Get Better, Faster Results from Splunk

With the NetApp Data Fabric

Mike McNamara, Hoseb Dermanilian

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Session Speakers

HOSEB DERMANILIAN

EMEA, Industry Solutions Manager

MIKE MCNAMARA

Product and Solutions

splunk> .conf18

Agenda

- Digital Transformation
- NetApp Data Pipeline (Edge to Core to Cloud)
- Splunk Infrastructure Deployments: Which Option Is the Best?
  - NetApp Value Proposition
  - NetApp® Solutions for Splunk
  - TCO Analysis
- Customer References
- Key Takeaways

Digital Transformation

NetApp Data Fabric (edge to core to cloud)

splunk> .conf18

In a world where technology is changing our everyday lives, data-driven digital transformation is accelerating business outcomes.

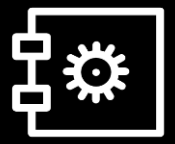
By 2020, it is expected that **50% of the G2000** will see the majority of their business depend on their ability to create digitally enhanced products, services, and experiences.

IDC Directions 02/17

Digital transformation spending is expected to reach $1.7 trillion worldwide by 2019, a **42% increase** from 2017

IDC FutureScape Report 11/17

Digital Transformation Is Changing Industries



Financial Services
18%

Oil and Gas
15.1%

Utilities
29%

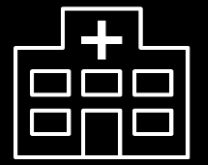
Government
17.5%

Traditional Revenue at Risk of Disruption

Industrial Equipment
20%

Retail
>25%

Hospitality
10.9%



Transport
14.2%

When successful in their data-driven digital transformation, organizations:

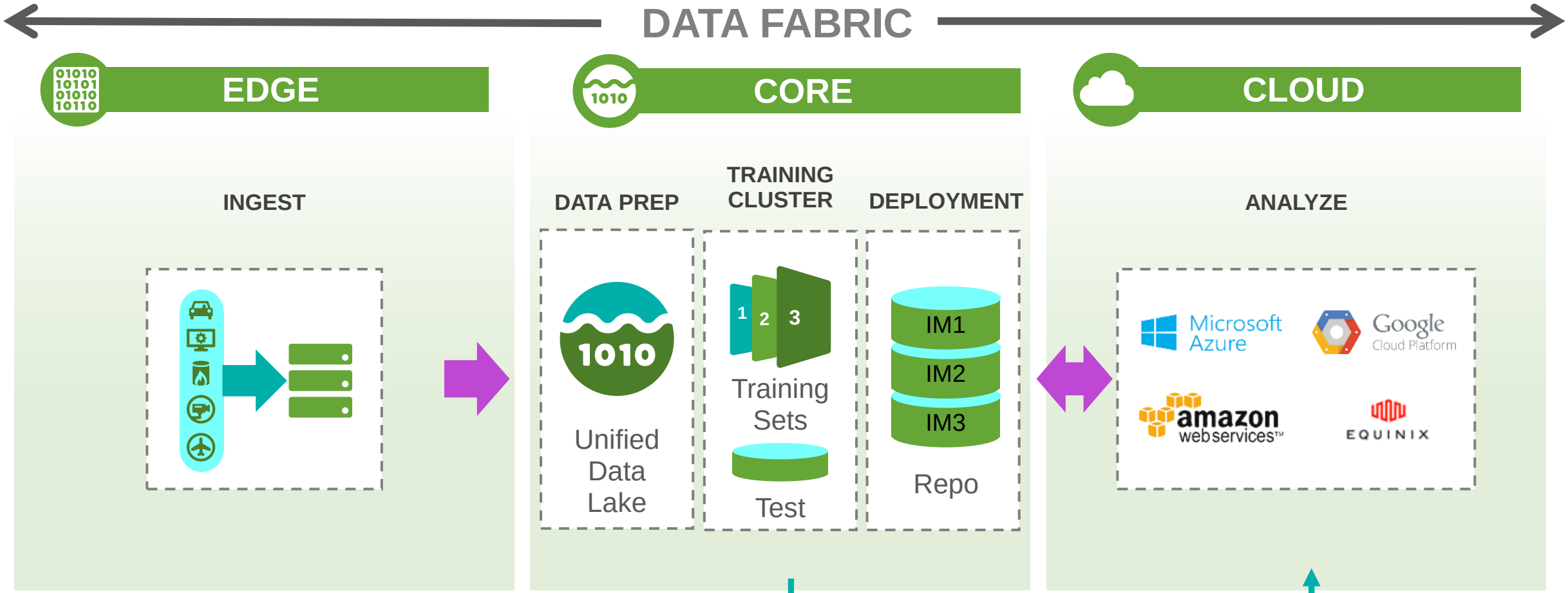
- Enable new customer touchpoints
- Create innovative business opportunities
- Optimize operations

