eBook

Insider Tips for Choosing the Perfect Data Security Platform

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

The Importance of Data Security for Businesses

Data has become the lifeblood of both private and public sector organizations. From financial records to personal information, data fuels decision-making, innovation, and operational efficiency. With an increasing reliance on data comes the need for robust data security measures to ensure data confidentiality, integrity, and availability. In today's data-driven world, the cost and consequences of cybercrime[1] have reached critical levels, making data security a priority for every business. This is key to safeguarding sensitive information and maintaining trust among stakeholders.

Data Security Challenges

Private and public sector organizations encounter a multitude of challenges when it comes to data security.

In the private sector, businesses face the constant threat of cyberattacks, ranging from sophisticated breach attempts to ransomware attacks and insider threats. As companies evolve their cybersecurity defenses to outpace malicious actors, the increasing array of security tools presents a critical problem for security teams. Vendor sprawl and managing multiple products brings complexity, limits visibility, and drives up costs.

If you add to this the sheer volume and diversity of data created daily and the resource constraints businesses face regarding budgets and lack of skills, it's easy to see how the situation can become overwhelming. For example, the Thales 2024 Data Threat Report highlights that 16% of businesses can classify little to none of their data, while operational complexity is identified as a critical concern for the majority of the companies[2].

Compliance with regulatory frameworks such as GDPR, HIPAA, or PCI DSS, as well as the introduction of emerging technologies such as 5G and GenAI, add more layers of complexity, requiring businesses to navigate intricate legal and technical requirements to keep data secure.

In addition to adhering to these legislative compliances, public sector entities have their own unique challenges in safeguarding sensitive information. Government agencies handle vast amounts of citizen data, including passport and social security numbers, health records, and financial information. Ensuring the security of this data is crucial for preserving individual privacy and upholding public trust in governmental institutions. Moreover, government entities have to deal with bureaucratic hurdles, which can hinder the implementation of robust cybersecurity measures.

Business Challenges

- Evolving cyber threats
- Vendor sprawl
- Constraint resources
- Data sprawl
- Compliance complexities

The Implications of Poor Data Security vs Benefits of Good Data Security

The consequences of poor data security can be catastrophic and far-reaching for both private and public sector organizations. Data breaches not only result in financial losses due to regulatory fines, legal settlements, and remediation costs[3] but also inflict damage to reputation that can result in an immeasurable loss of customer trust and loyalty[4]. The exposure of sensitive data can also lead to identity theft, fraud, and other forms of malfeasance, causing harm to individuals and businesses alike.

Conversely, investing in good data security practices brings many benefits for enterprises. By protecting data against unauthorized access, manipulation, or destruction, businesses can enhance their resilience to cyber threats and maintain operational continuity. Robust data security measures foster trust among customers, partners, and stakeholders, enhancing brand reputation and bringing a competitive advantage. Furthermore, compliance with regulatory requirements mitigates legal risks and demonstrates a commitment to ethical conduct and data protection.

1 https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
2 https://cpl.thalesgroup.com/data-threat-report
3 https://www.ibm.com/reports/data-breach
4 https://cpl.thalesgroup.com/resources/encryption/consumer-digital-trust-index-report

Data Security Best Practices

In today's digital landscape, data security best practices are essential for enterprises of all sizes and in every sector. By adhering to data security best practices, companies can mitigate risks, maintain regulatory compliance, and safeguard their reputation in an increasingly interconnected world.

The first step in any data security initiative is knowing what data you have. Conduct a comprehensive inventory of all data assets within your business. This includes identifying sensitive and non-sensitive data and understanding its scope and importance. The next step is knowing where your data is stored.

Map out the various storage locations where your data resides, whether it's on-premises servers, cloud platforms, or third-party systems. Understanding the storage infrastructure helps direct security resources to where they are needed most.

Data Security Questions

- What data do I have?
- Where is it stored?
- Where does it move?
- Who accesses it?
- How is it used?
- What is its sensitivity?
- What are the inherent risks and vulnerabilities?
- What are the available solutions?

