From: "John Farrell" <john@endgames.us>
To: "Aaron Barr" <aaron@hbgary.com>
Sent: Wednesday, January 20, 2010 3:05 PM
Attach: 2009_ARO_chapter.pdf; Topological Vulnerability Analysis Nov 09.ppt; Splunk_Executive_Brief.pdf; LE_Intel_Use_Case_03_22_09.pdf
Subject: Re: Endgames / HB Gary Federal

Aaron,
Yes, I will facilitate introductions to Bill Hornish, Splunk (former Mantech PM at State Dept) and John Williams, CEO, ProInfo (cauldron is their vulnerability analysis/management product I mentioned). I have attached their introductory briefs for your review. I have another company, ATS, but their product competes directly with Palantir. Also, LookingGlass CEO, Derek Gabbard, is someone who you should meet and discuss your model (see his attached whitepaper too).

Look forward to working with you. we're set for next Tuesday!

John

On Jan 20, 2010, at 11:24 AM, Aaron Barr wrote:

> Hi John,
>
> You mentioned a few other companies and reports I was wondering if you could send those to me. Thanks,
> Aaron
>
> On Jan 19, 2010, at 4:22 PM, John Farrell wrote:
>
>> Great meeting you. Look forward to advancing this relationship!
>>
>> Just confirmed other meeting for Wed morning. Can we do Tuesday afternoon or Wed afternoon with you and your CTO? Maybe Palantir after that. Thanks
>>
>> John
>> John M Farrell
>> VP Federal, Endgame Systems
>> 703.622.9025 M
>>
>> ----- Original Message -----
>> From: Aaron Barr <aaron@hbgary.com>
>> To: John Farrell
>> Sent: Tue Jan 19 10:46:25 2010
>> Subject: Re: Endgames / HB Gary Federal
>>
>> Sure thing.
>>
>> Greenberry Coffeehouse

>> 6839 Redmond Dr
>> Mc Lean? VA
>> United States
>>
>> From my iPhone
>>
>> On Jan 19, 2010, at 11:43 AM, John Farrell <john@endgames.us> wrote:
>>
>>> Aaron,
>>> It was good speaking with you. I look forward to meeting you at
>>> 230pm today. Please send me the address for the office or coffee
>>> shop and I'll see you there. Thanks
>>> John
>>> John M Farrell
>>> VP Federal, Endgame Systems
>>> 703.622.9025 M
>>>
>>> ----- Original Message -----
>>> From: John Farrell
>>> To: aaron@hbgary.com <aaron@hbgary.com>
>>> Cc: Chris Rouland
>>> Sent: Tue Jan 19 08:11:53 2010
>>> Subject: Re: Endgames / HB Gary Federal
>>>
>>> Can you call me and we can discuss? Thanks
>>> John
>>> 7036229025
>>> John M Farrell
>>> VP Federal, Endgame Systems
>>> 703.622.9025 M
>>>
>>> ----- Original Message -----
>>> From: Aaron Barr <aaron@hbgary.com>
>>> To: John Farrell
>>> Cc: Chris Rouland
>>> Sent: Tue Jan 19 06:56:52 2010
>>> Subject: Re: Endgames / HB Gary Federal
>>>
>>> Hi John,
>>>
>>> What does your week look like, maybe we can find some time to get
>>> together.
>>>
>>> Aaron
>>>
>>>
>>> On Jan 14, 2010, at 4:31 PM, Chris Rouland wrote:
>>>
>>>> John,
>>>>
>>>> I wanted to introduce you to Aaron Barr, the CEO of HBGary
>>>> Federal. This is a new company spun out of HB Gary focused on
>>>> classified government services in our space. Aaron may have an
>>>> opportunity to work with us on a Cayman/Corsica data feed for the
>>>> Army, as well as a few others. Hopefully you guys can get together
>>>> face to face soon in DC.

