WHITE PAPER

HALOCORE HELPS INFOSYS EXTEND DATA PROTECTION OUTSIDE THE ORGANIZATION

Infosys®
Navigate your next

About the Organization

Infosys is a global leader in next-generation digital services and consulting. It enables clients in 46 countries to navigate their digital transformation. With US $13 billion annual revenues last year, Infosys serves over 1500 customers, has human capital of 249,000 employees, and manages millions of square feet of real estate. This calls for an extensive and reliable technology backbone that can deliver next-gen user experience (UX), powered by smart analytics, and mobilized by leading digital platforms such as SAP S/4HANA.

The Need for Data Security

The Covid-19 pandemic forced enterprises across the world to adopt remote working models and operate through cloud-based platforms. As a fast-growing number of smart devices become ever more connected, there is increasing incidence of cyber attacks. Data breaches exposed 36 billion records in the first half of 2020. Technology became the most attacked industry, accounting for 25% of all attacks. According to the "Cost of a Data Breach Report 2021" by IBM, the average global cost of a data breach rose to US $4.24 million in 2021. Thus, even though enterprises have stepped up their cyber defenses, the threat landscape is changing at an alarming rate; cyber attackers are innovating and are becoming more sophisticated in their attacks.

In this scenario, there are many new compliance regulations being enacted around data protection. The General Data Protection Regulation (GDPR) requires businesses to protect the personal data and privacy of EU citizens. Non-compliance with GDPR can cost companies dear. Similarly, the Personal Data Protection (PDP) bill tabled by the Indian Government seeks to provide protection of personal data of individuals and create a framework for processing such personal data. It has also established the Data Protection Authority for this purpose. With data volumes ballooning, determining what level of security is needed for each piece of information and the required regulatory compliance has also become a high priority for organizations.

Top Cybersecurity Challenges

Complexity in securing the environment – The numbers of mobile devices, smartphones, laptops, and tablets are rapidly rising. Users connect devices to multiple networks for both work and personal use. While it is easier to control activity on such devices within the organization's network perimeter, when these devices move beyond the enterprise, ensuring fool-proof protection is immensely challenging. Cloud environments are also becoming increasingly complex and, hence, not all endpoints are always secure.

Rising sophistication of attacks – The nature of attacks is evolving. While phishing is still the most common method used by hackers to steal sensitive data like personal information and financial data, these attacks too are growing in intelligence. Malicious insider attacks are also on the rise through employees with access to corporate networks. These threats are very difficult to detect.

Internal limitations – Many enterprises have not yet cultivated a culture that insists on employees being aware of cyber security and practicing behaviors that adhere to their security policies and technologies. Further, there is usually a lack of appropriate tools to automate controls, conduct effective audits, and detect security threats.

Why Data Protection is Important for Infosys

For over two decades, Infosys has maintained a consistent record of managing its business processes in a well-organized and coordinated manner for all its subsidiaries as well as stakeholders across finance, human resources, and delivery units. Considering the sheer scale of IT consulting and digital transformation projects Infosys delivers for clients across the globe, its operations are quite complex and governed by the strict need for data security.

On an annual basis, Infosys handles the following key metrics:

- Over 600,000 invoices
- Over 700,000 vendor payments
- Nearly 2.5 million pay slips
- Over 40,000 client projects
- 650,000 employee claims
- Approximately 6000 tax compliances
- 94 subsidiaries

The SAP Digital Transformation Journey

SAP is the core enterprise platform for Infosys. It forms the backbone for all its key business areas including finance, human capital management (HCM), procure to pay (P2P), planning and budgeting, and data warehousing.

The SAP digital transformation journey of Infosys was planned with milestones every 2 to 3 years. Infosys ERP system, which was pre-S/4 HANA, interfaced with multiple non-SAP and custom-developed .NET applications. A host of technologies was used to establish connections to these applications. For instance, within the NetWeaver suite, ECC interfaces with the following satellite applications:

- SAP PO/PI
- SAP BW/BI
- SAP GRC
- SAP Ariba
- SAP Cloud platform

The following technologies/methodologies were used to establish the connections:

- SAP ALE
- OData API endpoints
- Web services
- Remote function calls
- IDOCS

Third party/custom-developed interfaces include:

- Finance applications (over 25 systems)
- HCM applications (over 50 systems)
- Open-source applications (over 10 systems)
- Mobile applications (over 20 systems)
- Banks (nearly 10 banks)
- Third-party applications (5 to 6 systems)

Over the years, Infosys has added terabytes of data to these systems. The challenge was to address its exponential data growth and the ensuing landscape complexity. Besides having to add and sustain large data volumes, they also wanted to improve data protection and data security.

