10/17 NCWG

Splunkのご紹介

Splunk Services Japan合同会社
須田　孝雄
tsuda@splunk.com

splunk>

自己紹介

- 須田　孝雄 (Suda Takao)
  - Twitter; dasu49
- 現職; Splunk Japan
  - 販売代理店開拓、ビジネス開発担当
- 経歴;
  - 某ネットワークインテグレーター
  - 某仮想化大手ベンター (SBC, VDI)
  - CloudStackビジネス開発

Spelunking; 洞窟探検
Splunking; ITシステムの探索・調査

splunk>

マシンデータをあらゆる人に、アクセス可能に、便利なものに、そして価値あるものに。

会社概要

会社

- 2004年設立, 2006年に最初のソフトウェアリリース
- 本社: カリフォルニア州、サンフランシスコ市
- 支社：香港、ロンドン
- 社員数、約800名（12カ国）
- NASDAQ　SPLK

財務

- レベニュー: 2012年度、198Mドル

6000 以上の顧客

- 90ヵ国以上にわたって5,000以上の顧客
- 最大規模顧客：100TB/日

THE WORLD'S MOST INNOVATIVE COMPANIES 2013

OUR ANNUAL GUIDE TO THE STATE OF INNOVATION IN OUR ECONOMY, FEATURING THE BUSINESSES WHOSE INNOVATIONS ARE HAVING THE GREATEST IMPACTS ACROSS THEIR INDUSTRIES AND OUR CULTURE AS A WHOLE. FOLLOW THE CONVERSATION ON TWITTER #FCMOSTINNOVATIVE

MOST INNOVATIVE COMPANIES 2013

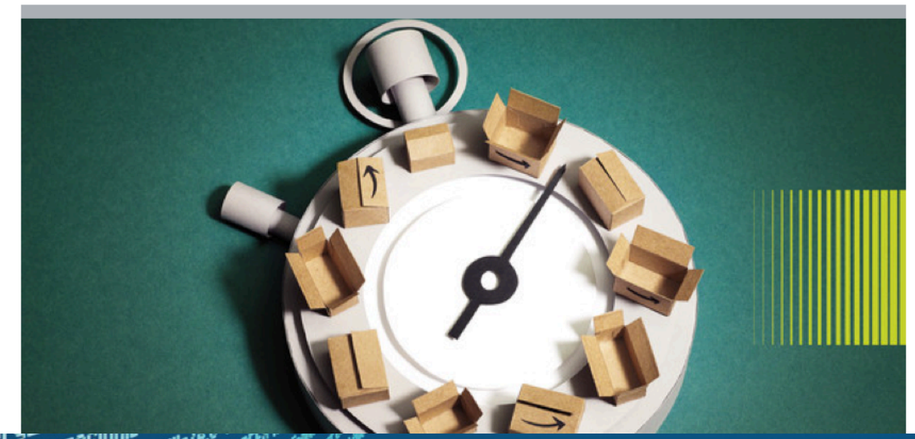
NIKE: THE NO. 1 MOST INNOVATIVE COMPANY OF 2013

FOR A PAIR OF REVOLUTIONARY NEW PRODUCTS AND A CULTURE OF TRUE BELIEVERS.

READ MORE »

BY: AUSTIN CARR

1.9k 1.9k 4.7k



Top 50
MIC 2013

1 - 10

01_ Nike	06_ Uber
02_ Amazon	07_ Sproxil
03_ Square	08_ Pinterest
04_ Splunk	09_ Safaricom
05_ Fab	10_ Target

11 - 20

21 - 30

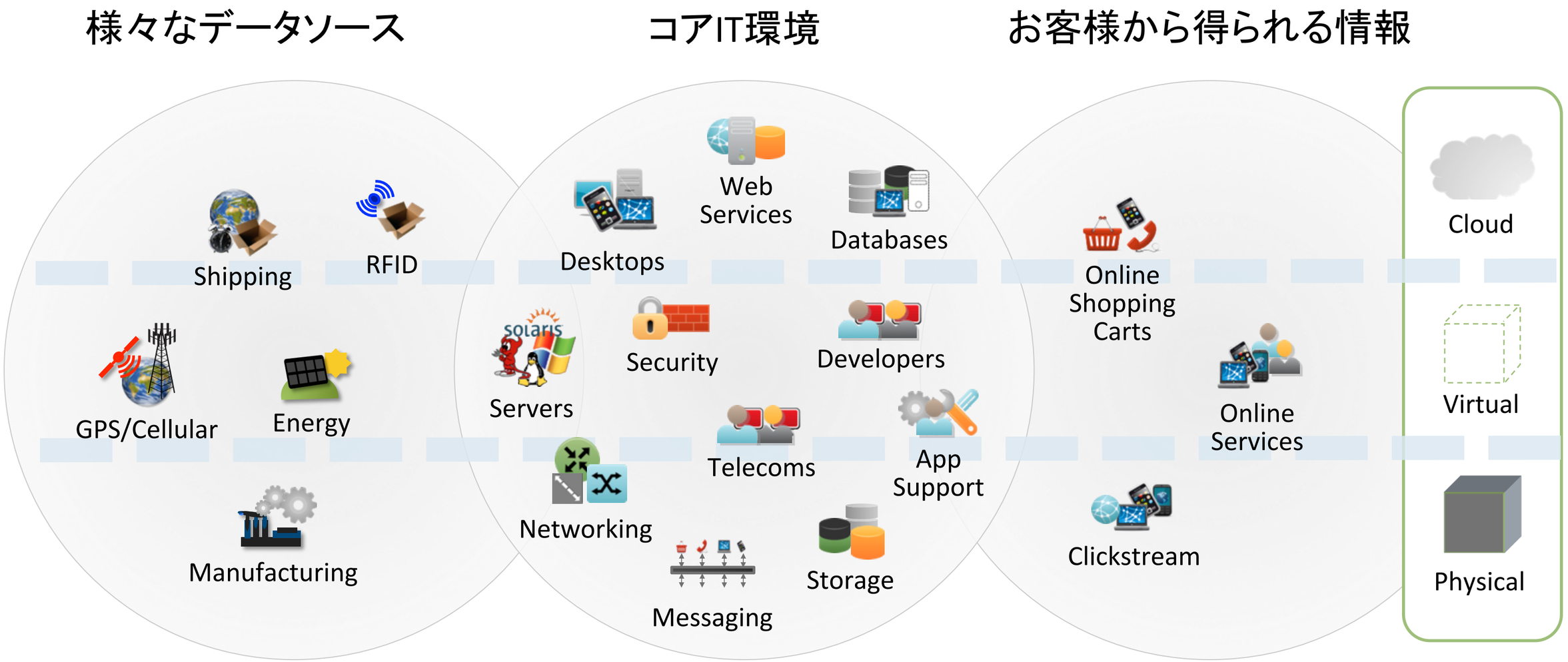
FAST COMPANY

#4 MOST INNOVATIVE

#1 INNOVATOR BIGDATA

http://www.fastcompany.com/section/most-innovative-companies-2013

ほとんどの企業データはマシンデータ



Splunk = マシンデータプラットフォーム
(あらゆる人に、アクセス可能に、便利なものに、価値あるものに)

Customer Facing Data

- Click-stream data
- Shopping cart data
- Online transaction data

Outside the Datacenter

- Manufacturing, logistics…
- CDRs & IPDRs
- Power consumption
- RFID data
- GPS data

