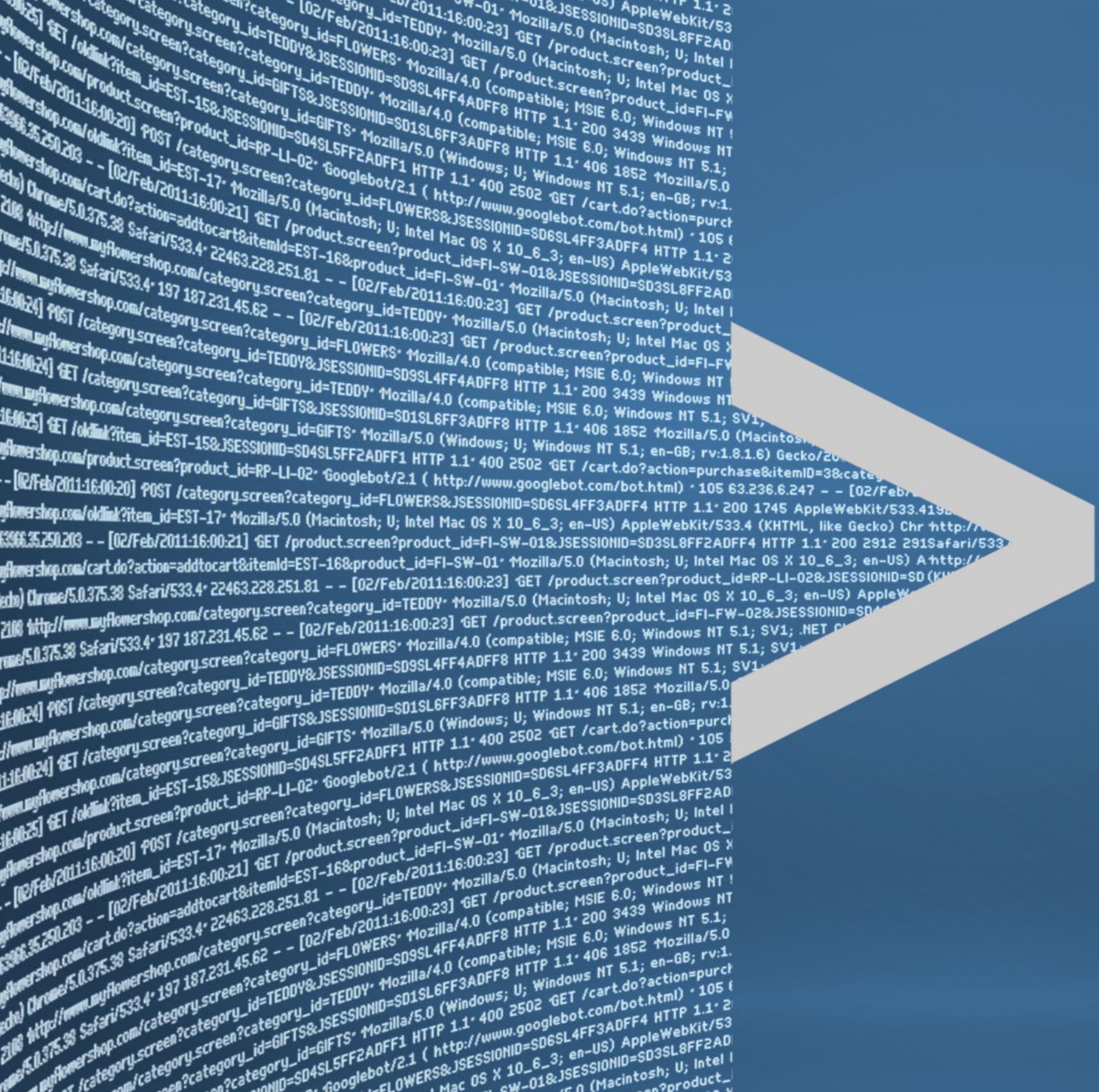
Extend Active Directory to Heterogeneous Environments

Secure and Manage Heterogeneous Environments with Centrify and Splunk

Corey Williams
Director of Product Management
Centrify Corporation

Ben Brauer
Director of Product Marketing
Splunk Inc.