Then, realize how your data moves by tracing the data flow within your company to identify potential vulnerabilities in transit. This involves analyzing data transmission pathways like networks, email systems, and file-sharing mechanisms. Also, understand who is accessing your sensitive data by implementing robust access controls and authentication mechanisms to restrict access to sensitive data only to authorized personnel. Enforce the principle of least privilege and regularly review user permissions and privileges to ensure they align with business requirements.

It's also important to know how your data is being used by monitoring data usage patterns to detect anomalous or suspicious activities that may indicate unauthorized or malicious behavior. In addition, logging and auditing mechanisms should be implemented to track data access and usage. In addition, know how your data is classified. Classify data based on its sensitivity and criticality to the organization and apply appropriate security controls and encryption techniques based on data classification to ensure adequate protection.

With myriad solutions available today, understanding the option to protect your data is key. Have a look at the security measures available to protect your data, including encryption, tokenization, robust authentication mechanisms, and secure communication protocols. Then, select these tools based on your organization's appetite for risk and compliance requirements.

Finally, understand the risks and threats that businesses today are dealing with. Stay informed about emerging cybersecurity threats and vulnerabilities relevant to your company's industry and data assets. Also, conduct regular risk assessments to identify potential gaps in your data security posture and prioritize remediation efforts accordingly.

Data Security Solutions

Introducing Data Security Platforms

Data Security Platforms are changing the game for information security. These comprehensive software solutions protect sensitive data across IT environments, including on-premises data centers, cloud infrastructures, and hybrid environments. According to Gartner[5], "Data security platforms (DSP) combining data security controls with business logic and fine-grained authorization lead to significant gains in efficacy and data security."

> " Data security platforms (DSP) combine data security controls with business logic and fine-grained authorization lead to significant gains in efficacy and data security."
>
> – Gartner

Rather than focusing on a single security measure, data security platforms integrate multiple security technologies into a centralized management system. This allows businesses to implement consistent security policies and controls across their entire data ecosystem, regardless of where the data is stored or how it is accessed.

These platforms provide organizations with a 360° approach to data protection, helping them mitigate risks, ensure regulatory compliance, and maintain stakeholder trust.

The Features of Data Security Platforms

Data security platforms provide a comprehensive array of features designed to address various aspects of safeguarding sensitive information. These include:

Granular Access Controls: Data security platforms provide granular access controls to manage user permissions and privileges, ensuring that only authorized individuals can access sensitive data. This includes role-based access control (RBAC), attribute-based access control (ABAC), and fine-grained access policies.

Encryption and Tokenization: They offer encryption and tokenization techniques to protect data both at rest and in transit. Encryption scrambles data into an unreadable format, while tokenization replaces sensitive data with non-sensitive placeholders, reducing the risk of unauthorized access.

Centralized Key Management: These platforms centralize key management to securely store, manage, and distribute encryption keys used to encrypt and decrypt data. This ensures consistent encryption practices and facilitates key rotation and auditing.

Data Discovery and Classification: This feature includes data discovery and classification capabilities to identify and classify sensitive data across the organization's IT environment. This enables organizations to prioritize data protection efforts based on data sensitivity and compliance requirements.

Posture Management: Data security platforms offer posture management features to assess and improve the company's overall data security posture. DSPM features include vulnerability scanning, configuration management, and security policy enforcement to identify and remediate security gaps.

Data Security Platforms Features

- Granular access controls
- Encryption and tokenization
- Centralized key management
- Data discovery and classification
- Posture management
- Threat detection and monitoring
- Accidental data leak prevention
- Compliance and auditing
- Risk identification
- Data detection and response

Threat Detection and Monitoring: These platforms incorporate threat detection and monitoring capabilities to identify suspicious activities, anomalies, and potential security threats. This involves continuous monitoring of network traffic, user behavior, and system logs to detect and respond to security incidents in real-time.

