Leonovus

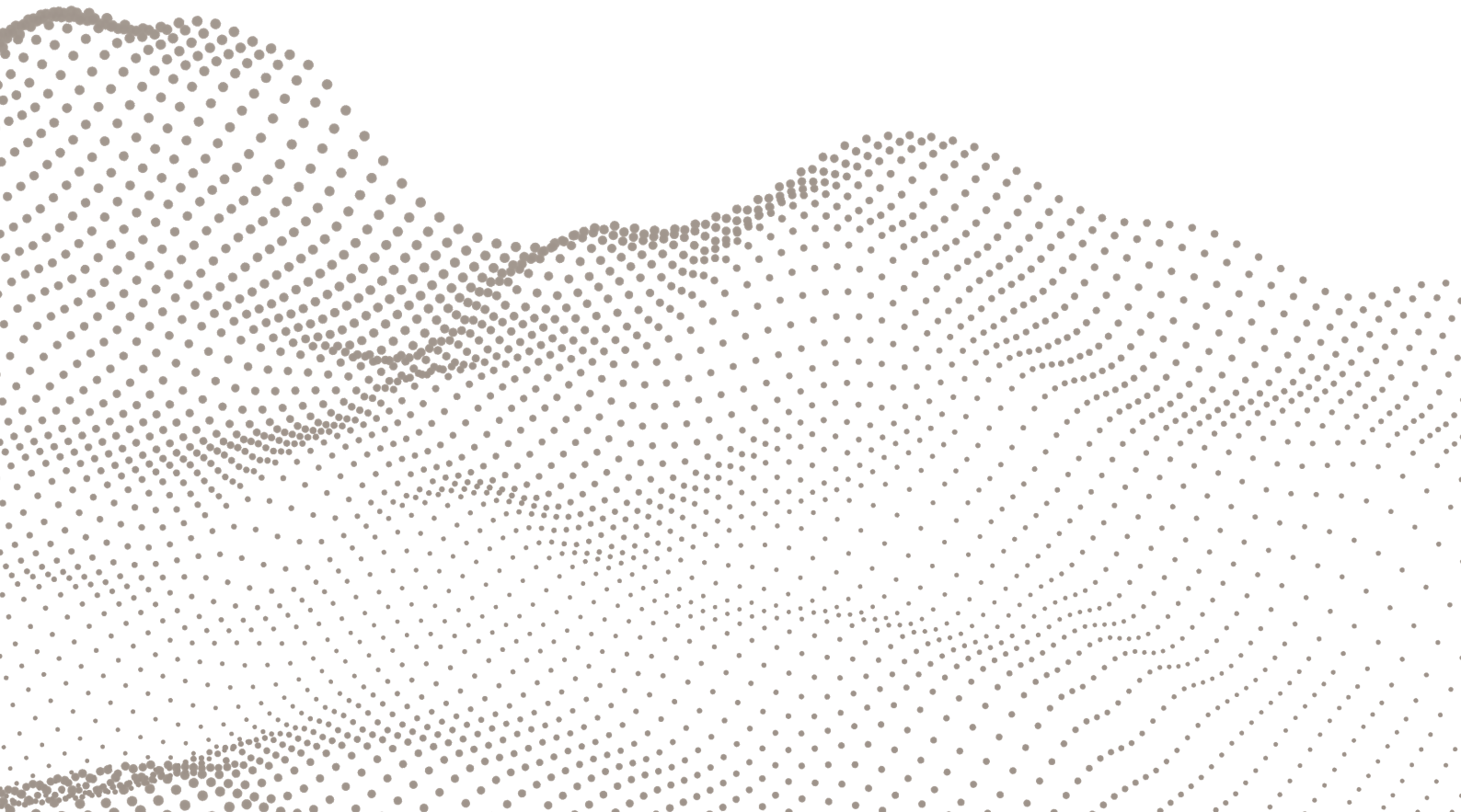
A Partial Solution to the SolarWinds Hack

Data-Centric Secure Storage Data Management Software.

Highly Secure Smart Data Lake

Whitepaper

January 2021



Introduction

In December 2020, USA, UK, and Canadian governments all warned the public of an active Advanced Persistent Threat (APT), which became known as the SolarWinds Hack. Security experts at FireEye had detected a compromise of the SolarWinds Orion software platform.

This cyber-attack, launched in March of 2020, went undetected until December of 2020. As of December 2020, SolarWinds had 300,000 customers, including virtually all the Fortune 500 and many government agencies. The attack affected 18,000 customers directly. There are enormous resulting costs to SolarWinds and its government and private sector customers.