Setting data protection as a key goal, Infosys adopted a parallel project landscape to minimize impact on business-as-usual. The S4/HANA platform was designed to ensure zero recovery point objective (RPO) with synchronous replication between primary and similar appliances near the disaster recovery site. Infosys' HANA deployment is the world's largest single instance of SAP Business Suite powered by SAP HANA on Hitachi Unified Compute Platform (6TB RAM).

SAP Data Protection – A Pioneering Goal for Infosys

Infosys has an uncompromising corporate governance philosophy underlined by values of integrity and transparency, which are vital to gain and retain the trust of its stakeholders at all times. Known for its out-of-the-box thinking, Infosys wanted to be a pioneer in data protection with the stated aim of making its business future-proof.

Migrating to HANA gave Infosys access to good security controls. But they wanted to ensure that data was secure at all times when shared internally and externally. Sensitive data, particularly, had to be made available only to its employees and safeguarded from any third-party views or downloads. This insight was driven by Srinivas Poosarla, Vice President and Head (Global), Privacy and Data Protection at Infosys. Based in Bangalore, Srinivas is responsible for ensuring that Infosys complies with data protection regulations globally in over 30 countries.

> “We manage huge amounts of data day in and day out for all our business processes. Cyber threats and data breaches are not confined to the security department alone; they are a growing problem and a great cause of concern because a single data breach can jeopardize the entire organization. We were looking for a smarter data security solution that is powerful, simple to deploy, with no new infrastructure, flexible and one that integrates with existing security technologies”
>
> **Mr. Srinivas Poosarla,**
> *VP and Head, Privacy and Data Protection, Infosys.*

Why Infosys Chose HALOCORE

To stay protected in today's unpredictable threat landscape, a multi-layered security approach is advisable. Standalone security solutions are insufficient for long-term 360-degree protection.

Infosys had already implemented several security solutions across perimeter and network levels such as the rights management system (RMS) as well as Azure Information Protection (AIP) at an enterprise level. However, they found themselves lacking an effective solution to protect data. Data encryption was not automated or rule-based and was unavailable at the SAP user level.

Thus, Infosys wanted a solution that would provide automated data protection at the SAP user level. After considering many vendors, they found HALOCORE to be the only solution that met their requirements.

HALOCORE is a data security software that protects intellectual property and sensitive information extracted from SAP systems. HALOCORE, in combination with Microsoft AIP, is a truly comprehensive solution that secures all SAP data exiting at endpoints. It extends the SAP access control shield for intellectual property and other sensitive information beyond SAP boundaries. It also silently and automatically classifies and protects SAP data without any user intervention and drives quick and seamless integration.

