The invisible security gap:

Why companies need to better protect SAP exports

WHITE PAPER

automatics

www.automatics.ai

automatics

Contents

Introduction

Cybercrime has changed dramatically in recent years. While traditional ransomware used to dominate, extortion using stolen data is now increasingly gaining attention. In its 2024 Federal Situation Report, the Federal Criminal Police Office (BKA) describes that data theft and data extortion are now among the greatest threats to companies. The latest SAPinsider benchmark study from May 2025 also confirms this trend: for the first time, data exfiltration is considered the greatest threat to SAP systems – even ahead of unpatched systems and credential compromises.

The reason for this is simple. SAP processes a company's most valuable information: personal data of employees and customers, highly confidential production and development secrets, financial figures, and information on supply chains and contracts. As long as this data remains in the SAP system, it is well protected by authorizations, encryption, audits, and monitoring. But the moment it is exported, this protection abruptly ends.

As soon as data is exported from SAP in the form of Excel spreadsheets, PDF reports, or Word documents, companies lose control. No one can know with certainty who exported which file, where it was forwarded, or who has access to it. These files end up unencrypted on laptops, in cloud folders, or in emails to external partners. From that moment on, a dangerous window opens that cybercriminals, insiders, or simply careless employees can easily exploit.

The consequences range from massive data breaches with hefty fines to the loss of business-critical secrets and even serious reputational damage. SAPinsider points out that 92% of companies classify their SAP systems as business-critical and contain highly sensitive data. Despite this, more than half of the companies lack a tested incident response plan specifically for SAP systems. The gap between the importance of the data and the existing protection measures is evident.

This white paper demonstrates why SAP exports, in particular, represent an invisible yet highly risky security vulnerability. We explain what exactly is at stake, which regulatory requirements are affected, and how companies can seamlessly integrate their SAP exports into a zero-trust, Microsoft Purview-based security concept with SecurityHub from automatics.AI.

What this white paper is about

With this white paper, we would like to contribute to answering precisely these questions and focusing on the essentials:

- why exporting from SAP can be so dangerous,
- what exactly is at stake,
- How to close this gap with automatics.AI SecurityHub and Microsoft Purview Information Protection.

Who is this white paper for?

This white paper is aimed at all those responsible for protecting corporate data:

- SAP decision makers & SAP Basis admins,
- CISOs & security teams,
- Microsoft Purview & Security Managers,
- Consultants & Auditors, who want to understand how they can seamlessly integrate SAP exports into their company's security concept.

Why Zero Trust Data Protection is Essential in the SAP Context

SAP systems are among the most complex and critical enterprise applications. They converge central business processes and contain a large portion of a company's most valuable data. Securing these systems has therefore rightly gained significant importance in recent years. Companies are investing in robust authorization models, network segmentation, system encryption, patch management, and continuous security monitoring.

As long as the data remains in the SAP system, these measures are reliable. They prevent unauthorized access, ensure the integrity of processes, and, in the event of an attack, provide usable logs for analysis and audits. However, this very protection breaks down the moment data is exported from SAP.

An exported document no longer has any role or permission logic. It becomes a file that can be stored on a device, sent via email, saved on a USB stick, or uploaded to a cloud folder. From this moment on, companies lose traceability and thus control. There is no longer any automatic logging, no restrictions on copies, and no technical barrier preventing sharing.

The Zero Trust principle provides the appropriate answer to this problem. Zero Trust means that no user, no device, and no application is considered trustworthy per se – rather, all access must be continuously reviewed and secured by policies. Applied to SAP data, this means: Protection must not end at the system boundary, but must be tied to the data itself. Only if files are classified, encrypted, and assigned dynamic permissions outside of SAP can a consistent security and compliance standard be maintained.

Microsoft is pursuing this approach with Purview Information Protection. Sensitivity labels enable files to be automatically tagged, assigned policies, and encrypted if necessary when they are created or exported. This ensures that a confidential document remains protected even after it has left the SAP system.

