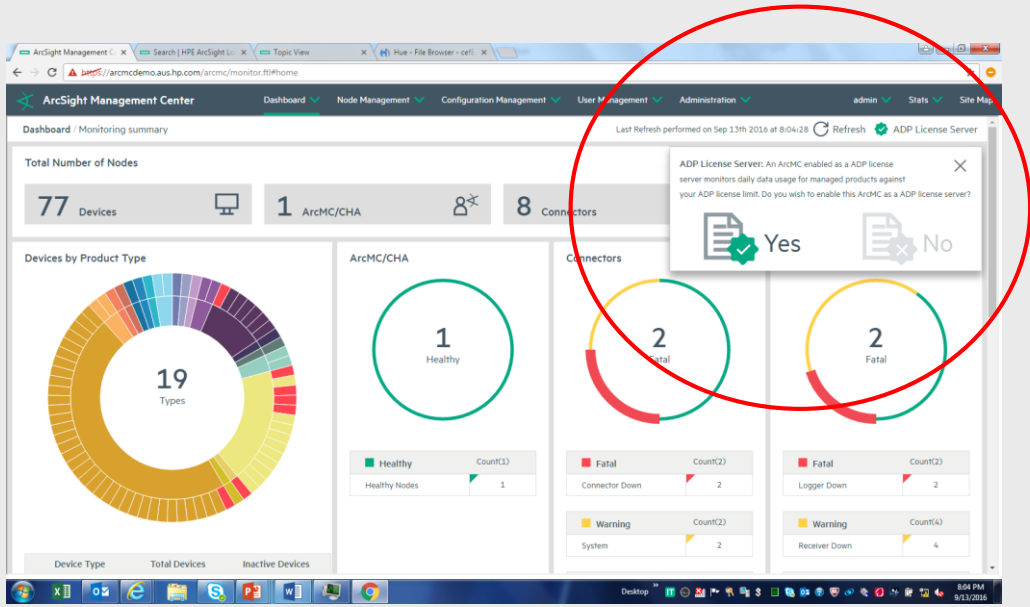
Recap: Licensed on Ingest

- Total raw ingest in GB per Day
  - Filtering/Aggregation tuning have performance impact but no impact on ADP license
  - The new measurement is done on direct web service between Connectors/Logger and ArcMC- no duplication (each managed entity is reporting it's sources)
    - Require ArcMC 2.5
    - Require Connector 7.3
- No use of Agent50 in ADP licensing (mechanism stay the same for Logger only license)
- Sending data to any destination has the same cost
  - No capacity measure on HA or NP
  - No fee for sending data to non-ARST destinations (was not allowed in previous ALA)



Recap: ADP 2.0 license technicalities

- Autopass has a new license file format
  - Any new installation or upgrade to Logger6.3 to ArcMC2.5 require download/install the new file
- Autopass ≠ADP license pool across the whole environment
  - On each Logger unit, SW or Appliances, install the base 5Gb/D (in case needed)
  - Configured the ArcMC as license server
  - Apply ADP capacity of the whole environment on ArcMC, measure as one number
- Event Broker is only licensed through ADP (can't be purchased separately)
- Appliance price is HW market price + SW + premium for packaging (45K with Logger, 40K with ArcMC)
- We measure SW instances to pay royalties, each instance is limited by 500 Gb/d Logger technical limit. Logger appliances limit to 250 Gb/d



Let‘s Start Selling

3 main scenarios for ADP migration trigger

– **Simplified Pricing** (unlimited devices/consoles)

– **Intelligent SOC vision**

- Want to leverage ESM data in big data architecture
- Subscribed to “Intelligent SOC” with multiple analytics apps and an investigation tool that master the SOC operations (“Foundation for Hercules”)

– **Large ESM** (happy with Logger/ESM only, need bigger environment)

ADP benefits customers – more business for you ☺

Platform	• Universal platform for ArcSight portfolio
Complete bundle	• Unlimited Connectors & FlexConnectors • Brand new Quick Flex parser tool • Unlimited device & Connector management ArcMC • New resilient Kafka Event Broker • Licensed Logger
Simplified Licensing	• Volume only in GB/day - pay once, consume many
HA & NP	• HA/NP does not license additional capacity
3rd party	• Support 3rd party destinations like Hadoop

