SHARDSECURE

White Paper

Advanced File-Level Protection With Fewer Resources

Introduction

A cornerstone of strong data security is separating data from the infrastructure owners, cloud storage providers, and system administrators who would otherwise have access to it. This separation of duties is crucial to prevent leaks and breaches, making it an important element of enterprise risk management and security. Indeed, data leaks are most commonly caused by improper access credentials and abuse of administrative access.

Separating data from third parties is also essential for maintaining compliance with cross-border data protection laws like the EU's General Data Protection Regulation (GDPR), financial regulations like the Sarbanes-Oxley Act (SOX), and guidelines from agencies like the National Institutes of Standards and Technology (NIST).

Because the separation of duties can increase costs, complexity, and management duties, it is typically only applied to the most mission-critical elements of an organization, such as sensitive data. This data is often less safe than people imagine; as one study shows, 83% of security professionals believe that sensitive data has been accidentally exposed at their organization.

In the past, companies have achieved data privacy and separation of duties with agent-based file-level encryption. Today, though, agent-based solutions often slow performance, drain resources, and present incompatibilities with newer workloads and cloud services.

ShardSecure offers an innovative alternative to agent-based file-level protection. With our easy and transparent plug-and-play software solution, we provide strong data confidentiality and resilience — while avoiding the need for agents altogether.

Copyright © 2023, ShardSecure, Inc.

The current state of file-level protection

Unstructured data: underprotected and growing

Unstructured data is any file or collection of files that isn't stored in a structured database format. Unstructured data makes up at least 80% of all enterprise data, and it's growing at a rate of 55 to 65% annually. This is four times faster than structured data — and yet unstructured data is still underserved in the encryption space.

Unstructured data comes in many forms, including text, image, video, audio, web server logs, social media, and much more. It lives in filesystems or blob stores, and it doesn't adhere to conventional data models.

Because of how it's stored, the privacy of unstructured data is reliant on the filesystem or the storage service it resides in. This creates privacy issues, as infrastructure administrators (cloud storage providers, local storage admins, server admins, and more) will always have access to it.

Traditional solutions meet new obstacles

File-level encryption has long been the gold standard for data protection. But this traditional solution has several drawbacks, and it increasingly needs to be supplemented to meet the demands of the future.

First, although encryption does provide strong privacy controls, it's resource-intensive. The constant encryption and decryption of data often affects the performance of applications and slows down operations.

Second, traditional encryption approaches do not offer data resilience. Encrypted files can still be tampered with and deleted in the most common types of cyberattacks, including ransomware. Although data confidentiality is maintained, integrity and availability suffer in attacks and outages.

Lastly, new architectures — including blob storage, S3 storage, K8s containers and many other cloud offerings — increasingly do not support the installation of software code to manage unstructured data. Taken together, these obstacles make data privacy much more complex and gaps within traditional security solutions much more likely.

The problem with agents

The most common way of implementing file-level encryption has traditionally been to install agents, or software code, onto each device, server, and client system. The agent is typically tied to a certain folder or file to protect data, and it controls access to those files.

Today, agents are increasingly difficult to manage and scale, and they require endpoint management. It can be challenging to install, configure, and maintain them on each device and server that requires file-level protection, and they can introduce a significant performance drawback — anywhere from 5% to 40%. Modern tools like network storage, cloud storage, Platform as a Service (PaaS) solutions, and containers were also not designed to have agents installed on them.

Fortunately, modern alternatives allow organizations to take advantage of new architectures and protect their data at the same time. Innovative technologies like ShardSecure's use an agentless file-level encryption approach and modern cryptographic solutions to protect data with little to no performance drawback, and without leveraging any servers or endpoints. Below, we'll discuss how we eliminate the need for agents and other resource-intensive processes while providing advanced data security.

Copyright © 2023, ShardSecure, Inc.