For companies, this means that Zero Trust data protection is not an abstract security strategy, but a concrete necessity in the SAP context. Only in this way can data protection, compliance, and protection against data misuse be consistently enforced – regardless of where the information is stored or who shares it.

SAP data in the focus of cybercrime

SAP systems as a worthwhile target

SAP systems are the backbone of many companies. They process not only transactions but also the most sensitive data sets: personal information of employees and customers, financial and tax data, production information, supply chain and contract details. This makes SAP systems an extremely attractive target for attackers, as a successful attack has immediate economic and regulatory consequences.

The threat landscape has noticeably worsened in recent years. According to the Federal Criminal Police Office, data-driven extortion is now one of the most serious cybercrime phenomena. This is particularly evident in the current federal situation report: Attackers are combining system encryption with the exfiltration of sensitive data ("double extortion"). Companies are being extorted not only because their systems are crippled, but also because confidential data is at risk of being published.

Independent analysts also confirm this trend. The SAPinsider Benchmark Study 2025 shows that for the first time, data exfiltration is considered the greatest threat to SAP systems, even ahead of traditional risks such as uninstalled patches or compromised access data. This makes it clear that protecting sensitive data, and in particular securing the export path, is becoming the center of every modern SAP security strategy.

Why attackers target SAP data

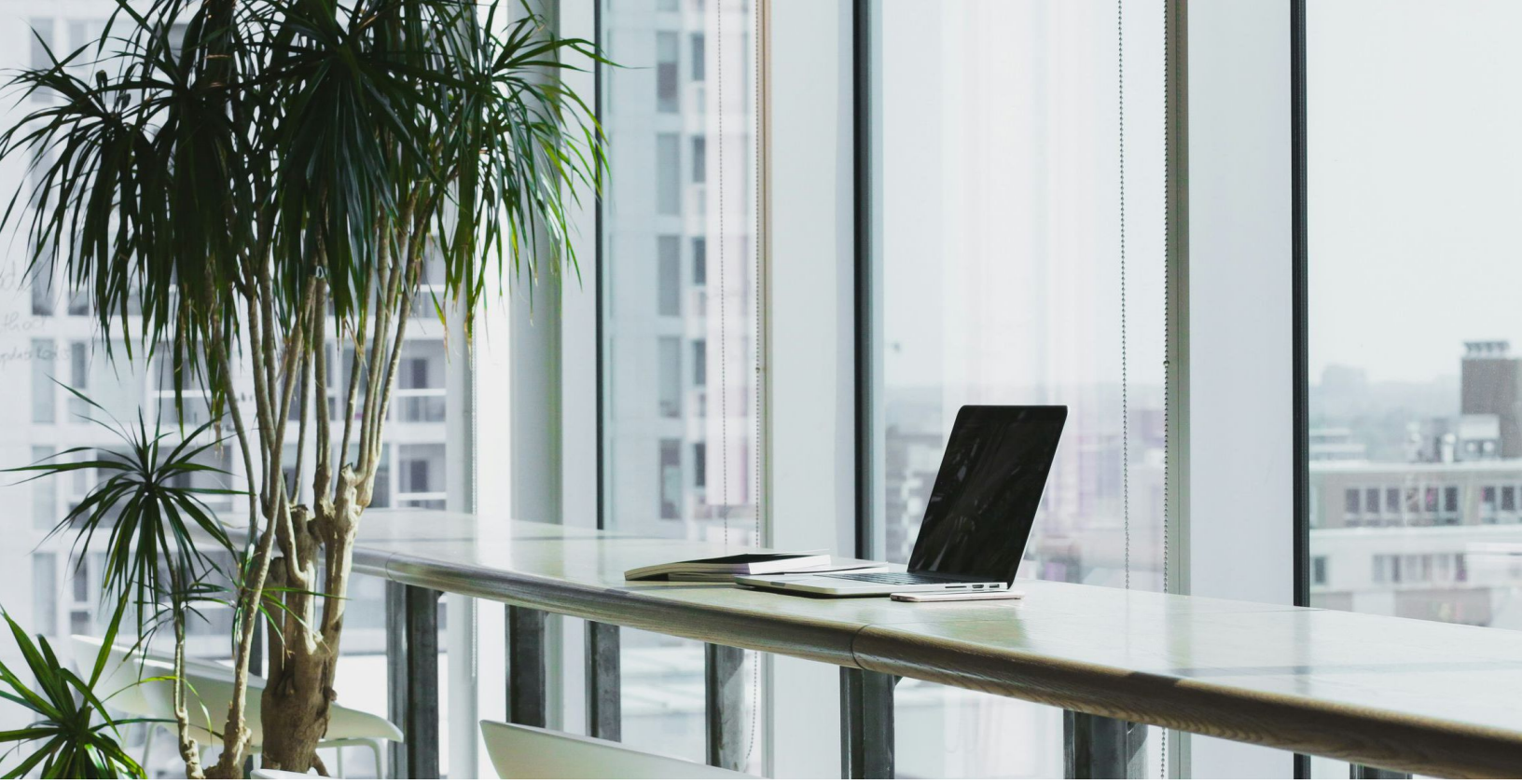
The attractiveness of SAP data to cybercriminals stems from three factors: its high business value, its sensitivity in the regulatory context, and its availability via exports.

