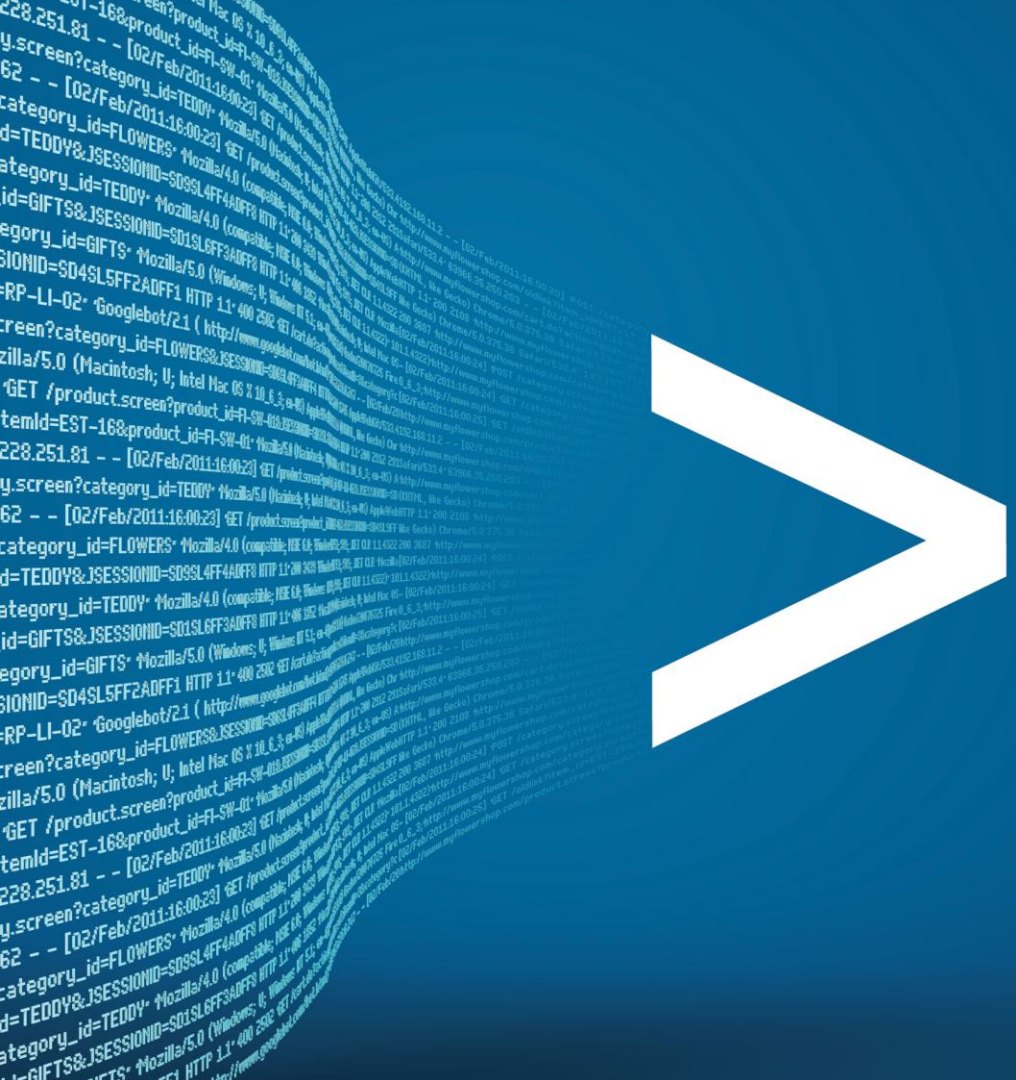


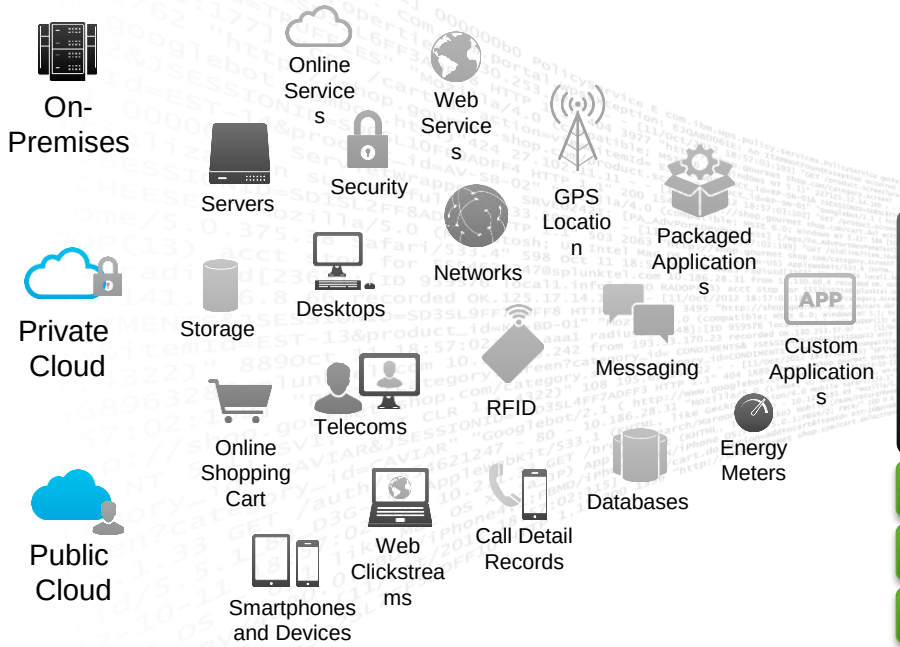
Splunk Enterprise Monitoring Overview

splunk>

What is Splunk? A Platform For Machine Da

Universal Machine Data Platform

Machine Data: Any Location, Type, Volume



Answer Any Question

Ad hoc search | **Monitor and alert** | **Report and analyze** | **Custom dashboards** | **Developer Platform**

splunk>enterprise

splunk>cloud

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

Industry Leading Platform For Machine Data

Schema on the Fly

Machine Data: Any Location, Type, Volume