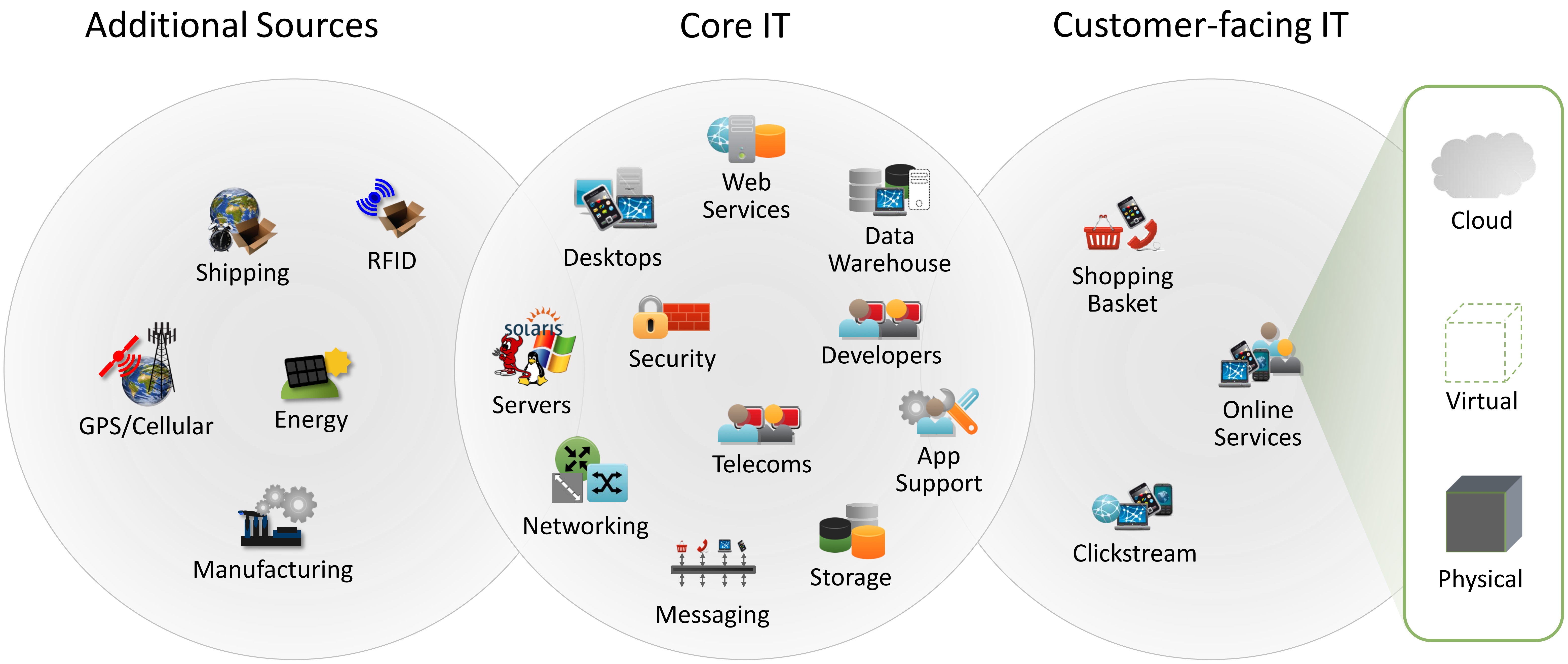


Introducing Splunk

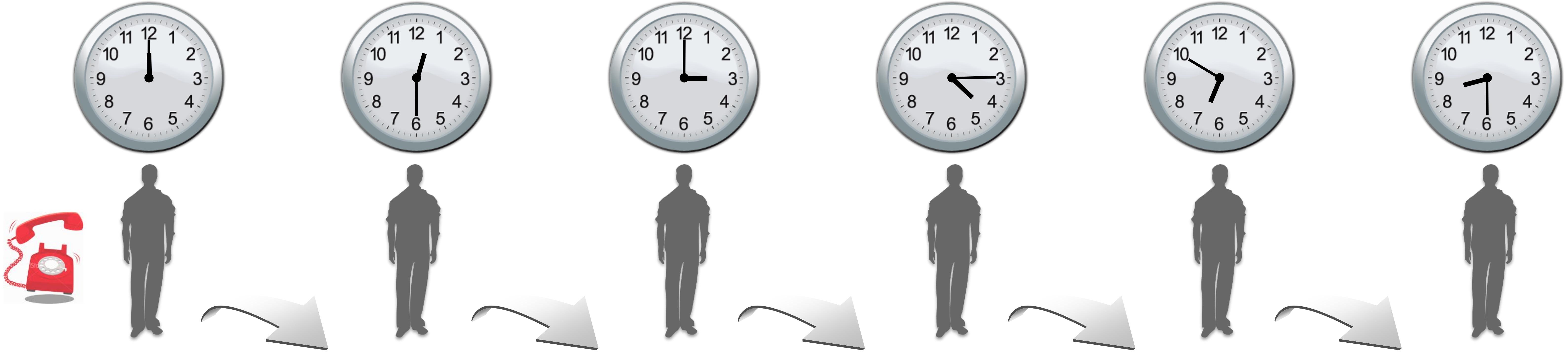
Ben Brauer
Product Marketing Director

April 2011

Today’s IT Reality: Complex, Silo-based Systems



In the Trenches



Service Desk

Log call. The console says everything is green.

Escalate.

Application Support

Java monitoring tools don’t show anything either. Call the developer.

Escalate.

Application Developer

Stop working on new code to troubleshoot. Need production logs!

Escalate.

Systems Administrator

Stop what they’re doing to identify and gather production logs for developer.

Respond.

Application Developer

Manual investigation establishes not application problem.

Escalate.

Database Administrator

DBA analyzes audit logs which points to bad query.

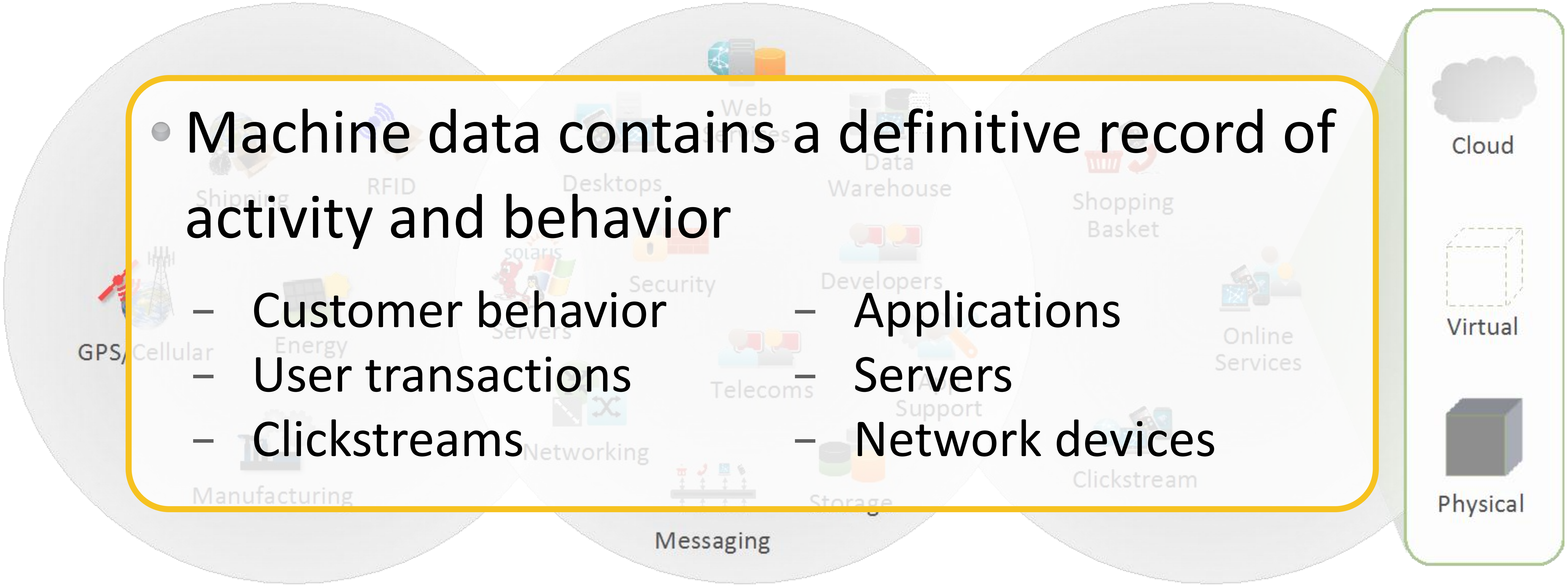
Now what?

The Answer is in The Data

Additional Sources

Core IT

Customer-facing IT



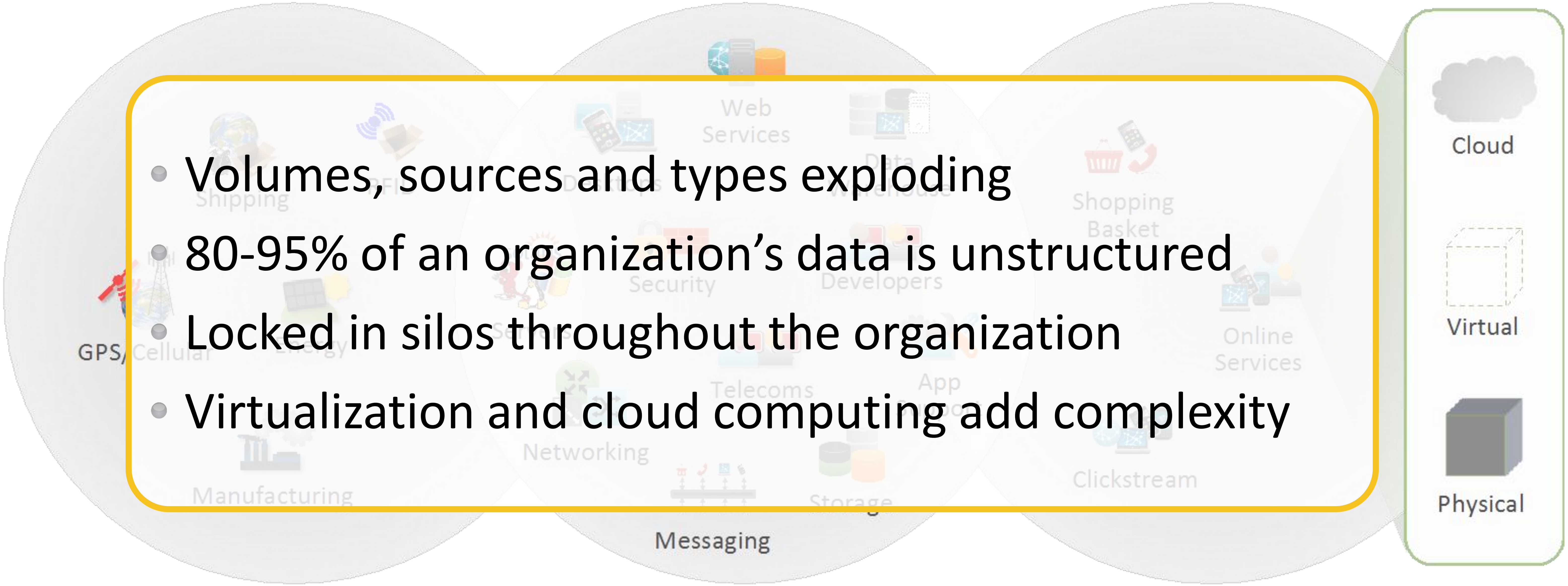
- Machine data contains a definitive record of activity and behavior
  - Customer behavior
  - User transactions
  - Clickstreams
  - Applications
  - Servers
  - Network devices