Achieving strong, cost-effective file protection with ShardSecure

ShardSecure provides unbeatable file-level protection with no performance hit, no agents, and "set and forget" management. Our solution allows companies to secure their data from internal and external threats without the cost and complexity of agent-based encryption solutions. Organizations can protect their unstructured data and separate it from infrastructure owners to ensure strong confidentiality — and much more.

Agentless file-level protection

ShardSecure does not use agents, which means no endpoint management, no installation issues, and no drag on processing power. Our API-based abstraction layer sits between your application and your infrastructure, where it performs advanced file protection. The design allows for an easy plug-and-play implementation without changes to data flows or user behaviors.

Unlike agent-based performance drawbacks of up to 40%, ShardSecure involves minimal to no performance drawbacks. Its low latency and fast throughput can sometimes even improve performance. There are no agents, and data on the end devices can be accessed exactly as usual, with no visible changes to user or data workflows.

Separation of duties for confidentiality and compliance

With ShardSecure, the data owner controls exactly who has access to their data, as well as where that data is stored. Our technology works in on-prem, cloud, and hybrid- and multi-cloud environments to separate infrastructure admins and other third parties from data. By splitting data into very small pieces (microshards) and then distributing those containers to multiple customer-owned storage locations, we ensure that data is unintelligible to unauthorized users — including cloud providers and other infrastructure admins.

Advanced data protection features

Our technology prevents third parties from reconstructing data. Even in the highly unlikely scenario that someone is able to gain access to all the microshards from every storage location for a given data set, that data still cannot be reassembled.

- Our technology strips file content, filenames, file extensions, and all other metadata, meaning that there is not enough identifying information for reassembly.
- Our technology allows organizations to add a configurable amount of poison data to their real data.
- Our solution also requires multiple components to be used in concert with both each other and the complete data set for reassembly, meaning that it's not possible for an unauthorized user to deploy their own instance of ShardSecure to reconstruct data.

Adding resilience to data protection technology

In addition to guaranteeing the privacy of data, ShardSecure also provides high availability and strong data resilience. Unlike traditional solutions, which often focus on data confidentiality alone, ShardSecure ensures data integrity and availability in the face of outages and attacks.

Our self-healing data detects when data is lost, deleted, tampered with, or otherwise compromised. If there are any problems with data, automatic controls begin to reconstruct the affected data immediately and transparently, returning it to its original state in real-time. We also send alerts to the company's security teams for faster incident response, reducing the need for restoring from backups and the likelihood of costly downtime.

Our solution keeps data available and accurate. With ShardSecure, organizations can maintain their critical operations, avoid reportable security breaches, and mitigate third-party data access — even in the face of ransomware attacks, cloud provider outages, misconfigurations, and more.

Copyright © 2023, ShardSecure, Inc.

Easy integration, migration, and access

ShardSecure is easy to manage and has a low impact on operations teams. Without the overhead and complexity of traditional file-level encryption, it is vendor-agnostic and works in the background as a zero-downtime event. Because our technology is transparent to users, workflows do not change and retraining is not necessary.