Answer Any Question

On-Premises

Private Cloud

Public Cloud

Online

Servers

Networks

Desktops

Storage

Packaged Applications

Databases

Energy Meters

Call Detail Records

Smartphones and Devices

Ad hoc search

Monitor and alert

Report and analyze

Custom dashboards

Developer Platform

splunk>enterprise

splunk>cloud

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

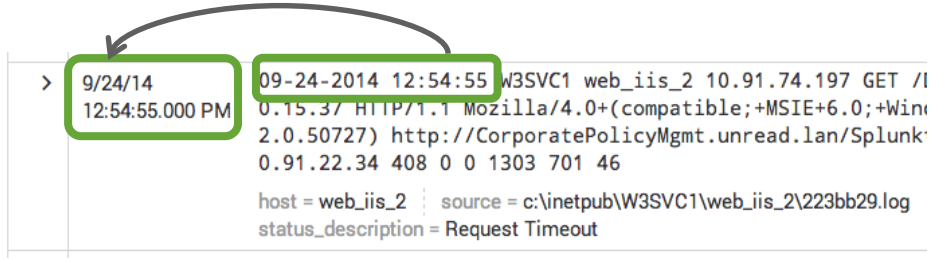
Any amount, any location, any source

Schema-on-the-fly | Universal indexing | No back-end RDBMS | No need to filter data