Growing Volumes and Complexity

Additional Sources

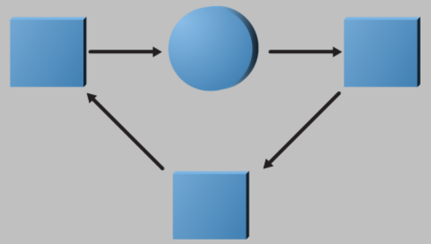
Core IT

Customer-facing IT



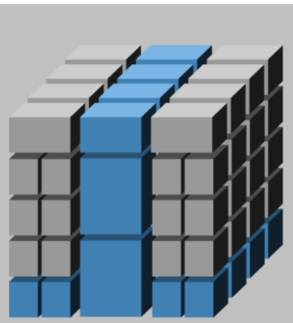
- Volumes, sources and types exploding
- 80-95% of an organization’s data is unstructured
- Locked in silos throughout the organization
- Virtualization and cloud computing add complexity

What's Different About Machine Data



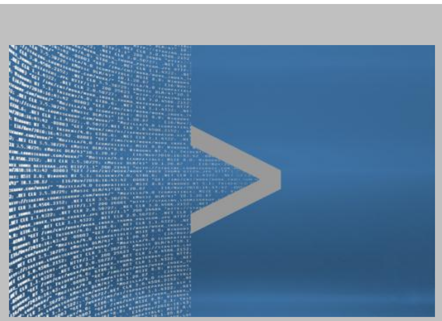
Relational Databases

- Financial records, manufacturing and logistical information, personnel data
- Data highly structured — database highly structured
- Inflexible schema, long deployment cycle



Multidimensional Databases

- Multidimensional data for business management and statistics
- Math computation strength – dense data
- Pivots data for flexible financial analysis
- Monthly reporting, not for real-time events



Engine for Machine Data

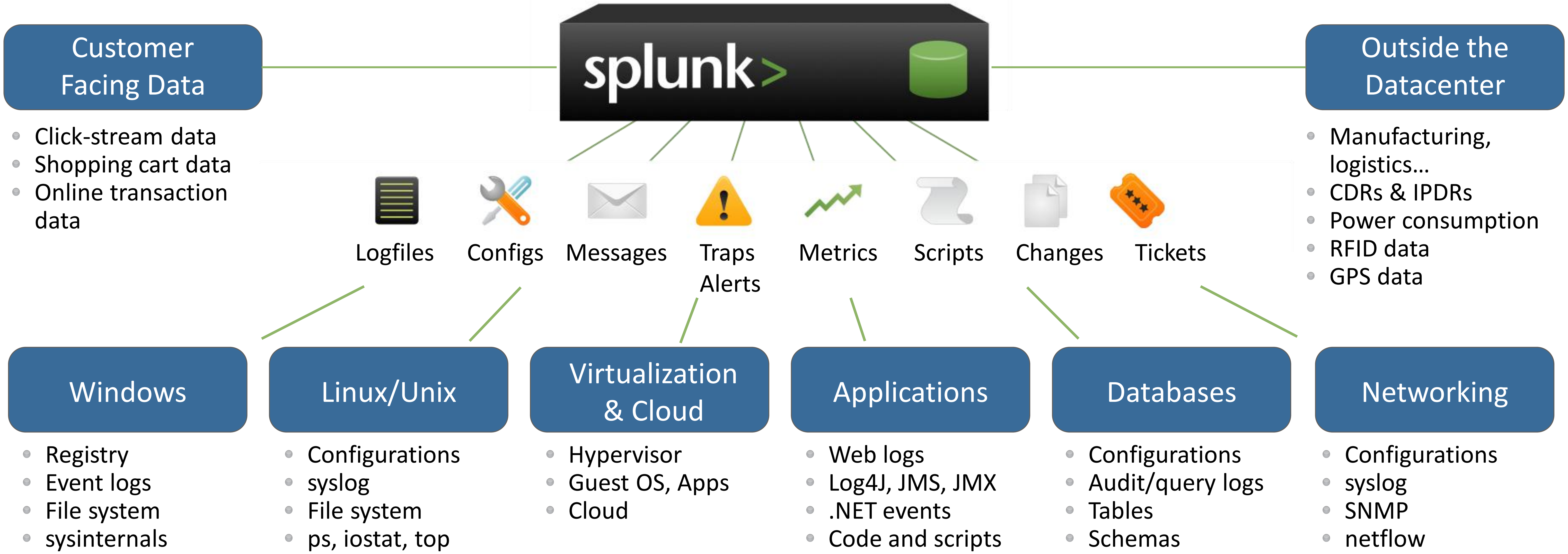
- Time series unstructured data, with no predefined schema
- Generated by all IT systems, non-standard data, unpredictable formats
- Massive volume; fast navigation and correlation paramount

splunk>®

Collect, index and harness your machine data to identify issues, patterns, risks and opportunities and drive better decisions for IT and the business

Splunk: The Engine for Machine Data

No predefined schema, no custom connectors, no RDBMS, no need to filter/forward.



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

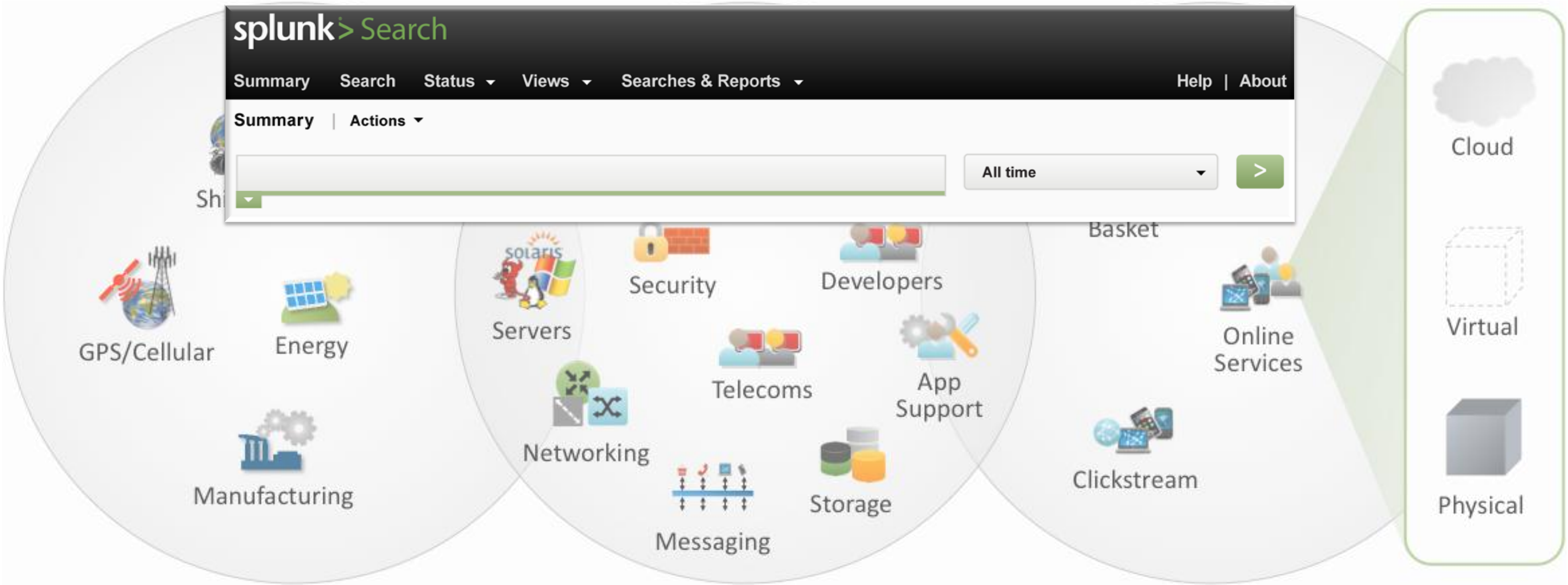
- Configurations
- Audit/query logs
- Tables
- Schemas