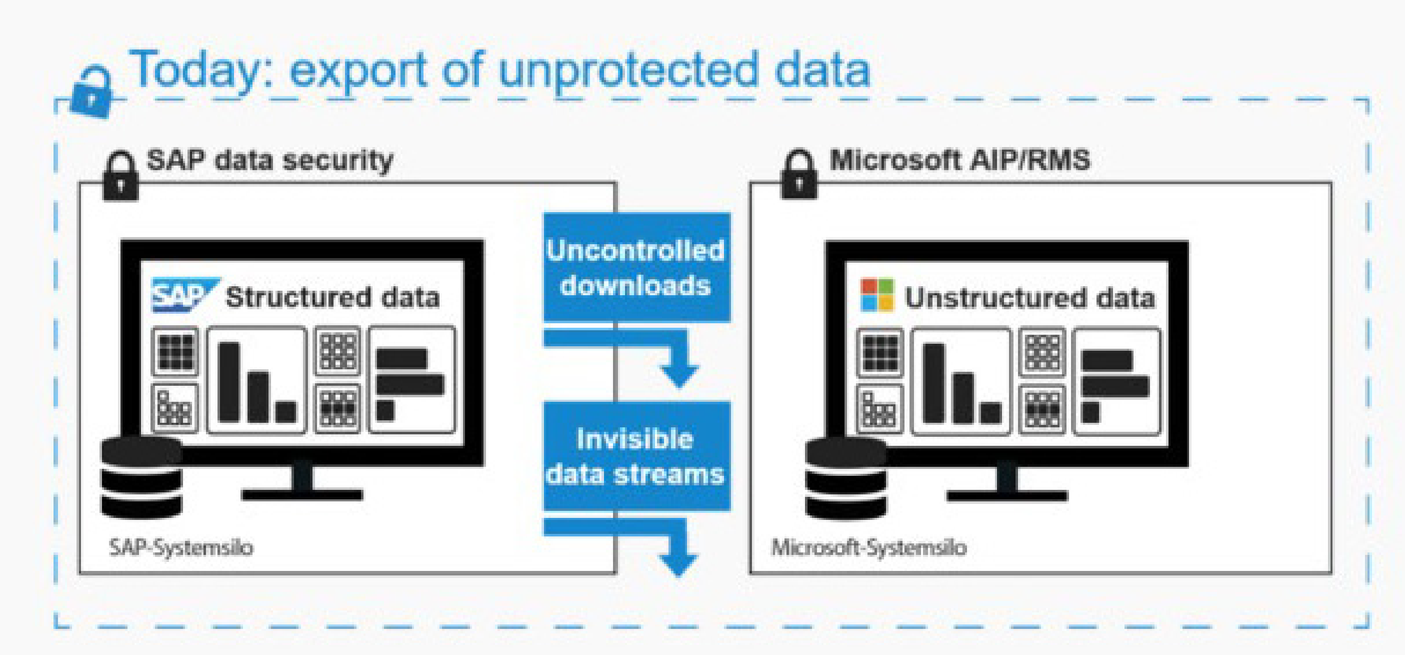

Figure 1 – Unique integration of MS AIP into SAP

Figure 1 shows how unprotected data is exported into various systems. Typically, once a document leaves a company's network, there is no control over how it can be accessed or used.

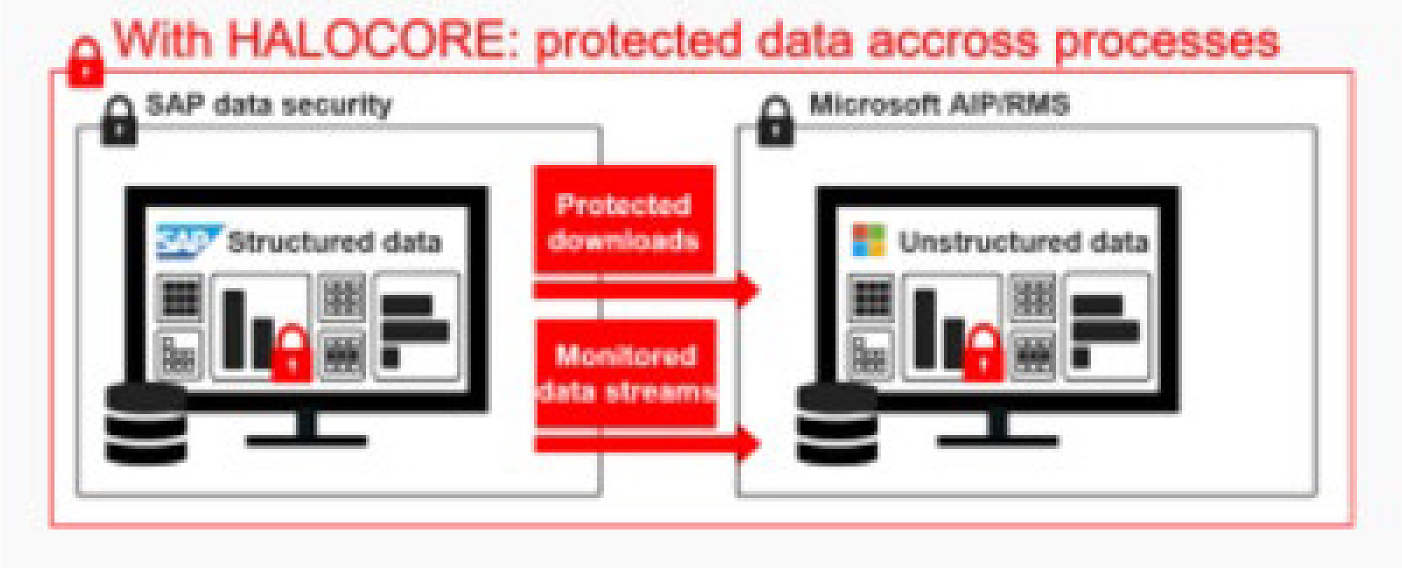

Figure 2 – Data protected with HALOCORE

Figure 2 shows how HALOCORE, through its PROTECT module, extends the SAP access control shield for intellectual property (IP), personally identifiable information (PII), toxic data, and other sensitive data moving beyond SAP's boundaries.

