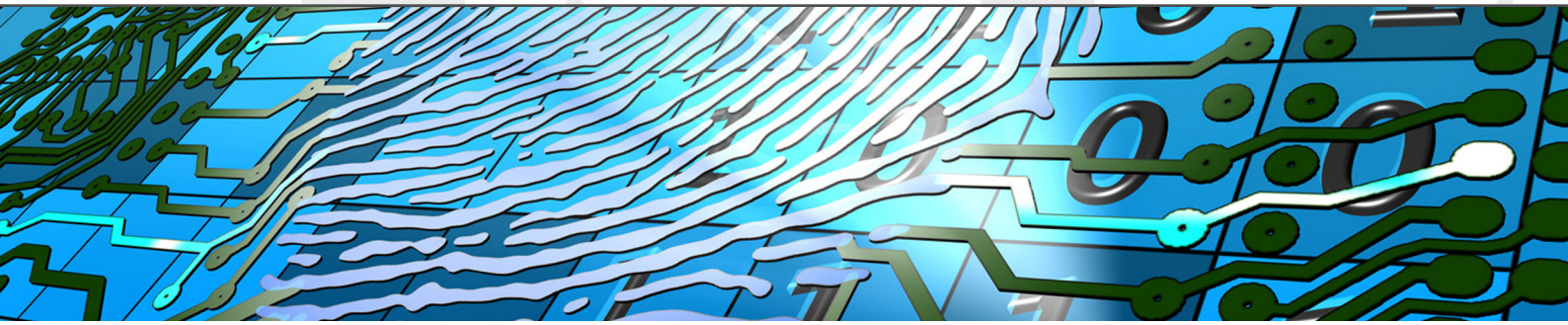
dotSec
dot com security

Customer case study: Superannuation business gains operational visibility and proactive monitoring



Background and Challenges

Our client is an award-winning, top-10 Australian superannuation company with a focus on providing leading and innovative on-line services for its personal and business customers. The business relies heavily on its information processing infrastructure, which is constantly evolving in order to support new and innovative business models, and which needs to remain secure, lean and responsive.

Our client's information processing infrastructure is heterogeneous, and includes core Unix servers, and hundreds of supporting Linux and Windows servers, most of which are virtualised. The business supports an aggressive and agile program of innovative application development, and hosts a number of sophisticated n-tier, Internet-facing applications for business and personal customers.

Executive Summary

Business challenge
Improve efficiency and reduce ongoing costs by gaining an improved understanding of, and additional insights into, various business operations.

Solution
Deploy Splunk and integrate it with a range of core services, so as to gain a holistic view of the entire business.

Results
Greater efficiency and reduced issue-resolution time, greater ability to identify and address process and technology issues, before they escalate.

The Solution

The IT operations team already understood the need to maintain a holistic understanding of the entire computing environment, but they were unsure of how to achieve that goal.

DotSec deployed a Splunk infrastructure that was able to collect hundreds of gigabytes of logging data from hundreds of heterogeneous systems, from a range of core services, and from an increasing number of applications. The infrastructure takes advantage of Splunk's search-head clustering (which appeared in Splunk 6.2) to provide faster searching through horizontal scaling, and high-availability through service replication.

Thanks to the Splunk deployment, it is now possible for the operations team to quickly identify and understand system issues, anomalies and relationships. In particular, it is much easier to understand the causality and correlation between events that occur across the distributed components of the

organisation's n-tiered web-application environment. That means that issue resolution for customer-facing systems has become far less time-consuming and costly to the business.

Other areas of the business have also been able to capitalise on the new Splunk infrastructure. For example, when deploying a new business to business gateway (a major development and integration project) the gateway team was able to use Splunk to solve integration issues that may not otherwise even have been identified. Similarly, the executive team is now presented with a consistent overview of the organisation, thanks to DotSec's deployment and integration of a Splunk mobile access server.

The Outcomes

By gaining a better understanding of the operations of the business, our client was able to achieve a number of important outcomes:

- Improved efficiency. The underlying issues that give rise to operational shortcomings can be quickly identified and addressed. The business can easily see the status of core services and identify issues in customer-facing systems far more effectively than was previously possible.

- Improved operational oversight. The business can quickly see where operational issues exist, before those issues escalate and get out of hand. Daily, weekly and on-demand reports allow management to quickly gain an understanding of the operations of the entire computing environment.

- Reduced time and associated cost. The mean time to resolution is reduced because events across disparate systems can be correlated and analysed with real-time queries and reports. Long gone are the days of tedious, time-consuming (and therefore expensive) manual log collection and analysis

- Support for various business units. The new Splunk deployment provides benefits for a range of business units. The security and compliance team can use the new Splunk infrastructure to quickly understand the security status of hundreds of servers; the software development team can use the same infrastructure to identify and debug application issues; and the operations team can use Splunk to review the completeness and effectiveness change management and change control processes.

The Next Steps

DotSec has many years of commercial Splunk experience, we are Splunk certified (including Splunk 6 Architect certification) and we use Splunk in-house as well. Get in contact with us now, to discuss how improved business intelligence will provide immediate and real benefits to your business.

splunk> CERTIFIED ARCHITECT V.6

DO MORE BUSINESS, MORE SECURELY

https://www.dotsec.com/
+61 7 3221 2442
enquiries@dotsec.com
Level 2, 303 Adelaide St.
Brisbane. QLD. 4000