Technology Solutions to Support the Warfighter & the Mission

From AI to data management and analytics to cybersecurity, we are working to fundamentally transform the Department of Defense into a cognitive enterprise.

ibm.com/federal

Your Private Beach at the Data Lake

Making Data Accessible & Quickly Available

Many organizations struggle to quickly get value from data; IT is less than responsive, finding valuable data is perplexing at best. Getting trusted access to trusted data is a never-ending battle. Imagine if you had your own "Private Beach"— not the perfect grilled burgers and ice-cold beer type — but the kind where you and your invited guests have on-demand services to connect, organize and analyze your sensitive raw data alongside the wide range of data from across your enterprise. And only if you want: you can share what you want, when you want, with whom you want. OK, then; it's time to get this data party started.

Data Risk Management & Data Protection

There is a thriving market dealing in stolen information that is critical to the mission and survival of the organization. These assets, that can include "Crown Jewels" data, are inclusive of Personally Identifiable Information (PII), intellectual property and mission-related data, product/project designs, financial information, and more. A combination of robust data security tools — IBM Data Risk Manager and Guardium Data Protection — can provide organizational leaders and their teams a mission-consumable data risk control center. Additionally, it can offer smarter data protection that will help uncover, analyze and provide an intuitive at-a-glance visualization of data-related organizational risks so they can take the actions necessary to protect their mission.

Join IBM for Featured Presentation

Zero Trust & Data Protection

Monday, August 26, 2019 | 10:30am | Riverview 1

John Dombroski, *Security Systems Cybersecurity Specialist, IBM*

Cyber Security continues to evolve as technologies and attack methods change. The concept of Zero Trust in Cyber Security has the potential to provide better security across the enterprise. Specific to this talk, we'll discuss Zero Trust and the factors that ensure data security.

The first factor is the location of the data. Many enterprises are now looking to move data storage into the cloud. While moving data into cloud storage may make the administration and cost of data management less of a burden, it is important to note the responsibility for the data security still remains with the enterprise that collects it.

The second factor is the classification of the data. Not all data carries the same weight. Tooling exists to crawl unstructured and structured data to find sensitive data. Based on your findings, the enterprise can apply the necessary regulatory or internal policy for data security.

The third factor is access to the data. Many breaches occur at the hands of privileged users with direct access. These users need to be monitored. Additionally, users should only be given the privileges necessary to perform their job. Account privileges should be reviewed periodically to maintain least privilege.

As enterprises move from the Industrial Age to the Information Age, data becomes the key "natural resource" that enables this transition. The Zero Trust model allows enterprises to ensure data security and the ability to transition into the digital-driven future.

Join us in Booths 412 and 414 to learn how IBM can help you better support and secure the mission.