Windows

- Registry
- Event logs
- File system
- sysinternals

Linux/Unix

- Configurations
- syslog
- File system
- ps, iostat, top

Virtualization & Cloud

- Hypervisor
- Guest OS, Apps
- Cloud

Applications

- Web logs
- Log4J, JMS, JMX
- .NET events
- Code and scripts

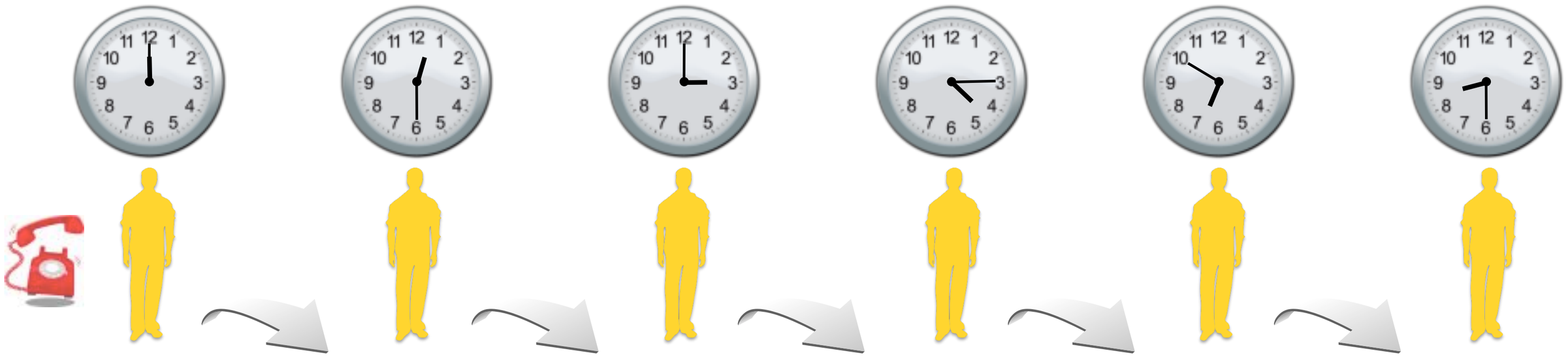
Databases

- Configurations
- Audit/query logs
- Tables
- Schemas

Networking

- Configurations
- syslog
- SNMP
- netflow

こんな経験ありませんか？



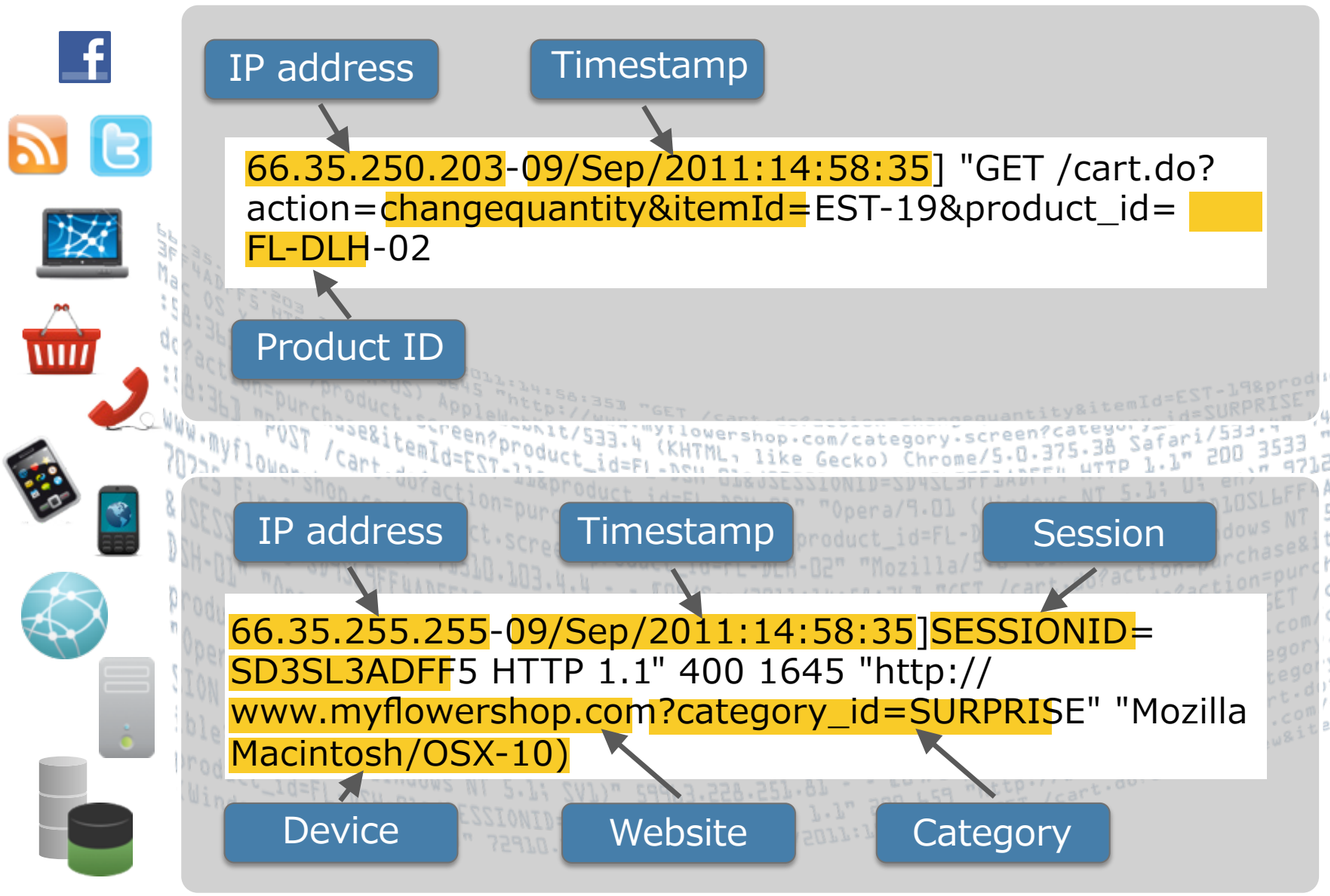
サービスデスク	運用	開発	システム管理者	開発	データベース管理者
トラブルの連絡あり。コンソールは見る限り、すべてグリーン	Java監視ツールは何も検知していない。開発チームに支援要請	新規開発を止めて、問題対応を開始。本番環境のログを要求	作業を中断して本番環境のログ収集を開始。	送られたログをみる限り、アプリ側の問題ではなさそうだという　結論	Auditログを見る限り、おかしなQueryが出ていることは判明したが。。
エスカレーション	エスカレーション	エスカレーション	レスポンス	エスカレーション.	NOW WHAT?