Leonovus' end-to-end data-centric security and smart data management solution could have significantly reduced the damage caused by the SolarWinds Hack. Leonovus seamlessly extends data-centric controls across the organization's existing storage infrastructure and network architecture—on-premises, in the cloud, or both, with cybersecurity capabilities for the entire lifespan of the data and beyond.

The Leonovus data-centric security solution combined with a smart data management solution has considerable added benefits to the organization. The effect on the end user is seamless. Data and analytics leaders can still be agile while using a hyper-secure system. It is essential to know each data element, where it lives, and gain additional information about each data element in a data-centric system.

Because of the data-centric architecture, IT operations and data science experts benefit from more metadata and contextual information. Data lakes are smarter. Analytics are

faster and richer. Data warehouses become better and more secure. Leonovus also dramatically reduces the overall cost of data integration and storage because it can seamlessly optimize data storage—another benefit of a data-centric design.

The SolarWinds hack reminds us that the cyberthreat landscape is becoming even more pervasive and dangerous. The variety of bad actors and the reasons behind their activities have grown. Companies still need to continue delivering business systems that support processes and supply insights while securing underlying information. Why not install a system like Leonovus that is both smart and secure?

(Cimpanu, SEC Filings: SolarWinds says 18,000 customers were impacted by recent hack, 2020)

"Installing Leonovus before the SolarWinds Hack would have reduced the cyber threat surface at server and cloud storage end points. Uncredentialed users probing for valuable data will only see encrypted fragments."

- Michael Gaffney, Chair and CEO, Leonovus Inc.

Three Fundamental Truths for Cyberthreat Survival

The cyber threat surface is large and growing larger. The cyber battlefield is dangerous, and protection tools are evolving. Perimeter security is a necessary line of cyber defense but no longer the last or most important. Three fundamental truths are the foundation for new cyber defense paradigms. With these three truths, organizations are now rethinking how they prepare for and fight the cybersecurity war.

#1

Breaches will occur, accept them and account for them.

#2

Zero Trust: Assume no place in your network is safe and trusted.

#3

Data/information is the real asset that needs protection.

1. Breaches Will Happen

Historically, the cyber protection strategy has been perimeter protection.

Just as moats, drawbridges, outer walls, inner walls, and kill zones would protect a medieval castle -- cybersecurity was all about more robust firewalls, services gateways, virtual private networks (VPNs), and honey pots. It was oriented towards better and more robust equipment, methodologies, and services to keep the bad actors out of the network. Or when they did get in to lure and trap the interloper where they would catch them. This strategy has been flawed since the 1970s. There is always an exploitable flaw in the armour. Confoundingly, the genuine possibility that the attacker, potentially an insider or allied with one, does not start outside the network.

The threat surface is no longer constrained to on-premises assets. With SaaS, PaaS, IaaS, and more, the perimeter now includes hybrid, cloud-based, cloud-native facilities, applications, and services. You are defending a non-contiguous, sometimes invisible perimeter, over part of which you have no control—a daunting challenge.

Perimeter security is still necessary as 7/24/365 attacks target finding connected systems without perimeter security. However, armouring the perimeter with too many layers and too much complexity often leads to configuration challenges or outright errors, opening threat gaps where none previously existed.

The correct approach is to protect the perimeter but assume that the bad actors will get in. If the bad guys get in your house, make sure they get nothing. This approach's key aims are to minimize access, protect the data after a breach, and know whenever and wherever a breach occurs. This whole data-centric security solution must work on-premises, hybrid or cloud.

2. No Place Is Safe – Zero Trust

Too many security architectures and strategies depend on the assumption that the core network, services, and identity and access management (IAM) work. However, when we revisit the first truth, "Breaches Will Happen," then the assumption of trusted actors inside your network is false.

Trust but verify is the correct approach. Do not assume trust in users' access rights or their identity and privilege. This approach forms the basis of a Zero-Trust strategy.

3. Protect the Data: Data-Centric Security

A security paradigm based on protecting the data is known as data-centric security. The control criteria necessary for a comprehensive data-centric security solution include preventive, detective and administrative.

- Preventive controls secure the data itself, and ensure the data is made useless to bad actors.
- Detective controls include understanding data content, tracking its usage, and noting/recognizing/reporting any abnormal behaviours about the data.
- Administrative controls govern and manage access to content and, where applicable, even elements within the range.

Based on these control criteria, the critical facets of data-centric security are:

DISCOVER

Discover - know what data you have.

PROTECT

Protect – in-flight and at rest; only authorized and authenticated access.

TRACK

Track – make a record of all interactions and activities concerning the data.

MANAGE

Manage – keep tight administrative control.