- **Financial data:** Quarterly reports, cash flows, and balance sheets contain confidential information that, if published, could trigger price movements or reputational damage.
- **HR data:** Employee lists, salary data, and social security information are subject to strict data protection regulations. Loss of these data directly results in fines under the GDPR.
- **Supply chain data:** Information about suppliers, partners, and contracts can be misused by competitors or used for blackmail.
- **Production and IP data:** Recipes, design plans, and patents are often a company's most important intellectual property. Their leakage directly threatens competitiveness.

Consequences of data exfiltration

A successful attack on SAP data is not a purely technical problem, but an existential threat to the company. The impact manifests itself in several dimensions:

- **Regulatory risks:** Violations of GDPR, SOX, or BSI standards result in significant fines and documentation obligations.
- **Reputational losses:** Confidential data on the dark web or in media reports undermines the trust of customers and partners.
- **Financial damages:** In addition to ransom demands, costs arise from business interruptions, recovery efforts, and litigation.
- **Strategic risks:** The loss of IP or business data permanently shifts competitive advantages.



SAP systems today are at the center of a dual threat: On the one hand, they are business-critical and indispensable, yet on the other, they are highly attractive to attackers. Scenarios in which data is exported from the systems and thus falls outside the protected context are particularly dangerous. This is precisely where one of the biggest security gaps lies that must be closed – not through traditional protection measures within the system, but through a data-centric zero-trust approach that ensures protection even outside of SAP.

The blind spot - When SAP data is exported

Protection within SAP

Companies have been investing considerable resources for years to protect their SAP systems against attacks. Authorization models, encryption, network security, and monitoring ensure that data in the system is reliably protected. Role and rights concepts regulate access, and logging provides valuable information for audits and incident response.

But this protection ends abruptly as soon as data is exported. The moment a table, report, or document is output to Excel, PDF, or Word, it loses its connection to the SAP security architecture.

The moment of loss of control

An exported document is no longer tied to SAP authorizations. It becomes a file that can be saved on a device, forwarded via email, or uploaded to cloud services. From this point on, the following applies:

- **No role logic:** Access is no longer restricted by SAP authorizations.
- **No logging:** There is no tracking of who opens or forwards the file.
- **No security mechanisms:** Classification and encryption are not required unless supplemented externally.

Typical risks in everyday work

Precisely because exporting is part of the everyday life of many SAP users, risks arise not from malicious intent, but from routine:

- **HR department:** Export of employee lists for external service providers, sent unencrypted via email.
- **Finance Team:** Creation of monthly or quarterly reports that are stored in unsecured folders.
- **Supply chain:** Exchange of supplier data with partners, which later circulates uncontrolled.

In all cases, companies lose traceability and thus control over their most sensitive information.

Shadow IT through exports

Exported files quickly migrate to areas outside the IT control room: onto USB sticks, private cloud drives, or messaging services. This shadow IT is barely visible to companies, but it significantly increases the risk. Cybercriminals exploit precisely these gaps to steal data or misuse it for extortion.