Our Purpose

Empowering customers to change the world with **DATA**

splunk> .conf18

NetApp Integrated AI/DL Data Pipeline



splunk> .conf18

Splunk Infrastructure Deployments

Which option is the best?

splunk> .conf18

Splunk Indexing Tier

Hardware considerations for indexers

- Reference indexer specification:
  - Intel 64-bit chip architecture
  - 12 CPU cores at => 2GHz
  - 2GB of RAM
  - 800 IOPS on average
- Data storage considerations:
  - Important to ensure that you have enough disk space
  - Replication factor and search factor
  - A master is not aware of the amount of storage on individual peer nodes

How many indexers?

300GB ingest per day per indexer

The Trend

What we see every now and then

Ingest Rates

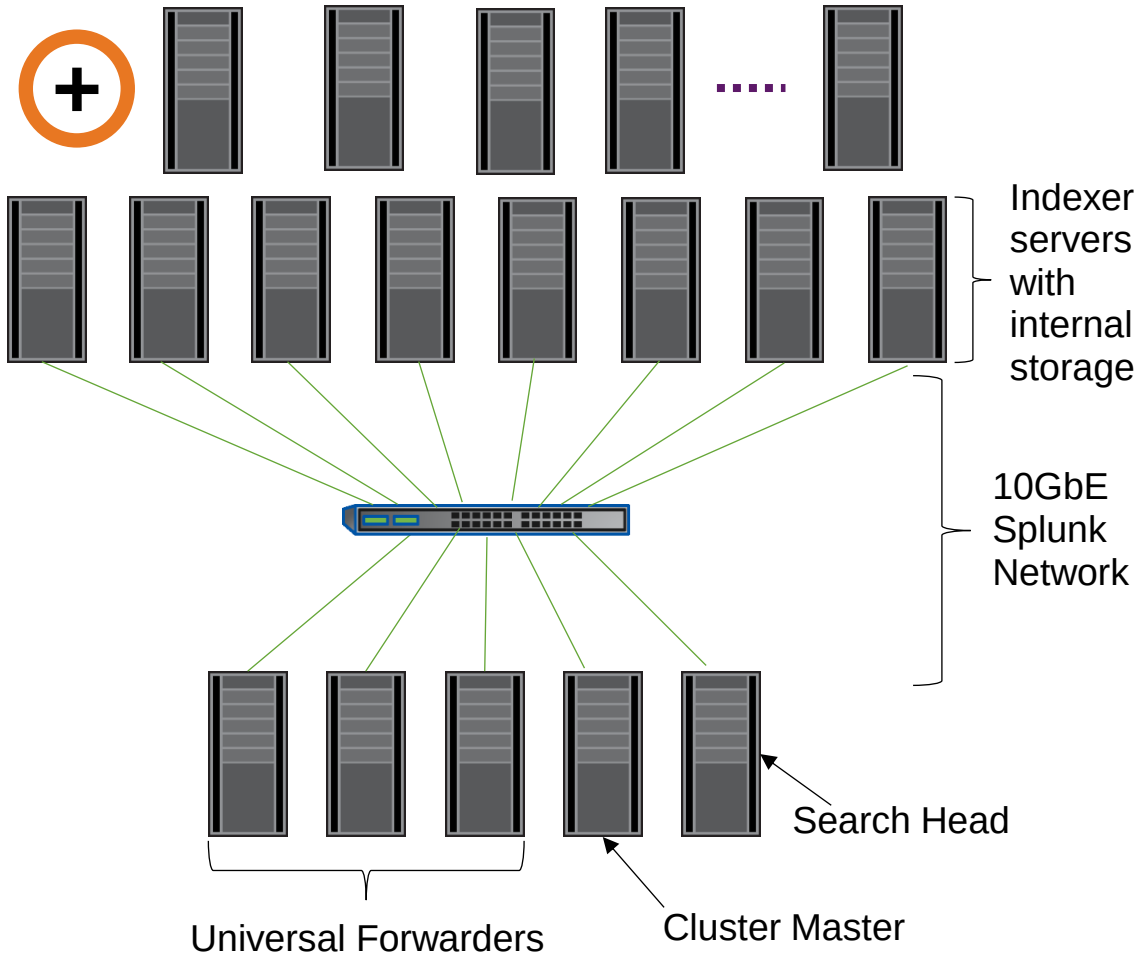
Performance

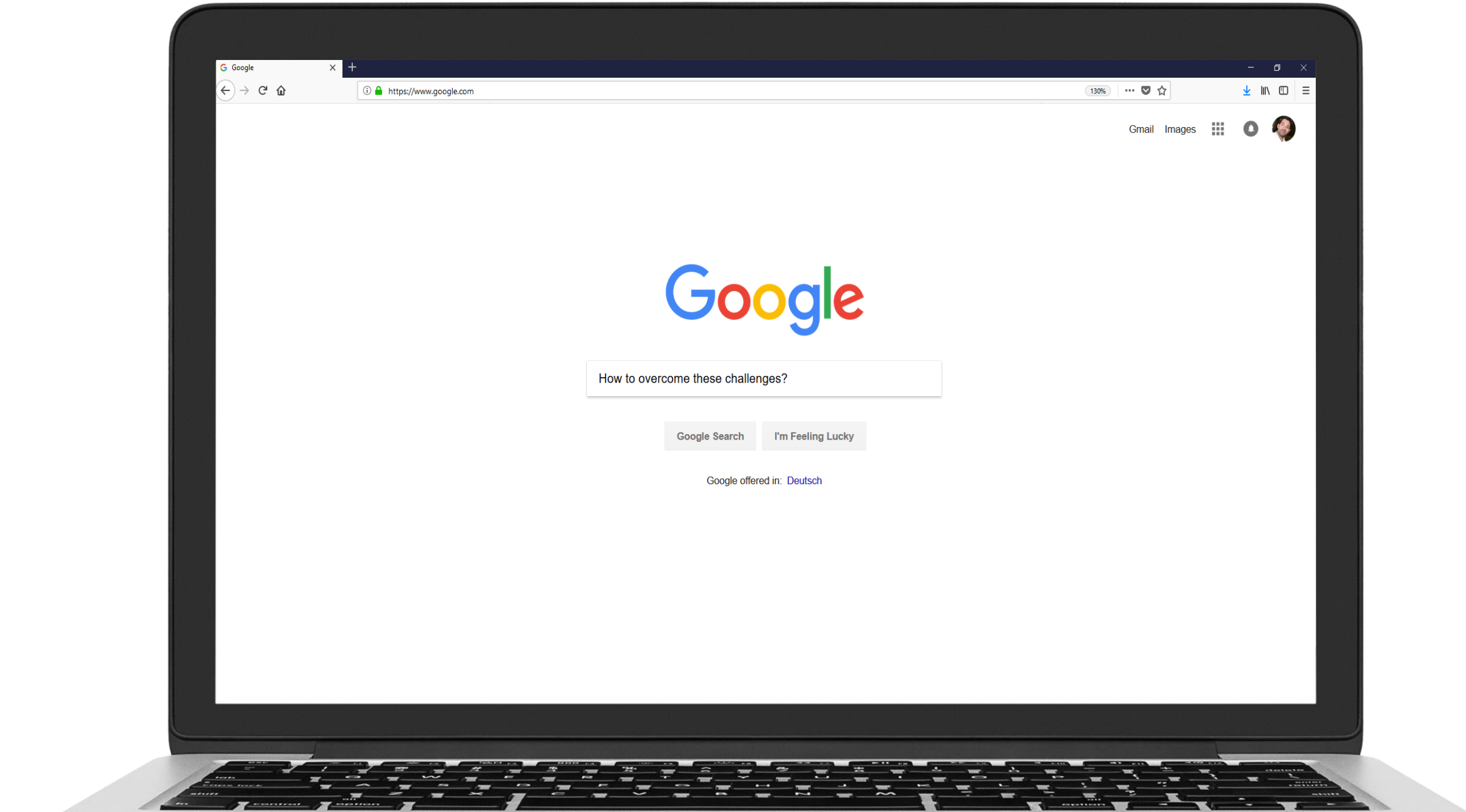
Availability & Scalability

Splunk Architectures

Option 1: Indexers with internal direct-attached storage (DAS)