Discovery

In a data-centric system, it is important to know what each data element is, where it resides and know information about the data (metadata). Metadata, indicates state, when it was created, last modified, its size, its type or structure and similar characteristics. It can also be used to tag the data element with useful information like what level of protection should be maintained on the data or who can do what actions to the data.

Protection

It is vital to ensure no unauthorized access to protected data. The current acceptable state of the art for protected data at rest or in transit is 256-bit based encryption.

Stopping undetected data tampering or alteration is achieved by maintaining a hash or fingerprint function on the data using 256-bit based hashing. A change in the data element would result in a change in its calculated hash.

Given that encryption makes the data unreadable, full protection includes enforcement that allows only authorized access. Authorized access privileges apply to all users, applications, and services active within the system and pertain to all forms of access to the data object, creating, reading, updating, moving, or deleting. These privileges also apply to the data's metadata in question and may also include knowledge of a data object's existence.

A robust data-centric security model keeps the protection paradigm throughout the system, which means only the data creator and their designates can determine who has access to any specific data element. Even administrators do not have access to the data element unless granted by the owner/creator. Access can be either user or role-based or both. Had Leonovus been installed, before the SolarWinds Hack, the cyber threat surface at the storage end points would have been reduced on file servers and cloud storage. Uncredentialed users probing the storage systems can only access the encrypted fragments.

Tracking

The system tracks every data element interaction for its entire lifespan and beyond, including all attempted and failed or denied interactions. The tracking system maintains data interaction records in a manner that is accessible when needed. But like any other data element, only accessible by those with access privileges.

The system keeps data tracking records and prevents tampering or alteration of the records. All logs are seamlessly available, along with the discovery records and metadata, to Security Information and Event Management (SIEM) tools. This added information enhances the monitoring for unusual patterns, cyber-attacks, and for other higher-order security infringements, such as would be found by Data Loss Prevention (DLP) analytics engines.

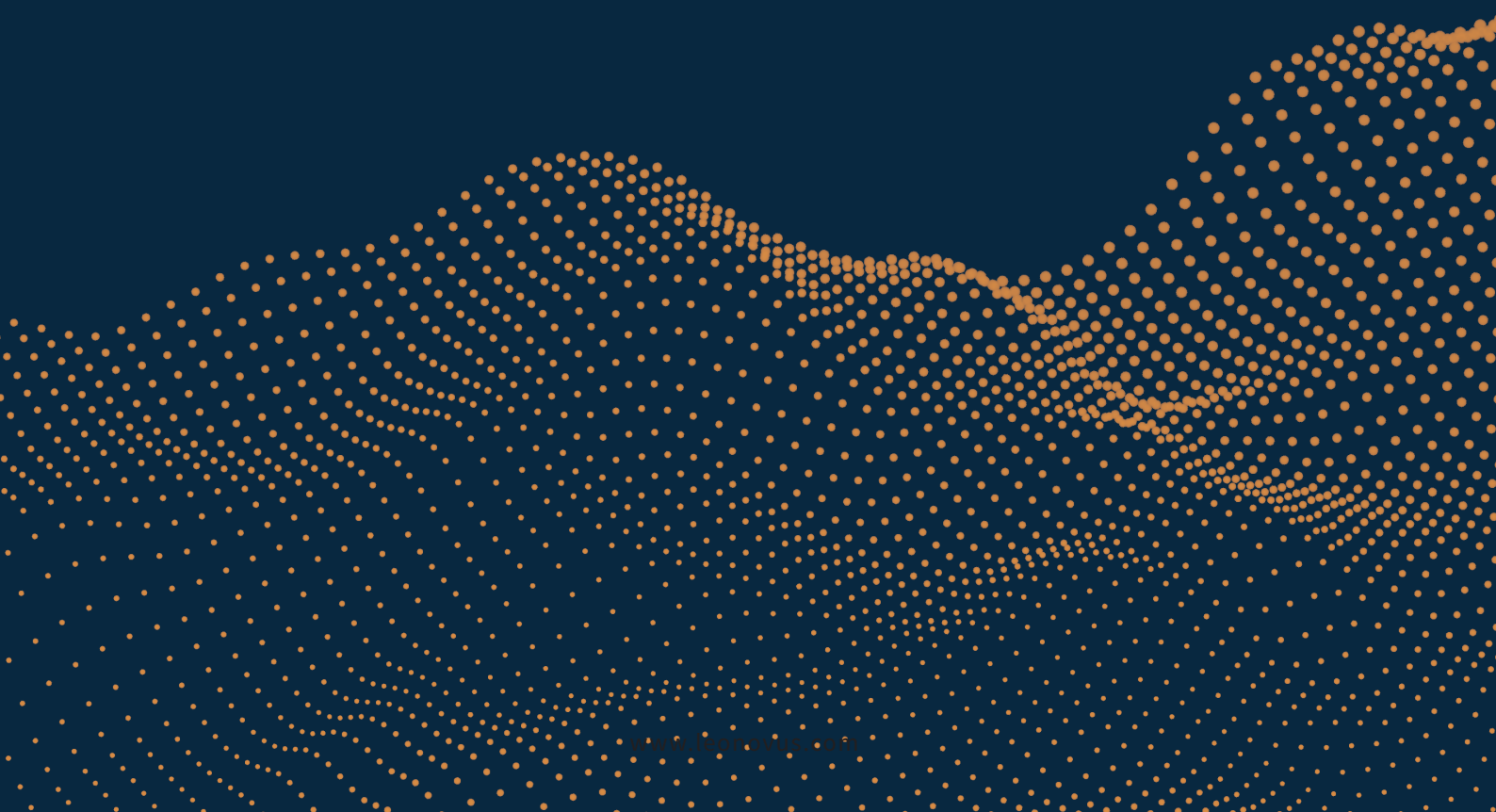
From a governance and regulatory compliance perspective, SIEM analysis and reporting are imperative to protect the corporation's assets and avoid regulatory penalties.