時系列（タイムスタンプ）

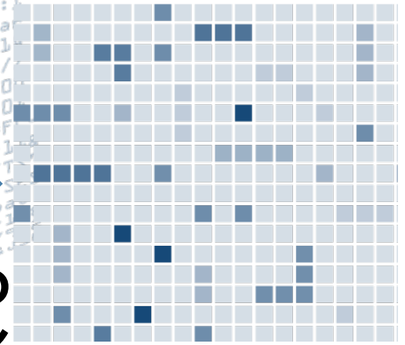
アスキー（テキスト形式）

殆どのエンタープライズデータはマシンデータ
情報の金山

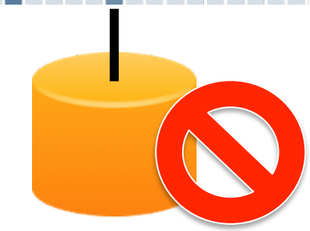
Splunkにマシンデータを
突きつけて、質問を問いかける



Splunk インデックス



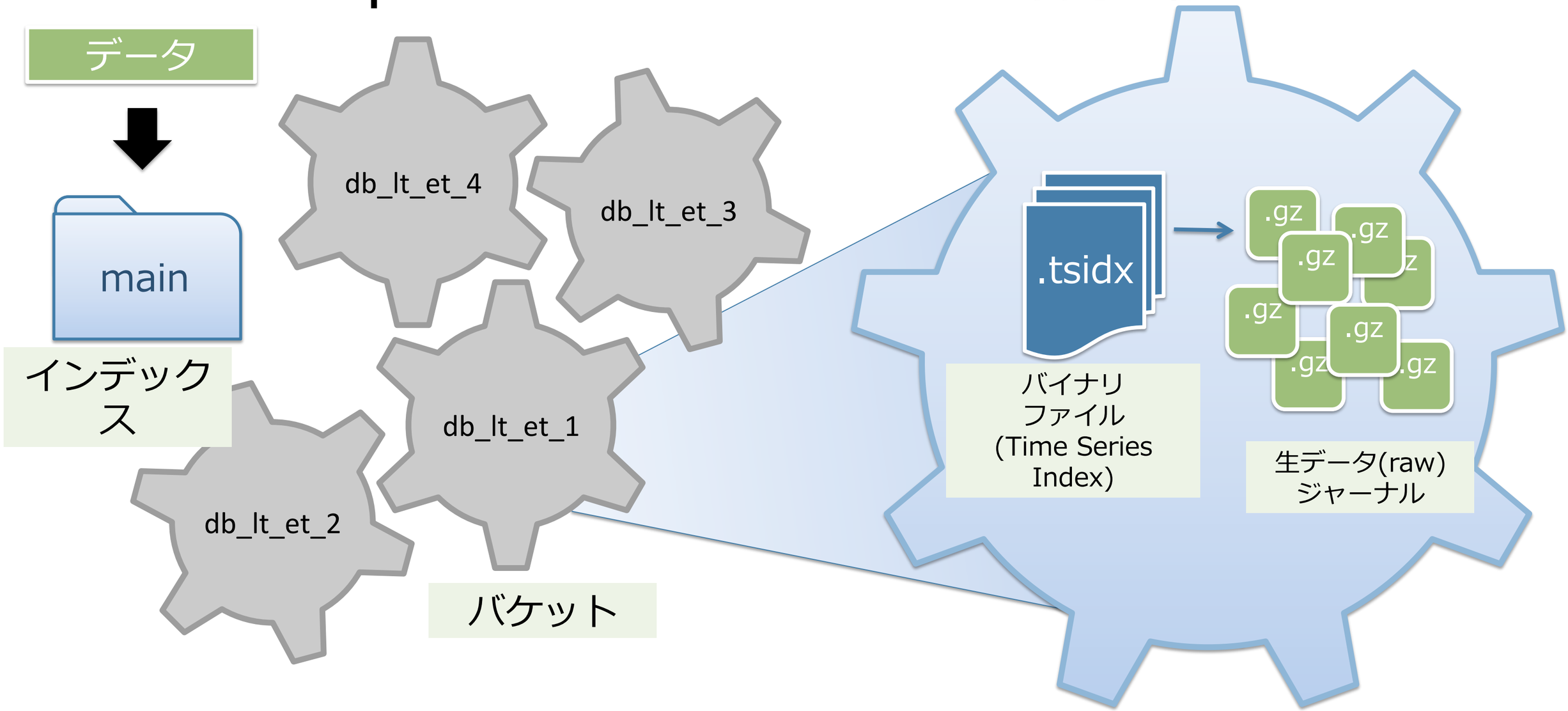
リアルタイムでのデータ収集&インテックス化



No RDB

マシンデータの収集、インデックスが容易！

Splunkにおけるデータ保持構造



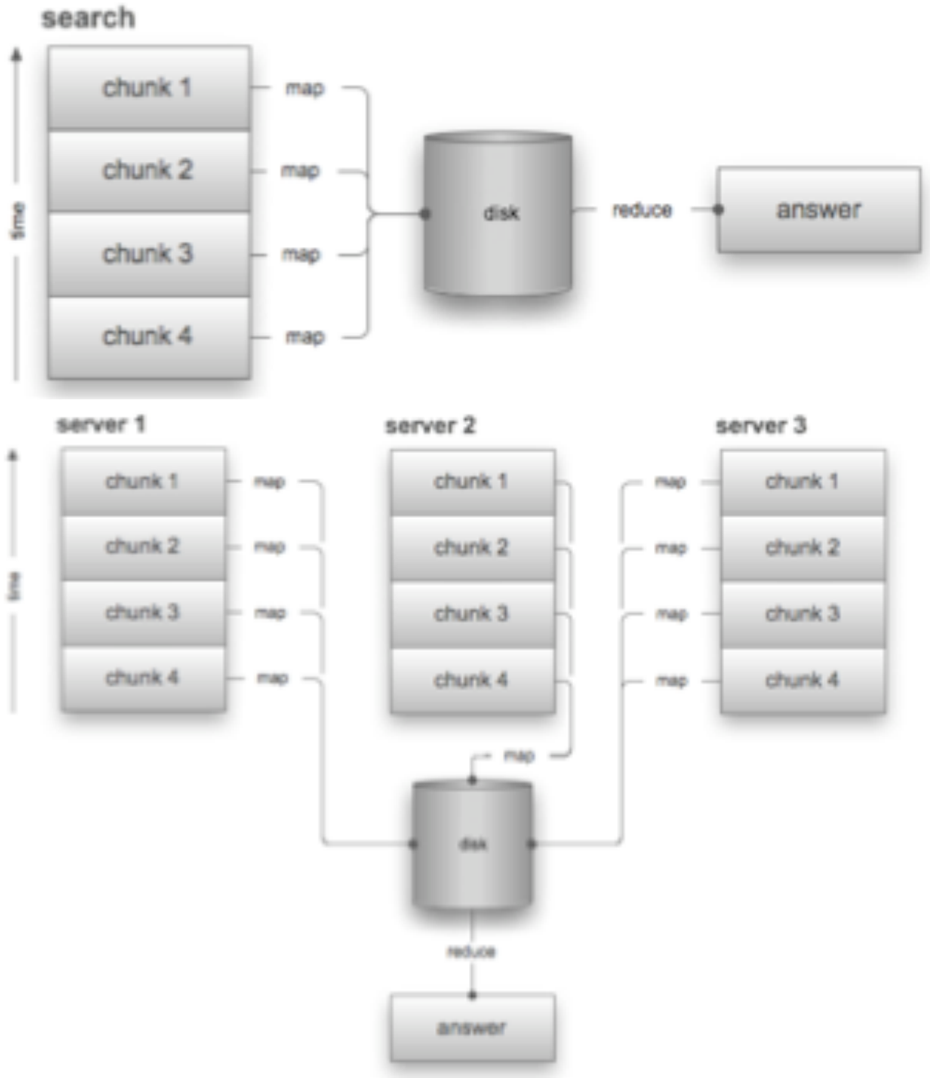
MapReduce による Splunkエンジン

2004年にGoogle社が発表した、大規模なデータを分散処理するためのプログラミングモデル

- 2段階処理による分散処理
  - map処理　＝　分割されたデータの断片に何らかの加工を施し、必要な情報を抽出
  - reduce処理　＝　mapで抽出した情報を束ねてデータ全体についての整理された処理結果を取得

For large scale batch processing and high speed data retrieval, common in Web search scenarios, MapReduce provides the fastest, most cost-effective and most scalable mechanism for returning results.

Splunk's Map-Reduce since 2004



Splunk、4つの主要な機能

- サーチとレポート機能 (Search Head)

- インデックスとサーチサービス (Indexer)

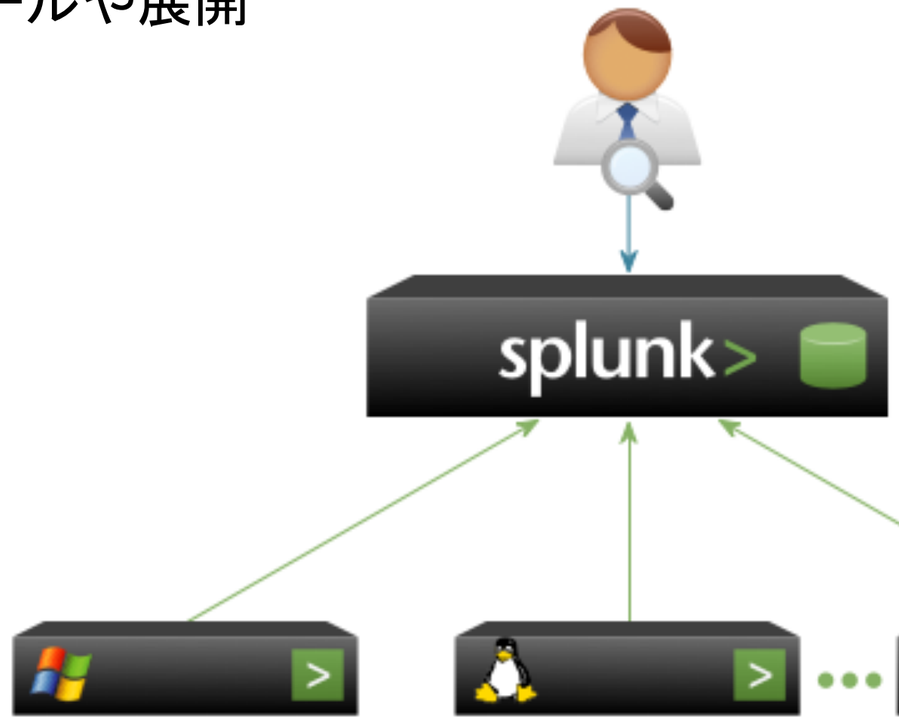
- データ収集および転送機能 (Forwarder)

- ローカルおよび分散管理 (Deployment Server)

全機能もしくは特定機能をインストール可能...

環境全体のデータアクセス一元化

- リモートシステムのデータは、ユニバーサルフォワーダによりSplunkへ送信
- 最低限のシステムリソースを利用
  容易なインインストールや展開
- 分散している数万ものエンドポイントから、セキュアにデータ収集を実現

