SHARDSECURE

White Paper:

Addressing B2B Data Security Requirements

The growing customer need for data security

Data protection has become a critical concern for organizations in a wide range of industries. B2B customers are seeking assurance that their sensitive data will remain protected, while company partnerships are looking for robust data security measures to facilitate the exchange of critical information.

From healthcare to manufacturing, customers and partners want to know how their sensitive data will be safeguarded. They place a particular emphasis on encryption and other security protocols as well as features like data integrity and availability. They are also aware that legacy solutions may no longer offer comprehensive protection against the ever-evolving cyber threats they face.

In this white paper, we explore the increasing demand for strong data protection practices. We also discuss the key features that B2B customers require to protect their sensitive data, and we explore the benefits of the ShardSecure platform for strengthening data security.

Examples of B2B customer data security requirements

Interconnectivity within and among industries is increasingly common today. In our global economy, many organizations share sensitive data with a wide range of providers, vendors, and other partner companies. As we explore with our examples below, these organizations demonstrate a need for strong data security regardless of their industry.

Service provider for financial services

Financial institutions are often highly regulated and, understandably, concerned about the security of their customer data. Service providers for the finance industry are therefore expected to adhere to a stringent set of security requirements. At minimum, they need to demonstrate equivalent encryption practices and access controls to prove that customer data will remain confidential and protected from unauthorized access. Generally, service providers will also need to produce a report showing SOC 2 compliance — the standard set by the American Institute of Certified Public Accountants — to illustrate their data security practices in this industry.

Original equipment manufacturer for the automotive industry

Automobile manufacturers provide intellectual property (IP) like designs and sensitive product information to original equipment manufacturers (OEMs) of automobile parts. Since manufacturers are aware that their sector experiences a high number of cyberthreats, they tend to be very concerned about the risks of sharing proprietary information. OEMs, therefore, must provide solid evidence of their data security practices to assure these automobile manufacturers that their IP will be safeguarded throughout the production process.

Software provider for healthcare providers

Healthcare providers use software solutions from SaaS providers to manage patient data. Because of the highly

sensitive nature of this patient information, healthcare organizations typically require assurance from SaaS providers about not only data security practices but also compliance with privacy regulations like HIPAA and third party assessments like SOC 2. These healthcare organizations may also ask about additional controls for protecting unregulated healthcare data.

Top requirements for customer data security solutions

The significance of effective and well-documented data security measures cannot be underestimated in B2B customer partnerships. Strong data protection measures help to enhance trust and drive strong business relationships.

Although there is no one-size-fits-all security solution, organizations should generally seek a data protection solution that addresses the following key requirements.

Key Requirements for B2B Data Security
1. Advanced data security
2. Easy implementation
3. Low management burden
4. Support for regulatory compliance
5. The freedom to pursue business goals

1. Advanced data security

The first requirement is simple and non-negotiable: Organizations need to protect their customers' data. But how they achieve that protection is much more complicated, and some solutions are more suited to meeting complex threats than others.

The majority of B2B customers will request that organizations encrypt customer data. Depending on a company's architecture, this request can be as easy as clicking a checkbox or as difficult as rearchitecting an entire software stack. However, most customers will also require cryptographic tenant separation, which is generally not supported with out-of-the-box solutions.

Additionally, customers will need to ensure data security for not only structured data but also unstructured data, which is notably overlooked by most solutions in the encryption space. Companies should focus on implementing solutions that can effectively secure this type of data without impacting existing data and user workflows.

2. Easy implementation

While stringent data security measures are vital, those measures should not complicate or disrupt an organization's daily operations. Companies should seek data security solutions that seamlessly integrate into existing workflows without causing disruption to users. These solutions should be transparent to both end users and the underlying systems, and they should offer largely frictionless deployment, integration, and maintenance.

3. Low management burden

Meeting customer data security needs should not require extensive resources for maintenance and management. The ideal solution will have a minimal impact on operations teams and IT staff. It will also integrate seamlessly with existing infrastructure and applications, minimizing the need for complex configurations or extensive changes to the IT environment.

This is in contrast to solutions that require constant attention, like data loss prevention (DLP) tools, data discovery, key rotation, and other high maintenance technologies. The goal is to strengthen security without adding unnecessary complexity, increasing workloads, or requiring significant team resources.

4. Support for regulatory compliance

The ideal data security solution will not only strengthen an organization's data practices but also help them meet compliance with third-party assessments. AICPA's SOC 2 standard, for instance, is based on five pillars that include strong data security, privacy, confidentiality, integrity, and availability. Data protection services should improve a company's posture in at least several of these core areas.

Demonstrating voluntary compliance with SOC 2 has value in facilitating smoother due diligence processes for business relationships. It provides better transparency on how data is handled, and it can foster mutual trust among B2B partners.

5. The freedom to pursue business goals

While strong data security is imperative for meeting B2B customer needs, it ultimately serves another goal as well, supporting an organization's ability to focus on its core business objectives. An effective data security strategy will accomplish several things at once:

- It will protect a company from cyberattacks and outages.
- It will allow a business to allocate its resources and attention to strategic initiatives that drive revenue growth.

- It will empower organizations to drive innovation, pursue growth opportunities, and inspire trust among customers and partners.

How ShardSecure addresses customer security requirements

The ShardSecure platform offers several benefits to help organizations meet their B2B customer and partner data security requirements.

Advanced file-level protection

First, the ShardSecure platform maintains the security, privacy, and resilience of unstructured data on-premises, in the cloud, and in multi- and hybrid-cloud environments. Our technology provides advanced, agentless file-level protection to keep data safe from unauthorized access.

Traditional agent-based solutions can slow performance and drain security team resources. They are difficult to manage and scale, and they can be incompatible with newer workloads and cloud services. The ShardSecure platform offers an innovative alternative, allowing companies to secure their data from internal and external threats without the cost and complexity of agent-based solutions.

Support for SOC 2 compliance

ShardSecure's strong data security and resilience features significantly strengthen the security posture of organizations looking to comply with SOC 2 requirements. Our technology is based on the CIA triad of data confidentiality, integrity, and availability, which form three of the five cornerstones of SOC 2.

ShardSecure also supports the remaining two AICPA cornerstones of data privacy and security by mitigating unauthorized data access from infrastructure providers and other third parties. Robust data resilience and file-level protection features help to simplify the path to SOC 2 compliance.

Seamless integration and implementation

The ShardSecure platform offers easy plug-and-play implementation without unnecessary changes to existing data and employee workflows. Data can be accessed and moved easily, and only a few lines of code change are required for integration.

Because the ShardSecure platform appears and behaves like storage to other applications, companies can integrate it into their current security workflows without redeveloping their architecture or adding to their operation team's workload.

Conclusion

The B2B customer landscape is marked by a growing emphasis on data protection for sensitive information. Organizations across various industries are recognizing the need to address customer concerns around data security — and the importance of implementing robust measures to safeguard critical information for business partners. To earn and maintain the trust of B2B stakeholders, companies must prioritize data security as an integral component of their operations.

The ShardSecure platform offers an innovative approach to meeting B2B customer data security requirements. With its advanced file-level protection, easy implementation, and support for SOC 2 compliance, ShardSecure's technology can protect sensitive business data and facilitate important partnerships, regardless of where data is stored.

For more information about the platform, review our other white papers or schedule a demo today.

@ShardSecure
@ShardSecure
@ShardSecure

101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

info@shardsecure.com