- Challenge in scaling when you have storage and compute coupled:
  - There's growth in data ingest
  - There are more users
  - There are premium apps
  - There's heavy reporting or searches (performance)
- Other challenges follow the first: TCO, operations, and regulations

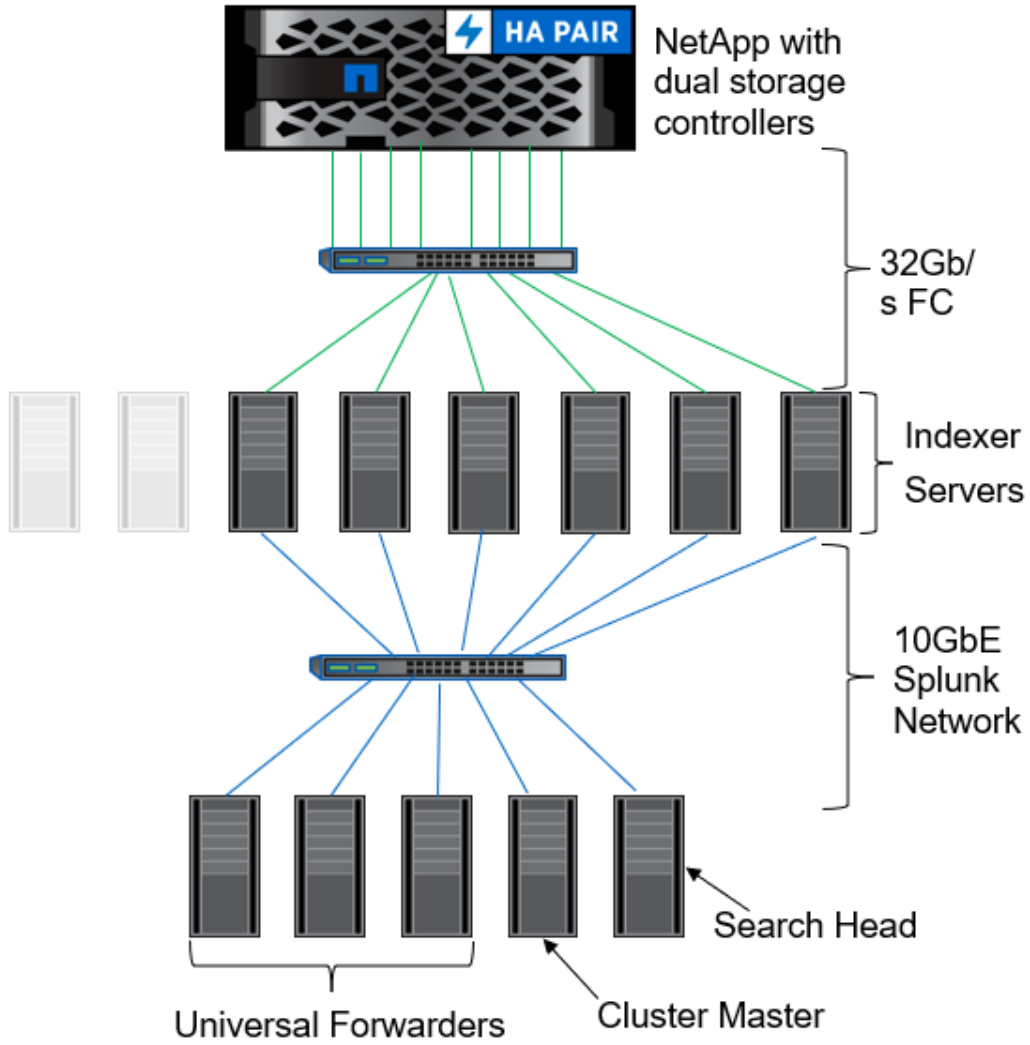




Splunk Architectures

Option 2: Decouple servers from storage

- Advantages:
  - Lower TCO
  - < number of indexers; no need for three copies
  - Use of storage efficiency features
  - Flexible scalability
  - Suitable for sharing with other apps
  - Faster searches
  - Long retention (compliance)
- Myths?
  - Overlooked; assumed to be difficult to configure (can fool)?
  - Needs to be architected properly?
  - Suitable for small installations?



