Secude

Case Study

How a multinational professional services company uses Secude's HaloCORE to protect financial data downloaded from SAP and certify its financial statements.

Background

The global professional services company provides strategic, technological and operational solutions to leading organizations in over 120 countries. As one of the largest multinational consultancies in the world, the company has the cybersecurity resources to secure its infrastructure, operations and servers. But with an increasing reliance on cloud-based platforms, the company was worried about data leaving its secure systems.

With a brand value in excess of $40 billion, even a 1% hit from a data breach would cost $400 million - but the reputational damage would be significantly worse if information was exposed during the company's restricted periods. With over 700,000 employees exacerbating the risk of inadvertent data loss, the company sought a solution that would automatically protect data coming out of its secure systems.

What's more, as a public company, the professional services company needed to prove its financial data security in order to comply with the 2002 Sarbanes-Oxley Act (SOX Act). This included maintaining internal controls to protect financial data, regularly performing compliance audits and passing an annual independent audit of its financial statements.

The Challenge

The global professional services company is one of the largest Microsoft Information Protection users in the world, but this protection does not extend

At a Glance

Vertical
Technological Services and Solutions

Company
Professional Services

Employees
700,000+

Location
Multiple locations worldwide

Highlights

The client needed to protect its sensitive financial data downloaded from the SAP system and shared outside the company.

HaloCORE protected the client's SAP data from the application layer, automatically securing all SAP downloads from accidental disclosure and rogue actors.

The client was able to prevent damaging leaks during its closed accounting periods and meet its regulatory requirements, including certification of its public financial statements.

About Secude

Secude, a Microsoft and SAP Partner, is a global leader for Zero Trust data protection and data governance.

Secude has been protecting the data of Fortune 500 companies for over 25 years. Our Microsoft Purview Information Protection (MPIP) extension embeds Zero Trust protection and data governance into our customers sensitive files from creation, preventing data leakage, reputational damage and non-compliance. With branches in Europe, North America and Asia, Secude supports customers with the implementation of IT security strategies through a global network.

HaloCORE

Member of
Microsoft Intelligent Security Association
Microsoft Security

beyond its internal network. In addition, the company's existing security solutions protected its data at various layers (i.e. at the gateway, OS, and database layers), but didn't protect content downloaded from its secure systems, such as SAP.

The professional services company uses SAP S/4HANA to store sensitive financial, payroll and HR data, but as soon as data is extracted from the SAP system, they lose control of it. The company wanted to protect the confidentiality of its SAP downloadables and prevent departing employees from accessing this data, but also share extracted SAP data with external parties when required.

What's more, the company needed a security tool that enabled it to meet its legal controls and audit requirements under the SOX Act, which requires all public companies in the US to prove the accuracy and security of its quarterly and yearly financial reports.

The Solution

The company found only one product on the market that matched its requirements and met its strict security policies: Secude's HaloCORE.

HaloCORE is purpose-built to protect sensitive data extracted from SAP systems and provided the company with:

- **Automatic protection of SAP data downloads.** HaloCORE embeds Microsoft Purview Information Protection (MPIP) directly into SAP's application layer, automatically protecting the most sensitive financial and non-public insider information coming out of the SAP system. Unlike data loss prevention (DLP) products that trigger MPIP at the laptop level, HaloCORE is embedded in files from creation, so SAP downloads are protected no matter which device is used.

- **Authorization control outside of the company's secure system.** HaloCORE leverages MPIP labels to automatically encrypt data with chosen classifications, adding a tag which lives with the file even if it's moved outside the company's network. As HaloCORE is embedded at the application level, this security follows extracted data wherever it travels.

- **Data monitoring and access logs for compliance.** HaloCORE automatically protects SAP data exports without affecting the end-user experience, enabling the company to share data to third parties seamlessly and securely. In addition, HaloCORE also monitors data access and file edits, storing this information in accessible logs to simplify compliance requirements.

The Results

Through a direct SAP integration, HaloCORE protected the professional services company's extracted SAP data by default and ensured the company complied with its regulatory requirements.

In particular, HaloCORE helped the company:

- **Prevent damaging data breaches.** With over $60 billion in annual revenue and more than 700,000 employees worldwide, the professional services company was worried about the potential impact of data breaches arising when employees downloaded files from SAP. As HaloCORE is integrated at the application layer, all of the company's sensitive SAP information was automatically protected - both before and after extraction from the SAP system. As such, the company's SAP data is protected from accidental disclosure and targeted attacks no matter who downloads the data, what device is used, or where it travels.

- **Avoid accidental leaks during closed accounting periods.** As a public company listed on the New York Stock Exchange, the company was particularly concerned about leaks when conducting its financial close, which could cost in excess of seven figures and have a damaging impact on its reputation. During closed accounting periods, only insiders are allowed to access sensitive financial information ahead of publication, but the company was worried that a departing employee could take this material with them and couldn't guarantee that it hadn't been accessed. HaloCORE's automatic labeling checks user credentials every time the data is accessed - even if files are outside the company's network or already in the hands of a rogue actor. As such, the company has peace of mind that leaks are highly unlikely to occur during restricted periods.

- **Ensure compliance with regulatory requirements.** As a public enterprise, the professional services company must certify its financial statements and guarantee the security of its financial information in order to function. HaloCORE's lifelong file access control and detailed monitoring makes it easy for the company to comply with all the regulations under the SOX Act. What's more, HaloCORE ensures that HR data held in SAP is compliant with General Data Protection Regulations (GDPR). Even if an HR member with access to highly confidential information moves to a new role with different access permission, HaloCORE guarantees that new access rules apply, thereby helping the company to avoid GDPR fines (i.e. GDPR violations can reach up to $20 million) and bad press.

Summary

Secude's HaloCORE for SAP security enabled the multinational professional services company to:

- Automatically protect SAP downloads from unauthorized access and accidental leaks - especially during closed accounting periods.

- Protect the company from rogue actors leaving the company or employees moving roles with different access permissions to sensitive data.

- Meet stringent regulatory requirements, including certifying its financial statements according to US rules for publicly-traded enterprises.

> Once data leaves our secure SAP applications we lose control. But with HaloCORE automatically protecting the data coming out of the system, it's much safer. Preventing information leaks saves us the time and cost to repair the damage and protects our brand reputation.

Global IT Technology Director for SAP, Global Professional Services Company

---

For more information about Secude: www.secude.com

Phone: USA/Canada: +1 800-900-9633　|　India: +91 44 4777 9704　|　Switzerland: + 41 41 510 70 70
Email: USA/Canada: AmericasSales@secude.com　|　EMEA: EMEASales@secude.com