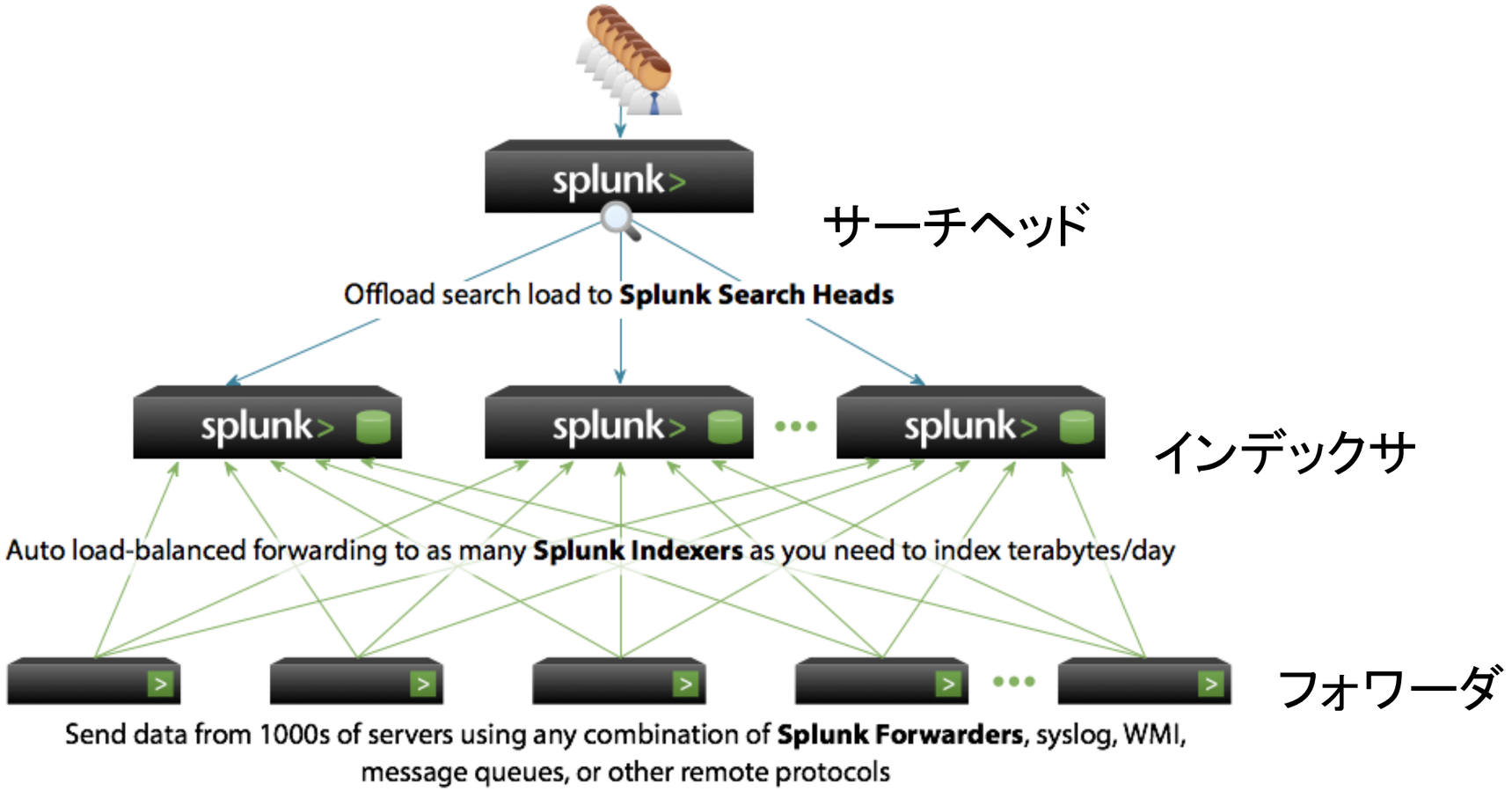


インデックサー（インデックス処理）＋
サーチヘッド（検索処理）

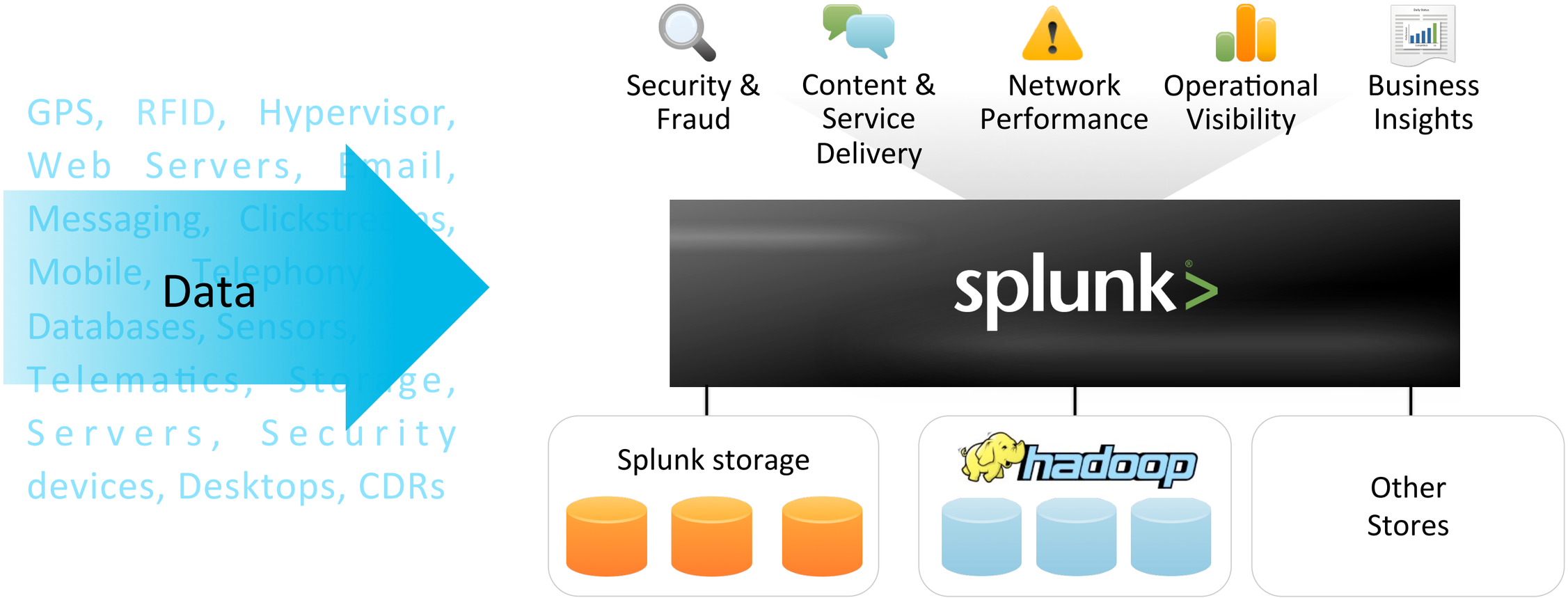
フォワーダ
（データ取得、フィルタ、転送）

テラバイト/日や数千ユーザへの拡張

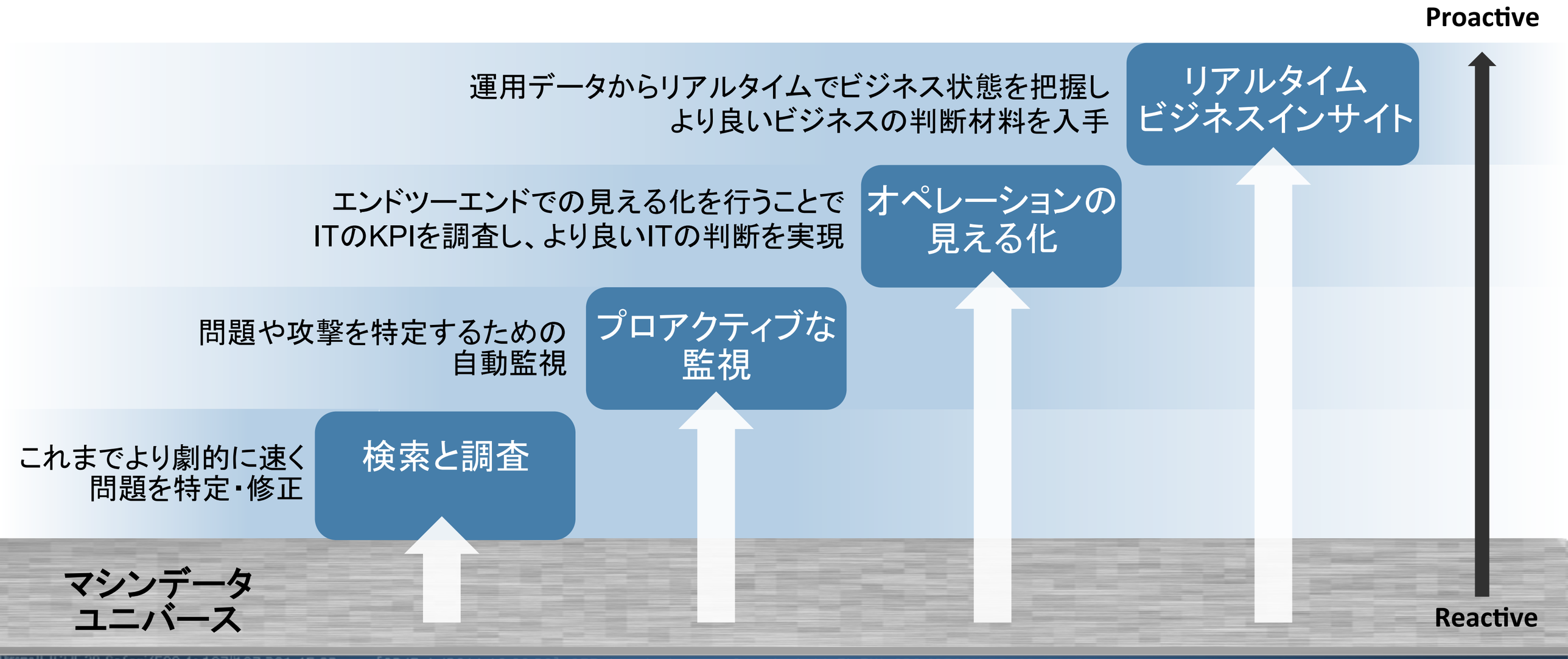
- 負荷分散によりインデックス性能がリニアにスケール
- 分散検索やMapReduceにより、検索やレポーティング性能がリニアにスケール



Splunkと他のデータベース技術との連携



マシンデータの利用



SplunkはITやビジネス全域で利用できます

IT Operations	*App Mgmt*	*Security*	*Compliance*	*Business Analytics*	*Web Intelligence*
IT オペレーション	アプリケーション管理	セキュリティ	コンプライアンス	ビジネス分析	ウェブ分析

開発者向けフレームワーク

splunk>

16TB/day	**6TB/day** LinkedIn	**4TB/day** Expedia
2.5TB/day Bank of America	**1.5TB/day** INTUIT	
1TB/day comcast, Time Warner Cable, The University of Texas at Austin, Viacom, metroPCS, salesforce.com		

Splunk ROI – 多種多様な変化に、迅速に、柔軟に対応

収益の増大

Macys.com 自社のeコマースのインフラをプロアクティブに監視・分析
数ヶ月かかったダッシュボード作成を1ヶ月かからず実装。Splunkでシステム全体を見通す事ができるようになり、100%の稼働時間を達成。全IT部門で100ユーザー以上が、役割毎にダッシュボードを作成して管理。インシデントあたり3000万円のチャンスロスを回避。

システムの継続性

TransUnion 自社のインフラをプロアクティブに監視・分析
システムのダウンタイムを90%改善。サービス(信用情報管理)の品質が向上し、収益upを実現。

生産性の向上

HealthTrans
問い合わせから問題を特定するまで(ユーザトランズアクション調査)に7,8時間かかっていたものを5分で解決。

コスト削減

Large mutual fund コンプライアンス用途でSplunkを使用
コンプライアンスレポートの作業が効率化。1ヶ月で費用回収ができた。

セキュリティリスクの低減

Large telecoms company セキュリティ監視に使用
不正アクセス検知などセキュリティ脅威に対する監視と対応プランの作成、問題の傾向把握などが実現し、投資効果を1ヶ月で実現。

サービスの最適化

Top five US wireless carrier ARPU増とコスト削減につながるCDR分析
提携するキャリアの中から最安料金となるルーテリングを選択し接続。提携キャリアのパートナーシップを強化し、サービス品質を向上。