TCO Impact

NetApp versus server-based DAS

-15%

Software and OS licenses (not Splunk licenses)

-26%

Reduction in hardware cost

-31%

No separate backup or archive hardware

-20%

Reduced power/ cooling/ rack space

>20%

Total TCO reduction over 3 years

splunk> .conf18

NetApp Solutions for Splunk

Meeting your dynamic requirements

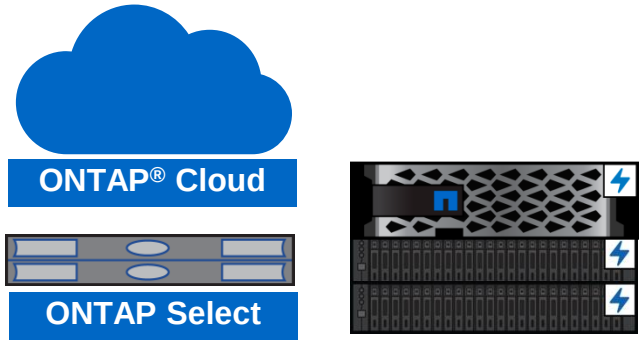
splunk> .conf18

NetApp Solutions for Splunk

Meeting all your needs

Splunk on NetApp® ONTAP®

- Share with other apps
- Use storage efficiencies
- Cloud integration: edge to core to cloud
- ONTAP based backup and recovery



Splunk on NetApp E-Series

- Cost and simplicity
- No cloud requirements
- Direct attach (eliminate networking)
- Combine with Cisco servers in a converge infrastructure

NetApp® E-Series Arrays

Splunk on NetApp HCI

- Start very small (below 100Gb ingest)
- Share with other apps
- Eliminate third-party server vendor
- Use for hot buckets and move data through S3 for cold

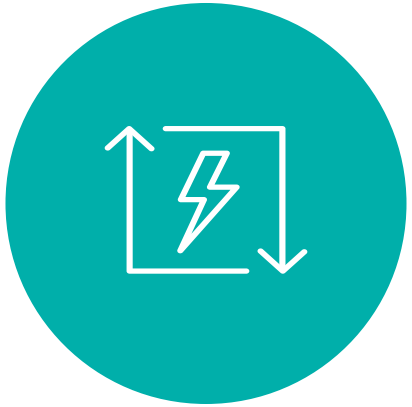
splunk> .conf18

Splunk on ONTAP

Performance, efficiency, availability, and operations considerations

Up to 300% search performance improvement

No performance impact failures (drives and controllers)