Networking

- Configurations
- syslog
- SNMP
- netflow

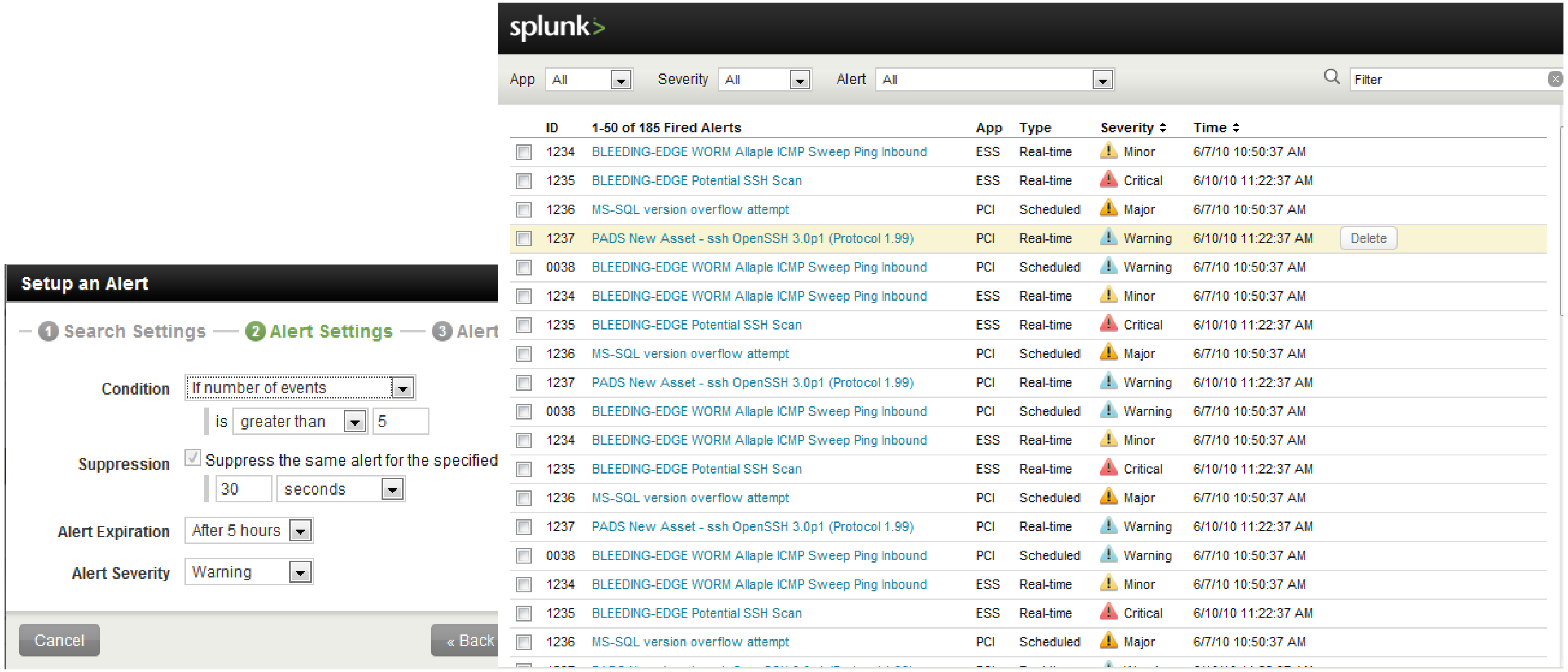
Splunk is a Powerful Search Engine for IT

Find and fix problems dramatically faster across your organization.



Splunk Proactively Monitors for Incidents

Automatically monitor all your infrastructure in real-time to identify issues, problems and attacks before they impact your customers and services.



Setup an Alert

① Search Settings — ② Alert Settings — ③ Alert

Condition: If number of events
is greater than 5

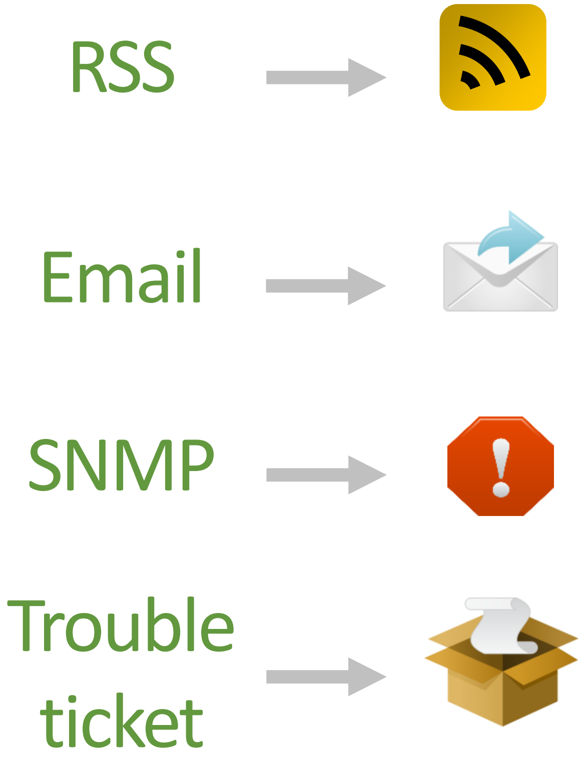
Suppression: ☑ Suppress the same alert for the specified
30 seconds

Alert Expiration: After 5 hours

Alert Severity: Warning

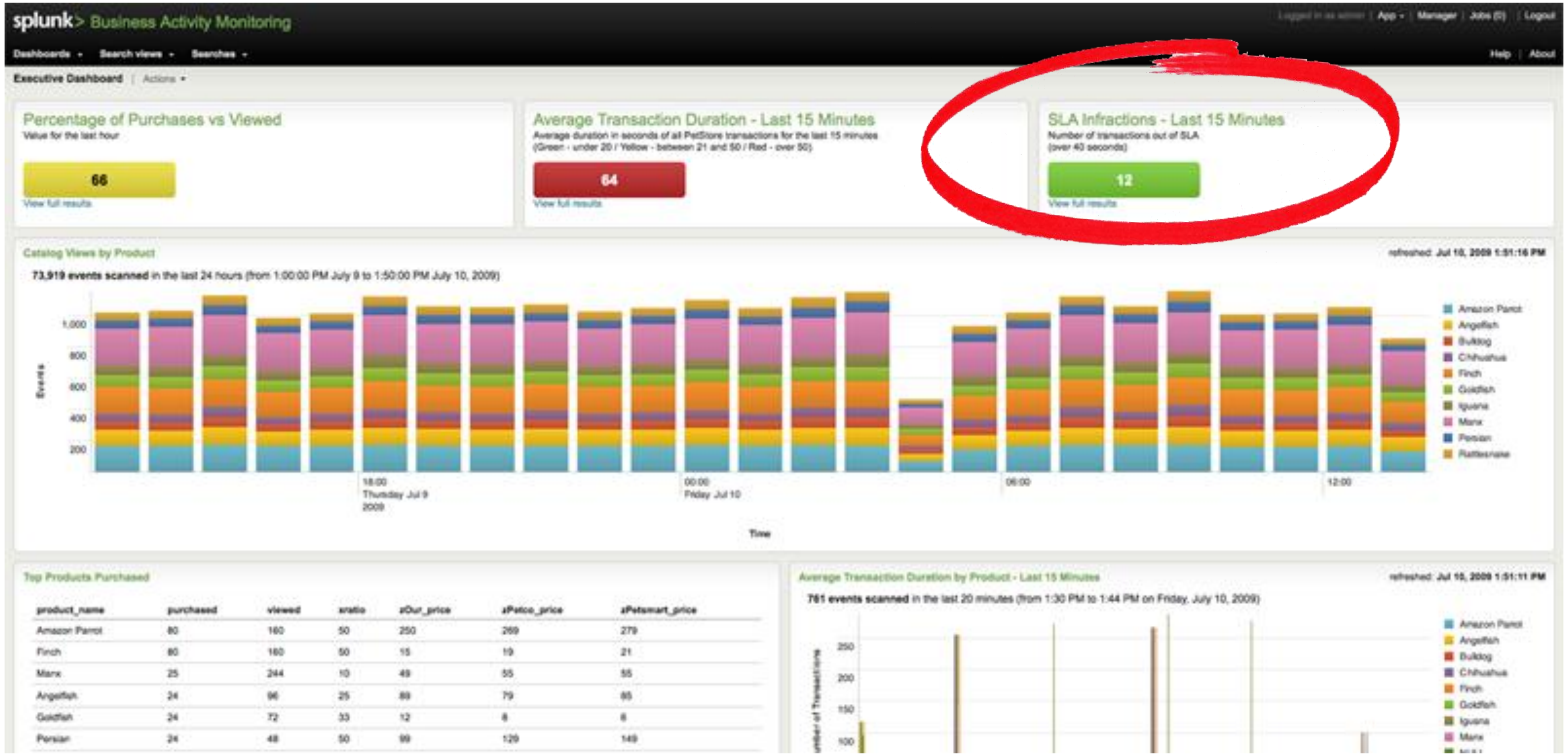
App: All | Severity: All | Alert: All | Filter

	ID	1-50 of 185 Fired Alerts	App	Type	Severity	Time
□	1234	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	ESS	Real-time	Minor	6/7/10 10:50:37 AM
□	1235	BLEEDING-EDGE Potential SSH Scan	ESS	Real-time	Critical	6/10/10 11:22:37 AM
□	1236	MS-SQL version overflow attempt	PCI	Scheduled	Major	6/7/10 10:50:37 AM
□	1237	PADS New Asset - ssh OpenSSH 3.0p1 (Protocol 1.99)	PCI	Real-time	Warning	6/10/10 11:22:37 AM
□	0038	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	PCI	Scheduled	Warning	6/7/10 10:50:37 AM
□	1234	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	ESS	Real-time	Minor	6/7/10 10:50:37 AM
□	1235	BLEEDING-EDGE Potential SSH Scan	ESS	Real-time	Critical	6/10/10 11:22:37 AM
□	1236	MS-SQL version overflow attempt	PCI	Scheduled	Major	6/7/10 10:50:37 AM
□	1237	PADS New Asset - ssh OpenSSH 3.0p1 (Protocol 1.99)	PCI	Real-time	Warning	6/10/10 11:22:37 AM
□	0038	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	PCI	Scheduled	Warning	6/7/10 10:50:37 AM
□	1234	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	ESS	Real-time	Minor	6/7/10 10:50:37 AM
□	1235	BLEEDING-EDGE Potential SSH Scan	ESS	Real-time	Critical	6/10/10 11:22:37 AM
□	1236	MS-SQL version overflow attempt	PCI	Scheduled	Major	6/7/10 10:50:37 AM
□	1237	PADS New Asset - ssh OpenSSH 3.0p1 (Protocol 1.99)	PCI	Real-time	Warning	6/10/10 11:22:37 AM
□	0038	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	PCI	Scheduled	Warning	6/7/10 10:50:37 AM
□	1234	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	ESS	Real-time	Minor	6/7/10 10:50:37 AM
□	1235	BLEEDING-EDGE Potential SSH Scan	ESS	Real-time	Critical	6/10/10 11:22:37 AM
□	1236	MS-SQL version overflow attempt	PCI	Scheduled	Major	6/7/10 10:50:37 AM



Splunk Delivers Operational Visibility

Gain end-to-end visibility to track and deliver on IT KPIs
and make better-informed IT decisions.



Percentage of Purchases vs Viewed
Value for the last hour
66

Average Transaction Duration - Last 15 Minutes
Average duration in seconds of all PetStore transactions for the last 15 minutes (Green - under 20 / Yellow - between 21 and 50 / Red - over 50)
64

SLA Infractions - Last 15 Minutes
Number of transactions out of SLA (over 40 seconds)
12

Catalog Views by Product
refreshed: Jul 10, 2009 1:51:16 PM
73,919 events scanned in the last 24 hours (from 1:00:00 PM July 9 to 1:50:00 PM July 10, 2009)

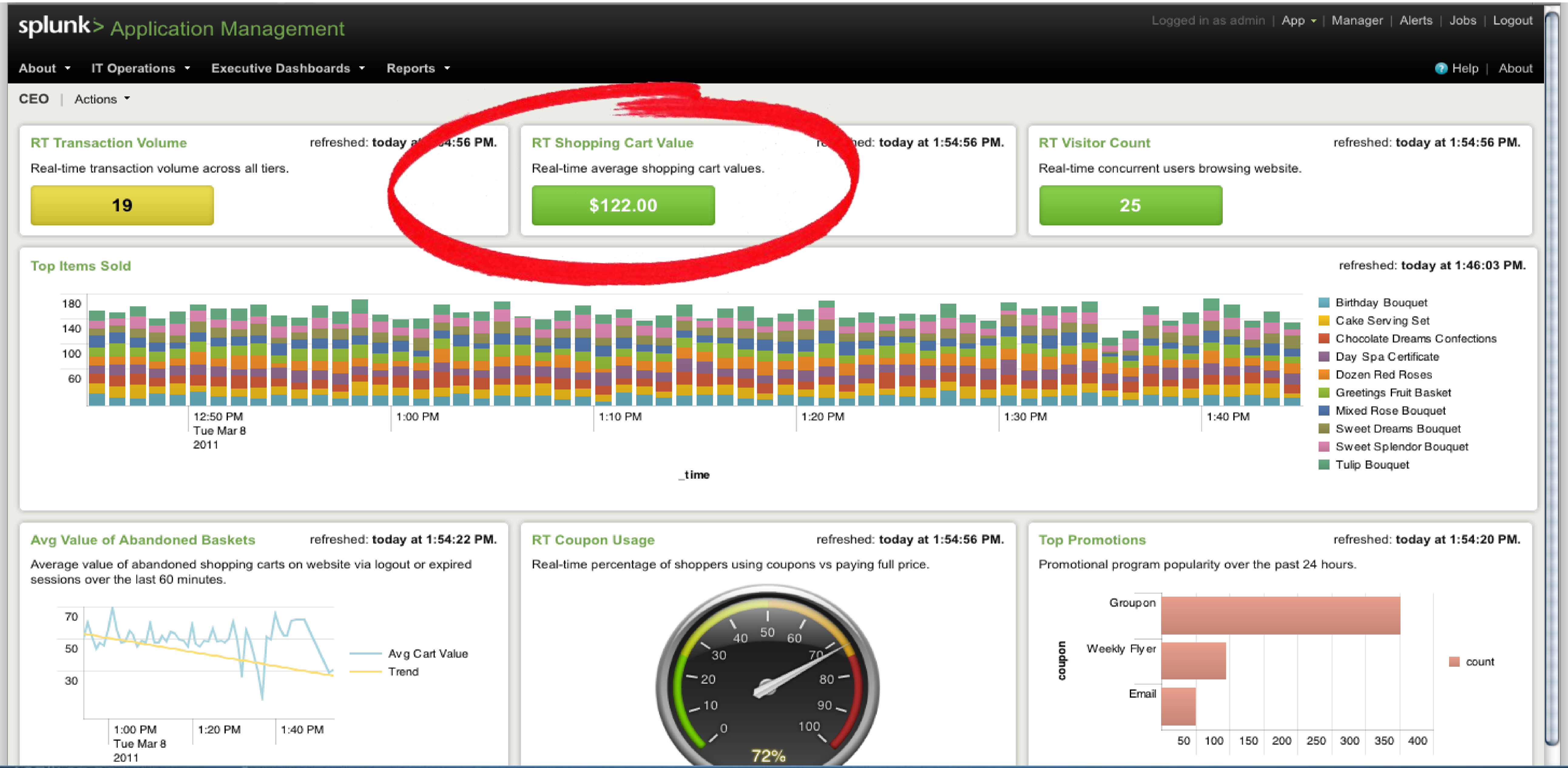
Top Products Purchased

product_name	purchased	viewed	%ratio	$Our_price	$Petco_price	$Petsmart_price
Amazon Parrot	80	160	50	250	269	279
Finch	80	160	50	15	19	21
Manx	25	244	10	49	55	55
Angelfish	24	96	25	89	79	85
Goldfish	24	72	33	12	8	6
Persian	24	48	50	99	129	149

Average Transaction Duration by Product - Last 15 Minutes
refreshed: Jul 10, 2009 1:51:11 PM
761 events scanned in the last 20 minutes (from 1:30 PM to 1:44 PM on Friday, July 10, 2009)

Splunk Provides New Insights for Business

Gain new insight from operational data to make better-informed business decisions.