>>>>
>>>> Thanks,
>>>>
>>>> Chris
>>>>
>>>> --
>>>> Chris Rouland
>>>> CEO
>>>> Endgame Systems
>>>> chris@endgames.us
>>>>
>>>>
>>>>
>>>>
>>>
>>> Aaron Barr
>>> CEO
>>> HBGary Federal Inc.
>>>
>>>
>>>
>
> Aaron Barr
> CEO
> HBGary Federal Inc.
>
>
>

John M Farrell
VP Federal
Endgame Systems
75 5th Street Suite 208
Atlanta, GA 30308
john@endgames.us

splunk>

Executive Brief:

IT Management is Broken:
It's Time to Stop the Silo Madness

Splunk Inc. | 250 Brannan Street | San Francisco, CA 94107 | www.splunk.com | info@splunk.com

Introduction: The Rise of IT Data

IT Is Under a Lot of Pressure

At a time when it's tougher than ever to compete, the ability to use IT to achieve results is even more business critical. In 2008 IT spend reached more than $1.5 Trillion globally. [1] But 75% of the IT budget was spent on legacy systems, including support, maintenance, application troubleshooting, security and compliance. [2] Enterprises are spending far too much managing their IT infrastructures. This is draining precious resources and prevents IT from being a strategic business enabler. IT management is fundamentally broken.

The Answer is in the IT Data

The key to managing, securing and auditing IT more effectively is locked inside the data that IT systems generate. Every second of every day, hundreds to thousands of IT components record the activities of the enterprise, from the details of application transactions, to the access and use of sensitive data, to potential security attacks.

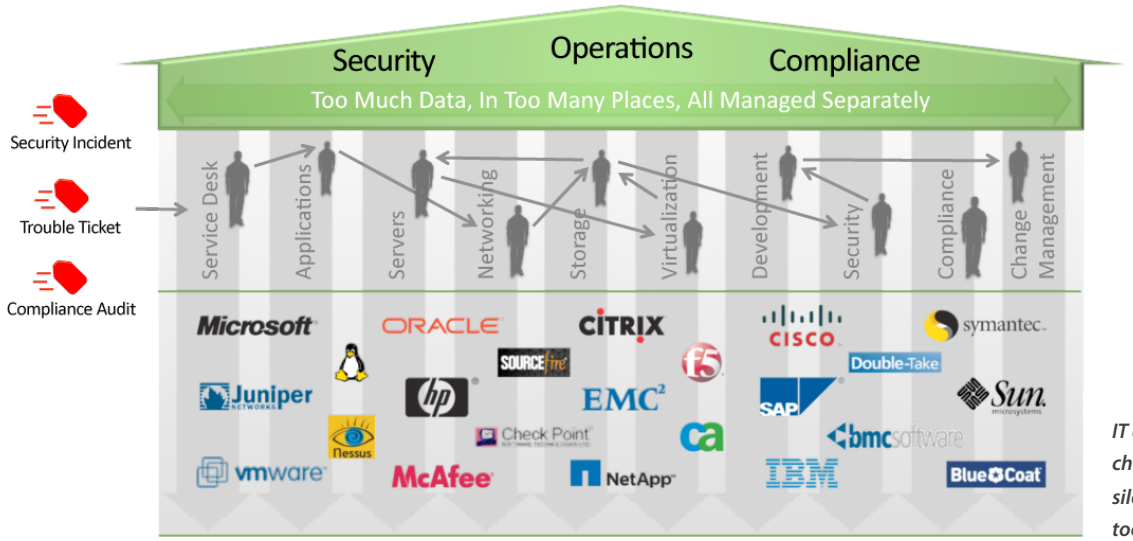
This 'IT data' is the critical source of the truth regarding what applications, servers, network devices and users have been doing. It's vital for identifying application failures, investigating who accessed sensitive data, or summarizing authorized and unauthorized configuration changes. It's also needed for maintaining and improving service levels, providing proof of compliance with regulatory and corporate governance mandates and ensuring security. The problem lies in getting to and making sense of all this data.

Existing Approaches Are Cumbersome, Costly and Don't Scale

Traditional approaches for using and analyzing this IT data are limited and locked into technology or functional silos. A separate tool is required for each type of data and every kind of task. As IT complexity increases, organizations now find themselves with many point solutions that don't work together, are expensive to maintain, and don't deliver the answers they need.

Many IT organizations have now deployed layers of high-level management systems. The idea is to gain a view across the silos, but these technologies filter out much of the essential IT data. Operations, security and compliance staff are forced to still pick through systems by hand to find the data they need to troubleshoot problems, investigate security incidents, and pull together compliance reports. It's no wonder the cost of IT management is so high and precious resources and budgets that could otherwise be spent innovating and creating competitive advantage are being squandered. The performance and efficiency of critical business functions is severely constrained by the technology and functional silos that exist.

