Data-centric security solution prioritize safeguarding data itself over traditional perimeter defenses. It focuses on data classification, encryption, and granular access controls. By securing data regardless of its location or the underlying infrastructure, organizations can mitigate the risk of data losses and unauthorized access, maintain data integrity, confidentiality, and compliance with regulatory requirements, fostering a robust cybersecurity posture in an increasingly interconnected and data-driven economy environment.

Achieve the “Unachivable”

Stopping future data loss and ensuring compliance with data-centric approach

APF Technologies LLC

ACHIEVE THE "UNACHIEVABLE"

STOPPING FUTURE DATA LOSSES AND ENSURING COMPLIANCE WITH DATA-CENTRIC APPROACH

In today's digital landscape, data breaches have become a pervasive threat, causing significant financial losses, reputational damage, and privacy concerns for individuals and organizations alike. Despite advancements in cybersecurity measures, traditional approaches have proven inadequate in stemming the tide of data breaches. However, by challenging conventional wisdom and embracing innovative strategies, a groundbreaking solution emerges—one that is revolutionizing the way we safeguard sensitive information. This white paper explores the concept of data-centric security solutions as a proactive approach to safeguarding critical data assets. By focusing on data protection at its core, organizations can mitigate the risk of data breaches, ensure compliance with regulatory mandates, and enhance their overall cybersecurity posture.

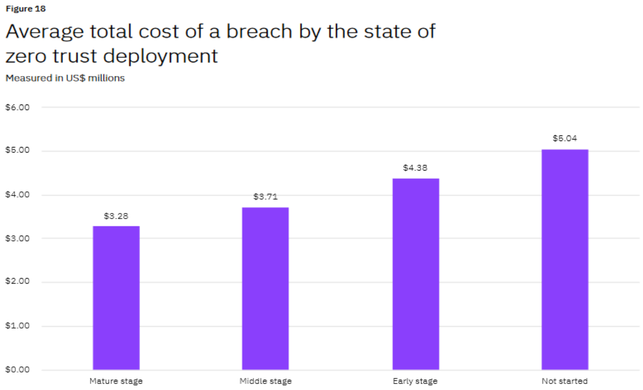
STOPPING DATA BREACHES IS A NECESSITY, NOT AN OPTION

Data is the new oil in the digital economy, fueling everything from product development to customer service. The proliferation of technologies has revolutionized the way organizations collect, store, and utilize data. However, this digital transformation has also exposed organizations to unprecedented cybersecurity risks, including data breaches, ransomware attacks, and insider threats. Chinese hackers penetrated the email accounts of Commerce Secretary Gina Raimondo and other State and Commerce Department officials in the weeks before Secretary of State Antony J. Blinken traveled to Beijing in June 2023.

Stopping data breaches are now seen as the holy grail of cyber defense, because the increasing frequency and sophistication of cyberattacks have rendered traditional cybersecurity measures insufficient in protecting valuable data assets. From large-scale data breaches at multinational corporations to targeted attacks on governments, the ramifications of data loss are profound and far-reaching.

Cyber criminals target the critical data assets because they can monetize the stolen data for profit, which in turn finances more cyber-attacks. Breaking this financially self-sustained positive feedback loop will slow down the advancement of cyber criminals and eventually stop cyber-attacks. To quote Uncle Ben to the young Peter Parker (Spider-Man), "With great power comes great responsibility." Data breaches have to be stopped, now, even though it seems unthinkable.

Soon after the SolarWinds attack, the National Security Agency (NSA) admits that emphasizing on perimeter defense cannot be sustained, because for organizations, *"…a breach is inevitable or has likely already occurred"* (NSA). IBM came to the same conclusion in its 2022 edition of *"Cost of a Data Breach Report"*. The report, for the first time, provided the evidence that the Zero Trust implementations that zero in on network and device security like Zero Trust Architect (ZTA), fell far short to stop data breaches. Thirty-five percent of reporting companies that had either fully or partially implemented Zero Trust programs lost an average of $3.2 million from what might be considered a *"run of the mill"* data breach, which is a very disappointing result for a cybersecurity approach that carries very high hopes as the chosen one to prevent next much more sophisticated *"SolarWinds"* type attacks.