Managing

The “Need-to-know” concept is directly applicable here. Keeping privileges tight, limiting administrative access and capabilities are key facets. In addition to tracking all data, so too are all management and system operations, with the same level of analytics available to detect unwarranted or unusual behaviors.

The Leonovus Solution

The most powerful cyber protection solution is a hybrid of the three fundamental truths. The solid survival kit for cybersecurity in the 2020s is a zero-trust strategy with a data-centric security-based system core to the primary application.



The Leonovus Solution

The most powerful cyber protection solution is a hybrid of the three fundamental truths. The solid survival kit for cybersecurity in the 2020s is a zero-trust strategy with a data-centric security-based system core to the primary application.

As illustrated in Figure 1, the Leonovus solution withstands and accepts cyber intrusion using a data-centric architecture. All data is known, protected, and tracked. All interactions are only with recently authenticated and authorized entities. Ownership is tightly controlled and managed; even administrators do not have access to data objects unless granted by the owner.

As in the SolarWinds hack, if an intruder were to gain entry, with no credentials they would not have access to data elements. If they were to obtain the credentials for a valid user, they would be constrained to accessing only the user's data elements. In the case of an artificially created set of credentials, there is no access to data.

Should a data object be altered or removed, it will be detected. Also, in the Leonovus data-centric solution, any nefariously changed data is restored to its original state.

Should a breach occur, the system will record all the breacher's interactions, allowing full knowledge of the impact and reporting and regulatory compliance on this impact in a prompt fashion.