Accidental Data Loss: They include accidental data loss measures to prevent unauthorized transmission or leakage of sensitive data. These might include content inspection, policy enforcement, and data masking to prevent data loss through various channels like email, web, and removable storage devices.

5 https://cpl.thalesgroup.com/resources/encryption/gartner-report-2024-market-guide-for-data-security-platforms

Compliance and Auditing: These platforms facilitate compliance with regulatory requirements and industry standards by providing compliance management and auditing features. This includes generating audit trails, conducting compliance assessments, and automating compliance reporting to demonstrate adherence to data protection regulations.

Risk Identification: Data security platforms help companies identify and mitigate data security risks by conducting risk assessments and prioritizing risk remediation efforts. This involves analyzing vulnerabilities, threat intelligence, and security incidents to proactively address potential risks to sensitive data.

Data Detection and Response: They enable businesses to detect and respond to data security incidents in real-time through automated response actions and incident investigation tools. This includes alerting, containment, forensic analysis, and incident response workflows to minimize the impact of security breaches.

The Benefits of Data Security Platforms

Data security platforms offer essential protections for businesses by safeguarding sensitive information, mitigating risks, and enhancing overall cybersecurity posture.

There are many compelling reasons for companies to embrace these platforms. For one, data security platforms facilitate secure migration to cloud environments by providing robust encryption, access controls, and visibility across cloud services. This enables businesses to leverage the scalability and agility of the cloud without compromising data security. Moreover, by centralizing data security management, these platforms give organizations greater control over their data, regardless of where it resides. This includes implementing consistent security policies, enforcing access controls, and monitoring data usage across diverse IT infrastructures.

Business Benefits

- Control data security
- Realize cost efficiencies
- Enhance compliance
- Enable business continuity
- Secure distributed workforce

Data security platforms leverage advanced technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics to enhance threat detection and response capabilities. These technologies enable proactive identification of security incidents and anomalies, improving overall security posture. And with real-time monitoring, threat intelligence integration, and automated incident response capabilities, data security platforms help companies detect and respond to emerging threats rapidly. This reduces dwell time for cyber threats and minimizes the potential impact of security breaches.

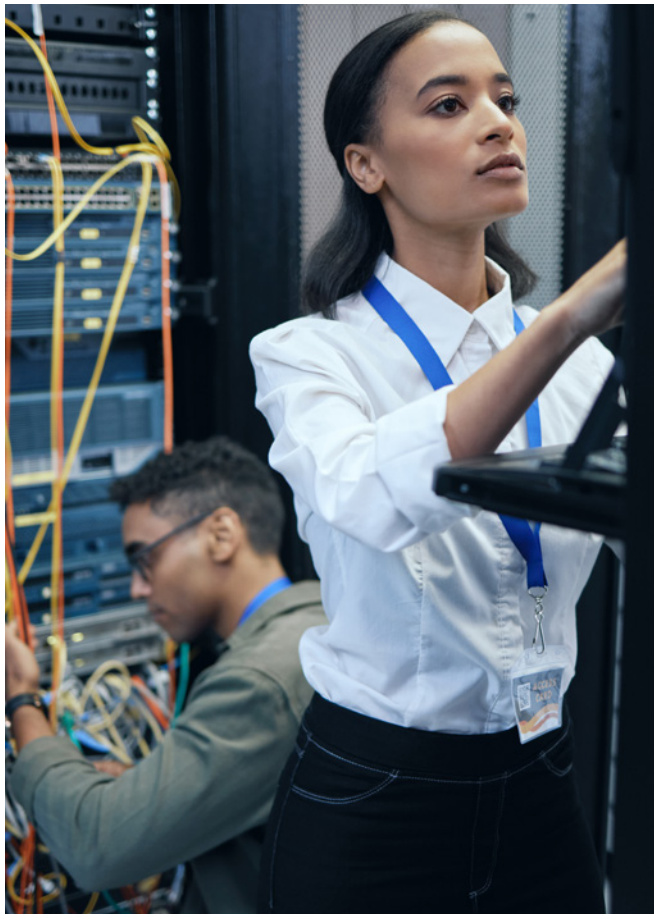
Data security platforms also enable organizations to:

Realize cost efficiencies: Consolidating data security functions within a single platform can save costs by reducing the need for siloed security tools and point solutions and streamlining operational processes. Automated security workflows and policy enforcement also contribute to operational efficiency and resource optimization.