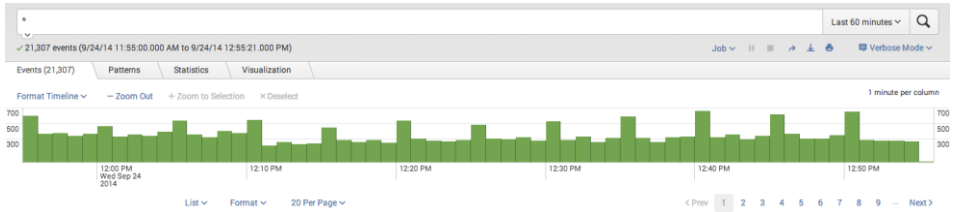
Inside Universal Indexing

Automatic event boundary identification

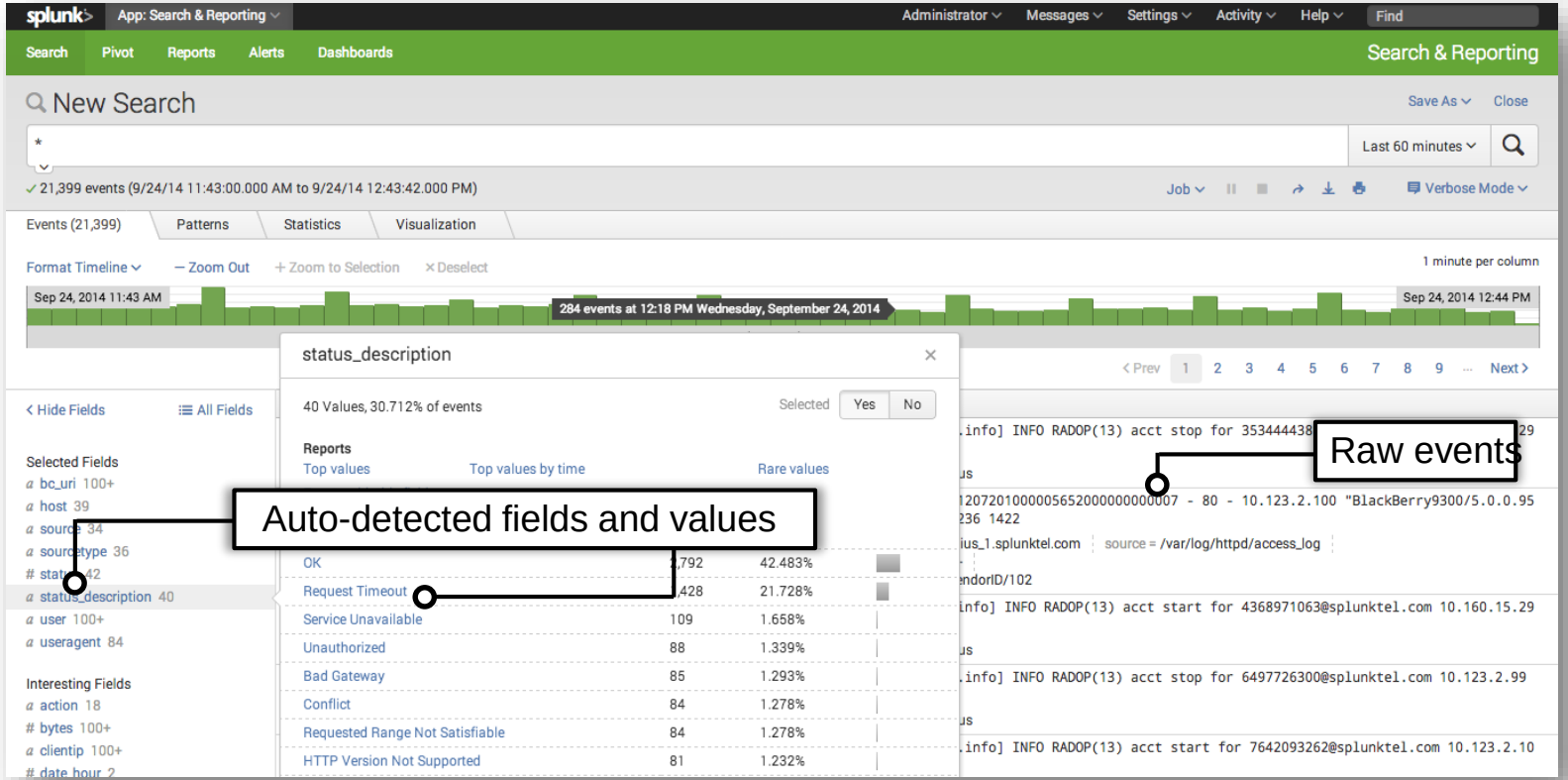
Automatic timestamp normalization



Accurate searching and trending by time across all data