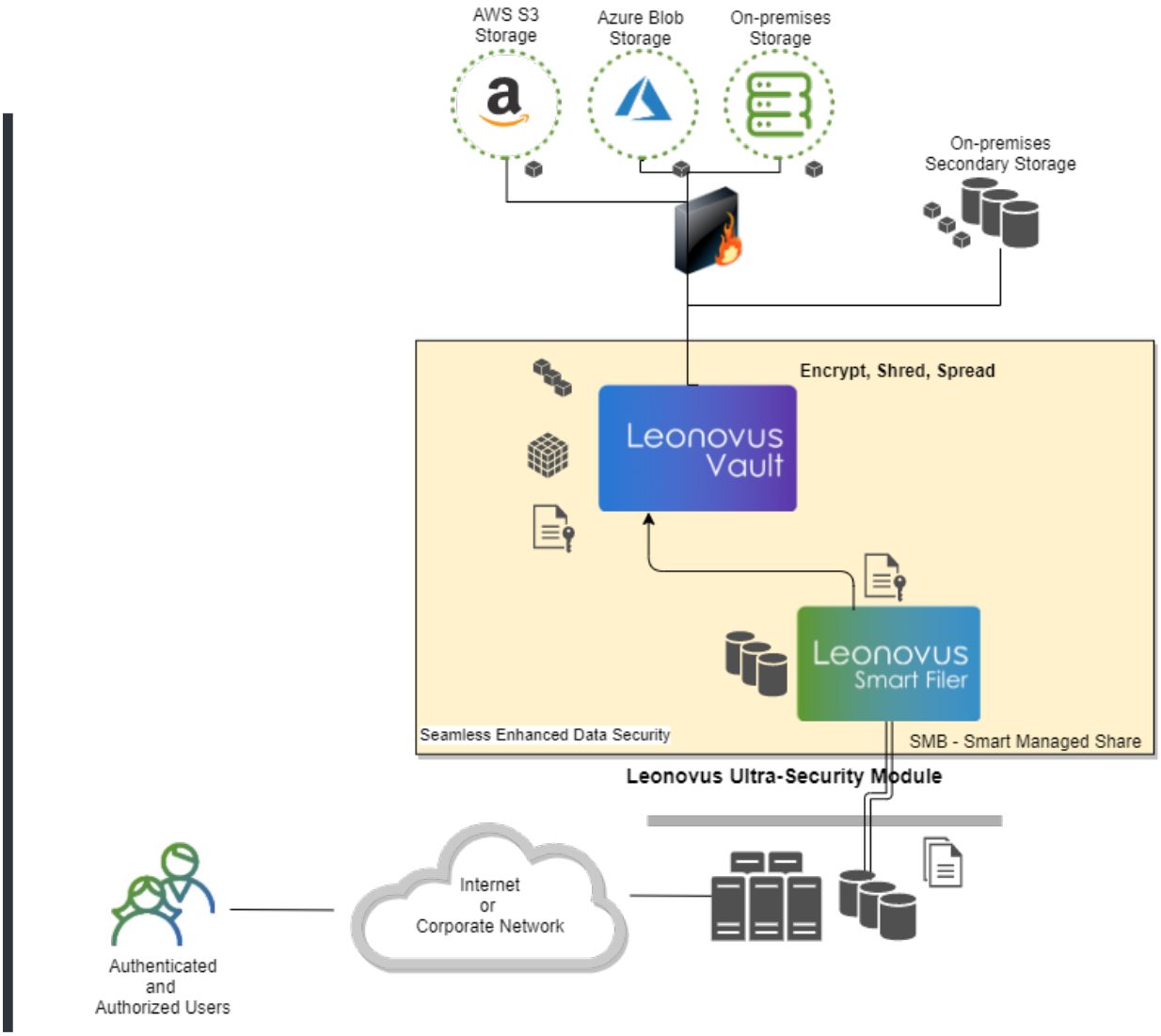


Figure 1 – Data-centric security via encrypt, shred, and spread.

Leonovus Hyper-Secure Smart Data Management Solution

Leonovus provides a complete end-to-end data-centric software architecture tailored to meet the demands of today's cyber threat landscape combined with a robust suite of data management tools.

This solution can stand on its own or easily integrate with the organization's zero-trust strategy and architecture. It takes seamless advantage of the organization's existing storage infrastructure and network architecture, working on-premises, in the cloud, or both. It extends the data-centric controls across the entire architecture, including cloud resources. And it supplies these cybersecurity capabilities for the full lifespan of the data and beyond.

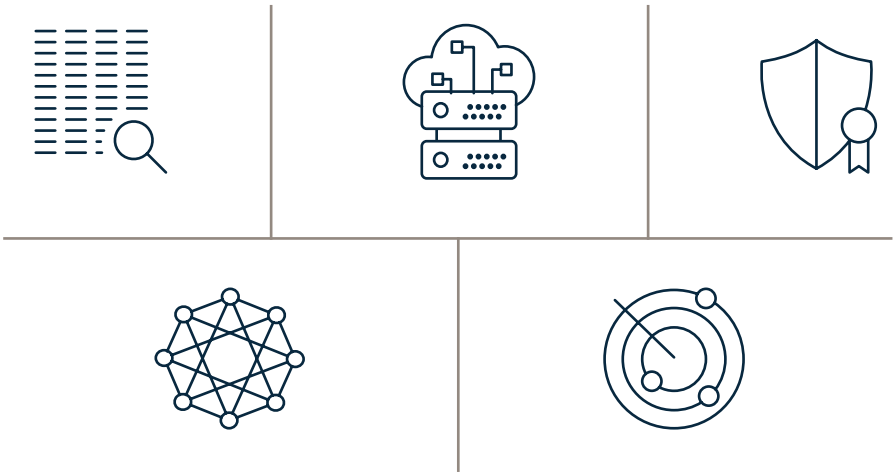
Designed for simplicity and flexibility, the solution does not require internal data use changes. Applications, services, and users all interact with the data the same way they always have. The system ensures the right users get access to the correct data, at the right time, but securely.

In addition to working with existing systems, the Leonovus Smart Data Management solution aids in the organization's digital transformation by enabling state-of-the-art features necessary for the data-driven world. These hyper-secure data management capabilities require little operations effort and no new skills or expertise needed.

The major features of the Leonovus Smart Data Management suite are:

- DATA DISCOVER TOOL classification and understanding of your existing data sets
- SMART FILTER transparent file-based data controls for cost, flexibility, and scalability
- VAULT multi-cloud data management for data lifespan
- DATA VIEW GATEWAYS controlled repository internal/external data sharing
- CONSOLIDATA a multi-sourced context-rich smart and secure data lake or repository for advanced analytics

Each feature is available independently or together as a comprehensive solution set.



Data Discovery Tool

Data Discovery allows administrators to mount Server Message Block (SMB) network-attached file storage and discover the nature of the data stored on it. The Data Discovery operation is storage vendor agnostic and can work across heterogeneous storage environments provided that an SMB interface is available for mounting the network file storage system.

Data Discovery operations help administrators inventory their network file storage environments and visualize the mix of active vs. infrequently accessed files. With this level of visibility, administrators can create data management strategies specific to their use cases and business requirements. The customizable classification capabilities of Data Discovery empower the administrators in performing inventory, policy, and what-if analytics.

Data Discovery operations are read-only and are safe to run in production environments. Running Data Discovery creates an inventory report of the target mount, file last access dates, and the file type/extension.

Smart Filer

Smart Filer provides organizations with the visibility and control necessary to implement and run data management strategies for growing volumes of unstructured data while significantly perfecting existing storage and reducing costs. Smart Filer enables organizations to create hybrid storage environments that leverage existing on-premises storage environments for data that is actively used or worked on frequently and leverage the economics and virtually unlimited cloud capacity for data infrequently accessed.

Similarly, Smart Filer can assume the role of a storage gateway, automatically transiting data from traditional to secured data configurations. As a part of a data-centric security solution, Smart Filer supplies seamless, transparent data transitions that allow users and applications to use their data the same way they always have, even when found elsewhere.

As a part of a zero-trust strategy, Smart Filer integrates directly with the organization's existing IAM systems ensuring seamless user and role management.

Smart Filer automatically analyzes existing file storage and transparently extends its capacity, which helps the organization cut costs and manages continuous data growth without the constant capital expenditures of ever-expanding primary storage systems.

Vault

As its name implies, Vault is the key feature of the Leonovus data-centric security solution, locking your data for your protection. Leonovus securely stores your data without reducing its reachability and availability, but only for the authenticated and authorized users who have permission to access it. Even administrators do not have access to Vaulted data unless the owner grants it to them.

The vaulting of a user file follows four main phases: file presentation, encoding, distribution and local cache removal. Through its encrypt, shred, and spread process, Vault ensures the protections of data stored on the organization's file servers and cloud environments. Protections include data preservation, tamper and alteration detection and correction, and unauthorized access/reading prevention.

Vault includes 256-bit encryption (FIPS 140-2 certified) both in-flight and at-rest, ensuring bad actors see nothing meaningful, including the metadata.

Vault provides this security functionality extending your data governance controls across on-premises, hybrid, or

multi-cloud storage infrastructures. The data-centric security solution provides comprehensive tracking of all data interactions.

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct user direct active management. Leonovus Vault enables multi-cloud computing with vendor neutrality; organizations are free to select the combination of clouds that best-fits their needs.

On-premises-level data security is now a requirement in the public cloud. The data security industry has recognized that, while it is essential to guard and protect the IT environment's infrastructure, it is critical to focus on and safeguard the data, data-centric security in the cloud. In fact, with this data-centric protection model delivered by the Leonovus Vault technology, corporate data is far safer and more durable in a multi-cloud architecture than in an on-premises data center.