Q & A

petr.hnevkovsky@hpe.com

Call to Action

Data Sheet
Key features and customer benefits of ADP 2.0

Beat the Hackers Customer Webinar
Customer facing webinar

Sales Enablement Training
Learn what's new in ADP 2.0

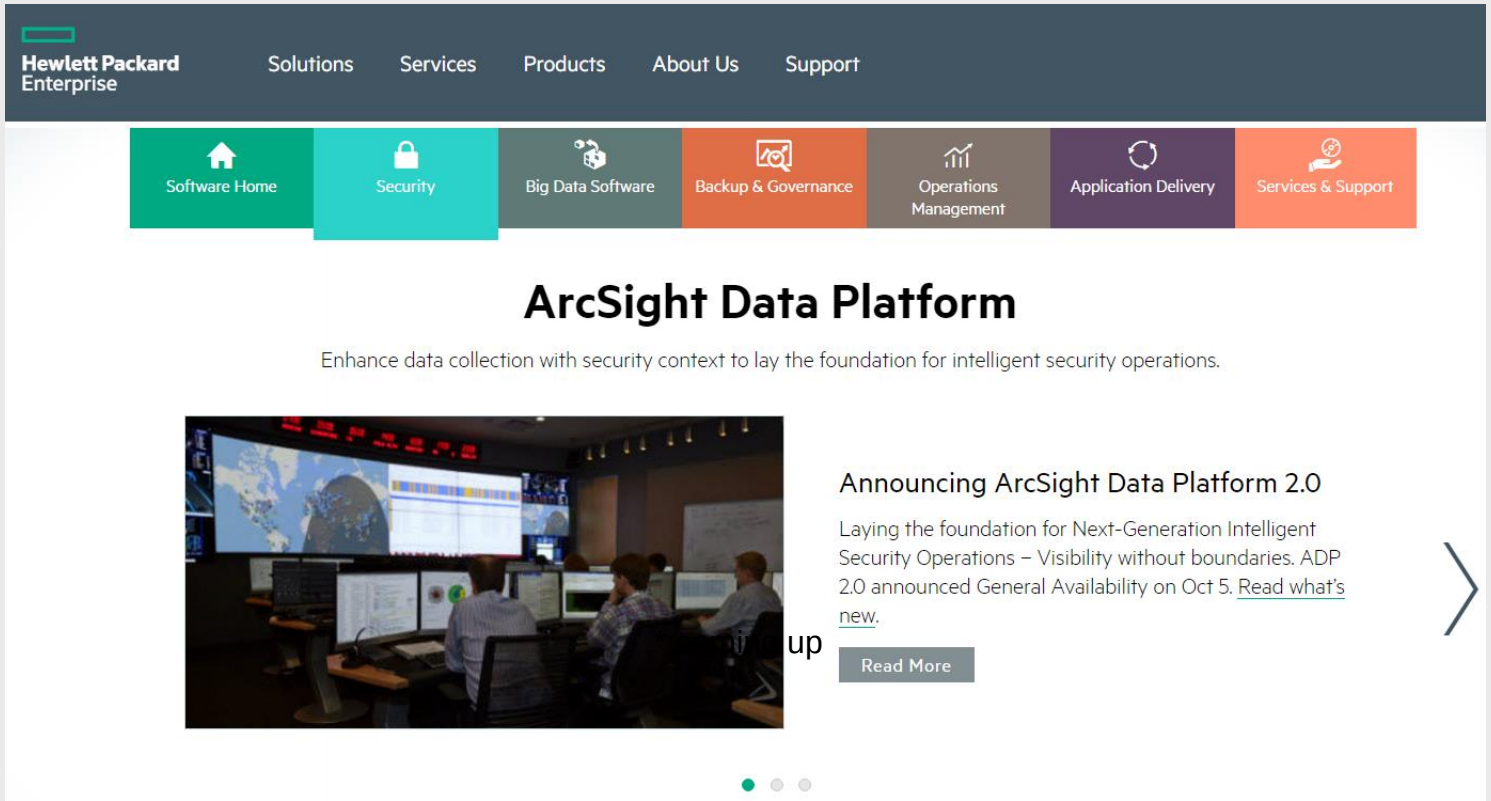
ArcSight Customer Facing Deck
Presentation to share with customers

ArcSight Pricing & Licensing webinar
ADP pricing, licensing and migration costs

Pricing Calculator
Calculate deployment cost to customer

Lay The Foundation Gold Standard video
Scripted sales pitch

Technical Whitepaper *
Deep-dive into technical solution



up