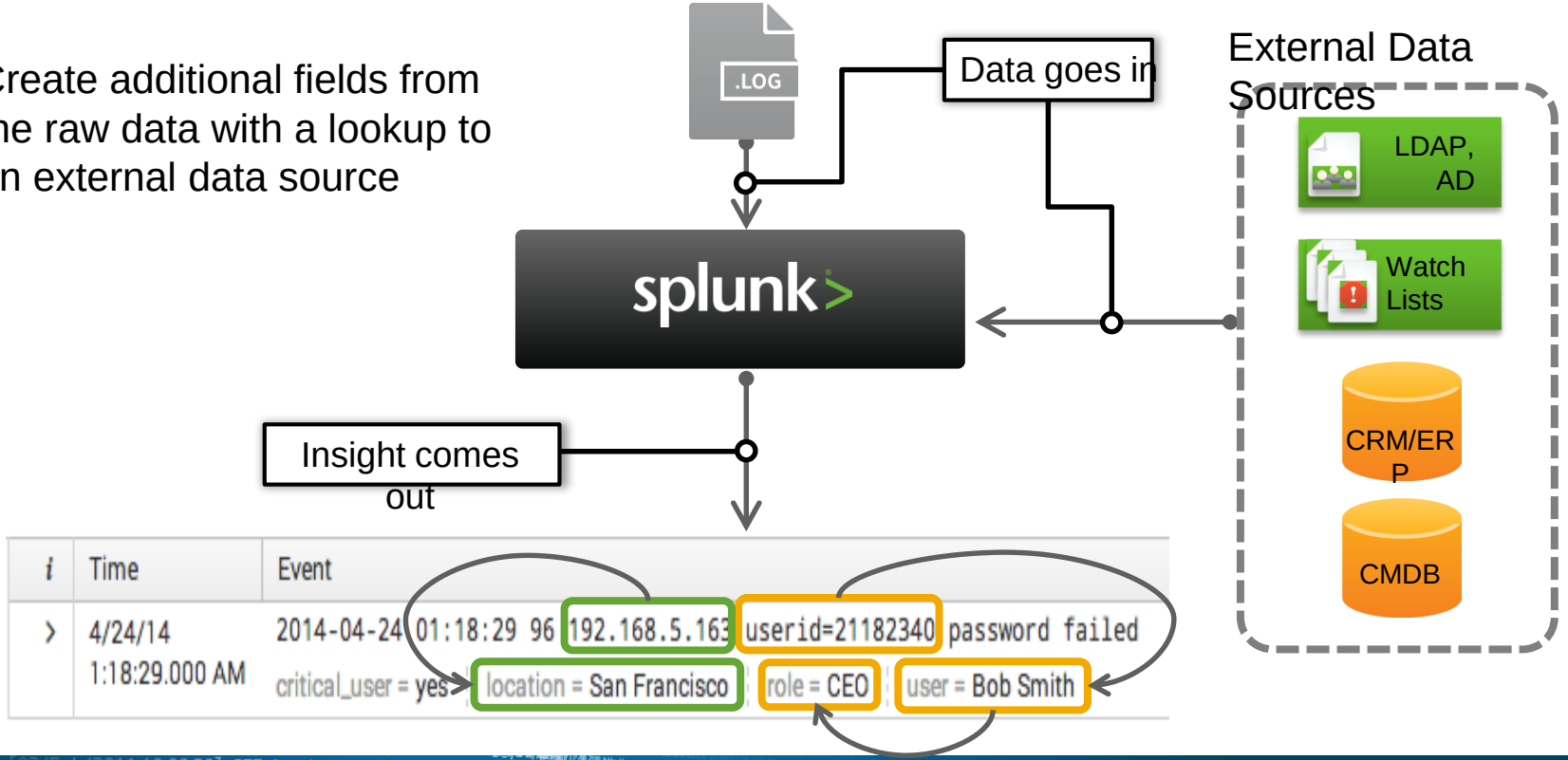
Schema-on-the-Fly



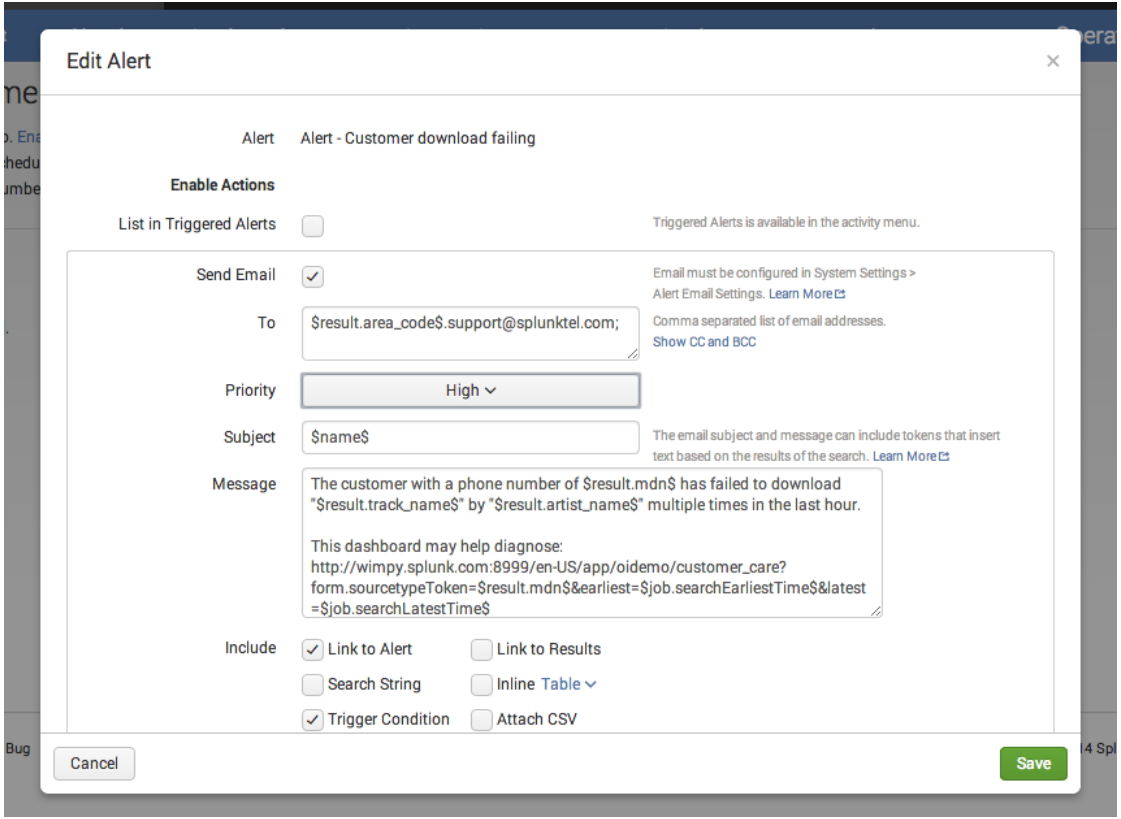
Schema on the Fly

Enrich Raw Data to Make It More Meaningful

Create additional fields from the raw data with a lookup to an external data source