Enhance compliance with regulations: Data security platforms facilitate compliance with regulatory requirements and industry standards through advanced security features. This ensures that organizations adhere to data protection regulations such as GDPR, HIPAA, DORA, NIS2, and PCI DSS, mitigating the risk of non-compliance.

Enable Business continuity: By protecting critical data assets from unauthorized access, data loss, or corruption, these platforms contribute to business continuity and resilience. In the event of security incidents or disruptions, these platforms help minimize downtime and maintain operational continuity.

Secure distributed workforces: With the rise of remote work, data security platforms enable companies to secure data access and facilitate collaboration for distributed workforces. Features such as secure remote access, endpoint security, and secure file sharing ensure that employees can work remotely without compromising data security.



Choosing the Right Data Security Platform

What to Look for in a Data Security Platform

All data security platforms are not created equal, so when selecting a platform, it's essential to consider various factors to ensure it meets your business's specific requirements.

There are many factors that need to be taken into account. For instance, look for platforms that offer diverse deployment options to accommodate different business needs, including hybrid deployments and as-a-service models. This flexibility lets you choose the deployment model that best fits your company's infrastructure and scalability requirements.

Ensuring the solution can scale up and down seamlessly to accommodate fluctuations in data volumes, seasonal demands, and business growth is also crucial. Any platform should evolve alongside your business without disrupting operations or data security. Cloud readiness is also important, so choose a platform designed for the cloud, with a native cloud environment and service support, ensuring compatibility and optimal performance in cloud-based infrastructures.

In today's stringent regulatory environment, compliance also needs consideration, so verify that the solution helps comply with regulations and industry standards relevant to your geographic location and industry vertical. These include GDPR, HIPAA, PCI-DSS regulations, and other local data protection laws like India's DPDP, the PDPA in Singapore, POPIA in South Africa, California's CCPA, and the LGPD in Brazil. Also, look for features that enable sensitive data discovery and classification, allowing you to identify, protect, and control sensitive data with granularity and precision.

Ensure the tool offers robust key management options to control data security, including centralized key management and encryption key lifecycle management. This is critical because by being in charge of data security, businesses can control the sovereignty of their data. In addition, select a platform that integrates seamlessly with data catalogs, popular identity directories, and existing systems within your IT ecosystem. This facilitates interoperability and streamlines data security workflows.

In order to be able to define and enforce fine-grained access controls based on user roles, attributes, and the risk environment, look for solutions that support granular authorization policies. Similarly, to reduce the need for human intervention and manual overhead, seek platforms that offer self-service capabilities and automated workflows to streamline data security operations, improve efficiency, and reduce manual overhead.

Ensure the platform provides comprehensive audit trails and logs for interpretability and compliance reporting purposes. These must-haves include tracking data access, usage, and security events across the platform. Also, evaluate the solution's adjacent capabilities, such as integration with DevSecOps tools, secrets management, and ransomware protection. Consolidating multiple security functions into a single platform can add value by simplifying management and reducing complexity.

Taking into account the total cost of ownership (TCO) is also vital. This should consider the platform's full lifecycle, including initial deployment costs, ongoing maintenance expenses, and potential savings from operational efficiencies. Reviewing independent reports, such as Forrester's TCO analysis, can provide insights into long-term cost implications.

Finally, look for unique features and capabilities that differentiate the platform from competitors, such as comprehensive data protection and visibility solutions. Consider factors like ease of implementation, extensive integrations, and vendor reliability when assessing the platform's value proposition.

How to choose a Data Security Platform

- Diverse deployment options
- Scalability
- Cloud-ready
- Compliance-ready
- Robust key management options
- Fine-grained access controls
- Self-service capabilities and automated workflows
- Audit trails
- Integration capabilities
- Total cost of ownership

Bringing the Right Provider on Board

Choosing a cybersecurity vendor with a long-standing presence in the industry guarantees reliability and stability, as they have demonstrated their ability to adapt to evolving threats and technological advancements over time, offering a track record of experience and expertise in addressing complex security challenges.

Choosing the right data security platform requires careful evaluation of deployment options, scalability, regulatory compliance, key management capabilities, integration capabilities, and total cost of ownership.

By selecting a platform that aligns with your organization's needs and priorities, you can effectively safeguard sensitive data and mitigate security risks.

Implementing a Data Security Platform

Having a robust implementation plan is key as it will ensure smooth integration and deployment, alignment with business goals, and the risk environment. The devil's in the detail.

These steps include:

Identify Your Goals: Clearly define the objectives and goals of implementing a data security platform, such as protecting sensitive data, achieving regulatory compliance, and enhancing overall cybersecurity posture.

Assess Your Current State: Conduct a thorough assessment of the organization's current data security practices, infrastructure, and vulnerabilities. Identify areas of weakness and potential risks that need to be addressed.

Design a Roadmap: Develop a comprehensive roadmap for implementing the platform, incorporating governance structures and best practices. Utilize frameworks like NIST CSF 2.0[6] to guide governance decisions and prioritize security initiatives.

Get Stakeholders on the Same Page: Engage key stakeholders across the organization, including executives, IT teams, security professionals, and end-users, to ensure alignment and support for the implementation efforts. Communicate the importance of data security and the benefits of the proposed platform.

Training: Provide training and awareness programs to educate employees about data security best practices, policies, and the use of the new platform. Ensure that staff members understand their roles and responsibilities in maintaining data security.

Testing and Validation: Conduct thorough testing and validation of the solution to ensure its effectiveness and compatibility with existing systems. Test different scenarios, including security incidents and data breaches, to assess the platform's response capabilities.

Monitoring and Review: Implement continuous monitoring and review processes to track platform's performance and identify any emerging threats or vulnerabilities. Regularly review security controls, policies, and procedures to ensure they remain practical and up-to-date.

6 https://www.imperva.com/blog/data-security-perspective-for-nist-cybersecurity-framework-2-0/

How Thales Can Help

Choosing the right data security platform is crucial for organizations looking to safeguard their sensitive data, mitigate security risks, and ensure compliance with regulatory requirements.

Many companies are also looking at rationalizing the array of security products and services by selecting fewer vendors to fulfill various security needs. By consolidating vendors, businesses can streamline their security infrastructure, leading to several benefits, such as improved operational efficiency by simplifying management processes and reducing the complexity of integration between different solutions.