フリーダウンロードのSplunk Appsで
より多くのデータを素早く分析

コミュニティ

テクノロジ パートナー

開発者

Splunk ビルド

400 Apps
増加中

有料

開発者向けフレームワーク

splunk>

90カ国以上、6000以上の法人顧客

Cloud and Online Services

Education

Energy and Utilities

Financial Services and Insurance

Government

Healthcare

Manufacturing

Media

Retail

Technology

Telecommunications

Travel and Leisure

IT Operation

Splunkの活用により
～機会損失を防ぎ、効果的なインフラ投資に役立てる～

- 課題／背景
  - 見込み客管理システムでのパフォーマンス劣化へのピンポイント解析 (数百社、数千カスタムアプリ)
  - 利用者が感覚的に感じている不満を数値として分析出来ていなかった
- ソリューション
  - テクニカルサポートと開発部門でSplunkを活用。
  - Apacheアクセスログ(レスポンスタイムを追加してSplunkへ)からパフォーマンス対策と潜在的なクレーム対応処理
- 導入効果
  - 機会損失を防ぐ事が出来るようになった(投資対効果が高い)
  - 非エンジニアによるテクニカルサポートが可能に (Viewerとして渡せる)
  - 効果的なインフラ構築が可能
  - 付加価値として、豊富なアドオン(Splunk App)の活用
- データソース
  - メール配信ログ、Apache、アプリケーションログ、APIログ
- 今後の展望
  - データソースを増やしてより広範囲なSplunk活用を検討

エレベーターの監視データ分析にSplunkを採用
～保守サービスの向上実現を目指す～

- 課題／背景
  - 十数万台のエレベータから送信されるデータの活用
  - エレベータの監視データ分析に際し、RDBからデータを抽出、加工し、レポート作成作業に時間と負荷がかかっていた
- ソリューション
  - Splunkを導入したビッグデータ分析システムの構築
- 導入効果
  - データ抽出から加工、レポーティングまでの時間の大幅短縮
  - エレベータの利用状況をグラフ化することで、場所や地域での利用方法の違いや利用の傾向を明確に把握
- データソース
  - エレベータの監視データ
- 今後の展望
  - より多くのデータの取得し、より詳しく状況を把握できるようにしたい
  - 顧客ごとの保守サービス最適化し、顧客満足度の向上に役立てたい

セキュリティ

統合ログ監視システムの実現にSplunkを採用
～脅威をいち早く検出、解析して迅速に対処～

- 課題／背景
  - ログを収集し、鳥瞰的に事象を捕らえる仕組みの実現
  - 脅威の範囲などをいち早く検出、解析し、迅速に対処
  - SOX法やIT監査に対応した、発見的統制の実現
- ソリューション
  - Splunkを採用した統合ログ監視システムの構築
- 導入効果
  - 他社製品に比べ開発期間を約2分の1に短縮
  - 洗練されたダッシュボードでレポート作成を効率化
  - 平均4週間かかっていたマルウェア感染等のインシデント対応を数時間に短縮
- データソース
  - メール, プロキシ, アンチウイルス, IDS/IPS, ファイルサーバ監査, ファイアウォールなど10数種類のログ
- 今後の展望
  - PSOCやCSIRTなどのソリューションにおいてもSplunkを活用したい

ビジネス全体のオペレーショナル・インテリジェンス

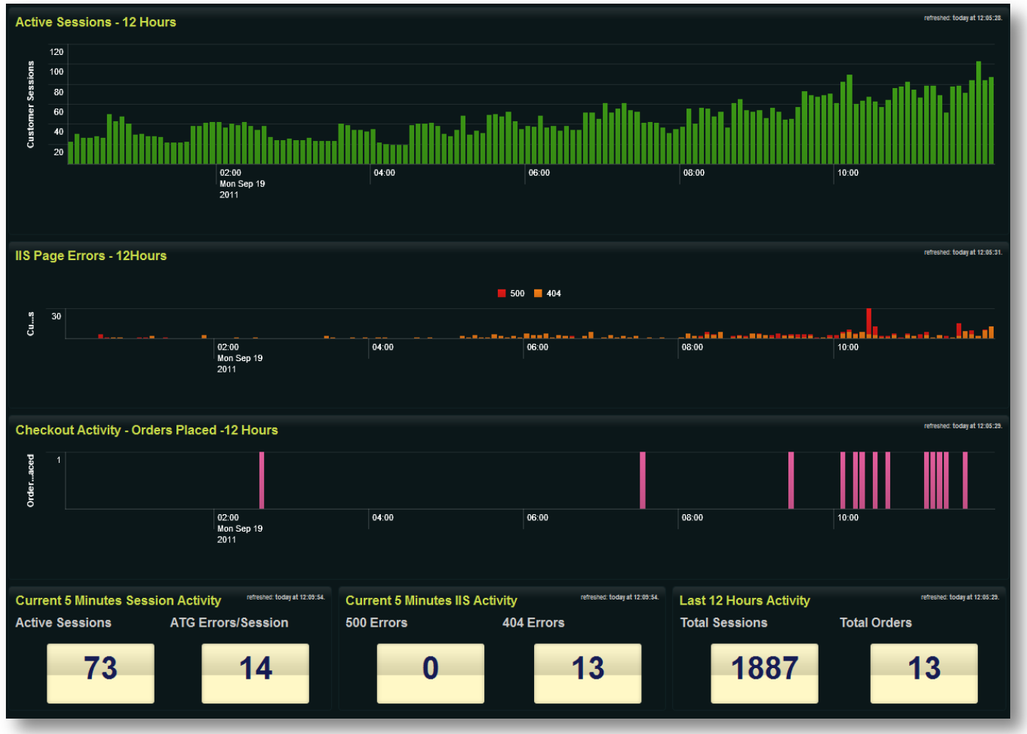
"アプリケーション・パフォーマンスのトラブルシューティングを実現する事で87,000ものユーザーを更に増やす事ができた"

"Splunkを実際に使ってみるまで、我々はデータを活用することの本当の意味に気づいていなかった。"

Narayan Bharadwaj
Director, Product Management

- 新サービスの提供：お客様へのe-mailキャンペーンに関するレポートの提供
- ソーシャル・プラットフォーム・サービスやForce.com上のappsに関するビジネス分析の提供
- より高いサービスレベルを実現

お客様の動向を理解する



Splunk の利用:

- 巨大化した本番環境全体に適用
- 10の環境に400サーバー / 50の異なるログ・タイプ
- 監視, トランザクションのトラッキングとWeb分析

"エンジニアリング・チームは、Splunkで提供できる情報に、本当にビックリしました。彼らは、今開発しているアプリもすべてSplunkがあることがわかっているので、特別なプログラムを作成せずにいます。"

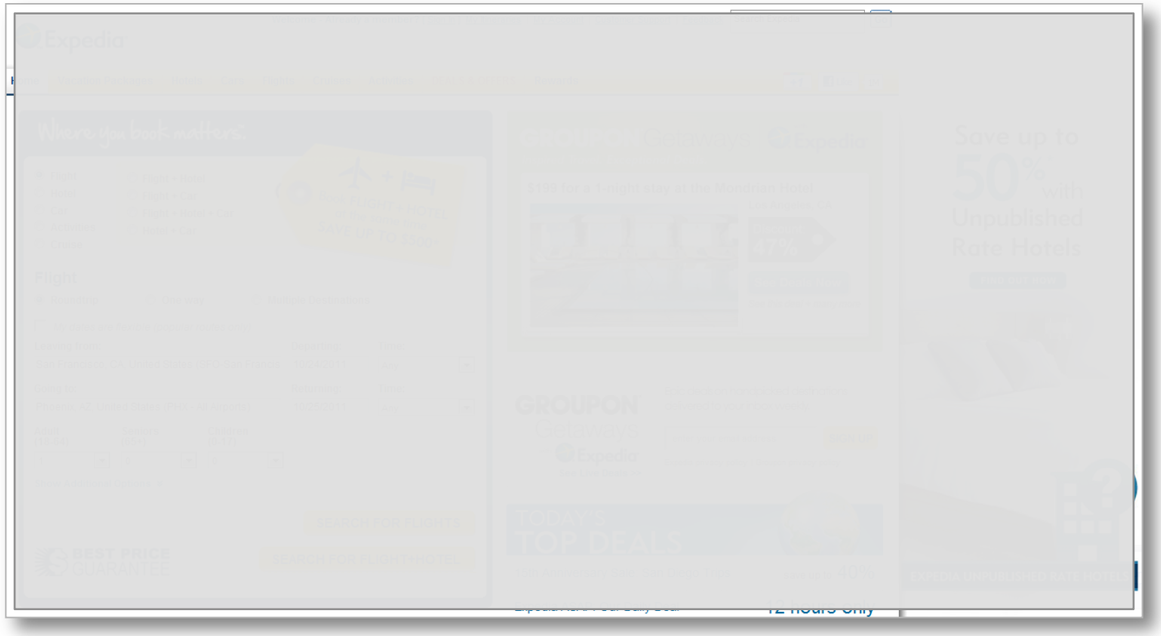
TESCO
Every little helps

得られたバリュー:

- 迅速な解析時間と、より効果的なシステム監視
- 顧客満足度の向上と経験値の取得
- 今まで、実現できなかった顧客動向分析
- ビジネスの可視化とパフォーマンス

広範囲の活用で、とてつもない価値を提供

"たった9ヶ月でSplunkへの投資の25倍以上の価値を回収できた。"



Splunk の利用:

- インフラ全体の98%を監視
- 11,000以上のサーバーからデータを取得 / 1日あたり4TB以上
- ユースケース: **アプリケーション監視, インフラ管理,Web分析**

得られた価値:

- **たった9ヶ月で25倍以上のROI**
- 不要なサーバーの除去で、数百万ドルの**コスト削減**
- 問題対応にかかる時間(MTTR)を75%も削減して、**システム稼働時間を大幅に改善**
- オペレーションではなく、**イノベーションにフォーカス** / 1,400 以上のユーザー数

