Die unsichtbare Sicherheitslücke:

Warum Unternehmen SAP-Exporte besser schützen müssen

WHITE PAPER

automatics

www.automatics.ai

automatics

Inhalt

Einleitung

Cybercrime hat sich in den letzten Jahren dramatisch verändert. Während früher klassische Ransomware im Vordergrund stand, rückt heute immer stärker die Erpressung mit gestohlenen Daten in den Fokus. Das Bundeskriminalamt beschreibt in seinem Bundeslagebild 2024, dass Datendiebstahl und Data Extortion mittlerweile zu den größten Gefahren für Unternehmen zählen. Auch die aktuelle Benchmark-Studie von SAPinsider aus Mai 2025 bestätigt diesen Trend: Datenexfiltration gilt erstmals als die größte Bedrohung für SAP-Systeme – noch vor unpatched Systems und Credential-Kompromittierungen.

Der Grund dafür ist einfach. In SAP werden die wertvollsten Informationen eines Unternehmens verarbeitet: personenbezogene Daten von Mitarbeitern und Kunden, streng vertrauliche Produktions- und Entwicklungsgeheimnisse, Finanzkennzahlen sowie Informationen zu Lieferketten und Verträgen. Solange diese Daten im SAP-System verbleiben, sind sie durch Berechtigungen, Verschlüsselung, Audits und Monitoring gut geschützt. Doch im Moment des Exports endet dieser Schutz abrupt.

Sobald Daten in Form von Excel-Tabellen, PDF-Berichten oder Word-Dokumenten aus SAP exportiert werden, verlieren Unternehmen die Kontrolle. Niemand kann mit Sicherheit sagen, wer welche Datei exportiert hat, wohin sie weitergeleitet wurde und wer darauf Zugriff hat. Diese Dateien landen unverschlüsselt auf Laptops, in Cloud-Ordnern oder in E-Mails an externe Partner. Ab diesem Augenblick öffnet sich ein gefährliches Fenster, das Cyberkriminelle, Insider oder schlichtweg unachtsame Mitarbeiter leicht ausnutzen können.

Die Folgen reichen von massiven Datenschutzverletzungen mit hohen Bußgeldern über den Verlust geschäftskritischer Geheimnisse bis hin zu gravierenden Reputationsschäden. SAPinsider weist darauf hin, dass 92 % der Unternehmen ihre SAP-Systeme als geschäftskritisch mit hochsensiblen Daten einstufen. Trotzdem existiert in mehr als der Hälfte der Unternehmen kein getesteter Incident-Response-Plan speziell für SAP-Systeme. Die Kluft zwischen der Bedeutung der Daten und den bestehenden Schutzmaßnahmen ist offensichtlich.

Dieses Whitepaper zeigt, warum gerade SAP-Exporte eine unsichtbare, aber hochriskante Sicherheitslücke darstellen. Wir erläutern, was konkret auf dem Spiel steht, welche regulatorischen Anforderungen betroffen sind und wie Unternehmen mit SecurityHub von automatics.AI ihre SAP-Exporte nahtlos in ein Zero-Trust- und Microsoft-Purview-basiertes Sicherheitskonzept integrieren können.

Worum es in diesem Whitepaper geht

Wir möchten mit diesem Whitepaper einen Beitrag leisten, um genau diese Fragen zu beantworten und den Blick auf das Wesentliche zu lenken:

- warum der Export aus SAP so gefährlich sein kann,
- was genau auf dem Spiel steht,
- wie Sie diese Lücke mit automatics.AI SecurityHub und Microsoft Purview Information Protection schließen.

Für wen ist diese Whitepaper?

Dieses Whitepaper richtet sich an alle, die Verantwortung für den Schutz von Unternehmensdaten tragen:

- SAP-Entscheider & SAP-Basis-Admins,
- CISOs & Security-Teams,
- Microsoft-Purview- & Security-Verantwortliche,
- Berater & Auditoren,

die verstehen möchten, wie sie SAP-Exporte nahtlos in das Sicherheitskonzept ihres Unternehmens integrieren können.