[1,2] Forrester, Global IT Survey, 2009



IT departments are characterized by silos of systems, tools and people.

The tools we have to manage IT have not kept pace with the rapid change in technology. Innovations designed to help us maximize resources, like service-oriented architecture (SOA), virtualization and cloud computing, can't be realized due to ineffective IT management.

"The largest IT operations management software vendors, built through acquisition, have significant market share, but the product innovation needed to meet some of today's IT infrastructure challenges remains in the hands of the smaller, more-agile vendors."

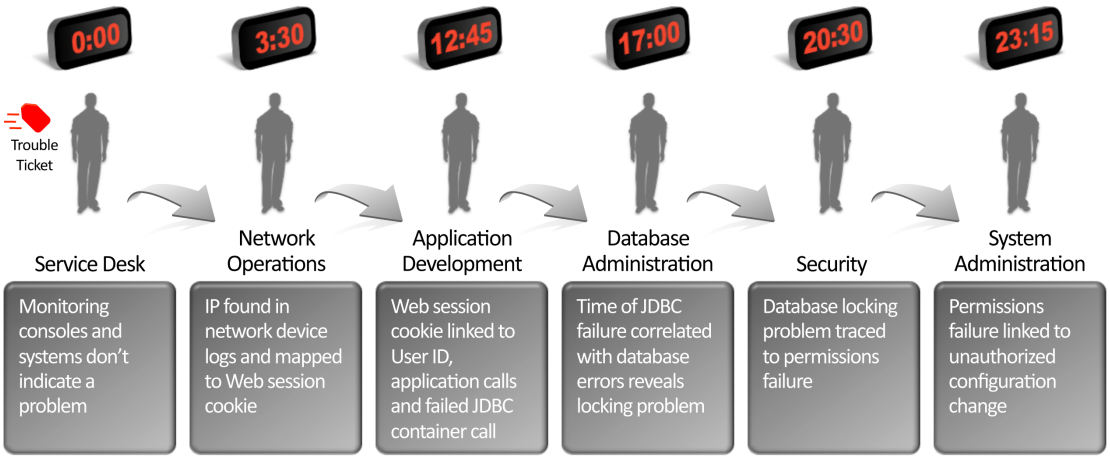
"Has Market Consolidation Killed IT Operations Management Tool Innovation?" Gartner , March 2009

The pressures on IT continue to be relentless. New paradigms such as SOA, virtualization, and cloud computing add further complexity. ITIL and ITSM stress greater accountability and governance. More sophisticated security attacks require more sophisticated protection. New regulatory and financial mandates introduce additional workload and constraints. The sheer volume and types of data generated within today's IT infrastructures is enormous and continues to multiply.

Put simply, there is too much data, generated by too many technologies, in too many locations, all managed separately. And there's no centralized way to aggregate and make sense of the data to meet the escalating operational, compliance and security needs of the business.

IT Silos Drive Enormous Inefficiencies

Time consuming manual labor-based systems create complicated, time-consuming processes. Take the scenario of troubleshooting an application problem below:



Time spent (23 hours) and silos traversed to troubleshoot a failure

Is this picture familiar? Hundreds of times a day, in every IT organization, trouble tickets, security incidents and requests for compliance audits arrive at the service desk. Lacking information, service desk staff create a ticket and escalate the issue to other teams. Silos of data, tools and processes hinder any effective collaboration, and the escalations bounce around the IT organization like a pinball from one department to another. Industry analyst firm, Forrester Research, estimates 74% of service desk issues are escalated beyond Tier 1 staff. [3]

Manually traversing these silos of data takes hours or days, when in fact the business needs answers in seconds. It's no wonder 75% of IT budgets are spent managing and maintaining existing applications and infrastructure.

In today's scale out, virtualized and dynamic IT environments, achieving better results requires thinking differently. Managing and monitoring individual IT technologies or functions is no longer the problem. It's now the interaction between technology and functional silos that affects downtime, obscures new security threats and makes it time consuming to audit activities. What is not visible in one silo is often only discoverable when looking across multiple layers of the technology stack and IT functions. A dramatic shift in the approach to integrating data and achieving visibility across IT silos is required to eliminate massive inefficiencies and ensure that the right information is available to the right people at the right time.