Leading online travel company

お客様事例: Groupon

Splunkのプロトタイプを使用して、Hadoopとのインテグレーションを作成

日次、週次、月次のプロモーション間のメトリクスで、売り出しや受け入れのレートをレポーティング

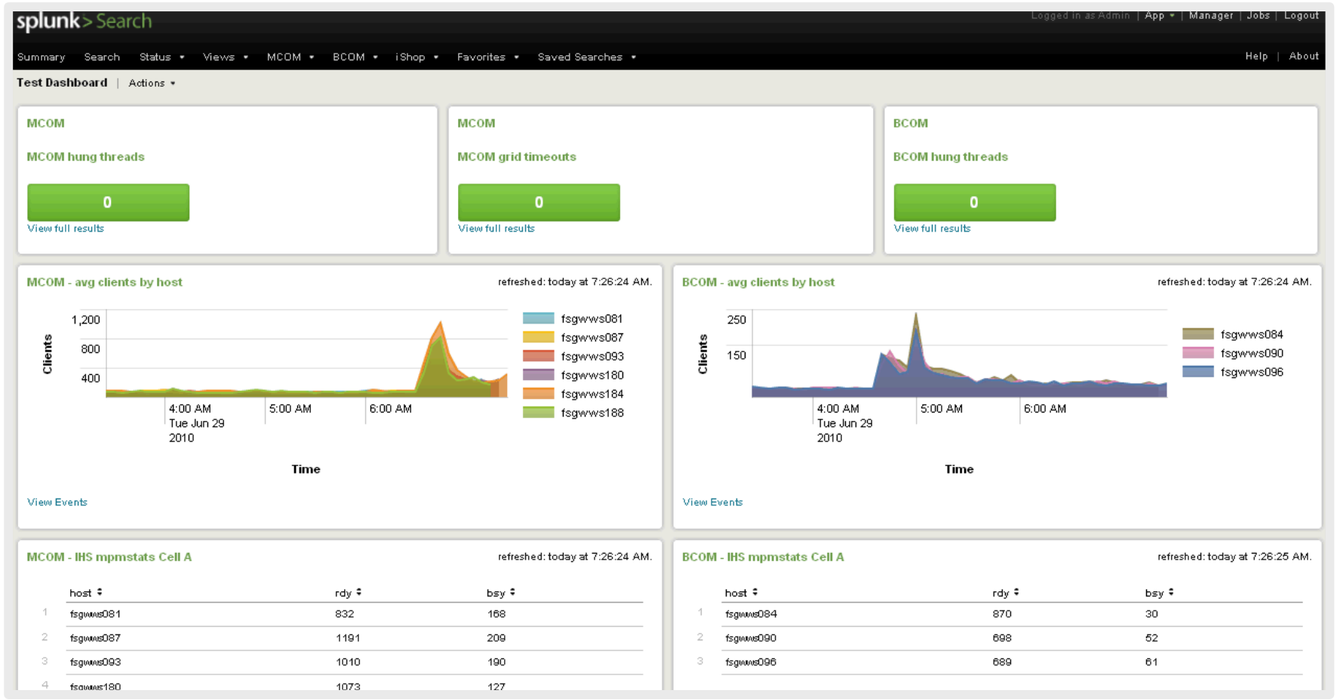
アプリケーション・パフォーマンス・マネジメント (APM) とシステムの状態監視

マシンデータのETL – HDFSへ信頼のデータデリバリーを実現。

長期のデータ・ウェアハウスとトレンドなどの分析

ウェブサイトのインフラ管理と分析

"macys.com は最初の6年間、一度もダウンしなかった。トラフィック分析の結果、ピークシーズンでも50%程度しか増えない事がわかったからだ。"



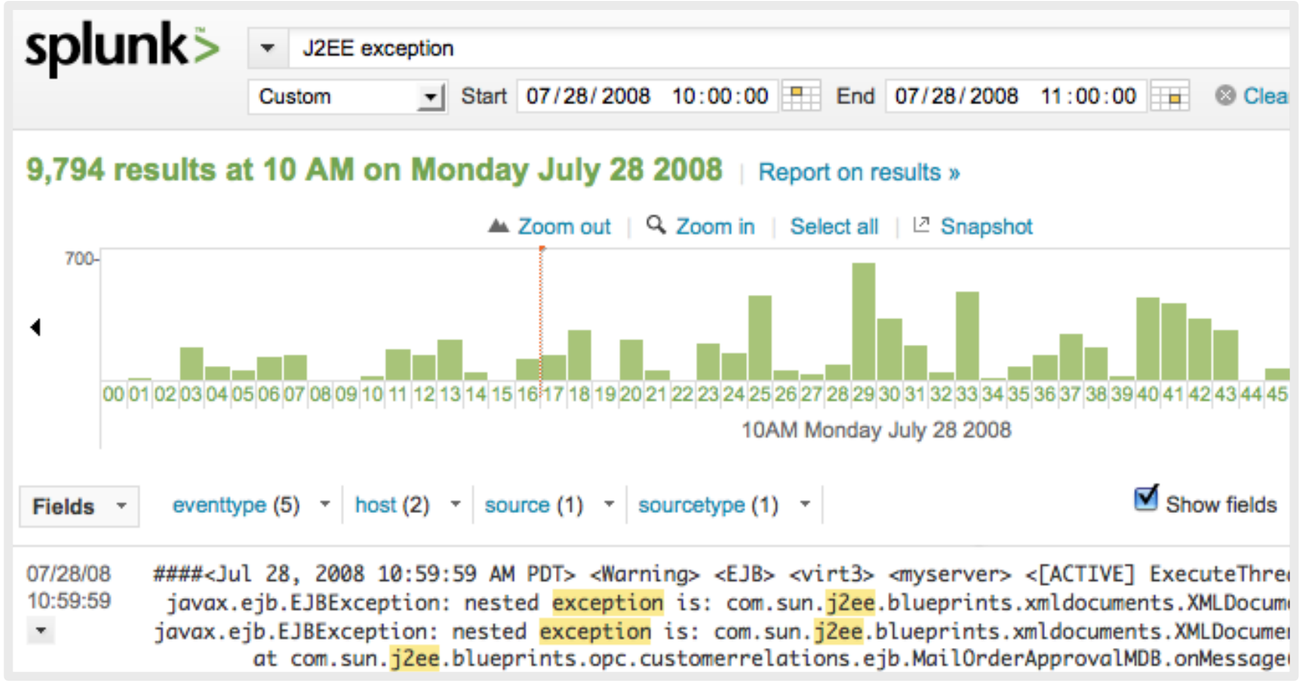
- Splunkでシステム全体を見通す事ができるようになった。
- 100%の稼働時間を達成。ピークシーズンでも50% upであることを実証できたことによる。
- 全IT部門で100ユーザー以上が、役割毎にダッシュボードを作成して管理している。

macy's

Camille Balli
Senior Analyst,
Architecture Team

サービスデスクの効率化

"Splunkで問題解決に
対するエスカレーションが
90%も削減された。"



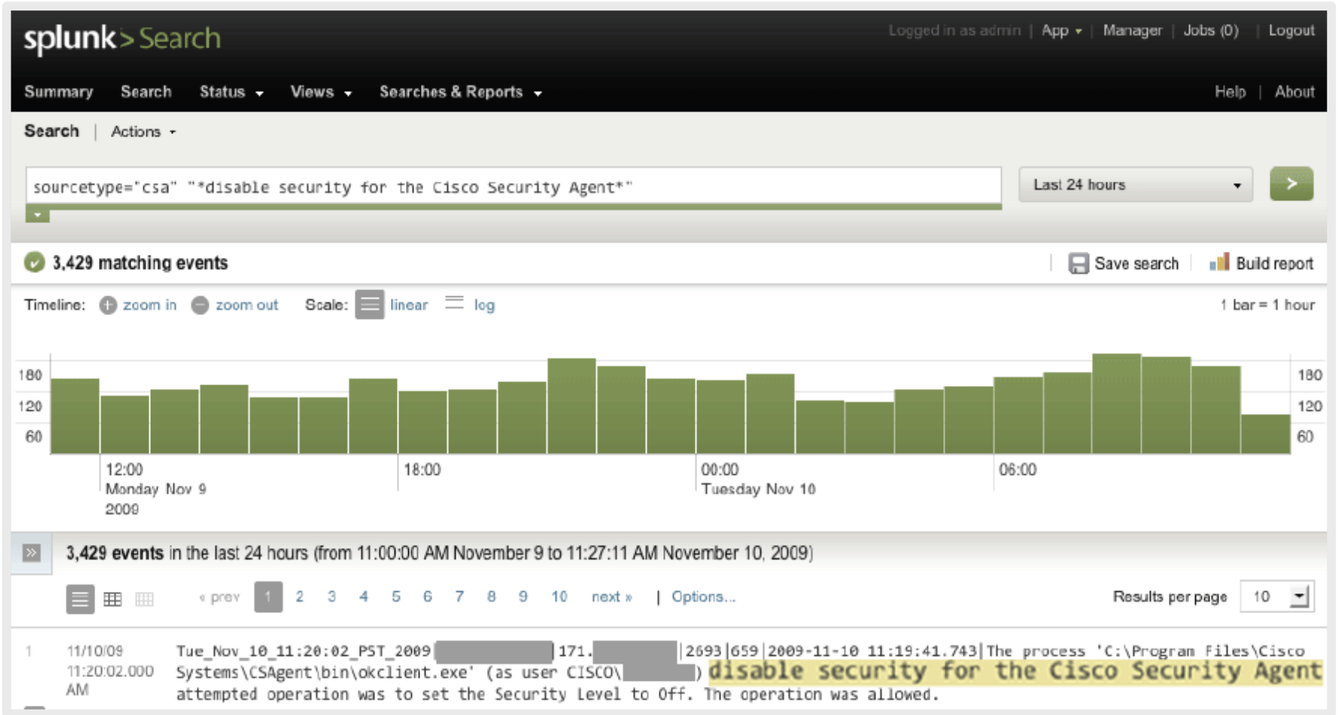
vodafone

Paulo Carvalho
Director Operations

- 迅速な問題対応とトラブルシューティングで3Gサービスの高品質化を図れた。
- Java & J2EE等のインフラにおいて、迅速に問題個所を発見する事ができるようになった。
- サービスデスクが必要な情報をすぐに見つける事ができるようになり、顧客満足度が飛躍的に向上した。