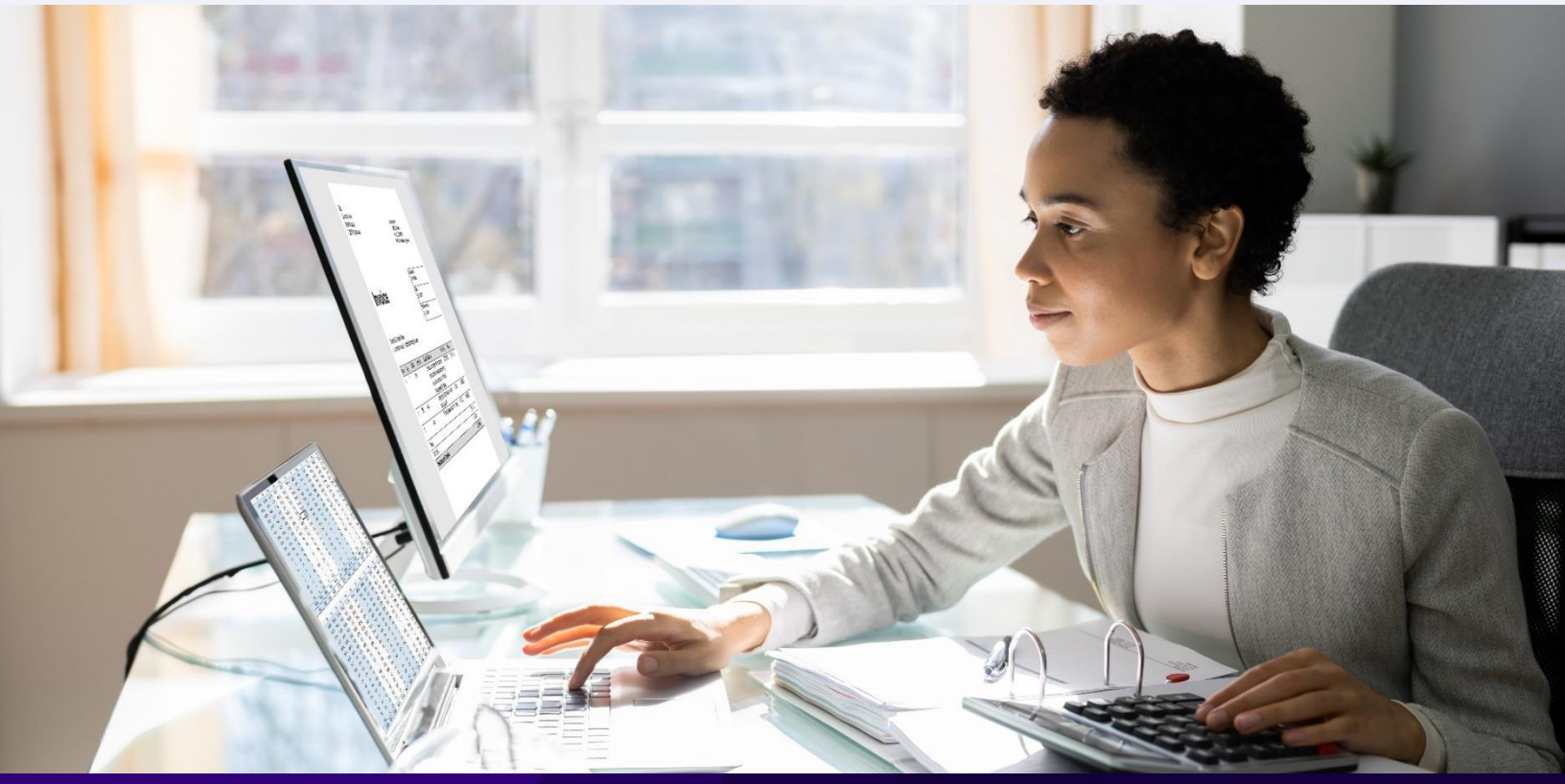
ShardSecure's technology also allows for instant data access and fast data migration with just a few clicks. It is quick and seamless to integrate, with only one line of code change needed to get started.

Conclusion

Moving to the cloud is key for many organizations. From cutting costs to scaling up with the newest technologies, the benefits of cloud migration are abundant, and yet organizations often struggle to take advantage of them. The difficulty of file-level protection — not to mention the resource-intensive processes of agent installation, key management, and more — consumes valuable time and resources. It is a challenge for businesses to keep their data private not just from malicious users but also from third parties like cloud providers.

ShardSecure offers an innovative approach to file-level protection in the cloud. With our strong data privacy technology, self-healing data, ease of integration, and robust data resilience, we make advanced file-level protection a reality so organizations can reap the rewards of the cloud.

For more information on ShardSecure and file-level protection, visit us online 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