2:1 inline deduplication and compression efficiency

Connect to cloud and archive into S3

Splunk app for NetApp® ONTAP®

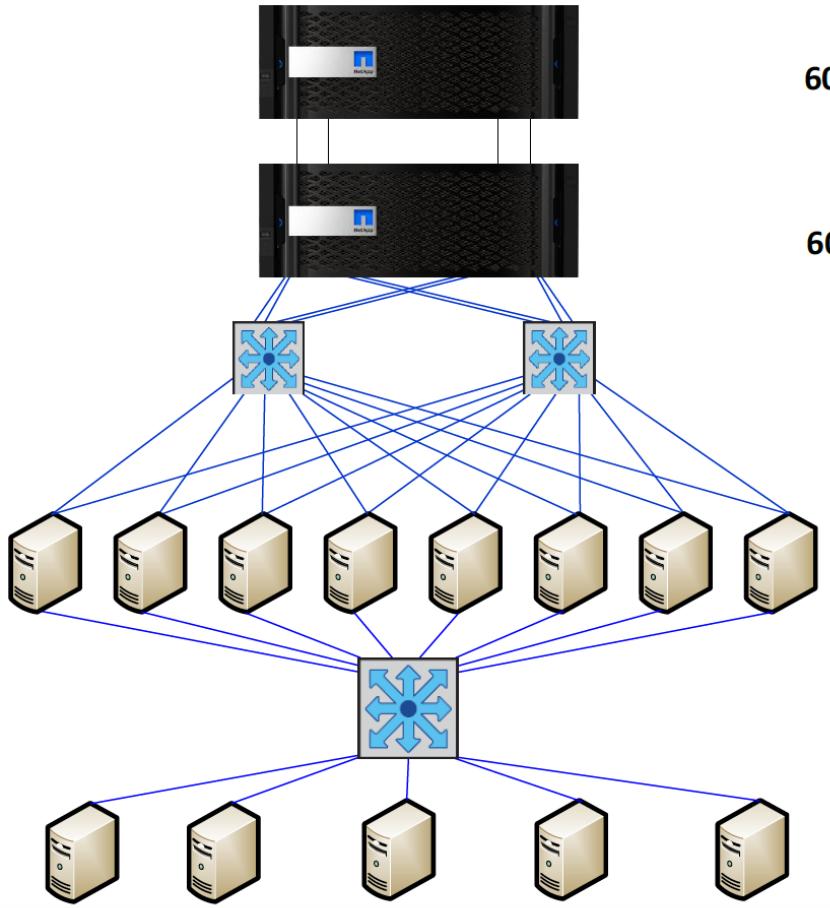
and NetApp Active IQ®

splunk> .conf18

Splunk on E-Series

Facts and figures

- Directly attach storage to servers (eliminate networking)
- >100% search performance increase
- Single pane of glass in managing over 70PB of storage
- Lower TCO
- Six nines of availability



E-Series DE460C
60 drive expansion shelf