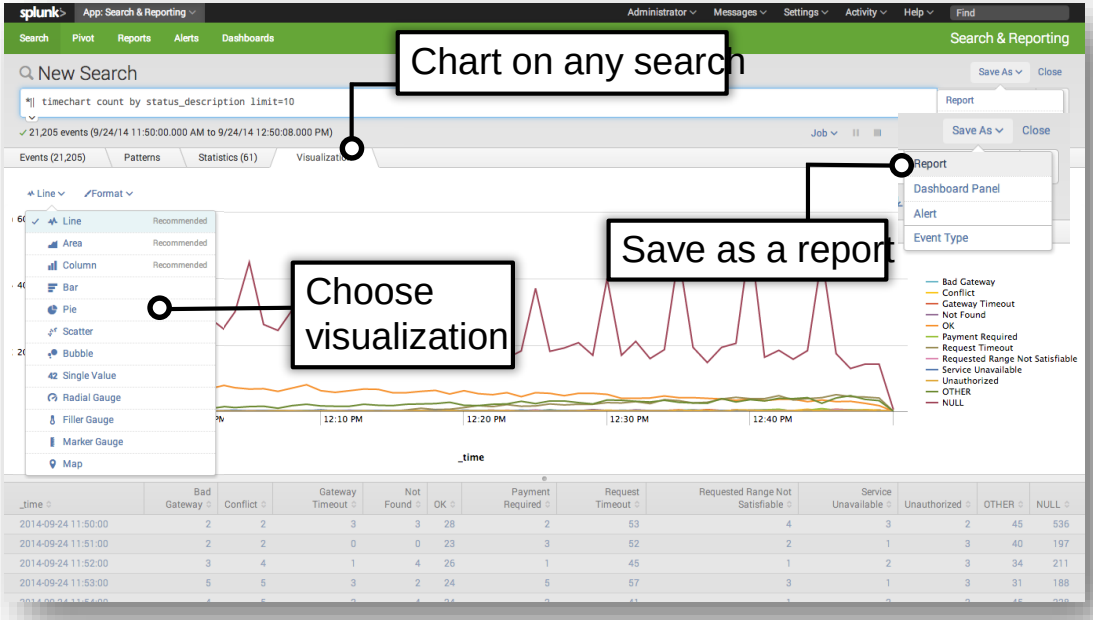


Actionable Alerting



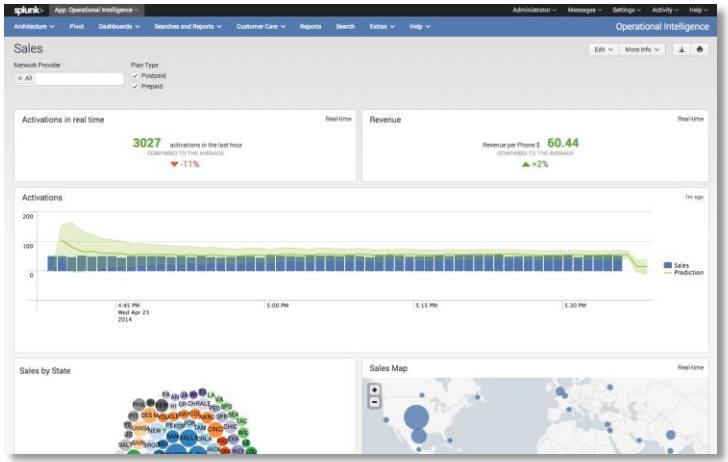
Dynamic Reporting

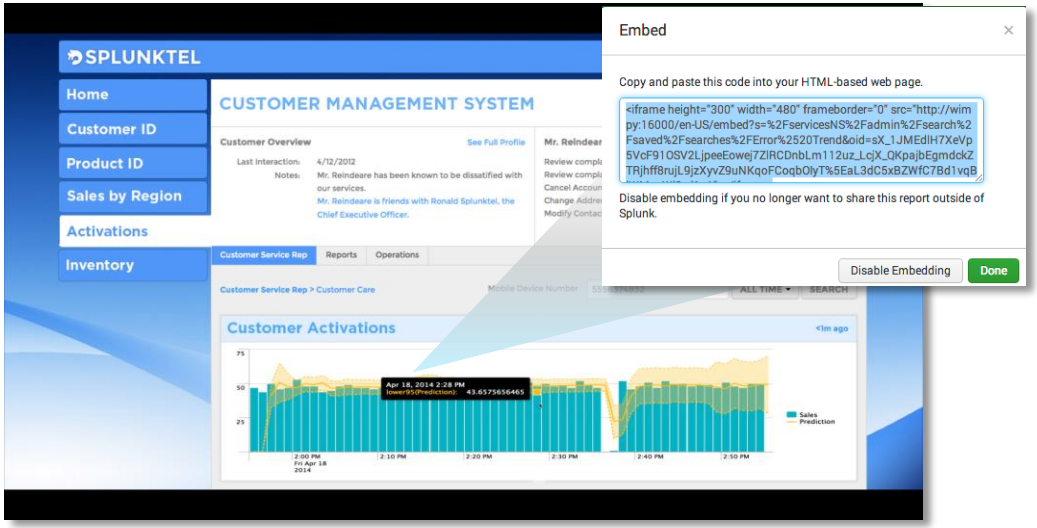
Agile Reporting and Analytics



Combine Reports to Create Dashboards

Use the built-in dashboard editor

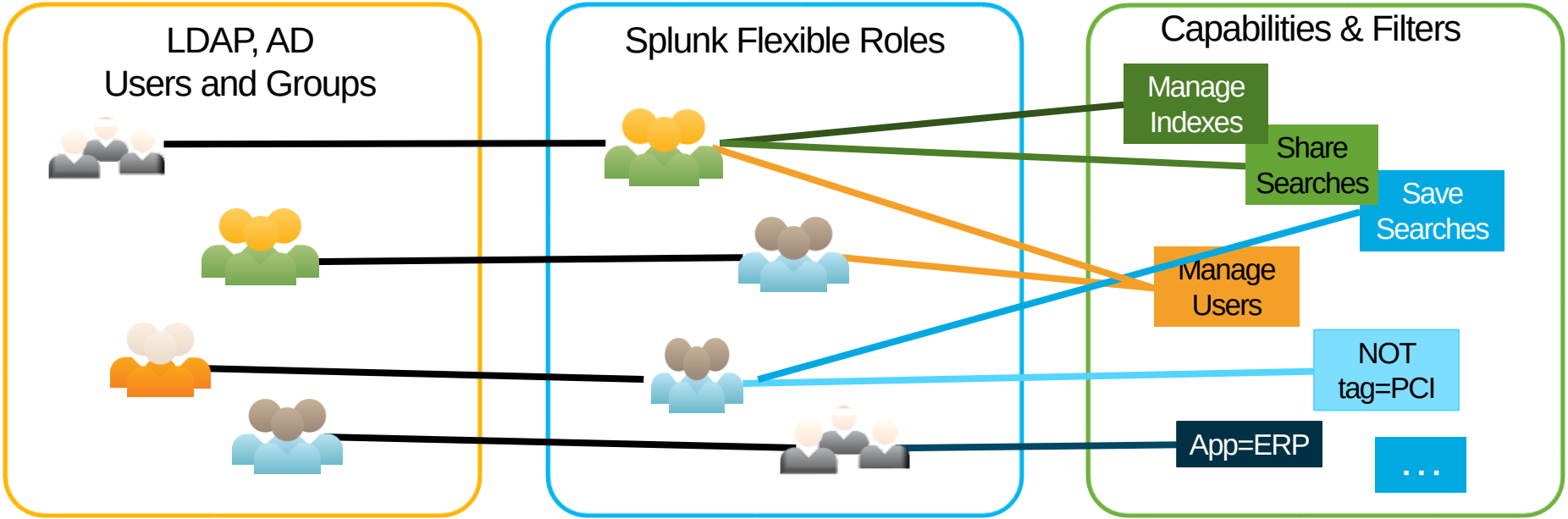




Or embed the reports into external sites like a wiki

Role Based Access Control

Integrate authentication with LDAP and Active Directory.



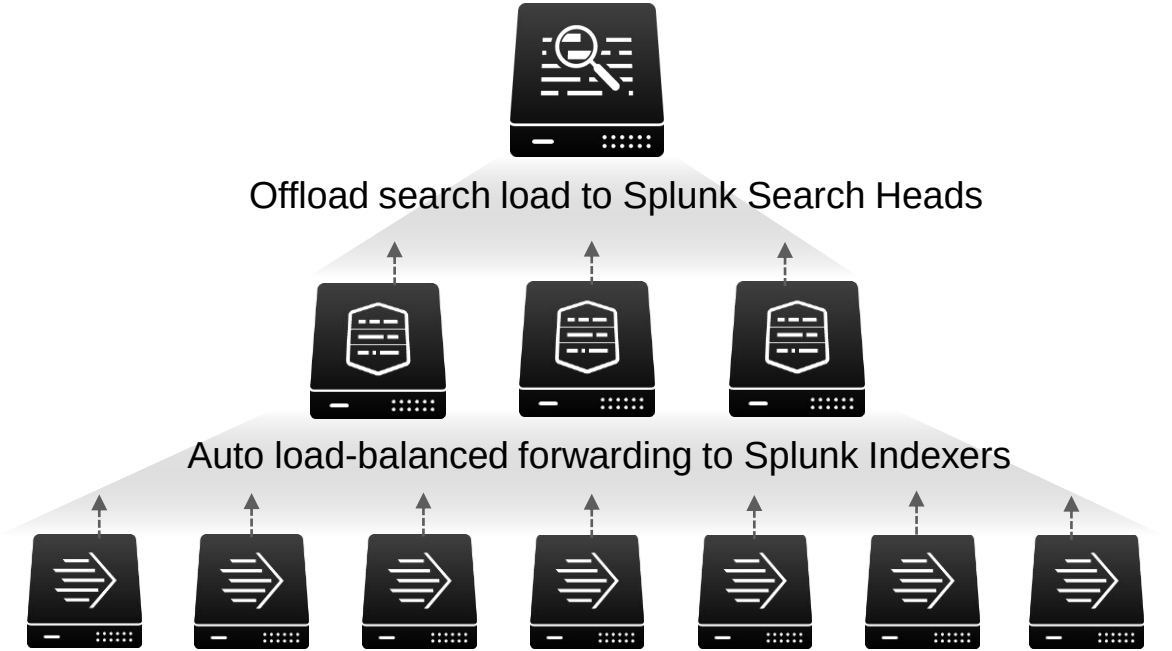
Map LDAP & AD groups to flexible Splunk roles. Define any search as a filter.