プロアクティブなセキュリティ監視とフォレンジクス

"Splunkにより複数の個別ログの横断的な解析が迅速にできるようになり、監視と対応が格段に改善された。"



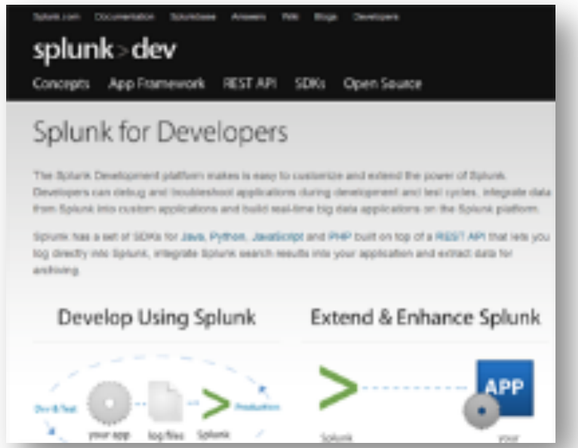
CISCO

Dave Schwartzburg
Computer Security Incident Response Team

- セキュリティ脅威に対する監視と対応プランの作成、問題の傾向把握などが実現できた
- 統合ビューの作成と個別問題対応のための活動が一つの画面からできるようになった。

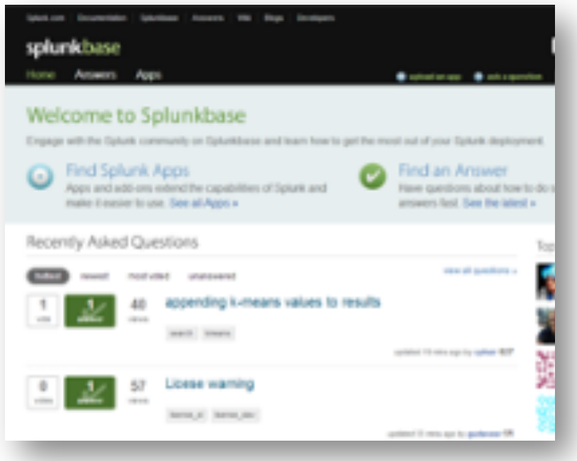
コミュニティが活発です！

Developer Portal



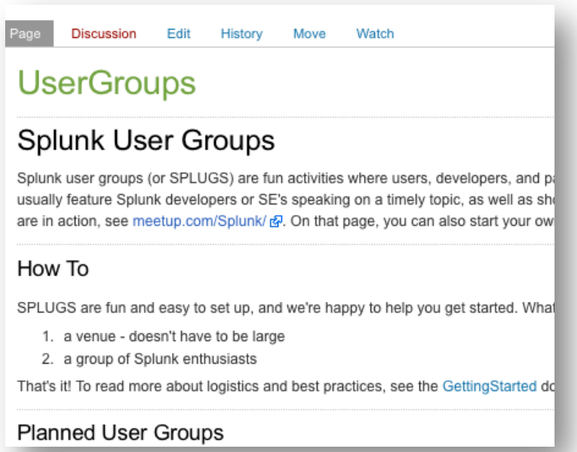
毎週1,000以上の
ユーザーが
アクセスしています。
dev.splunk.com

Splunk Answers



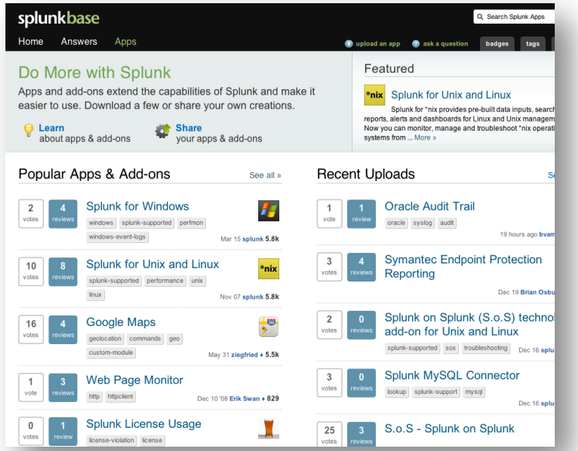
20,000以上の
Q&Aが
登録されています。

Community Events



ユーザー・グループや
SplunkLive イベント
等

Splunkbase



400以上の apps

2013/6/26

“Hunk” Beta アナウンス

SplunkによるHadoop内データの相互利用、探索、分析、そして可視化を完全に新しいプロダクトとしてリリース予定

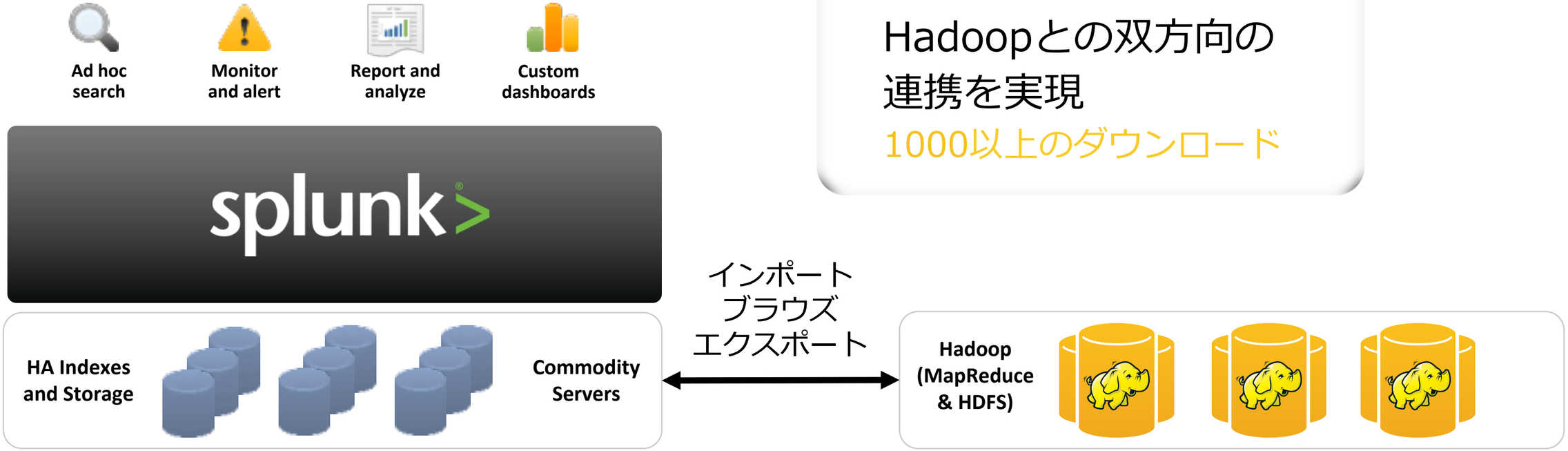
Splunk Hadoop Connect (2013/2)