RT Transaction Volume refreshed: today a 4:56 PM.

Real-time transaction volume across all tiers.

19

RT Shopping Cart Value re ed: today at 1:54:56 PM.

Real-time average shopping cart values.

$122.00

RT Visitor Count refreshed: today at 1:54:56 PM.

Real-time concurrent users browsing website.

25

Top Items Sold refreshed: today at 1:46:03 PM.

Avg Value of Abandoned Baskets refreshed: today at 1:54:22 PM.

Average value of abandoned shopping carts on website via logout or expired sessions over the last 60 minutes.

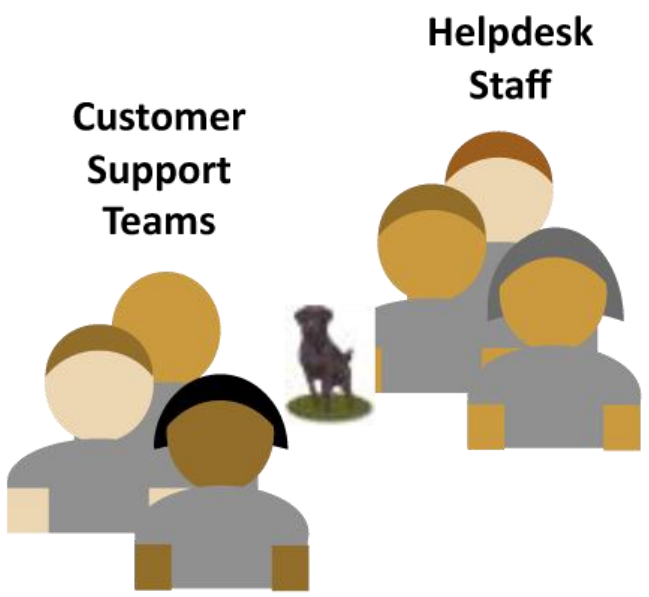
RT Coupon Usage refreshed: today at 1:54:56 PM.

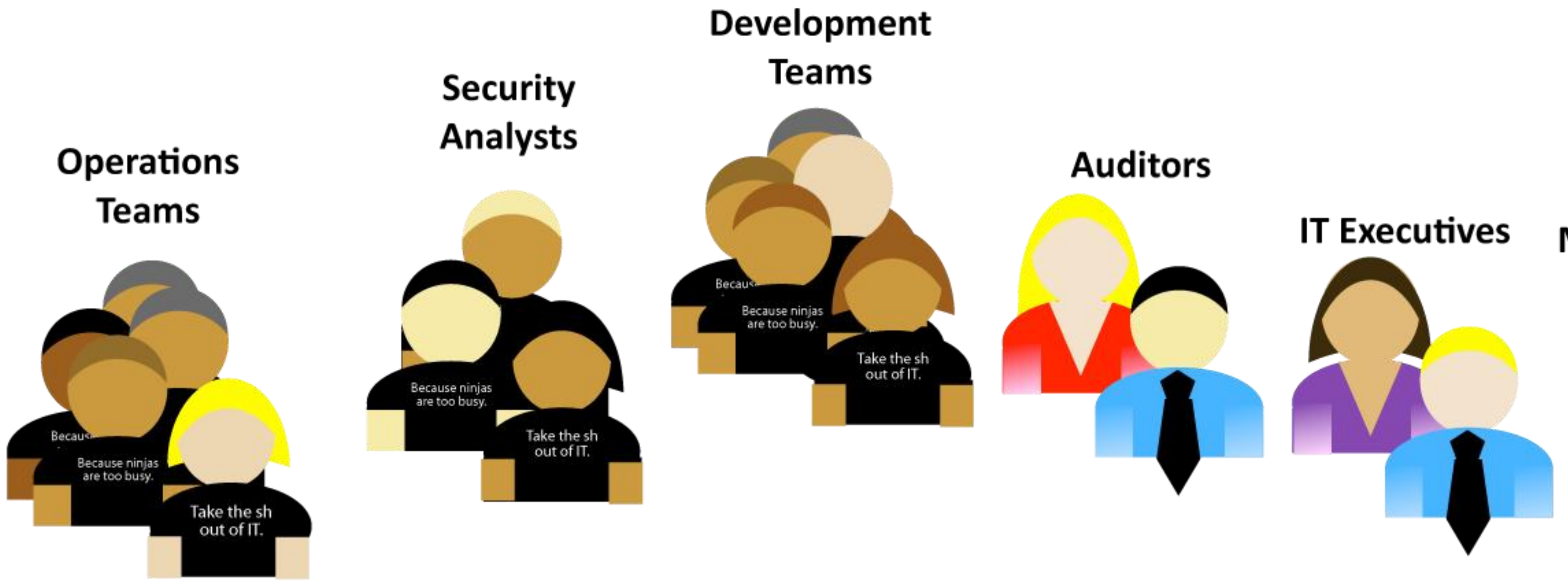
Real-time percentage of shoppers using coupons vs paying full price.

Top Promotions refreshed: today at 1:54:20 PM.

Promotional program popularity over the past 24 hours.

Delivers Visibility Across IT and the Business





Marketing & Business Analysts
Other Executives & Business Owners

Last refreshed: 03.08.2009 21:48:07 -0700 | Refresh | Logged in as jhart | Admin | Preferences | Help | Logout

splunk> Apache Errors by Environment show as text | permalink

Environment PROD

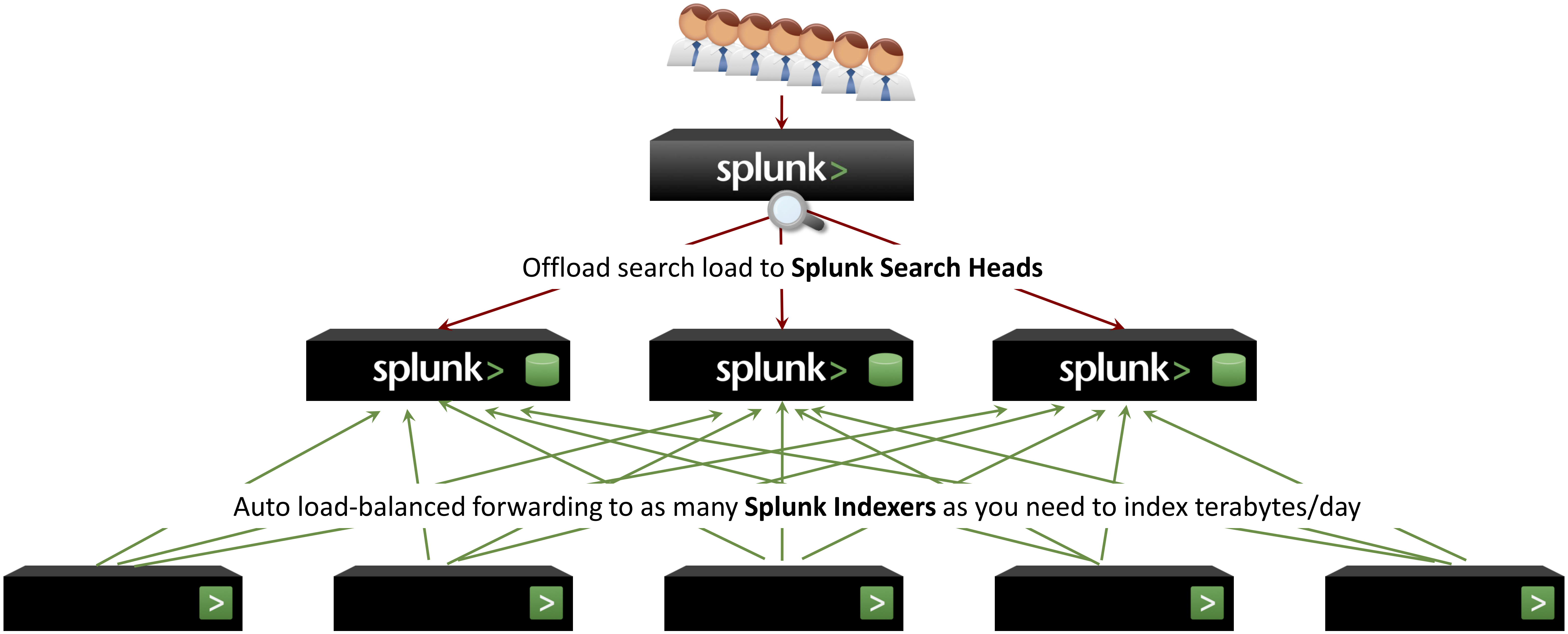
Server 4 of 4 servers

Timerange Last 24 hours

Search

splunk>

Scales to Tens of Terabytes Per Day



Offload search load to **Splunk Search Heads**

Auto load-balanced forwarding to as many **Splunk Indexers** as you need to index terabytes/day

Send data from 1000s of servers using combination of **Splunk Forwarders**, syslog, WMI, message queues, or other remote protocols

Splunk for Monitoring Active Directory

- Windows native tools are ineffective for auditing Active Directory
- Identify Who, What, Where, and When in real time
  - Get full context—see both *before* and *after* values for each setting
- Ensure provenance of audit and security logs
- Archive, search and report on logs at the ID and Object levels
- Integration with SCOM for leveraging the Active Directory Management Pack

What Makes Splunk Different?

