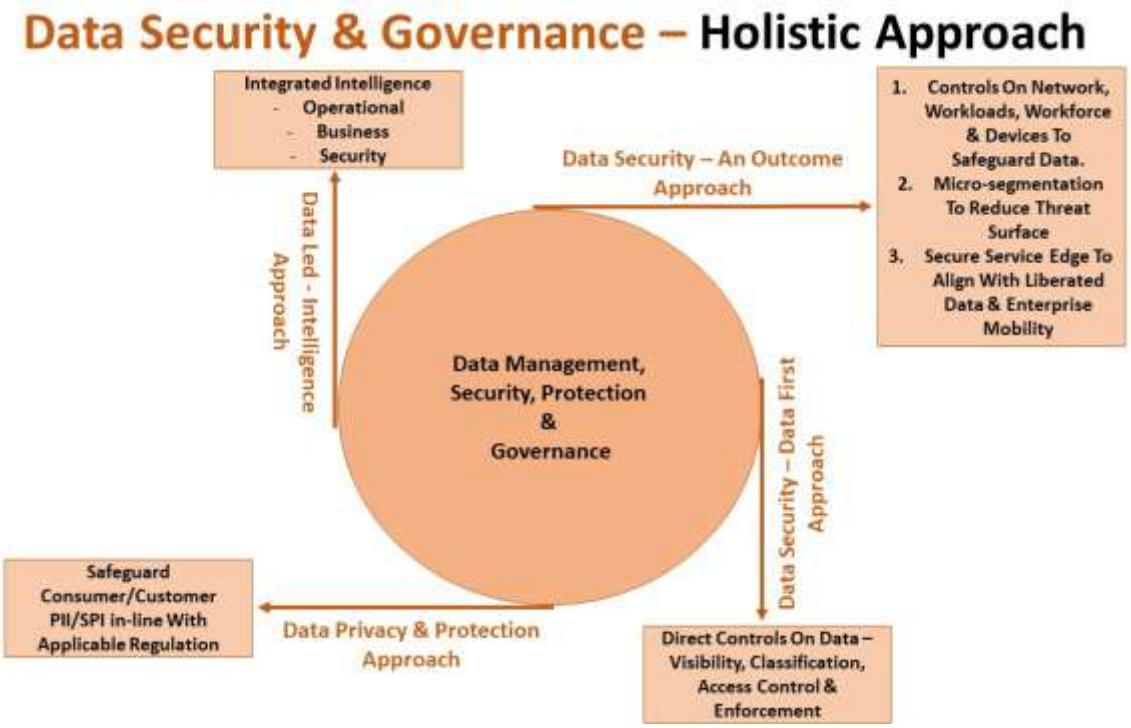
Joined-Up Approach To Fortify Enterprise Data

With the rise of digital led businesses and the increasing interconnectedness of systems, organizations now generate and collect vast amount of data. This data holds valuable insights and information that can be leveraged to improve customer experience, guide innovation, architect compelling products, improve operations, and gain competitive advantage.

While the enterprises are learning to effectively use this "Business Tool" to their advantage, other dimensions of Data**, especially Data security and governance have to be embraced & mastered holistically to address "Business Risk".**

Different approaches are being adopted by the enterprises to safeguard their Data, and these vary based on industry vertical; type, location, size & scale of Data Stores; prevailing organization readiness & Business Risk appetite to name a few.

This paper covers different approaches and dimensions of Data to improve Data Management & Posture of an enterprise.



Data Security - An Out-come Approach

This approach started right with the on-set of Cyber Security in late 1980s, and has successfully safeguarded enterprises against many Cyber Risk generations – Viruses to Network anomalies, to Application compromises, to Multi-Vector & Advanced Persistent Threats.

The approach has multiple propositions, but fundamentally hinges around fortifying enterprise perimeter, with controls across Networks, Applications, Devices & People to safeguard DATA.

The traditional Castle & Moat model has been extremely successful proposition for many years to safeguard enterprise Data in the centralized model, where entire traffic backhauls to the central Data Center.

Data liberation & enhanced mobility challenged the Castle & Moat model, which is being fast replaced/augmented by Secure Access Service Edge(SASE) in last few years, and the transition has further caught pace during and post pandemic. SASE is a decentralized, cloud-native architecture, which leverages a network of globally distributed points of presence (PoPs) to provide security controls and network services closer to the enterprise users.

To further strengthen the security controls in this approach, a net new technology aligned with “Zero Trust Frame-Work”, named Micro-Segmentation has been making significant contribution in safeguarding enterprise Data.