Warum Zero-Trust-Datenschutz im SAP-Kontext unverzichtbar ist

SAP-Systeme zählen zu den komplexesten und zugleich kritischsten Unternehmensanwendungen. In ihnen laufen zentrale Geschäftsprozesse zusammen, und sie enthalten einen Großteil der wertvollsten Datenbestände eines Unternehmens. Die Absicherung dieser Systeme hat deshalb in den vergangenen Jahren zurecht erheblich an Bedeutung gewonnen. Unternehmen investieren in robuste Berechtigungsmodelle, Netzwerksegmentierung, Verschlüsselung im System, Patchmanagement und kontinuierliches Security Monitoring.

Solange die Daten im SAP-System verbleiben, greifen diese Maßnahmen zuverlässig. Sie verhindern unberechtigte Zugriffe, stellen die Integrität von Prozessen sicher und liefern im Falle eines Angriffs verwertbare Protokolle für Analysen und Audits. Genau dieser Schutz bricht jedoch in dem Moment weg, in dem Daten aus SAP exportiert werden.

Ein exportiertes Dokument kennt keine Rollen- und Berechtigungslogik mehr. Es wird zu einer Datei, die auf einem Endgerät liegt, per E-Mail verschickt, auf einem USB-Stick gespeichert oder in einen Cloud-Ordner hochgeladen werden kann. Ab diesem Augenblick verlieren Unternehmen die Nachvollziehbarkeit und damit auch die Kontrolle. Es gibt keine automatische Protokollierung mehr, keine Einschränkungen für Kopien und keine technische Barriere, die eine Weitergabe verhindert.

Das Zero-Trust-Prinzip liefert die passende Antwort auf diese Problematik. Zero Trust bedeutet, dass kein Nutzer, kein Gerät und keine Anwendung per se als vertrauenswürdig gilt - vielmehr müssen alle Zugriffe kontinuierlich überprüft und durch Richtlinien abgesichert werden. Übertragen auf SAP-Daten heißt das: Der Schutz darf nicht am Systemgrenze enden, sondern muss an die Daten selbst gebunden sein. Nur wenn Dateien auch außerhalb von SAP klassifiziert, verschlüsselt und mit dynamischen Rechten versehen sind, kann ein konsistenter Sicherheits- und Compliance-Standard aufrechterhalten werden.

Microsoft verfolgt diesen Ansatz mit Purview Information Protection. Sensitivity Labels ermöglichen es, Dateien beim Erstellen oder Exportieren automatisch zu kennzeichnen, mit Richtlinien zu versehen und gegebenenfalls zu verschlüsseln. Damit wird sichergestellt, dass ein vertrauliches Dokument auch dann geschützt bleibt, wenn es das SAP-System verlassen hat.

Für Unternehmen bedeutet das: Zero-Trust-Datenschutz ist keine abstrakte Sicherheitsstrategie, sondern eine konkrete Notwendigkeit im SAP-Kontext. Nur so lassen sich Datenschutz, Compliance und Schutz vor Datenmissbrauch konsequent durchsetzen – unabhängig davon, wo die Informationen gespeichert sind oder wer sie weitergibt.

SAP-Daten im Fokus von Cybercrime

SAP-Systeme als lohnendes Ziel

SAP-Systeme sind das Rückgrat vieler Unternehmen. Sie verarbeiten nicht nur Transaktionen, sondern auch die sensibelsten Datenbestände: personenbezogene Informationen von Mitarbeitern und Kunden, Finanz- und Steuerdaten, Produktionsinformationen, Lieferketten- und Vertragsdetails. Für Angreifer sind SAP-Systeme damit ein äußerst attraktives Ziel, da ein erfolgreicher Angriff unmittelbare wirtschaftliche und regulatorische Folgen hat.

Die Bedrohungslage hat sich in den letzten Jahren spürbar verschärft. Laut dem Bundeskriminalamt zählen datengetriebene Erpressungen mittlerweile zu den größten Cybercrime-Phänomenen. Besonders deutlich zeigt sich das im aktuellen Bundeslagebild: Angreifer kombinieren Verschlüsselung von Systemen mit der Exfiltration sensibler Daten („Double Extortion“). Unternehmen werden erpresst, nicht nur, weil ihre Systeme lahmgelegt sind, sondern auch, weil vertrauliche Daten drohen, veröffentlicht zu werden.

Auch unabhängige Analysten bestätigen diesen Trend. Die SAPinsider Benchmark-Studie 2025 zeigt: Erstmals gilt Datenexfiltration als größte Bedrohung für SAP-Systeme, noch vor klassischen Risiken wie nicht eingespielten Patches oder kompromittierten Zugangsdaten. Damit ist klar: Der Schutz sensibler Daten und insbesondere die Sicherung des Exportweges rücken ins Zentrum jeder modernen SAP-Security-Strategie.

Warum Angreifer SAP-Daten ins Visier nehmen

Die Attraktivität von SAP-Daten für Cyberkriminelle ergibt sich aus drei Faktoren: ihrem hohen geschäftlichen Wert, ihrer Sensibilität im regulatorischen Kontext und ihrer Verfügbarkeit über Exporte.

- **Finanzdaten:** Quartalsberichte, Cashflows und Bilanzen enthalten vertrauliche Informationen, die bei Veröffentlichung Kursbewegungen oder Reputationsschäden auslösen können.
- **HR-Daten:** Mitarbeiterlisten, Gehaltsdaten und Sozialversicherungsinformationen unterliegen strengen Datenschutzvorgaben. Ihr Verlust führt direkt zu Bußgeldern nach DSGVO.
- **Supply-Chain-Daten:** Informationen über Lieferanten, Partner und Verträge können von Wettbewerbern missbraucht oder für Erpressungen genutzt werden.
- **Produktions- und IP-Daten:** Rezepturen, Konstruktionspläne oder Patente sind oft das wichtigste geistige Eigentum eines Unternehmens. Ihr Abfluss gefährdet die Wettbewerbsfähigkeit unmittelbar.

Folgen von Datenexfiltration

Ein erfolgreicher Angriff auf SAP-Daten ist kein rein technisches Problem, sondern eine existenzielle Bedrohung für das Unternehmen. Die Auswirkungen zeigen sich in verschiedenen Dimensionen:

- **Regulatorische Risiken:** Verstöße gegen DSGVO, SOX oder BSI-Standards führen zu erheblichen Bußgeldern und Nachweispflichten.
- **Reputationsverluste:** Vertrauliche Daten im Darknet oder in Medienberichten untergraben das Vertrauen von Kunden und Partnern.
- **Finanzielle Schäden:** Neben Lösegeldforderungen entstehen Kosten durch Betriebsunterbrechungen, Wiederherstellungsmaßnahmen und Rechtsstreitigkeiten.
- **Strategische Risiken:** Der Verlust von IP oder Geschäftsdaten verschiebt Wettbewerbsvorteile dauerhaft.

SAP-Systeme stehen heute im Zentrum einer doppelten Bedrohung: Sie sind einerseits geschäftskritisch und unverzichtbar, andererseits hochattraktiv für Angreifer. Besonders gefährlich sind Szenarien, in denen Daten aus den Systemen exportiert werden und somit aus dem geschützten Kontext herausfallen. Genau hier liegt eine der größten Sicherheitslücken, die es zu schließen gilt – nicht durch klassische Schutzmaßnahmen im System, sondern durch einen datenzentrierten Zero-Trust-Ansatz, der den Schutz auch außerhalb von SAP sicherstellt.