E-Series E5760
60 drive controller shelf

Storage Network:
32Gb Fibre Channel,
10/25Gb iSCSI,
or 12Gb SAS

Indexer Nodes

1/10Gb Ethernet

Client Nodes

An Example of TCO Comparison

7TB ingest a day, 7 days hot/warm, 100 days retention for cold

DAS Based Architecture (option 1)

- 96 indexers are needed:
  - $10K per indexer capex
  - $22K per indexer opex
    - TCO for 3 years: $3,072,000

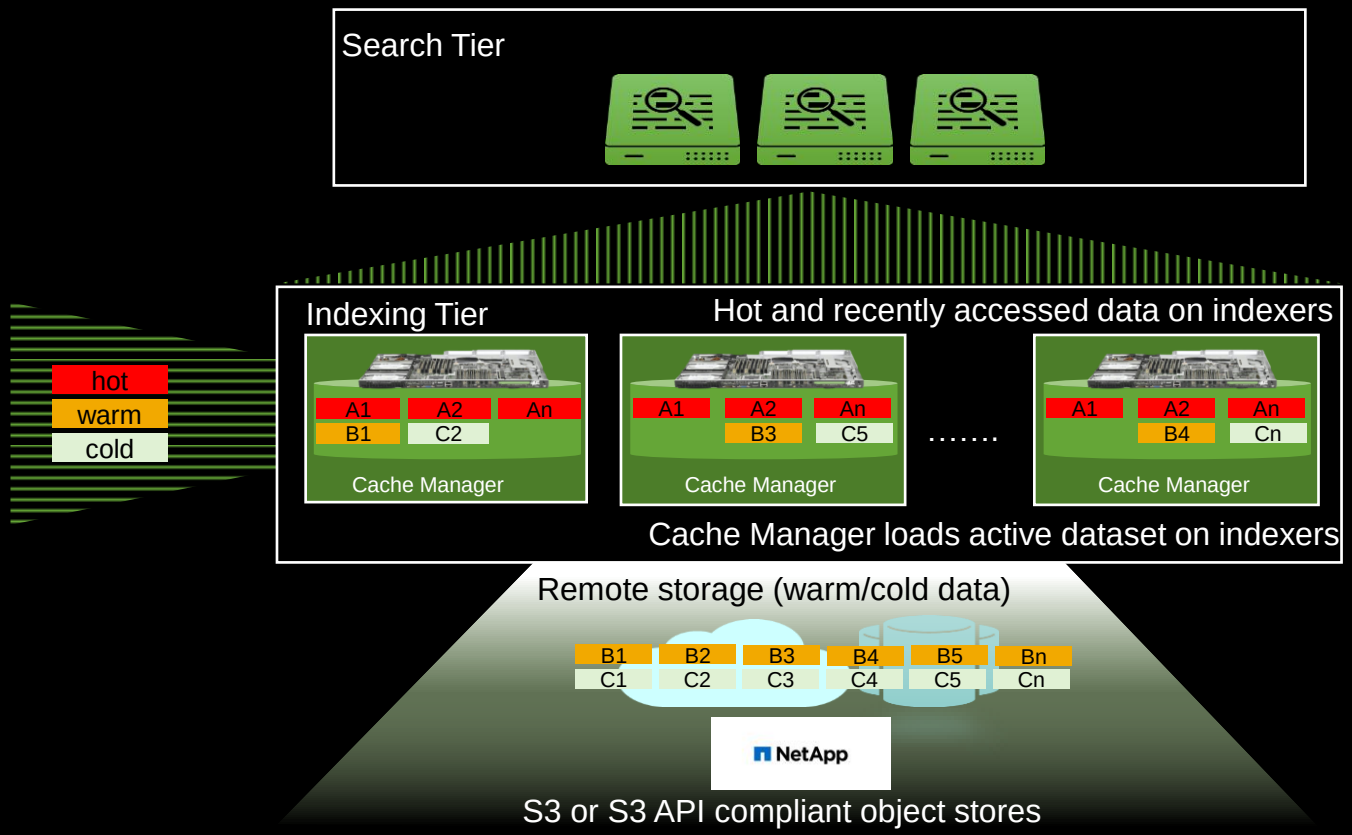
NetApp® Based Architecture (option 2)