[3] Forrester - Enterprise Software Trends 2009

Re-thinking the Problem: Taking Advantage of Your IT Data

The Answer is Within Reach. Getting to the Core of the Problem

IT data represents its own critical layer of information with the enterprise. Similar to operational and transactional data used to optimize supply chains and back offices, being able to harness IT data and see between the lines is now a competitive IT requirement.

The ability to use and analyze all the IT data from one place helps IT help the business in significant ways:

- See how customers are really using your services
- Observe service performance trends
- Support more comprehensive compliance controls
- Improve your IT security posture
- Develop and maintain applications more effectively
- Discover where to enforce better processes
- Drive IT as a service
- Prepare for known bottlenecks

Re-thinking the problem starts with understanding the data. The IT data generated by applications, servers and network devices is different from the structured business data typically managed by a database. IT data is different. IT data exists in many different places, in many constantly changing formats, and is created with an increasing velocity as IT scales. Much of the data needs to be retained for extended periods of time, from months to years, driven by internal and external mandates. All of this makes the task of managing IT data a new and difficult challenge. How can organizations quickly and efficiently process vast amounts of unstructured IT data intelligently, to deliver the useful results it needs?

Getting the Insight You Need

Splunk is software that revolutionizes how enterprises manage IT data. Splunk collects, stores, indexes and secures massive amounts of IT data in real time. Operations, security, compliance and even business owners can search, alert, report and analyze IT activities reducing what used to take hours or days to minutes. Splunk works with any application, server or network device and scales to terabytes of IT data cost effectively.

Splunk makes all an organization's IT data available for a variety of IT functions from application management, security, and compliance, to virtualization. With all the IT data indexed together, departments and functions no longer need to operate as independent silos with their own limited views. For the first time, organizations can use and analyze all their IT data from one place in real time, regardless of source, format, location or size.

Splunk introduces powerful capabilities to address multiple functions of IT.

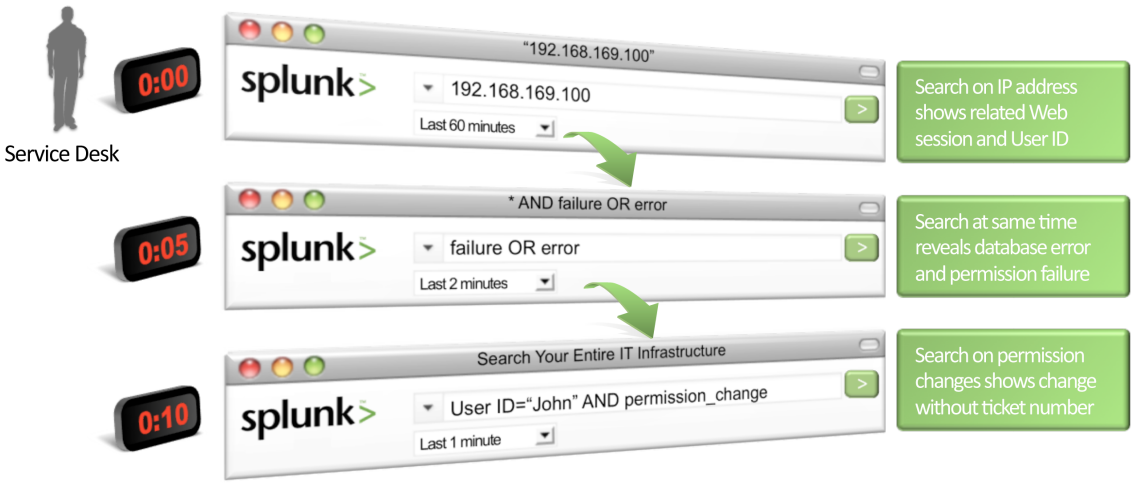
Here's how Splunk is used to deliver immediate and ongoing value:

- Start by indexing real-time data from all tiers of the IT stack – metrics, logs, events, traps, alerts, configurations, changes and more.
- Users report almost immediate payback using Splunk to search and investigate the root-cause of performance problems, application failures and security incidents.
- Splunk enables Tier 1 personnel to diagnose routine issues, eliminating many costly escalations. Customers report eliminating up to 65% of escalations.
- Users can share their own knowledge about the IT environment – identify common sources, hosts and events, add structured fields such as response time and identify thresholds to make their Splunk installation and the entire IT team smarter.
- Repetitive searches and tasks can be automated providing monitoring and notifications of specific conditions or complex activities.
- Statistical searches and charting enable users to build reports, dashboards and create a birds-eye view of service levels, traffic patterns, security threats, compliance posture, and more.
- Finally, as users get more productive, they get more proactive – searching, trending and filtering the IT data to identify problems and gain insight into system behavior.