Der blinde Fleck - Wenn SAP Daten exportiert werden

Schutz innerhalb von SAP

Unternehmen investieren seit Jahren erhebliche Ressourcen, um ihre SAP-Systeme gegen Angriffe abzusichern. Berechtigungsmodelle, Verschlüsselung, Netzwerksicherheit und Monitoring sorgen dafür, dass Daten im System zuverlässig geschützt sind. Rollen- und Rechtekonzepte regeln den Zugriff und Protokollierungen liefern wertvolle Informationen für Audits und Incident Response.

Doch dieser Schutz endet abrupt, sobald Daten exportiert werden. In dem Moment, in dem eine Tabelle, ein Bericht oder ein Dokument in Excel, PDF oder Word ausgegeben wird, verliert es die Bindung an die SAP-Sicherheitsarchitektur.

Der Moment des Kontrollverlustes

Ein exportiertes Dokument ist nicht länger an SAP-Berechtigungen gebunden. Es wird zu einer Datei, die auf einem Endgerät gespeichert, per E-Mail weitergeleitet oder in Cloud-Dienste hochgeladen werden kann. Ab diesem Zeitpunkt gilt:

- **Keine Rollenlogik:** Zugriff ist nicht mehr durch SAP-Berechtigungen eingeschränkt.
- **Keine Protokollierung:** Es wird nicht nachvollzogen, wer die Datei öffnet oder weiterleitet.
- **Keine Sicherheitsmechanismen:** Klassifizierung und Verschlüsselung entfallen, sofern sie nicht extern ergänzt werden.

Typische Risiken im Arbeitsalltag

Gerade weil der Export zum Alltag vieler SAP-Nutzer gehört, entstehen Risiken nicht durch böse Absicht, sondern durch Routine:

- **HR-Abteilung:** Export von Mitarbeiterlisten für externe Dienstleister, unverschlüsselt per Mail verschickt.
- **Finance-Team:** Erstellung von Monats- oder Quartalsberichten, die in ungesicherten Ordnern abgelegt werden.
- **Supply Chain:** Austausch von Lieferantendaten mit Partnern, die später unkontrolliert im Umlauf sind.

In allen Fällen verlieren Unternehmen die Nachvollziehbarkeit und damit die Kontrolle über ihre sensibelsten Informationen.

Schatten-IT durch Exporte

Exportierte Dateien wandern schnell in Bereiche außerhalb des IT-Kontrollraums: auf USB-Sticks, in private Cloud-Drives oder in Messaging-Dienste. Diese Schatten-IT ist für Unternehmen kaum sichtbar, erhöht aber das Risiko erheblich. Cyberkriminelle nutzen genau diese Lücken, um Daten abzugreifen oder für Erpressungen zu missbrauchen.

Brücke zur Lösung: Zero-Trust auch außerhalb von SAP

Der entscheidende Schritt ist, den Schutz nicht am Systemgrenze enden zu lassen, sondern an die Daten selbst zu binden. SecurityHub von automatics.AI setzt genau hier an:

- **Automatische Klassifizierung:** Jede exportierte Datei erhält ein Label entsprechend ihrer Sensibilität.
- **Verschlüsselung:** Schutzmaßnahmen begleiten die Datei unabhängig vom Speicherort.
- **Integration in Microsoft Purview Information Protection (MPIP):** Exportierte SAP-Daten werden Teil des Microsoft-Sicherheitsökosystems und unterliegen denselben Zero-Trust-Richtlinien wie andere kritische Unternehmensdaten.

So entsteht ein konsistenter Schutz über den gesamten Lebenszyklus der Datei - vom SAP-System bis in die Kollaborationsumgebung.

Die Lösung für sichere SAP-Exporte

Vom Kontrollverlust zur durchgängigen Sicherheit

Das zentrale Problem bei SAP-Exporten ist der sofortige Verlust sämtlicher Schutzmechanismen des Systems. SecurityHub setzt genau an diesem Punkt an und schließt die Lücke, indem es dafür sorgt, dass SAP-Daten auch nach dem Export den gleichen Sicherheits- und Compliance-Anforderungen unterliegen wie im System selbst.