HALOCORE PROTECT intercepts the data being downloaded from SAP and applies fully customizable classification labels to the document's metadata. Additionally, it is tightly integrated with Microsoft Azure Information Protection and fully supports the implementation of Active Directory, Office 365, and Azure Active Directory. Using Microsoft AIP, every document exported from SAP is automatically and efficiently encrypted at the server level before it arrives on any device.

With the automated HALOCORE classification engine, granular authorizations and user rights are assigned to sensitive data, allowing easy and secure exchange of documents between employees, partners, and suppliers.

Methodology: A Data Security Solution by SECUDE

SECUDE, a global security solutions provider, offers innovative data protection for users of SAP and CAD/PLM software. For Infosys, the following deployment strategy was adopted:

- The solution was initially deployed and tested in a standalone sandbox environment by the technical teams of both SECUDE and Infosys.
- Then, the solution was deployed in the production/development system. Different business rules were configured. Various teams like IS, DPO, ISG, business, etc., were consulted to decide the AIP rules and templates. The project was closely monitored even at the board level because it addresses crucial requirements of enterprise-wide data protection and compliance.
- Once the business rules were defined, configured, and tested in the development system, the solution was shifted to quality control where • functional testing, user testing, and user acceptance testing were performed.
- The solution was then successfully deployed in other systems like development systems, quality systems, etc., after which it was finally handed over to the Infosys team with SECUDE providing the necessary support.

How HALOCORE Met Infosys' Needs

By integrating directly with SAP, HALOCORE protects data with automated classification. It blocks unauthorized reports and helps generate fine-grained access policies. HALOCORE met all of the requirements of Infosys that included:

- Protecting sensitive HR and other data coming out of SAP system
- Leveraging existing AIP/MIP labels automatically to encrypt and protect data
- Defining granular business rules whereby the system can identify, fetch, and apply the appropriate AIP template for data that is being downloaded from SAP
- Building valid exceptions into the rules engine based on the business requirements and treating these exceptions appropriately
- Automating operations without affecting the end-user experience in any way and making encrypted data seamlessly available to all authorized users
- Providing a layer of governance and protection on the available data
- Ensuring that the data protection remains intact even when the files are shared with an identified external authorized vendor
- Creating awareness and user education concerning the handling of sensitive data as users see the downloaded files with the appropriate label

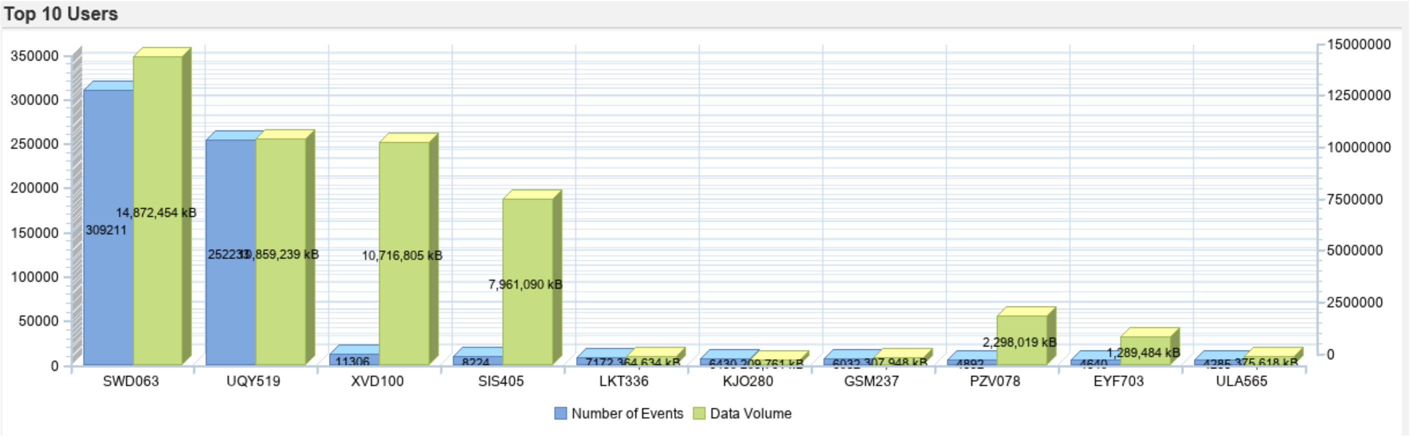

Figure 3 – Data volumes downloaded by Infosys users

The data shown in Figure 3 is captured from HALOCORE monitor reports and is presented in a pseudonymized form. Figure 4 shows the top 10 application components, file types, and IP address ranges from where data is downloaded into the HALOCORE system. Thanks to HALOCORE, the data remains protected no matter where it is downloaded.