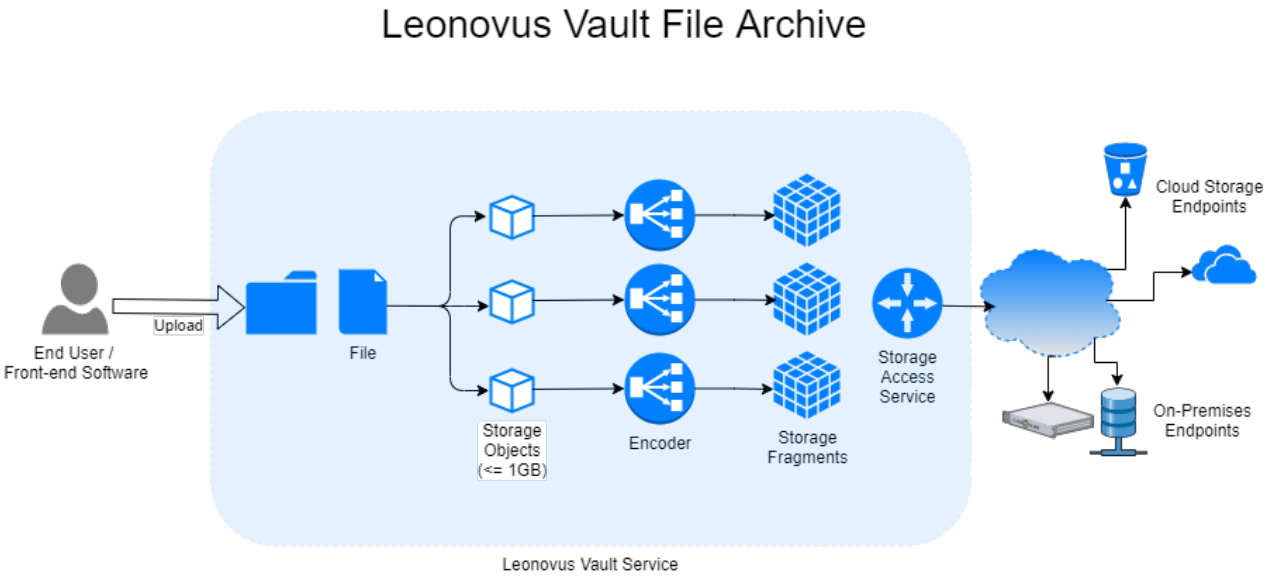


Figure 2 – Vault encrypt, shred, spread process.

Data View Gateways

It is not sufficient to secure and control data inside the organization's managed environment. With the breadth of software-as-a-service (SaaS) offerings and with the degree to which Internet-connected organizations interface with third-party partners, there is a genuine need for a means of securely share data beyond their internal infrastructure. "Tolerating the sharing of data and stepping in only where breaches occur is no longer enough. Sharing data across different organizations enables the whole eco-system to grow and can be a unique source of competitive advantage."

The Leonovus Data View Gateway supplies the capability for secure direct sharing between two groups to transfer the data or pooled data sets for several external analytics applications.

With View Gateway's, the data owner gains a secure mechanism where they can specify controlled access to file systems or repository/data lake-based data. The organization can manage subsets of data, sharing only what needs to be known, continuing to keep the remainder closed-off. As with the other Leonovus data management tools, only authenticated and authorized users gain access and then tracking and logging all interactions.

(MIT Technology Review Insights, 2019)