Within the MLS ecosystem

- Splunk Indexers can sit at separate security layers, displaying only the data accessible to that user
- At the highest security layer, Splunk can display the tagged information collected from the the entire stack
- Conversely, the highest security layer can visualize data only from the highest layer
- Collect, search, visualize, and alert by layer or across layers

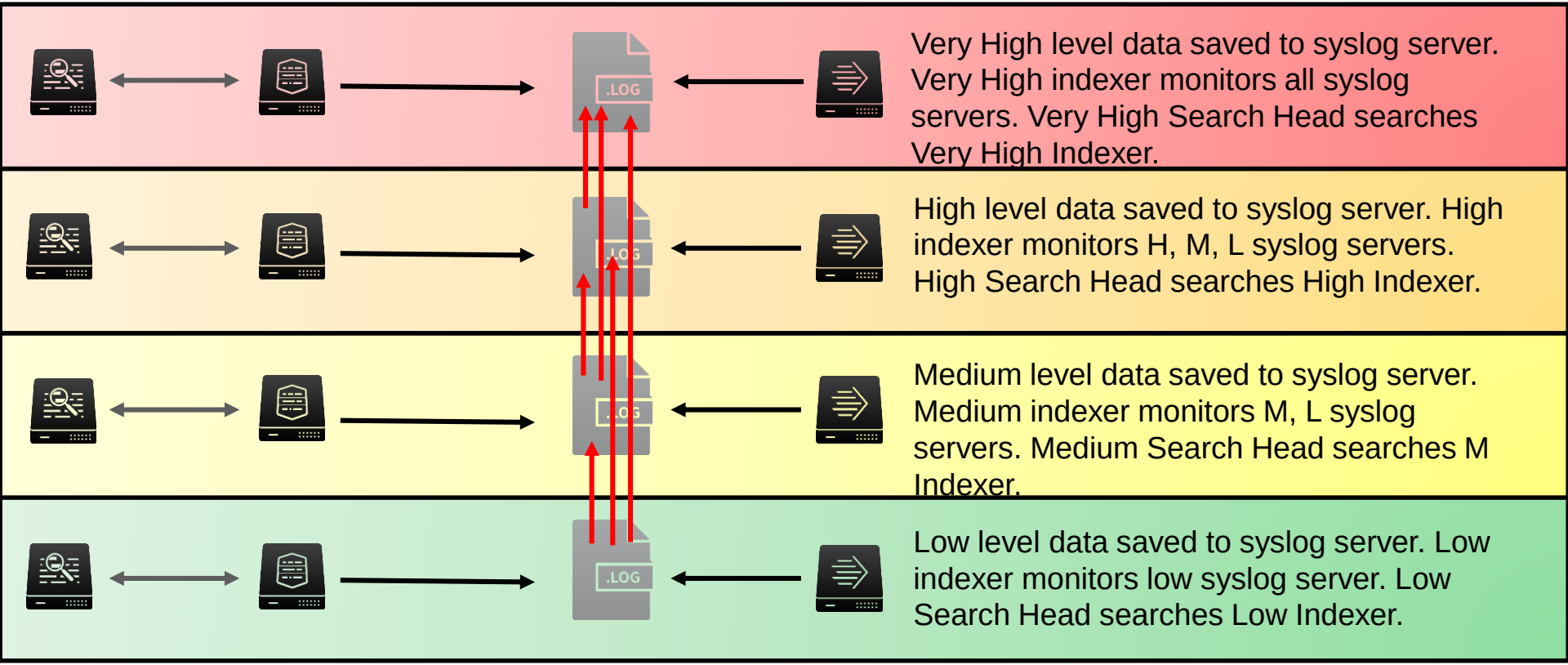
Splunk Enterprise

Enterprise-class Scale, Resilience and Interoperability



Send data from thousands of servers using any combination of Splunk forwarders

MLS – Reach down across data stores

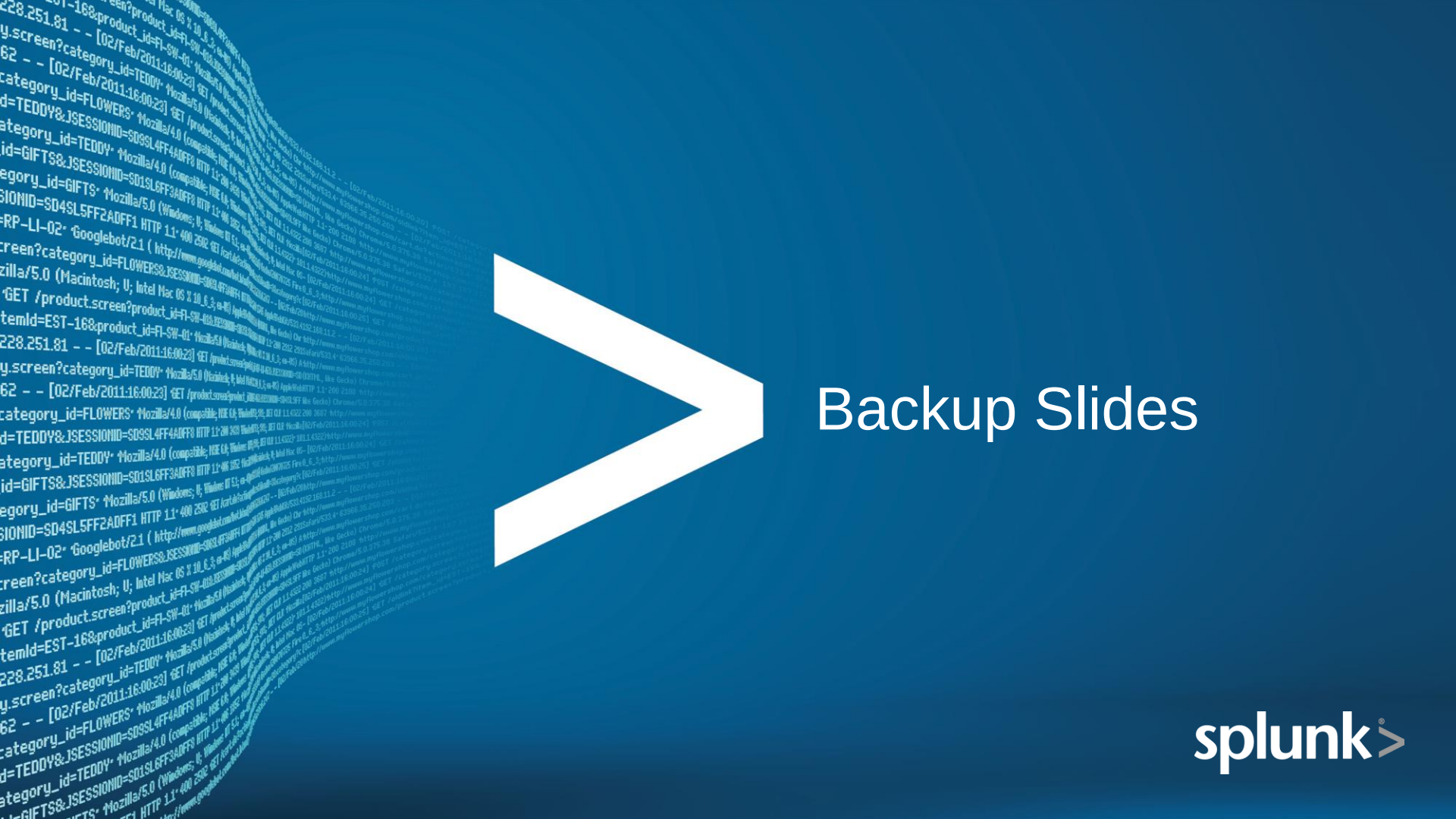


Very High level data saved to syslog server. Very High indexer monitors all syslog servers. Very High Search Head searches Very High Indexer.

High level data saved to syslog server. High indexer monitors H, M, L syslog servers. High Search Head searches High Indexer.

Medium level data saved to syslog server. Medium indexer monitors M, L syslog servers. Medium Search Head searches M Indexer.

Low level data saved to syslog server. Low indexer monitors low syslog server. Low Search Head searches Low Indexer.



Backup Slides

splunk>

Remember that Machine Data?

Sources

Order Processing

```
ORDER,2013-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100
```

Middleware Error

```
May 21 14:04:12.996  wl-01.acme.com Order 569281734 failed for customer 10098213.
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused
```

Care IVR

```
05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
```

Twitter

```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place”},
objectType:"person”,preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer!  RT if
you hate @ACME!!”,objectType:"activity”,postedTime:"2013-05-21T16:39:40.647-0600”}
```

Machine Data Contains Critical Insights

Sources

Order Processing

Middleware Error

Care IVR

Twitter

Customer ID Order ID Product ID

ORDER,2013-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadE… ould not create pool connection. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

Order ID

Customer ID

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type …98#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk 1451.16

Time Waiting On Hold

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213

Customer ID

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link: "http://dallascowboys.com/",location:{displ… …llas, TX",objectType: objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2013-05-21T16:39:40.647-0600"}

Twitter ID

Customer's Tweet

Company's Twitter ID

Splunk Unlocks Critical Insights