In summary, this approach has served well over the years, and continues to be relevant with newer architecture and technology in eventually securing Data, but lacks direct Data controls. Thus any gap in Network, Application, Workforce or Device controls, can lead to un-authorized Data access & significant business loss or disruption.

Data Security – Data First Approach

In this unbound Data driven economy, where enterprise Data is all pervasive, users work from anywhere, and internal threats are all time high, having layered security approach to protect data is inevitable.

Direct Data controls provide additional layer of security and granular Data protection. To achieve this approach, enterprises need to work on visibility of sensitive data, associated user access, and continuous activity observability across all Data stores- SAAS (sales force, google drive, teams, box, MS-365, Zoom, Slack), On-Prem, Directory Servers (AD, Azure AD), Structured Databases, Network Services (DNS, VPN, Proxy) etc.

The approach kick-starts with identification & classification of sensitive Data across enterprise estate, followed by assignment of appropriate Data ownership and access

control to reduce Blast Radius. The final step before continuous monitoring & anomaly detection is to enforce enterprise data polices backed with DLP, Encryption, Data masking technologies etc.

Tools supporting automation right from identifying sensitive data, to classification, to high-lighting unusual Data access patterns, and suspicious activities can fast-track organization's journey to achieve this approach.

To summarise, "Data Security- An Outcome Approach" alone is not enough to safeguard enterprise Data in this Contemporary Risk scenario. Achieving DSPM (Data Security Posture Management) alongside SPM(Security Posture Management), Attaining DAC(Data Access Control) besides Access Control, Engineering Data Detection & Response together with xDR/MDR, and establishing SSPM (SAAS Security Posture Management) in parallel with Infrastructure posture management is the way to attain ideal outcome.

Data Privacy & Protection Approach

Many countries and regions have enacted data protection laws and regulations to safeguard individuals' privacy rights. Organizations that handle personal data are required to comply with these laws, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), and in India we formally have "Digital Personal Data Protection"(DPDP) law, which has replaced earlier frame-work for Data Protection based on article 43-A of Information Technology (Amendment) Act, 2008. Non-compliance can result in significant financial penalties (varies from country to country) and damage company's reputation.

Data Privacy and Protection fundamentally focusses on Individual's right to keep their personal information (name, address, financial information, PAN card, Aadhar card) private, and ensure that Data Principals are consented as to how and why their personal Data is collected, used, shared & protected.

Complying to the norms starts with understanding the present state of enterprise readiness, and comprehensive efforts are involved in the following core pillars:

1. Visibility of Personal Data
2. Information Usage & Access Control
3. Data Privacy Organization
4. 3rd Party Contract Management
5. Privacy Awareness & Training
6. Personal Information Security
7. Privacy Monitoring & Incident Response
8. Alignment with Regulatory Norms of Appropriate Geographies

In Nut-shell, concerted effort to address data privacy and protection are vital to safeguard individual's rights, prevent identity theft, comply with regulations, mitigate data breaches.

Data Led – Intelligence Approach

Enterprises have been leveraging structured and un-structured Data from all possible Data sources to build comprehensive intelligence, whether from Operational or Business in-sites perspective.

Specialized platforms are being deployed to ingest, normalize & model Data to analyse and visualize in-sites, both on real-time and historical basis.

While the real-time observability is used for proactively managing any potential degradation or disruption in IT Systems, Networks & Applications on one side; on the other side, historical Data enables decision-makers to take informed actions based on trends & patterns. This reduces reliance on intuition and gut feeling, leading to more effective and de-risked business

Besides Operational and Business Intelligence, "Data Led – Intelligence Approach" has evolved traditional **Static Security Operations,** based on limited Data capability of an SIEM to **Next Generation Cyber Command Center (NGC3)**, where Security Data Lake is one of the four core pillars.

NGC3 is based on collecting and integrating data sources from structured and un-structured stores - Logs, network traffic, endpoint & cloud telemetry, threat intelligence feeds. It then leverages advanced analytics and machine learning techniques to process large volumes of security data with multiple Data sets (long-term and real-time storage) to identify patterns, anomalies, and potential threats.

These technologies enable NGC3 to automate threat detection, perform behavioural analysis, and detect sophisticated attacks, which may go unnoticed with traditional security approaches.

To sum-up, holistic approach to enterprise cyber security is suggested to be based on Data being the cynosure. Its possible to methodically progress to achieve desired state by considering all dimensions of safeguarding Data, and proportionately integrating them with appropriate mix.

Authored By : Silicon Comnet Pvt. Ltd.