- 56 indexers are needed:
  - $6K per indexer capex (no drives)
  - $18K per indexer opex
  - $455K storage cost (including support)
  - $177,367 networking, power, cooling
    - TCO for 3 years: $1,976,367

35.66% reduced TCO over 3 years

splunk> .conf18

Splunk SmartStore

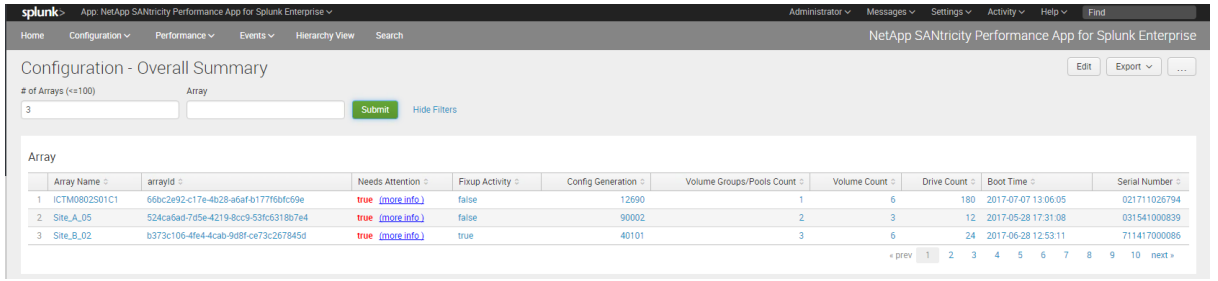


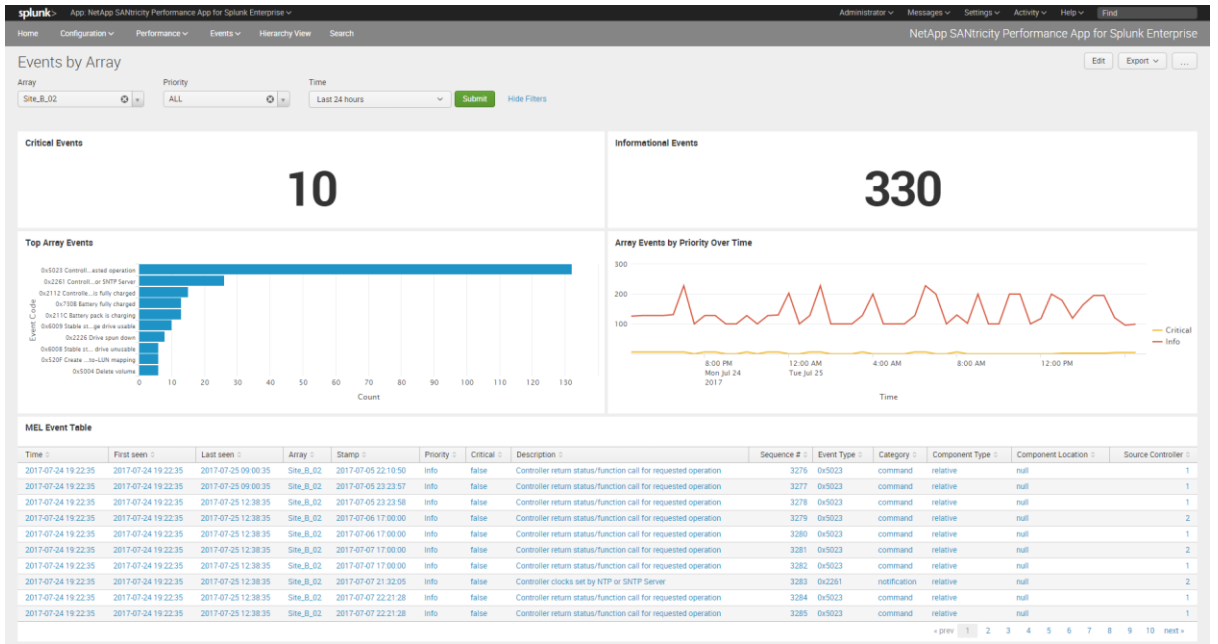
- Decoupled storage and compute
- Independently scale storage for longer data retention
- Scale out indexers based on performance demands
- Fewer indexers with hot + active data (only one full copy of warm/cold)
- Lower TCO with S3 & S3 API compliant object stores

NetApp Apps for Splunk

Better manage your infrastructure

- Available from Splunkbase:
  - NetApp® SANtricity® Performance App for Splunk Enterprise
  - NetApp ONTAP® App for Splunk
  - NetApp StorageGRID® App for Splunk





splunk> .conf18

Customer Examples

Running Splunk on NetApp systems

splunk> .conf18

ING DIRECT Success Story

"With the significant amount of machine-generated data captured every day, we rely on NetApp E-Series to deploy Splunk for monitoring and troubleshooting the multiple platforms in our environment."

Roy Shiladitya
Head of Information Technology
ING DIRECT Australia

Business challenge

- Deploy a high-performance solution that easily scales
- Improve customer retention and analysis

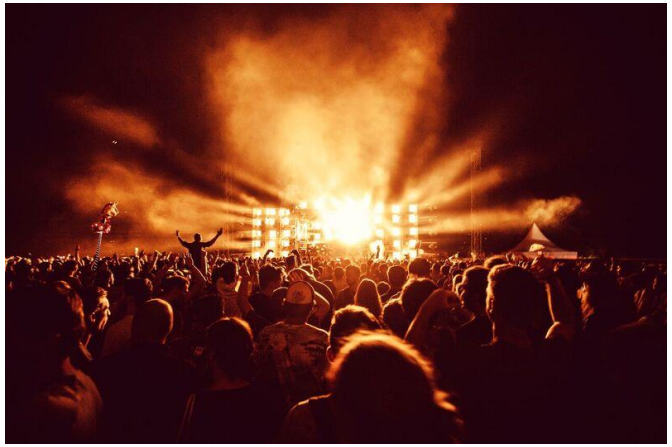
Solution stack

- Splunk, end-to-end monitoring, full display in operations center, over 1TB-a-day ingest, NetApp® E-Series hybrid flash storage systems

Why NetApp

- Provided scalable performance to start small (ingest 150GB a day) and grow very large (ingest over 1TB a day)
- Exceeded stringent SLAs
- Simplified deployment and management

Ticketmaster Success Story



Business challenge

- Quickly detect and block ticket scalpers who use bots to purchase volumes of tickets and drive up prices
- Improve availability and security

Solution stack

- Splunk network operations center (NOC) dashboards for capacity problems, availability issues, forensics, transaction tracing, failed transactions, and NetApp® E-Series hybrid flash storage systems

Why NetApp

- Exceeded performance and availability requirements
- Simplified and cost-effective deployment
- Enabled a new revenue opportunity

Key Takeaways

1. Edge to core to cloud for your data movements
2. Splunk architectural options
3. Decouple storage from compute for better results

Join us at Splunk .conf18

NetApp booth T4

Visit www.NetApp.com/BigData

Thank You

Don't forget to rate this session in the .conf18 mobile app