Bridge to the solution: Zero Trust also outside of SAP

The crucial step is to not let protection end at the system boundary, but to tie it to the data itself. SecurityHub from automatics.AI addresses this:

- **Automatic classification:** Each exported file receives a label according to its sensitivity.
- **Encryption:** Protective measures accompany the file regardless of its storage location.
- **Integration with Microsoft Purview Information Protection (MPIP):** Exported SAP data becomes part of the Microsoft security ecosystem and is subject to the same zero-trust policies as other critical corporate data.

This creates consistent protection across the entire file lifecycle – from the SAP system to the collaboration environment.

The solution for secure SAP exports

From loss of control to consistent security

The central problem with SAP exports is the immediate loss of all system protection mechanisms. SecurityHub addresses this issue and closes the gap by ensuring that SAP data is subject to the same security and compliance requirements after export as it is in the system itself.

SecurityHub doesn't complement SAP, but rather enhances it. Exports are not only monitored, but consistent protection measures are automatically applied. Companies thus gain not only transparency but also active control over the entire lifecycle of their data.

Real-time monitoring of exports

SecurityHub detects every export from SAP in real time.
Companies immediately see:

- Who exported which data?
- In what format (Excel, PDF, Word) are the files available?
- Where was the data exported or w ei t forwarded?

This transparency creates the basis for well-founded decisions and enables audit - proof traceability .

Automatic classification

Each export is automatically classified based on defined rules, for example:

- "Public"
- “Internal”
- "Confidential"
- “Strictly confidential”

The classification is consistent and prevents users from having to make decisions independently or based on gut feeling .

Encryption and Policy Enforcement

Based on the classification, SecurityHub can automatically apply encryption and enforce policies:

- “May only be read, not forwarded”
- “Access only allowed by certain groups or roles”
- “Only usable within the corporate network”

This means that the protection remains tied to the file no matter where it is saved or opened.

Auditable documentation

Every action - from export to classification to file use - is logged. Companies can track at any time:

- Which data was exported
- What measures were applied
- Who had access
- Whether guidelines were complied with

This not only strengthens internal security, but also ensures that regulatory compliance obligations can be reliably met.

Seamless integration with Microsoft Purview Information Protection (MPIP)

One of SecurityHub's greatest benefits is its deep integration with the Microsoft security ecosystem. Exported SAP files are automatically integrated into MPIP. This ensures the same zero-trust policies that companies already use for Microsoft 365 data apply:

- Use of sensitivity labels
- Enforcement of policies in Office applications (Outlook, Teams, SharePoint, OneDrive)
- Unified security and compliance strategies for SAP and Microsoft data

The result is consistent, company-wide data protection without SAP data taking on a “special role.”

Technical depth: What SecurityHub does in detail

SecurityHub is distinguished by its comprehensive monitoring of all relevant export paths from SAP. These include traditional downloads, sending via email, printing documents, and exports via RFC interfaces. Each of these paths is recorded and logged in real time, providing companies with transparency about the whereabouts of their data at all times.

Unlike proxy-based approaches, SecurityHub is integrated directly into the SAP server. This architecture ensures that no detours via external systems are necessary and the performance and stability of the SAP landscape are maintained. At the same time, this tight integration means that SecurityHub can be fully deployed in both traditional SAP ECC environments and modern scenarios such as RISE with SAP.

The solution is certified by SAP, providing companies with additional security during implementation and operation. SecurityHub also allows for flexible customization: Companies can define their own classifications for data exports, thus directly reflecting their own compliance requirements or industry-specific regulations.

Another key feature is its deep integration into the security infrastructure: Standardized interfaces allow export logs and classification information to be fed into Azure Sentinel and other SIEM systems. This makes SecurityHub the link between SAP and the company's central security ecosystem.

The solution remains completely transparent for users. Export processes run as usual, without requiring additional clicks or complex workflows. Security is thus automatically ensured without limiting user productivity.