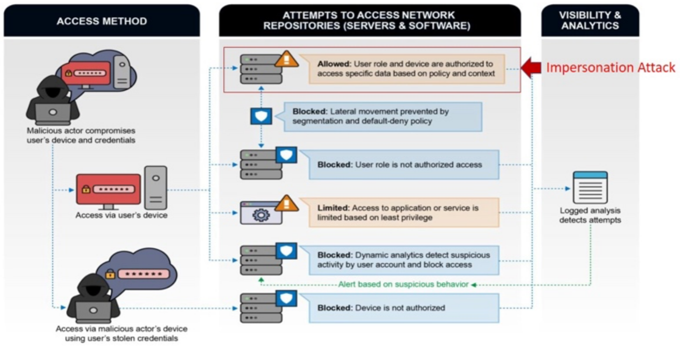


Source: IBM, "Cost of a Data Breach Report" 2022

NSA doesn't believe ZTA is enough to stop adversaries at the door, so it promotes the data-centric security solution that prioritizes the protection of critic data over ZTA' securing access to resources. *"The Zero Trust security model assumes that a breach is inevitable or has likely already occurred … data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources" (NSA).* The CISA of Homeland security and Department of Defense has taken the concepts of full encryption, data tagging, data classification and rights management at file level from the data-centric solution, and built them into their respective roadmaps as far-reaching goals.

UNDERSTANDING DATA-CENTRIC SECURITY SOLUTION

Data-centric security solutions prioritize safeguarding data at its source, focusing on encryption, access controls, and monitoring mechanisms to ensure its confidentiality, integrity, and availability. By classifying data based on sensitivity, importance and compliance contents, and applying appropriate security measures, organizations can prevent unauthorized access, mitigate the risk of data breaches, and maintain compliance with regulatory requirements. Key components of data-centric security include data classification, encryption, access controls, data loss prevention (DLP), and behavioral analytics.


ACCESS METHOD
ATTEMPTS TO ACCESS NETWORK REPOSITORIES (SERVERS & SOFTWARE)
VISIBILITY & ANALYTICS
Malicious actor compromises user's device and credentials
Access via user's device
Access via malicious actor's device using user's stolen credentials
Allowed: User role and device are authorized to access specific data based on policy and context
Impersonation Attack
Blocked: Lateral movement prevented by segmentation and default-deny policy
Blocked: User role is not authorized access
Limited: Access to application or service is limited based on least privilege
Blocked: Dynamic analytics detect suspicious activity by user account and block access
Alert based on suspicious behavior
Blocked: Device is not authorized
Logged analysis detects attempts

Embracing a Zero Trust Security Model – National Security Agency (NSA)

1. **Data Classification and Encryption**:
    - Data-centric security solutions facilitate the classification of data based on its sensitivity, importance and compliance contents, ensuring that appropriate security and compliance measures are applied.
    - Encryption techniques are employed to protect data both at rest and in transit, mitigating the risk of unauthorized access and data breaches.
2. **Granular Access Controls**:
    - Access controls are implemented at a granular level, allowing organizations to restrict access to sensitive and compliance data based on user roles, responsibilities, and permissions.
    - This ensures that only authorized individuals have access to specific types of data, as required by data privacy regulations.
3. **Data Loss Prevention (DLP):**
    - DLP solutions are integrated into the data-centric security platform to monitor and control the movement of sensitive data within and outside the organization's network.
    - Policies are configured to stop and alert unusually large data access, preventing impersonation attacks and ensuring compliance with regulations regarding data handling and sharing.
4. **Auditing and Reporting**:
    - Continuous monitoring capabilities enable organizations to track data access and usage, generating detailed audit logs for compliance reporting purposes.
    - These audit logs provide evidence of compliance with data privacy laws, demonstrating that appropriate measures are in place to protect sensitive information.

5. **Data Minimization and Retention Policies**:
    - Data-centric security solutions support the implementation of data minimization and retention policies, ensuring that organizations only collect and retain data necessary for legitimate business purposes.
    - By reducing the amount of sensitive data stored, organizations can minimize the risk of data breaches and ensure compliance with regulations governing data retention periods.
6. **Incident Response and Breach Notification**:

In the event of a data breach or security incident, data-centric security solutions facilitate timely incident response and breach notification procedures.

- Organizations can quickly identify and contain breaches, mitigate the impact on affected individuals, and fulfill their obligations to report data breaches to regulatory authorities and affected parties.

THE CHALLENGES TO IMPLEMENT A DATA-CENTRIC SECURITY SOLUTION

Besides Universal Data Shield (UDS) by APF, there is no other standalone data-centric security solution available today. Integrating different products into one that performs similar functions is difficult if not impossible. The National Cybersecurity Center of Excellence (NCCOE) was tasked to find a solution for data classification, the core of a data centric solution, and it failed with the conclusion that "numerous technological approaches to (data) labeling are currently in use, but no approach works universally across data assets, technologies, and organizations."