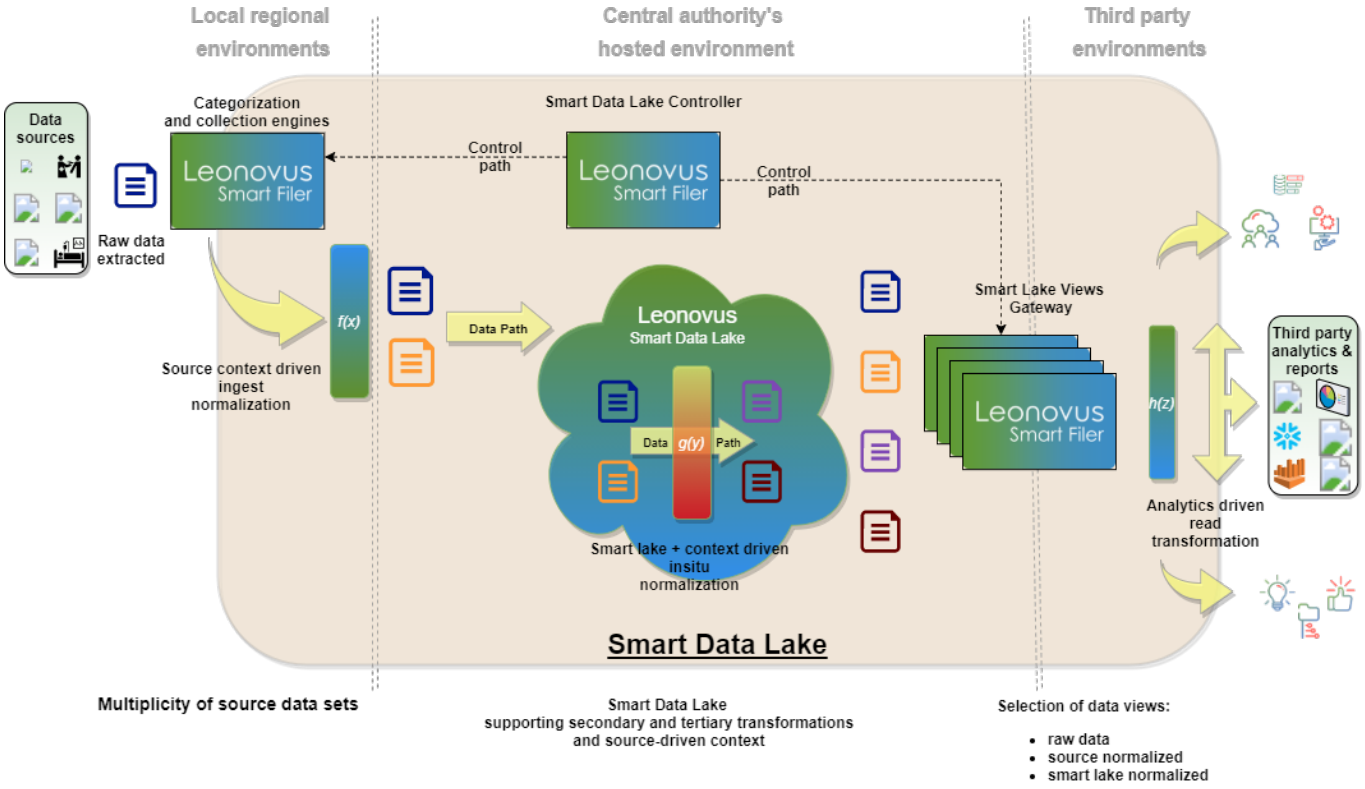


Figure 3 - Leonovus Smart Data Lake with deep context, concurrent data use, and multi-transformations.

Highly Secure Smart Data Lake

New data-centric security solutions must recognize and account for the data's use intentions, especially higher-order analytics. Data-driven business decisions and organizational actions based on analytical insights are rapidly becoming standard practice. Data analytics and data science have evolved from spreadsheets through business intelligence (BI) cubes to big data, streaming data, and comprehensive data sets for artificial intelligence (AI) and machine learning (ML). The use of collective data set repositories, such as data lakes and data warehouses, both on-premises and cloud-based, is rising. The Leonovus data-centric security solution supports these analytical architectures in its toolset.

The Leonovus Highly Secure Smart Data Lake (HSSDL) incorporates the capabilities of Data Discovery, Smart Filer, Vault and View Gateways to provide a data-centric secured solution for the management of organizational data sets and results in their analytics architectures. HSSDL provides analysts and data scientists with a means of managing and protecting their structured, semi-structured, and unstructured data sets.

Leonovus' HSSDL is the entry point of the organization's data pipeline, securing and enhancing the data's quality from its origin. From its contextually rich onboarding capabilities for both stream and file-based data sources to its normalized, managed data repository, the HSSDL offers a fully operational data lake. Its extraction, transformation, and loading (ETL) capabilities, combined with the sound data governance required of a data-centric security solution, ensure high-quality data and the controls to ensure the preservation of data integrity direct from the source of truth. HSSDL can be used directly as the source of data sets for analytics, either with third-party analytics or with its own bundled insights engine. Or it can be the critical first segment in a more complex data analytics pipeline, directly feeding industry-standard data warehouses, data lakes, and third-party analytics engines.

HSSDL increases the value of much of the data it on-boards. With a near-real-time onboarding automation engine and

obtaining data context and retaining that context through user-selected transformations, HSSDL provides richer data with higher performance analytics resulting in a shorter time to actionable insights. Controls and governance from the data origin and sourcing data are always maintained. With deeper context bundled and carried into the data lake, analytics are richer and more meaningful.

As an intrinsic part of its data-centric security model, HSSDL includes cost-saving data management and tiering of content within the data lake repository. Data sets can be retained, protected, and directly accessible as needed while managing costs by keeping idle data sets in lower-cost storage infrastructure. The cost savings, scalability, and elasticity of these capabilities enable affordable retention of larger, more meaningful data sets.

Leonovus maintains all the data protections outlined above throughout the data's residence in the Highly Secure Smart Data Lake. The data-centric security solution spans the data lake, including in-house analytics or, if necessary, all the way to secure data sharing with third-party analytics.

Impact Assessment and Regulatory Compliance

Because all data interactions are tracked and logged, the Leonovus managed system knows the extent of the intrusion and impact on the data would be readily available in the logs. These detailed logs supplement the logs of traditional file servers. Depending on the form of attack, they also offer another input for analytics. Instead of just file-level interactions, the Leonovus system works at a granularity of Vaulted file fragments. Therefore, post-incident analysis is fast. Generated reports thoroughly catalog any interactions and document the intrusion and compromised systems' extent and impact. The benefits are reduced business distraction and recovery times and supporting timely data privacy compliance, and the avoidance of fines.

Leonovus Secured Data Management Solution

Leonovus would not have avoided the SolarWinds hack. Still, Leonovus would have significantly reduced the attack's consequences, including the cost of data/information loss, revenue loss, or business disruption, as well as the social impacts on the organization

The system would have avoided almost all data and information loss due to passive system process observation. Similarly, Leonovus reduces and blunts ransomware. Where some loss might have occurred by stealing or forging valid and actively authenticated credentials, the length of time for which those credentials would be useful would be sharply restricted both by two-factor authentication and enhanced DLP analytics.