A practical look: SAP export without vs. with SecurityHub

Without SecurityHub:

An HR employee exports a list of salary data to Excel, saves it on her desktop, and emails it to an external service provider. From that moment on, there is no longer any control. No one knows whether the file will be forwarded or opened without authorization.

With SecurityHub:

Upon export, the file is automatically classified as "highly confidential" and encrypted. It can only be opened by the intended recipients, and forwarding is blocked. Every interaction with the file is logged. The company maintains control at all times while complying with GDPR and internal guidelines.

SecurityHub makes SAP data exports predictable and secure. Instead of losing control at the system boundary, companies maintain transparency, traceability, and protection measures throughout the entire data lifecycle. Integration with Microsoft Purview Information Protection makes SecurityHub a key component of a modern zero-trust strategy.

Assess risks and derive concrete areas of action

The underestimated gap in SAP security strategies

Many discussions with companies reveal that the greatest uncertainty lies not in whether data exports pose a risk, but rather in the extent of this risk in a specific case. Often, a structured assessment is lacking that clarifies which data is most critical, how often it is exported, and what regulatory requirements are associated with it.

Typical questions that companies should clarify

Which data regularly leaves the SAP system?
HR lists, financial reports, supplier data, production information.

Who exports this data and for what purpose?
Internal users, external partners, service providers.

Where does this data end up after export?
Local devices, file shares, cloud storage, emails.

What regulatory requirements apply?
GDPR, SOX, BSI IT-Grundschutz, NIS2, DORA, ISO27001, industry-specific regulations.

What impact would a data leak have?
Financial losses, fines, reputational damage, loss of IP.

A structured valuation approach

Companies can create transparency in just a few steps:

1. **Data inventory:** Record what types of data are exported regularly.
2. **Criticality analysis:** Classifying which of these data are particularly worthy of protection.
3. **Evaluate export channels:** Analyze which channels (email, cloud, USB) are used to distribute data.
4. **Play through risk scenarios:** Identify possible consequences of data leakage.
5. **Compare protective measures:** Check which controls are currently effective and where gaps exist.

SecurityHub as a tool for risk assessment and minimization

SecurityHub supports this assessment not only theoretically but also practically:

- **Real-time transparency:** Companies immediately see which data is being exported.
- **Risk-based classification:** Data is automatically classified according to sensitivity.
- **Continuous documentation:** Every activity is recorded in a traceable manner.

This turns an abstract risk analysis into an ongoing process that gives companies the opportunity not only to identify risks but also to actively manage them.

Conclusion

From the blind spot to resilient SAP security

Companies have invested heavily in protecting their SAP systems in recent years. Authorization models, encryption, monitoring, and compliance measures ensure a high level of security, but only as long as the data remains in the system. However, the moment of export, this protection abruptly ends. Files become uncontrolled copies whose whereabouts can no longer be traced. This is precisely where the invisible but most dangerous security gap lies: Attackers exploit exports to access sensitive information, employees often unknowingly act riskily, and companies lose control of their most valuable data.

Cybercrime is evolving rapidly. Data exfiltration and blackmail using stolen information are among the greatest threats facing companies today. Those who want to survive in this reality can no longer allow protection to end at the system's perimeter. Zero Trust is transforming from a buzzword to an essential principle: every file, every export, and every access must be reviewed and controlled.

This is precisely where SecurityHub from automatics.AI comes in. The platform no longer ties protection measures solely to systems, but directly to the data. It combines real-time visibility, automatic classification, encryption, and integration with Microsoft Purview Information Protection into a consistent line of defense. SecurityHub transforms export from an invisible vulnerability into a controlled and auditable process.

The message is clear: SAP security doesn't end at the system boundary. It must encompass the entire data lifecycle – from capture to export. Companies that take this step now not only ensure compliance and protection against attacks, but also create true resilience. They transform one of the biggest weaknesses in their security architecture into a strength – and make their SAP landscape fit for the future.

At automatics.AI, we understand your challenges.

Our customers know how important it is that security must extend beyond system boundaries.

We will accompany you on this journey.

automatics

SmartSecOps Platform

Automated.
Protected.
Smart.