Splunk初のHadoop連携をAPPとしてリリース

Splunk Hadoop Connect

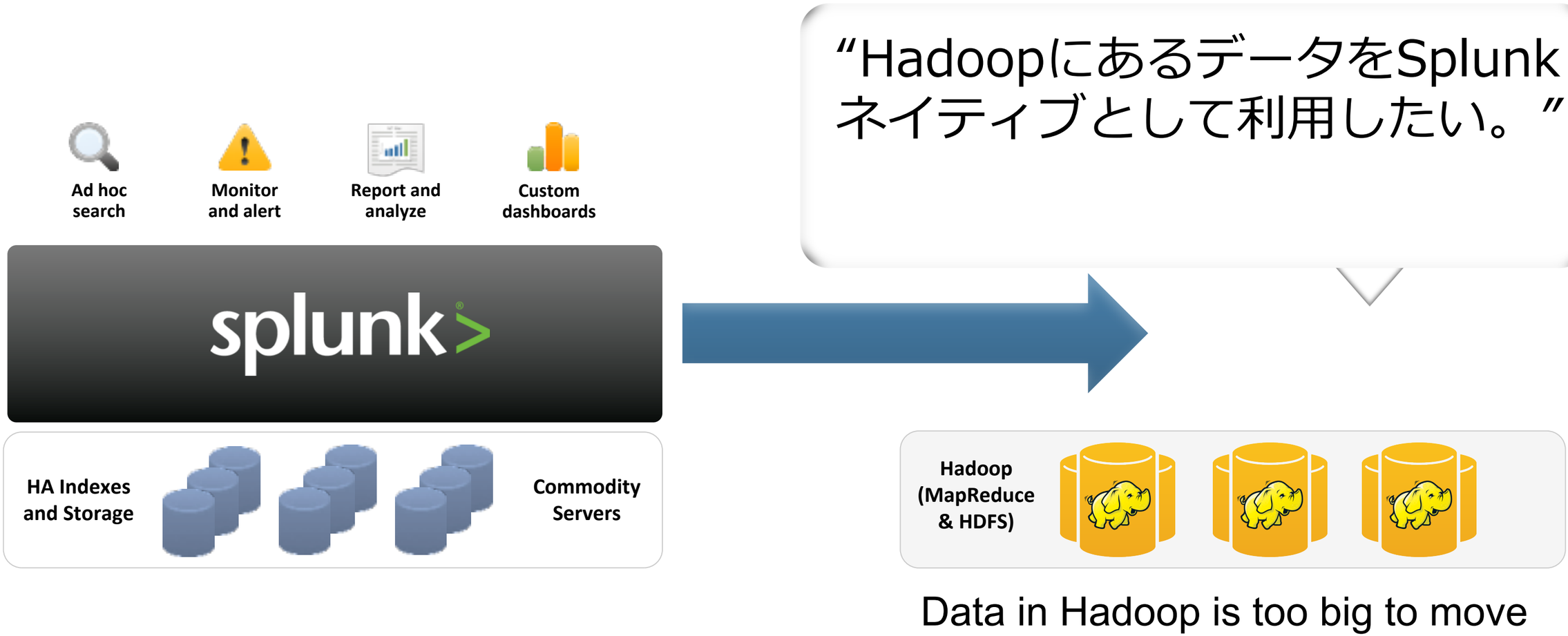
Hadoopとの双方向の
連携を実現

1000以上のダウンロード



次ステップ- Hadoopへダイレクトにアクセス

Splunk Enterprise とは異なる形態



Hunk: Splunk Analytics for Hadoop

完全に統合された製品

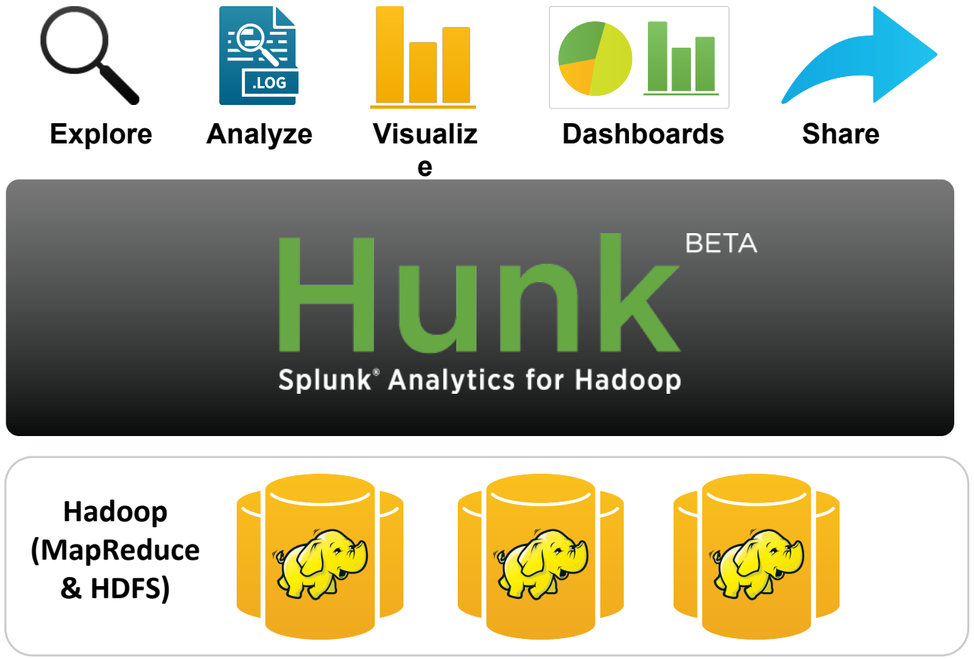
Hadoopデータの相互利用、探索、分析、可視化を実現

全てのユーザへインサイトを

組織内の幅広いユーザがHadoop内の生データを様々な視点で活用

様々なHadoopディストリビューションとの連携

業界をリードしている主なディストリビューションと連携し、投資効果を向上



Splunk 今後の取り組み

VERSIONS

4　4.1　4.2　4.3

エンジン

サーチエンジンの改良
・リアルタイム
・ダッシュボード

2009-2011

VERSION

5

プラットフォーム

アーキテクチャの進化
・レプリケーション
・レポート高速化

2012-2013

VERSION

Next

・より柔軟なUI
　BIユーザの操作
　可視化の向上

・アーキテクチャ改良
　クラスタリング
　サマリーによる高速化

・ビッグデータエコシステム
　Hadoop

・サーチ機能(コマンド)の追加

Splunk 6 ご紹介 サマリー

強力な分析

より高速且つ簡単な分析、可視化をビジネスユーザへ提供

より直感的なユーザエクスペリエンス

よりエンドユーザにとって生産性の高い機能

より簡素化された管理機能

より大規模導入に対するシンプル且つスケーラブルな管理機能

より充実した開発環境

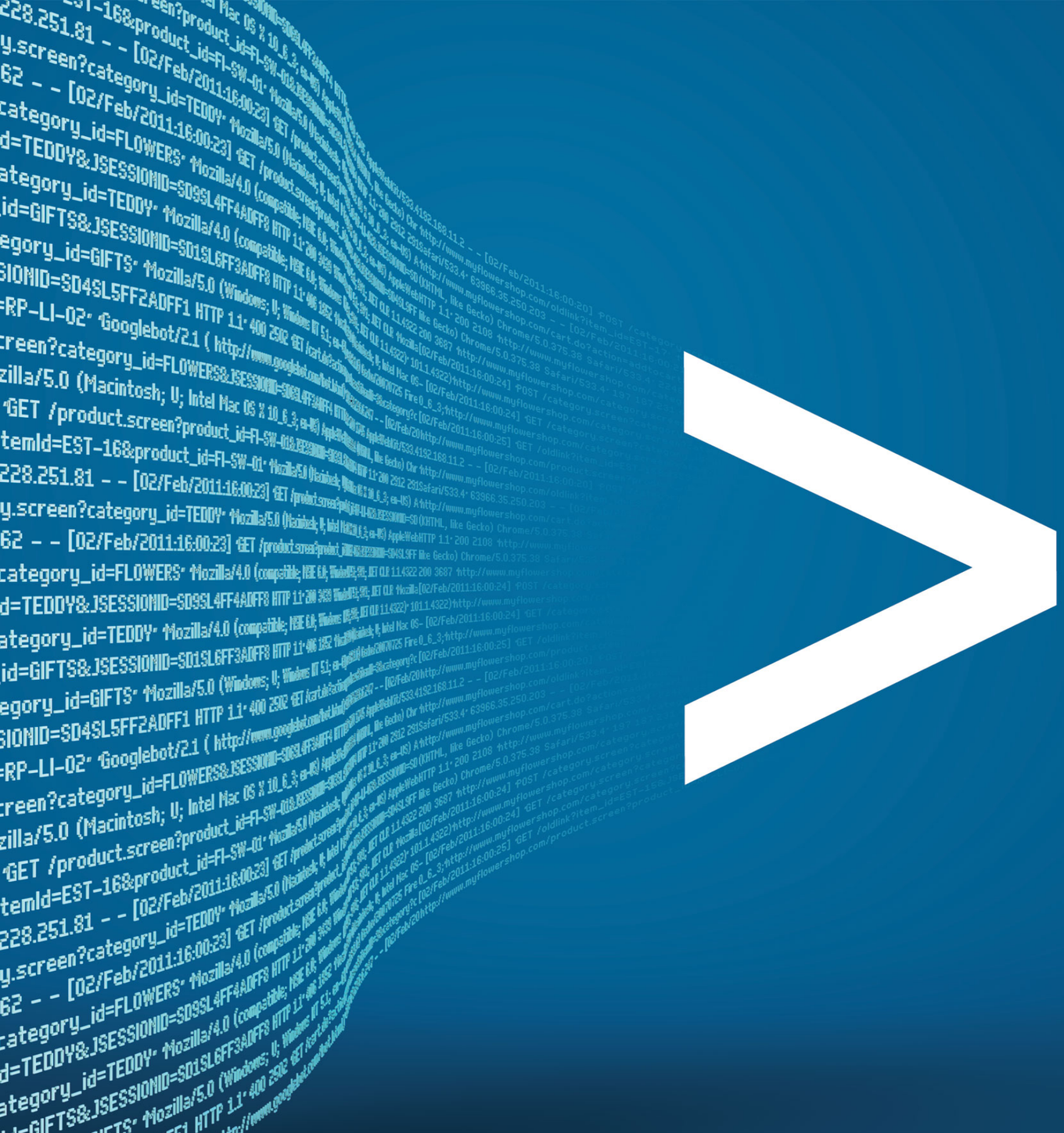
標準的なWebアプリケーション言語を基とした開発環境

まとめ

- Splunk=マシンデータプラットフォーム
  - 容易なデータ収集、強力なサーチ言語、柔軟なダッシュボード
- 今日ダウンロードしてすぐに始められます。デスクトップから分散構成まで。
- オープンなプラットフォーム。開発キット、APIなど。

ご参考

- Splunkのダウンロード(ユーザ登録が必要になります)
  - http://www.splunk.com/download?ac=get_splunk_download
- Splunk日本語マニュアル
  - http://docs.splunk.com/Documentation/Splunk/5.0.3/Translated/Japanesemanuals
- Splunkを使ってみよう (Splunk本です)
  - http://ja.splunk.com/goto/book
- Splunk Base (コミュニティです。AppやAnswersが使えます)
  - http://splunk-base.splunk.com/
- Splunk Development
  - http://dev.splunk.com/



ありがとうございました。

splunk>