SecurityHub ergänzt SAP nicht, sondern erweitert es. Exporte werden dabei nicht nur überwacht, sondern durchgängige Schutzmaßnahmen werden automatisch angewendet. Unternehmen gewinnen damit nicht nur Transparenz, sondern auch aktive Kontrolle über den gesamten Lebenszyklus ihrer Daten.

Echtzeit-Überwachung von Exporten

SecurityHub erkennt jeden Export aus SAP in Echtzeit. Unternehmen sehen sofort:

- Wer hat welche Daten exportiert?
- In welchem Format (Excel, PDF, Word) liegen die Dateien vor?
- Wohin wurden die Daten exportiert oder weitergeleitet?

Diese Transparenz schafft die Grundlage für fundierte Entscheidungen und ermöglicht eine revisionssichere Nachvollziehbarkeit.

Automatische Klassifizierung

Jeder Export wird anhand definierter Regeln automatisch klassifiziert, zum Beispiel:

- „Öffentlich“
- „Intern“
- „Vertraulich“
- „Streng vertraulich“

Die Klassifizierung erfolgt konsistent und verhindert, dass Nutzer eigenständig oder nach Bauchgefühl entscheiden müssen.

Verschlüsselung und Policy Enforcement

Basierend auf der Klassifizierung kann SecurityHub automatisch Verschlüsselung anwenden und Richtlinien erzwingen:

- „Darf nur gelesen, nicht weitergeleitet werden“
- „Zugriff nur durch bestimmte Gruppen oder Rollen erlaubt“
- „Nur innerhalb des Unternehmensnetzwerks nutzbar“

Damit bleibt der Schutz an die Datei gebunden – egal, wo sie gespeichert oder geöffnet wird.

Auditierbare Dokumentation

Jede Aktion - vom Export über die Klassifizierung bis zur Nutzung der Datei - wird protokolliert. Unternehmen können jederzeit nachvollziehen:

- Welche Daten exportiert wurden
- Welche Maßnahmen angewendet wurden
- Wer Zugriff hatte
- Ob Richtlinien eingehalten wurden

Damit wird nicht nur die interne Sicherheit gestärkt, sondern auch regulatorische Nachweispflichten können zuverlässig erfüllt werden.

Nahtlose Integration mit Microsoft Purview Information Protection (MPIP)

Einer der größten Mehrwerte von SecurityHub ist die tiefe Integration in die Microsoft-Sicherheitswelt. Exportierte SAP-Dateien werden automatisch in MPIP eingebunden. Damit gelten dieselben Zero-Trust-Richtlinien, die Unternehmen bereits für Microsoft 365-Daten einsetzen:

- Nutzung von Sensitivity Labels
- Durchsetzung von Richtlinien in Office-Anwendungen (Outlook, Teams, SharePoint, OneDrive)
- Einheitliche Sicherheits- und Compliance-Strategien für SAP- und Microsoft-Daten

Das Ergebnis ist ein konsistenter, unternehmensweiter Datenschutz, ohne dass SAP-Daten eine „Sonderrolle“ einnehmen.

Technische Tiefe: Was SecurityHub im Detail leistet

SecurityHub zeichnet sich dadurch aus, dass es alle relevanten Exportwege aus SAP vollständig überwacht. Hierzu zählen der klassische Download, der Versand per E-Mail, das Drucken von Dokumenten oder Exporte über RFC-Schnittstellen. Jeder dieser Wege wird in Echtzeit erfasst und protokolliert, sodass Unternehmen jederzeit Transparenz über den Verbleib ihrer Daten erhalten.

Im Gegensatz zu Proxy-basierten Ansätzen ist SecurityHub direkt im SAP-Server integriert. Diese Architektur stellt sicher, dass keine Umwege über externe Systeme notwendig sind und die Performance sowie die Stabilität der SAP-Landschaft erhalten bleiben. Gleichzeitig bedeutet diese enge Integration, dass SecurityHub sowohl in traditionellen SAP-ECC-Umgebungen als auch in modernen Szenarien wie RISE with SAP vollumfänglich eingesetzt werden kann.