Any Data

- Any format of data, from any source
- Full access to 100% of data for months/years
- Cradle-to-grave data management

Completely Flexible

- Supports any analysis, reporting or monitoring across IT silos
- Highly flexible dashboards present any view for any user
- Adapts to change—schema-on-the-fly design supports new or unexpected data

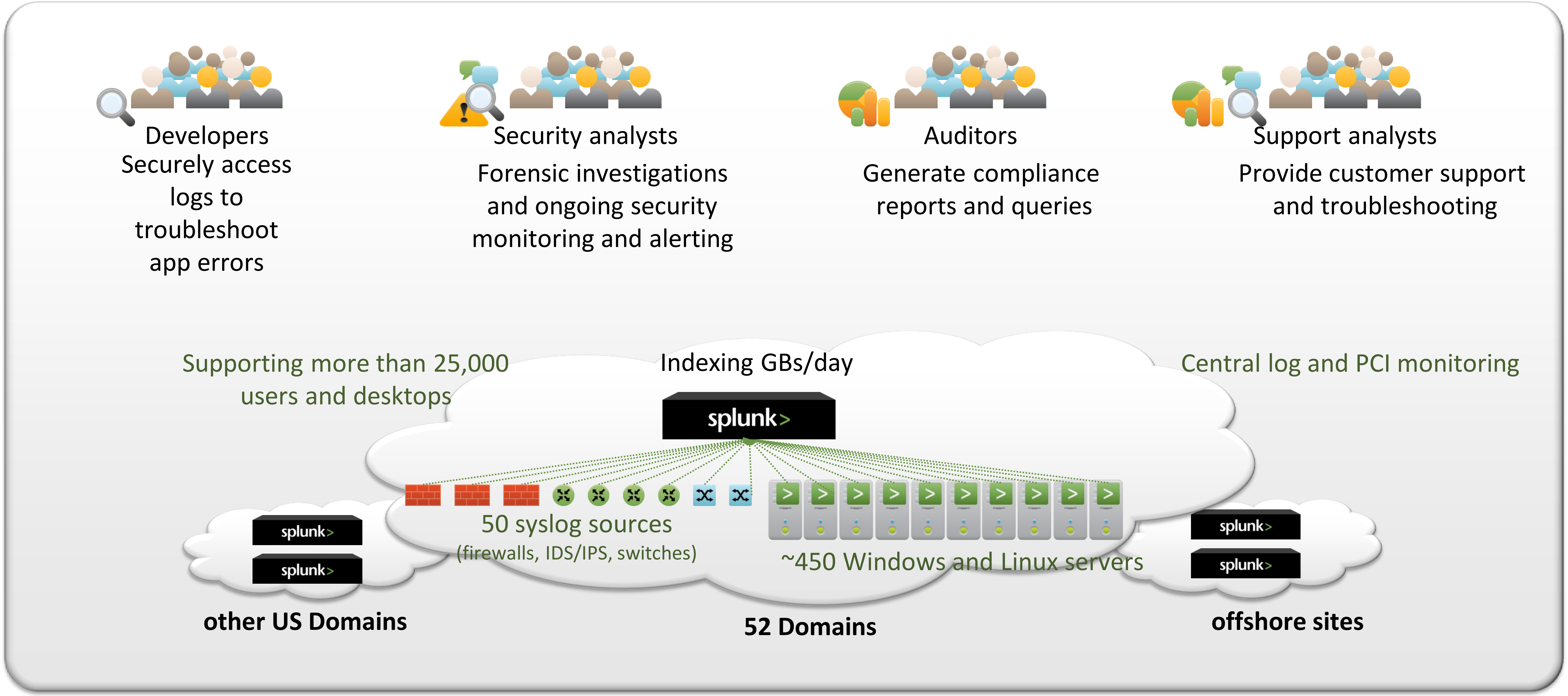
Immediate Results

- Free download, installs in minutes
- Can get started small and grow over time—from laptop to datacenters
- Initial benefits realized in hours or days

Splunk: The Engine for Machine Data

splunk>

End-to-End Visibility Across IT



Developers
Securely access logs to troubleshoot app errors

Security analysts
Forensic investigations and ongoing security monitoring and alerting

Auditors
Generate compliance reports and queries

Support analysts
Provide customer support and troubleshooting

Supporting more than 25,000 users and desktops

Indexing GBs/day

Central log and PCI monitoring

50 syslog sources
(firewalls, IDS/IPS, switches)

~450 Windows and Linux servers

other US Domains

52 Domains

offshore sites

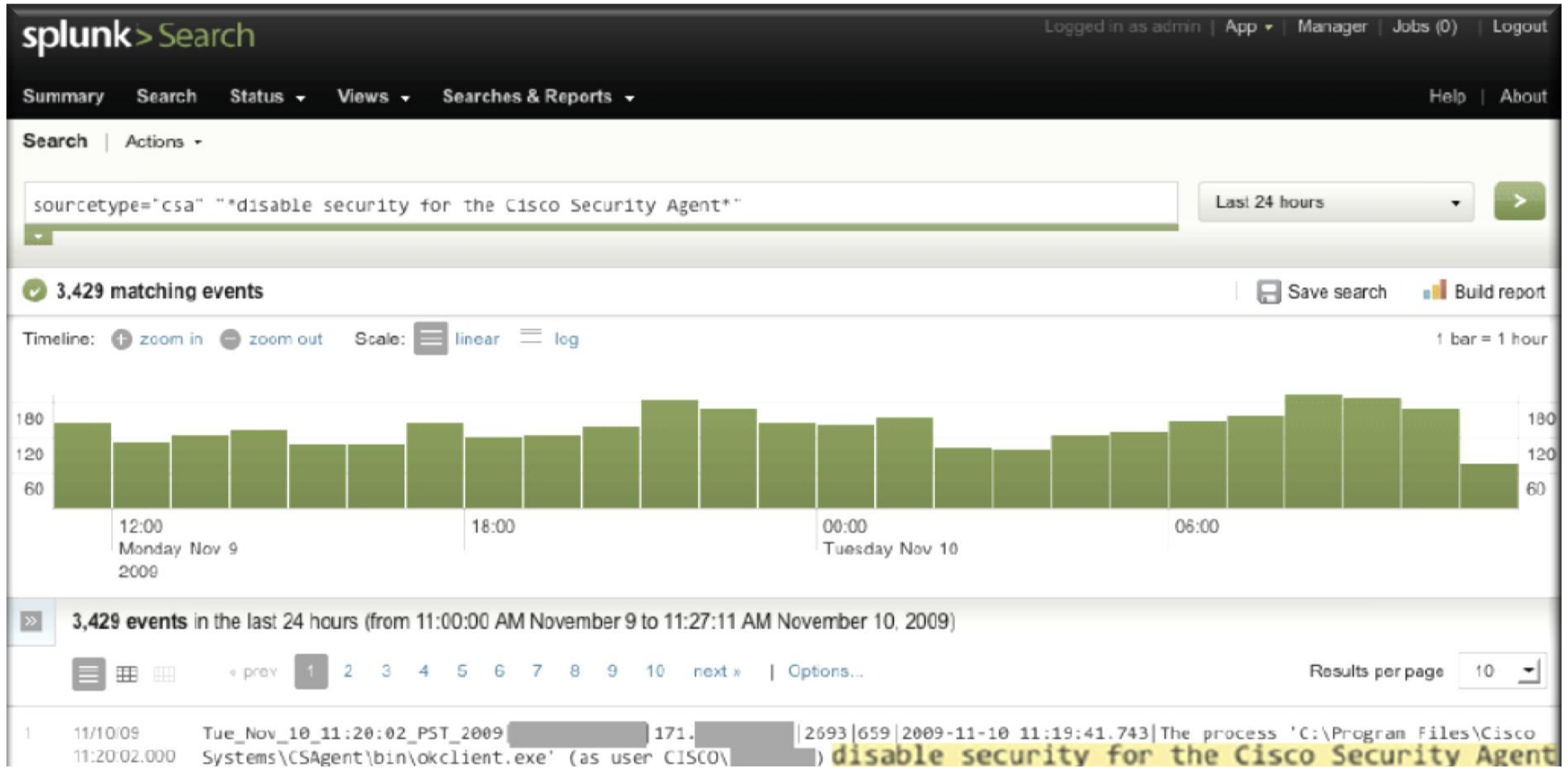
"The speed with which Splunk returns results makes you want to use it--it's addictive!"