In the Trenches with Splunk

With Splunk, the process of identifying problems, investigating security incidents or reporting on compliance activities is radically simpler and more directed, delivering results dramatically faster, while respecting organizational control boundaries.

In the previous example, troubleshooting an application failure resulted in an escalation to network operations, application development, database administration, security and then systems administration. Because Splunk provides a unified approach to navigating all the IT data, the Service Desk is able to search on a combination of IP address, database errors and permission changes to correlating diagnostic information across different silos of data. The initial scenario is a typical example using traditional silo tools and approaches. Using Splunk, the time to identify root-cause is reduced from an entire day to minutes.



In the trenches and troubleshooting with Splunk takes just minutes.

Scaling Across the Enterprise

Splunk works differently. It breaks down the traditional technology and functional IT silos and arms network engineers, system administrators, security and compliance analysts, developers, customer support, help desk staff, and even business users, with an immediate understanding of what's happening and what happened (the ability to replay a snapshot of the past) across the IT environment. These new capabilities: finding relevant information quickly, capturing knowledge on the go, and automating manually intensive processes, deliver powerful enterprise-wide utility across all IT departments and functions.

With Splunk there is no more logging into every application, server and network device to understand what's really happening. Organizations can quickly and cost-effectively turn all IT data into valuable and accessible information assets.

Dramatic Payback: See Value Immediately

Focus on the Users

The boundaries of technology and functional silos blocks IT's ability to operate efficiently and meet the needs of the business. At a time when organizations must drive more value from IT, they are demanding even greater value and performance from their IT spending. Enter Splunk.

Splunk is a new approach to managing, securing and auditing your entire IT infrastructure. Provided as a free download or low-cost enterprise license, Splunk is simple to deploy, scales from a single server deployment to global large-scale operations, and delivers immediate payback.

The power of the Splunk approach is the exponential value it delivers to users and to the business. IT data is vast in volume, unstructured, dynamic and held captive in silos of traditional point solutions. Splunk invented a new approach to managing IT data and unlocking its enormous value. By using Splunk as the engine to index, search and analyze all of this valuable IT data from one place in real time, users are changing the way they do their jobs and elevating the role of IT in their organizations.

Increased Productivity

Users experience significantly higher productivity using Splunk in the following ways:

- Doing their jobs much faster, from troubleshooting issues to investigating security investigations.

> *"We used to spend hours troubleshooting. Now Splunk does the troubleshooting in seconds."*
>
> **– Voxeo**

> *"With Splunk we can complete security investigations in 1.5 hours versus the 1.5 days it used to take to find the log data we needed just to **start** the investigation."*
>
> **– California ISO**

> *"Splunk means cutting our MTTR in half, and we don't have to escalate beyond first tier agents. Splunk translates to cost reductions and keeping our business running at a higher standard."*
>
> **– Dow Jones**

> *"It's easy to centralize our IT data into Splunk, enabling admins, developers, the monitoring team, anyone in IT, to securely access they data they need to solve problems more quickly."*
>
> **– T-Systems**

- Avoiding escalations so the Tier 1 service desk can resolve issues faster, and on their own.

  "Splunk reduced our escalations by 90% and our problem resolution time by 67%."

  – Vodafone

- Improve levels of automation, by monitoring for early warning signs on your applications, servers and network devices.

  "We use Splunk for our change monitoring requirements. Splunk's change management application does this more efficiently and with better functionality." **– Monash University**

Improved Uptime, Revenue and Customer Satisfaction

Businesses experience more uptime, less revenue disruption and happier customers.

- Reduce mean time to resolving issues and incidents causing downtime.

  "When we peak at 130 orders per minute, downtime is not an option. With Splunk we can zero in on a problem in seconds. Our speed of problem resolution has increased 5x. For the first time in six years, we had zero downtime on Macys.com during the peak holiday shopping season."

  – Macy's

- Find and resolve problems before they affect your customers.

