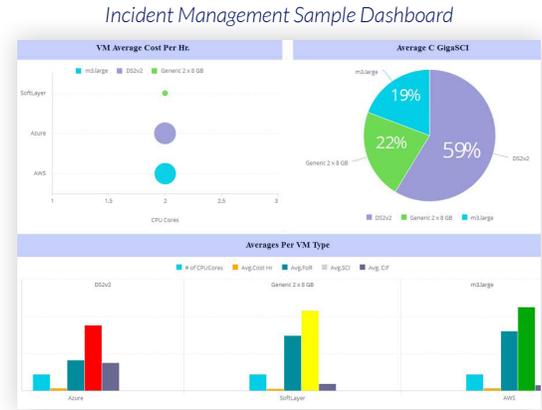




DATA ANALYTICS

Data value plays an integral part in driving top-level decision making for enhancing applications, products, operations, and securing intellectual property.

- Identify and increase monetary value
- Measure and improve end user experience
- Tier and manage data relative to the risks



Use Cases and Challenges

Outcomes and Benefits

Limited to No metrics and reporting with current IGA, PAM, SIEM, Vulnerability Management, and other types of Cyber-Security Tools/Technologies.



Eliminates the need of disparate metrics and reporting by accurately depicting changes and impacts to security violations, exceptions, entitlements, alerts, and application security with automated-on-demand dashboards that updates when data changes.

Complexities and constraints associated with GRC, incident, and change management metrics and reporting (i.e. Archer, ServiceNow, Remedy, Home Grown).



Achieves data accuracy and relevancy by saving at least 8hrs of time typically associated with manual scrubbing and right sizing of data and eliminates the need of using Excel and other third party tools.

Inability to extract data, translate the data, and provide monetary value relative to business operations and lines of business that are tasked with revenue growth and expansion.



Predictive analytics through recognizable patterns, linear and non-linear regression improves insight into business trends, market trends, end user experience and operational management by approx. 5x while consistently meeting SLAs, enhancing MTTR on average by approx. 4hrs, and increasing ROI.

Taking disparate data sources such as Financial, Marketing, Vulnerability Management, IAM, Application Performance, Third Party Risks, and depicting risk metrics (qualitative and quantitative, KRIs, KPIs, SLAs) relative to products and applications that account for X% of the business revenue.



Easily ingests, converges, models, correlates, classifies, rationalizes, visualizes, and translates how identities, vulnerabilities, performance, and cyber-security threats instantaneously puts lines of business revenue and the company brand at risk.



DATA ANALYTICS

What We Do

Due to data becoming unnecessarily complex, sprawled, and silo'd, we bridge the gap by integrating and converging traditional Business Intelligence Data with Information Technology/Cyber-Security data. BNS UEP provides data analysts, data architects, and software engineers for developing the UX and UI relative to the identified data sources, data models, and data outcomes relative to your data environment and data lifecycle.

How We Do It

Our mantra is to simplify your data by making it comprehensible, relevant, and usable. BNS takes a hybrid architecture and engineering approach by aligning with your budget, use cases, current constraints, and expected target state outcomes. We collaborate with our clients in identifying and defining business, performance, security, and risk management drivers by utilizing our experience in data analytics along with our patented data modeling methodology.

Why It Matters

BNS UEP provides efficiency, precision, and expediency by baselining and distilling massive amounts of data, which decreases the time it takes to discover, ingest, model, correlate, classify, rationalize, and visualise your data. As a result, this provides data relevancy, data security, operational efficiencies, and greater ROI. This is translated into interpretable and customizable visual dashboards depicting monetary value, risk based metrics, and end user experience relative and relevant for your business and cyber-security needs.



EMPOWERING PROGRESS

We're a technology research and development organization that brings together responsible, efficient, and sustainable solutions through Unified Enablement Partnerships (UEP) to deliver best of breed services in every vertical.

Learn more at bnsuep.com or email info@bnsuep.com