Die Lösung ist von SAP zertifiziert, was Unternehmen zusätzliche Sicherheit bei der Einführung und beim Betrieb gibt. Darüber hinaus erlaubt SecurityHub eine flexible Anpassung: Unternehmen können ihre individuelle Klassifizierung für Datenexporte definieren und so eigene Compliance-Anforderungen oder branchenspezifische Regularien direkt abbilden.

Ein weiteres wichtiges Merkmal ist die tiefe Integration in die Security-Infrastruktur: Über standardisierte Schnittstellen lassen sich Export-Logs und Klassifizierungsinformationen in Azure Sentinel und andere SIEM-Systeme einspeisen. Damit wird SecurityHub zum Bindeglied zwischen SAP und dem zentralen Sicherheits-Ökosystem des Unternehmens.

Für die Anwender bleibt die Lösung dabei vollständig transparent. Exportprozesse laufen wie gewohnt, ohne dass zusätzliche Klicks oder komplexe Workflows erforderlich sind. Sicherheit wird so automatisch gewährleistet, ohne die Produktivität der Nutzer einzuschränken.

Ein praxisnaher Blick: SAP-Export ohne vs. mit SecurityHub

Ohne SecurityHub:

Eine HR-Mitarbeiterin exportiert eine Liste mit Gehaltsdaten nach Excel, speichert sie auf ihrem Desktop und versendet sie per E-Mail an einen externen Dienstleister. Ab diesem Moment gibt es keine Kontrolle mehr. Niemand weiß, ob die Datei weitergeleitet oder unbefugt geöffnet wird.

Mit SecurityHub:

Beim Export wird die Datei automatisch als „streng vertraulich“ klassifiziert und verschlüsselt. Sie kann nur von den vorgesehenen Empfängern geöffnet werden, Weiterleitungen sind blockiert. Jede Interaktion mit der Datei wird protokolliert. Das Unternehmen behält jederzeit Kontrolle und erfüllt gleichzeitig die Anforderungen von DSGVO und internen Richtlinien.

SecurityHub macht SAP-Datenexporte planbar und sicher. Statt die Kontrolle an der Systemgrenze zu verlieren, behalten Unternehmen Transparenz, Nachvollziehbarkeit und Schutzmaßnahmen über den gesamten Lebenszyklus hinweg. Durch die Integration in Microsoft Purview Information Protection wird SecurityHub zu einem Schlüsselbaustein einer modernen Zero-Trust-Strategie.

Risiken bewerten und konkrete Handlungsfelder ableiten

Die unterschätzte Lücke in SAP-Security-Strategien

In vielen Gesprächen mit Unternehmen zeigt sich, dass die größten Unsicherheiten nicht darin liegen, ob Datenexporte ein Risiko darstellen, sondern wie groß dieses Risiko im konkreten Fall ist. Häufig fehlt eine strukturierte Bewertung, die klarmacht, welche Daten am kritischsten sind, wie oft sie exportiert werden und welche regulatorischen Anforderungen daran gebunden sind.

Typische Fragen, die Unternehmen klären sollten

Welche Daten verlassen regelmäßig das SAP-System?
HR-Listen, Finanzberichte, Lieferantendaten, Produktionsinformationen.

Wer exportiert diese Daten und mit welchem Zweck?
Interne Nutzer, externe Partner, Dienstleister.

Wo landen diese Daten nach dem Export?
Lokale Endgeräte, Fileshares, Cloud-Speicher, E-Mails.

Welche regulatorischen Anforderungen greifen?
DSGVO, SOX, BSI IT-Grundschutz, NIS2, DORA, ISO27001, branchenspezifische Regularien.

Welche Auswirkungen hätte ein Datenabfluss?
Finanzielle Verluste, Bußgelder, Reputationsschäden, Verlust von IP.