  "Splunk gives our customer service, NOC staff and network engineers comprehensive real-time event data for incident response, chronic problem identification and optimization." **– BT**

  "Splunk' s transaction search enables my team to quickly determine if a trade was executed. It's so fast they can do it while the broker is still on the phone." **– Nexa**

  "Thanks to Splunk, our application issues are identified and resolved before they become problems that affect our systems, transactions and customers." **– Freshdirect.com**

- Resolve customer issues faster.

  "It used to take hours, even days to track transactions for some customers. Now our Tier 1 support can respond to inquiries in seconds – while the customer is still on the phone."

  – Pegasus Solutions

Higher Service Levels for the Business

Businesses drive service-level excellence and implement more complete compliance and security at lower cost.

- Automatic monitoring for early warnings and faster MTTR ensures less downtime.

> *"Splunk allows us to quickly consolidate and correlate disparate log sources, which in turn allows sophisticated monitoring and response previously thought impossible."*
>
> **– Cisco**

- Demonstrate compliance faster and with less effort by monitoring all your IT data and rapidly responding to ad hoc auditor requests.

> *"Failure to comply with PCI equates to failure for our business. Splunk enables us to demonstrate compliance across all PCI DSS requirements."*
>
> **– Gala Coral**

> *"The QSA auditors loved Splunk. We can generate ad-hoc reports to track any transaction or user activity they want to see and easily show we are PCI compliant in minutes."*
>
> **– Carlson Marketing**

- Improve protection by detecting attacks, fraud and insider threats that previously went undetected.

> *"Splunk is faster, provides a more comprehensive view and is more efficient than SIEMs or log management. We look for more advanced security risks that traditional tools may not find."*
>
> **– Booz Allen Hamilton**

> *"Splunk's ability to collate and report on any log file or data stream helps us detect and investigate fraudulent activity quickly."*
>
> **– Gala Coral**

A Growing Family of Users

More than 1,000 licensed enterprises, service providers and government agencies and over 300,000 users worldwide use Splunk. This includes hundreds of Fortune 1000 companies who are realizing the value of Splunk to meet strategic business and IT initiatives, companies such as:

21st Century Insurance, Aetna, BEA, BT, Catholic Healthcare West, Chevron, Cisco, Comcast, Dow Jones, LinkedIn, Motorola, MySpace, NASA, Orbitz, Raytheon, Riverbed, Shopzilla, T-Mobile, Telstra, Verisign, Verizon, Visa, and Vodafone are achieving higher availability, investigating security incidents in record time, and meeting compliance requirements at lower costs with Splunk.

Recognized by the Industry

In addition to an increasing base of enthusiastic customers, users and partners, the leading industry analysts have also taken notice of Splunk.

> *"Splunk is predictive and forward thinking. Splunk helps you understand what's happened, what's happening, and what's likely to occur."*
>
> **– David Williams, Research Vice President, IT Operations and Enterprise Management, Gartner**

> *"The sky is the limit on what you can do with Splunk."*
>
> **– Glenn O'Donnell, Senior Analyst, IT Infrastructure & Operations, Forrester**

> *"The Splunk offering is so far ahead of the curve in addressing diagnosis, RCA, and Continual Service Improvement."*
>
> **– Liam McGlynn, Senior Analyst, IT Management, EMA**

> *"Splunk is awesome: it's multi-platform, easy to install and easy to use. And with an abstraction layer of logs, configuration files and system messages, traps and alerts, it's seriously useful."*
>
> **– Nick Selby, Research Director, Enterprise Security Practice, 451 Group**

A Different Type of Software Company

Splunk was conceived to fill a technology void. The company's founders, all with extensive IT management and datacenter backgrounds, created software they wanted to use and a business model that was transparent and innovative.

Splunk is available as a free download. It runs on a plethora of operating systems and installs in just a few minutes. Documentation, support and the product roadmap are open to the entire user community. Customers can see the value of Splunk for themselves. As their needs evolve and as they see the tangible value of Splunk, they can choose to upgrade to an enterprise license, which offers additional features, higher capacity and global 7x24 support.

At a time when businesses need every competitive advantage and IT is challenged with doing a lot more with a lot less, Splunk offers a radically different approach. Splunk IT Search empowers organizations to massively improve the efficiency of IT, by delivering relevant information, to the people who need it, in less time and with fewer resources.

For more information on Splunk, give us a call +1-866-GET-SPLUNK, send us an email info@splunk.com or please visit our website: www.splunk.com