In general, implementing a data-centric security solution presents several challenges:

1. **Data Discovery and Classification**: Identifying all data across disparate systems and accurately classifying its sensitivity level is complex, especially in large organizations with extensive data repositories.

2. **User Adoption and Training**: Educating users about the importance of data-centric security and training them on new policies and procedures is crucial but can be challenging, particularly in organizations with diverse user populations.

3. **Data Lifecycle Management**: Managing data throughout its lifecycle, including creation, storage, usage, and disposal, requires comprehensive policies and procedures to ensure consistent protection and compliance.

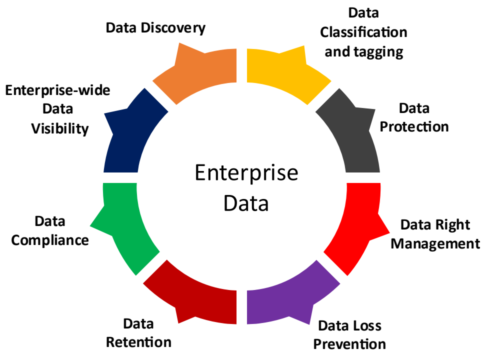
4. **Compliance and Regulatory Requirements**: Meeting regulatory mandates and industry standards, such as GDPR, HIPAA, or PCI DSS, adds complexity to data-centric security implementations, necessitating ongoing monitoring and audit capabilities.

5. **Cost and Resource Allocation**: Investing in data-centric security solutions, including hardware, software, and personnel, requires careful budgeting and resource allocation, which may be constrained by competing priorities.

6. **Balancing Security and Usability**: Implementing robust security measures without sacrificing usability and productivity for end-users can be challenging, requiring a delicate balance between security and user experience.

7. **Scalability and Adaptability**: Ensuring that data-centric security solutions can scale to accommodate growth and adapt to evolving threats and technologies is essential for long-term effectiveness.

ACHIEVE THE "UNACHIEVABLE", STOP FUTURE DATA LOSSES WITH DATA-CENTRIC SOLUTION



UDS Holistic System

When NSA, CISA and DoD put their faith in data-centric solutions to protect the nation's critical data, they made the right choice. A few years ago, we also came to the conclusion that data losses have to be stopped and data-centric is the best approach to it. So, we worked hard and worked smart. Now we built the Universal Data Shield (UDS), the only holistic data-centric security solution that is provided as an all-inclusive SaaS solution.

We worked hard on UDS to safeguard every data that exists now and will be created in the future. It scales seamlessly as business grows, so every bit of the success is protected. We future-proofed UDS with a quantum computer-safe encryption, ensuring data safety even in unforeseen events where quantum computing advances may threaten traditional encryption algorithms. We believe the likelihood of such developments occurring within the next decade is substantia.

Data-centric solutions like UDS provide the best return on investment. They consolidate many of existing data protection, data loss prevention and compliance products into a single solution with better features, reduces complexity, streamlines management, and lowers operational costs associated with maintaining multiple disparate security tools. Additionally, the effectiveness of data-centric solutions like UDS in preventing data losses and minimizing the impact of security incidents can lead to reduced financial losses, regulatory penalties, and reputational damage, further enhancing ROI. Moreover, the centralized data protection visibility and control over sensitive information, enabling organizations to optimize resource allocation, enhance productivity, and drive innovation while ensuring compliance with data privacy regulations. Overall, the holistic nature and efficiency contribute to a higher ROI compared to fragmented security approaches.

In conclusion, data-centric security solutions like UDS offer a proactive approach to safeguarding valuable data assets in an increasingly interconnected and data-driven world. By prioritizing data protection at its core, organizations can mitigate the risk of data breaches, ensure compliance with regulatory requirements, and enhance their overall cybersecurity posture. As the threat landscape continues to evolve, embracing data-centric security solutions is essential for organizations seeking to protect their most valuable asset: their data.

With a data-centric solution like UDS, the seemingly unthinkable task of preventing data losses can be achievable.

Contact APF Technologies to learn how data-centric security solutions and UDS can help you stop data losses and stay compliant with regulations.

Now is the time to take action, before it becomes too late.

www. apftechnologies.com

APF Technologies is redefining cyber defense with UDS, the holistic data-centric quantum-computing safe security solution. UDS stops future data losses by securing data at rest, in transit and in use regardless of location and underline infrastructure, and ensures compliance with data privacy laws and regulations.

https://www.apftechnologies.com