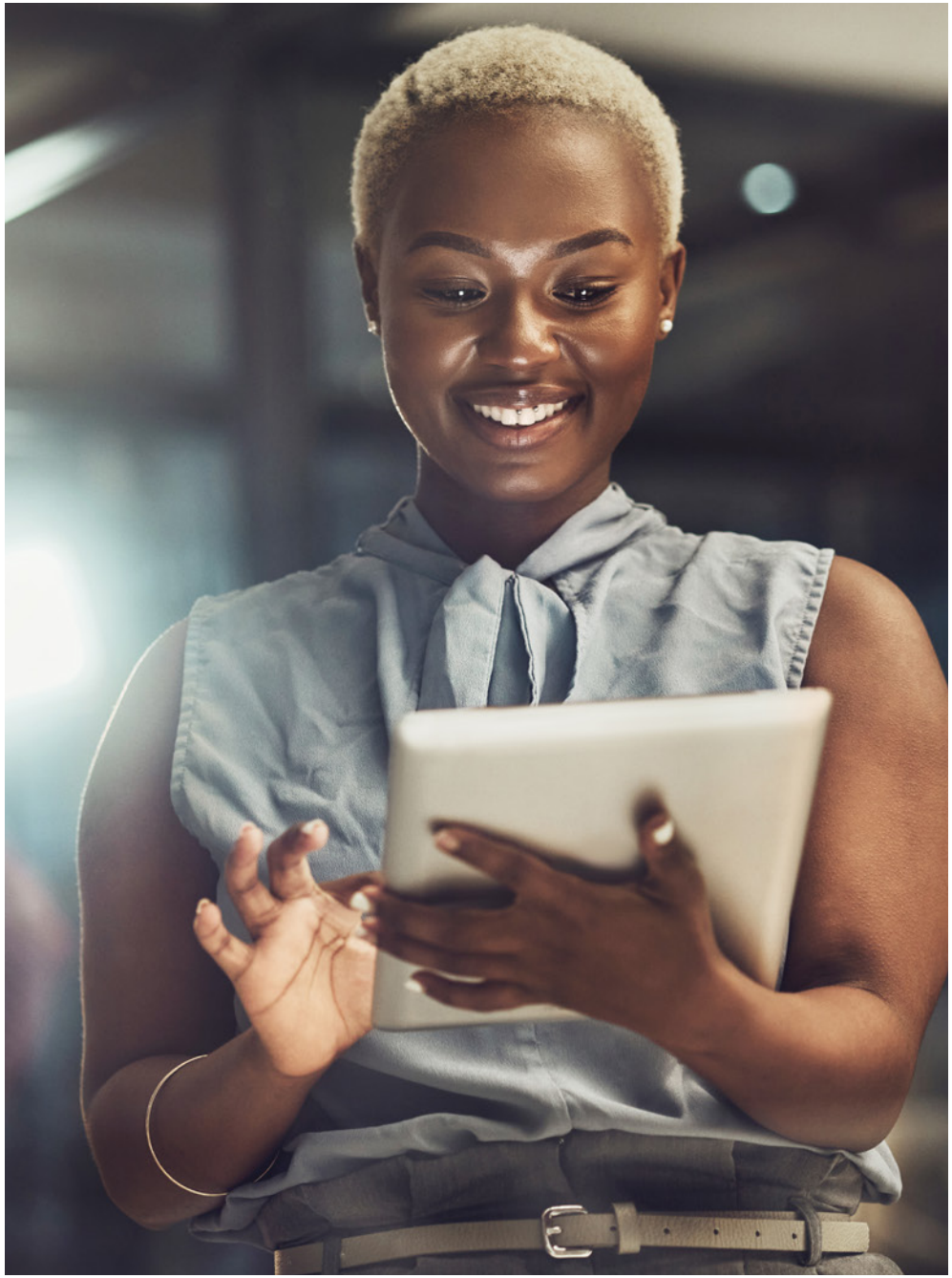
Another benefit is improved visibility and control over the security environment, enabling quicker detection and response to threats. It enhances collaboration and communication between security teams, fostering a more cohesive approach to cybersecurity across the business. Overall, security vendor consolidation promotes a more robust and effective security posture while optimizing resources and minimizing potential vulnerabilities.

Introducing the CipherTrust Data Security Platform, a comprehensive solution that offers robust encryption, access controls, threat detection, and compliance management capabilities. With CipherTrust, organizations can effectively protect their data assets across diverse IT environments while maintaining visibility and control. This platform is built on a modern micro-services architecture, is designed for the cloud, includes data discovery and classification, and fuses the best capabilities from the Vormetic Data Security Platform and KeySecure and connector products.

CipherTrust Data Security Platform unifies data discovery, classification, data protection, and unprecedented granular access controls with centralized key management – all on a single platform. This results in fewer resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

Take the next step towards enhancing your data security posture and safeguarding sensitive information. Explore the capabilities of CipherTrust Data Security Platform and discover how it can empower your organization to meet its data security goals.

https://cpl.thalesgroup.com/encryption/data-security-platform



THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com