Ein strukturierter Bewertungsansatz

Unternehmen können mit wenigen Schritten Transparenz schaffen:

1. **Dateninventur:** Erfassen, welche Arten von Daten regelmäßig exportiert werden.
2. **Kritikalitätsanalyse:** Einstufen, welche dieser Daten besonders schützenswert sind.
3. **Exportkanäle bewerten:** Analysieren, über welche Wege (E-Mail, Cloud, USB) Daten verteilt werden.
4. **Risikoszenarien durchspielen:** Mögliche Folgen bei Abfluss der Daten identifizieren.
5. **Schutzmaßnahmen abgleichen:** Prüfen, welche Kontrollen heute greifen und wo Lücken bestehen.

SecurityHub als Instrument zur Risikobewertung und -minimierung

SecurityHub unterstützt diese Bewertung nicht nur theoretisch, sondern praktisch:

- **Echtzeit-Transparenz:** Unternehmen sehen sofort, welche Daten exportiert werden.
- **Risikobasierte Klassifizierung:** Daten werden automatisch nach Sensibilität eingestuft.
- **Kontinuierliche Dokumentation:** Jede Aktivität wird nachvollziehbar protokolliert.

Damit wird aus einer abstrakten Risikoanalyse ein laufender Prozess, der Unternehmen die Möglichkeit gibt, Risiken nicht nur zu erkennen, sondern sie aktiv zu steuern.

Fazit

Vom blinden Fleck zur resilienten SAP-Security

Unternehmen haben in den letzten Jahren viel in den Schutz ihrer SAP-Systeme investiert. Berechtigungsmodelle, Verschlüsselung, Monitoring und Compliance-Maßnahmen sorgen für ein hohes Sicherheitsniveau, jedoch nur, solange die Daten im System bleiben. Doch im Moment des Exports endet dieser Schutz abrupt. Dateien werden zu unkontrollierten Kopien, deren Verbleib nicht mehr nachvollziehbar ist. Genau hier liegt die unsichtbare, aber gefährlichste Sicherheitslücke: Angreifer nutzen Exporte, um sensible Informationen abzugreifen, Mitarbeiter handeln oft unbewusst riskant, und Unternehmen verlieren die Kontrolle über ihre wertvollsten Daten.

Cybercrime entwickelt sich rasant weiter. Data Exfiltration und Erpressung mit gestohlenen Informationen gehören heute zu den größten Bedrohungen für Unternehmen. Wer in dieser Realität bestehen will, darf den Schutz nicht länger am Rand des Systems enden lassen. Zero Trust wird vom Schlagwort zum unverzichtbaren Prinzip: Jede Datei, jeder Export und jeder Zugriff muss überprüft und kontrolliert werden.

Genau hier setzt SecurityHub von automatics.AI an. Die Plattform bindet Schutzmaßnahmen nicht mehr nur an Systeme, sondern direkt an die Daten. Sie kombiniert Echtzeit-Transparenz, automatische Klassifizierung, Verschlüsselung und die Integration in Microsoft Purview Information Protection zu einer konsistenten Verteidigungslinie. Damit verwandelt SecurityHub den Export von einer unsichtbaren Schwachstelle in einen kontrollierten und auditierbaren Prozess.

Die Botschaft ist eindeutig: SAP-Security endet nicht am Systemgrenze. Sie muss den gesamten Lebenszyklus der Daten umfassen – von der Erfassung bis zum Export. Unternehmen, die diesen Schritt jetzt gehen, sichern nicht nur Compliance und Schutz vor Angriffen, sondern schaffen echte Resilienz. Sie verwandeln einen der größten Schwachpunkte ihrer Sicherheitsarchitektur in eine Stärke – und machen ihre SAP-Landschaft fit für die Zukunft.

Wir bei automatics.AI verstehen Ihre Herausforderungen.

Unsere Kunden wissen, wie wichtig es ist, dass Sicherheit über Systemgrenzen hinaus greifen muss.

Wir begleiten Sie auf diesem Weg.

automatics

SmartSecOps Platform

Automated.
Protected.
Smart.