Dennis Scales, Director, IT

FIS»
FIDELITY NATIONAL INFORMATION SERVICES

Proactive Security Monitoring After Splunk

> “Splunk allows us to quickly consolidate and correlate disparate log sources, enabling previously impractical monitoring and response scenarios.”



```
sourcetype="csa" "*disable security for the Cisco Security Agent*"
```

3,429 matching events

3,429 events in the last 24 hours (from 11:00:00 AM November 9 to 11:27:11 AM November 10, 2009)

```
1   11/10/09       Tue_Nov_10_11:20:02_PST_2009[redacted]171.[redacted]|2693|659|2009-11-10 11:19:41.743|The process 'C:\Program Files\Cisco
    11:20:02.000   Systems\CSAgent\bin\okclient.exe' (as user CISCO\[redacted]) disable security for the Cisco Security Agent
```

Dave Schwartzburg
Computer Security Incident Response Team

- Enabled proactive threat assessment, mitigation planning, incident trending with analysis, security architecture, incident detection and response
- Delivered a centralized view into user activities and in-scope systems

2,300+ Licensed Customers in 74 Countries

Michigan
University of Maryland
Cal
Texas
Washington State University
Stanford
Penn State
GW
USC Trojans

Education

PG&E
TOTSA Total Oil Trading SA
Alliant Energy
Ultra Petroleum
Westar Energy
Southern California Edison
An EDISON INTERNATIONAL® Company
California ISO
Shaping a Renewed Future
Chevron
noble energy
urenco

Energy & Utilities

CareFirst BlueCross BlueShield
Bank of America
New York Life
Wells Fargo
Credit Suisse
Aetna
Morgan Stanley
Goldman Sachs
VISA
Commerzbank

Financial Services & Insurance

USAID
From the American People
SOCOM
U.S. Army
U.S. Air Force

Government

UCLA Health System
Health Net
Covidien
St. Jude Medical
HealthSpring
Coventry Health Care
Magellan Health Services
AAMC
McKesson
medco

Healthcare

Raytheon
Lockheed Martin
PPG
Schlumberger
GE
Briggs & Stratton
Pitney Bowes
Northrop Grumman
Snap-on
General Dynamics

Manufacturing

BBC
Gannett
Dow Jones
Sony
Washington Post Media
Fox audience network
National Geographic
Discovery Communications
HBO
Comcast

Media

salesforce
white pages
LinkedIn
PayPal
facebook
edmunds.com
Ariba
StubHub!
ebay
Yahoo!

Cloud & Online Services

Best Buy
jcpenney
CVS Caremark
Target
adidas
Lowe's
macy's
Staples
The Home Depot
Wal*Mart

Retail

IBM
Cisco
Adobe
EMC²
intel
Intuit
Dell
Trend Micro
Qualcomm
Autodesk

Technology

metroPCS
vodacom
Time Warner Cable
SaskTel
Motorola
at&t
Telstra
T-Mobile
HughesNet
swisscom

Telecommunications

Vegas.com
Expedia
Pegasus Solutions
Toll
carlson marketing
Orbitz
Pinnacle Entertainment
starwood Hotels and Resorts
Wynn Resorts
sun country airlines

Travel & Leisure

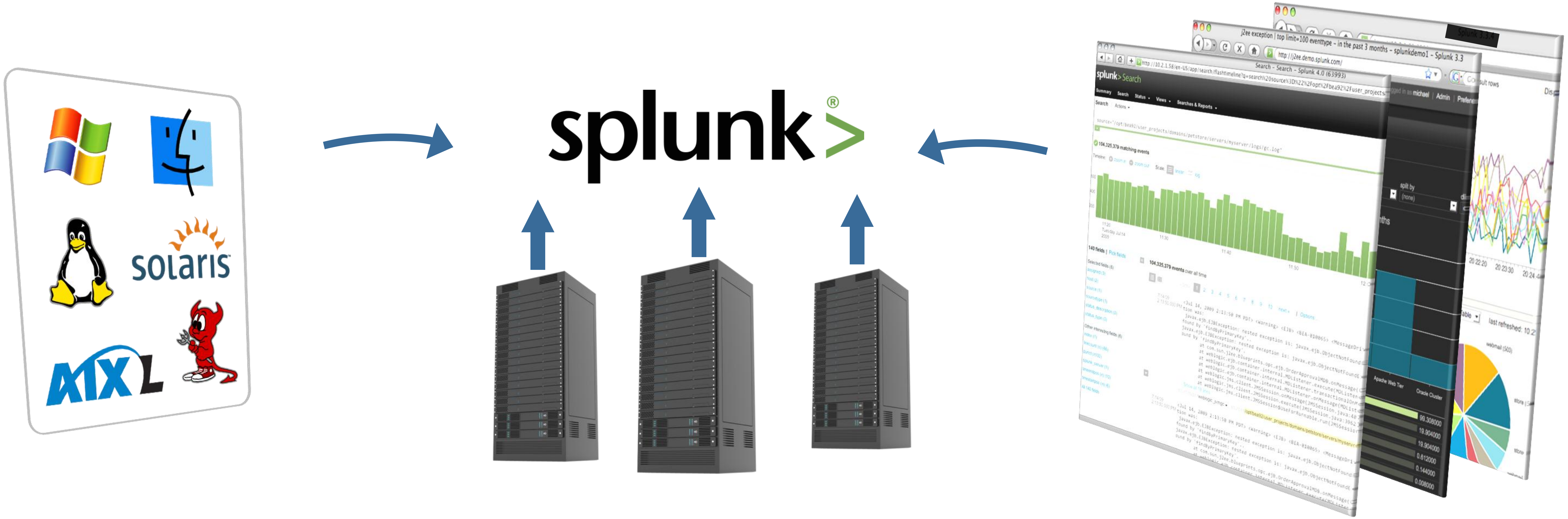
Easy to Get Started

Download and install in minutes.

1. Download

2. Eat your Machine Data

3. Start Splunking



Datacenter

How To Contact Us

WEB SITE	**www.splunk.com**	
TECHNICAL VIDEOS & MORE	**http://www.splunk.com/videos**	
DOWNLOAD FREE TRIAL	**http://www.splunk.com/download?r=header**	
CONTACT US	**info@splunk.com**	
PHONE	Worldwide:	**+1 (415) 848.8400**
	Europe:	+44 (0) 1628.509.031

SOCIALIZE SPLUNK:

- Post a question on Splunk Answers
- Find an app on Splunkbase
- Join the IRC channel #Splunk on efnet
- Become a Fan of Splunk on Facebook
- Join the Splunk Linkedin Group
- Follow @Splunk on Twitter
- Watch Splunk videos on YouTube