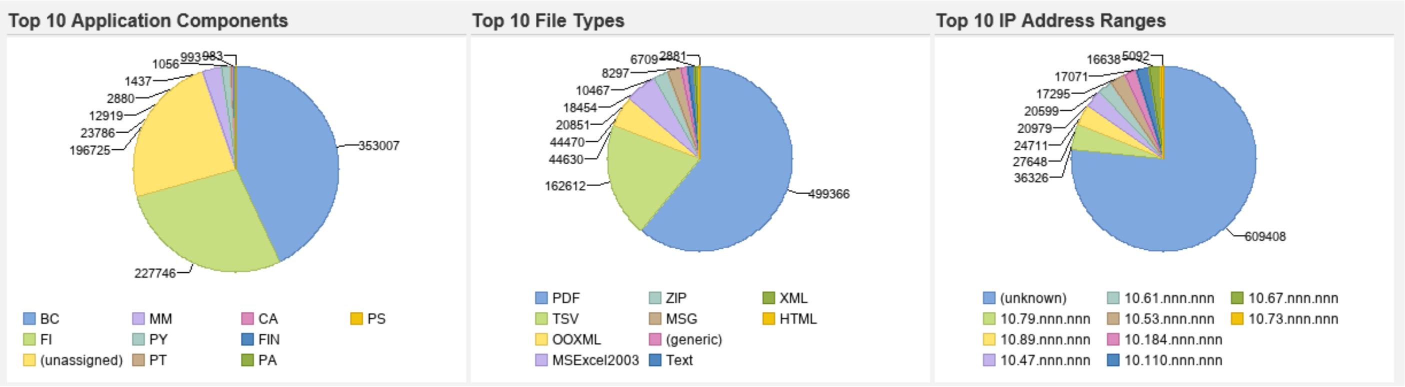

Figure 4 – How data is consumed through HALOCORE

In summary, HALOCORE provides automated protection even when many different systems communicate with each other and many users access and download data from different systems for various purposes.

> As organizations become more and more technology-oriented and resort to digitalization, privacy seems to slip away. Remote working styles, together with a huge amount of data being produced, are a cause for concern for organizations like Infosys. We value our clients' data and any infringement would cost us heavily. This is why we wanted a solution that protects all our sensitive data. Being a global organization, we didn't want any disruptions at the user end either. HALOCORE was the perfect solution for us. Data is automatically protected from unauthorized access. The entire project was completed without any hindrances to business as usual. We look forward to our continued relationship with SECUDE for data protection of our other systems.
>
> **Kiran Gole,**
> *Industry Principal, Head of SAP Practice, Infosys IT.*

Benefits of the Solution

HALOCORE provided Infosys with a data-centric protection solution across the entire data lifecycle. It is helping Infosys:

- Easily and securely exchange documents with anyone inside and outside the organization including colleagues, partners, and customers
- Support organization-specific scenarios on mobile devices, in the cloud, and on-premises
- Achieve secure storage of sensitive SAP documents on mobile and cloud platforms with support of all common file types
- Ensure strong document encryption without impairing business processes
- Automate AIP policy assignment for SAP downloads according to the classification

Table 1 displays the complete protection offered by HALOCORE. Nearly 20,000 transactions benefitted from HALOCORE data protection.

Table 1 – SAP HCM transactions protected through HALOCORE

Types of HCM transactions	Standard	Custom
PA-OM transactions	7405	458
Time/leave transactions	5550	309
Payroll transactions	5555	414
ECM (iRewards) transactions	0	309
Total	18,510	1,490

The Road Ahead

Currently, HALOCORE is in production for Infosys human capital management system. The Infosys Data Protection unit is further pushing for HALOCORE adoption in other modules, underscoring the confidence Infosys has in the data-centric properties of HALOCORE. Next in line for rollout is Infosys SAP BO (Business Objects) Platform. HALOCORE will be tasked with protecting data on SAP BO, the enterprise-wide reporting platform, for SAP as well as other non-SAP internal systems. Deployments are also planned for finance and other transaction modules.

Data protection is a journey, not a destination. The constant evolution of cyber threats means that data protection and employee education are constant requirements for enterprises looking to sustain their business. Data-centric protection acts as a business enabler, reducing the negative impact of data breaches, enhancing organizational reputation, and winning customer trust.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected