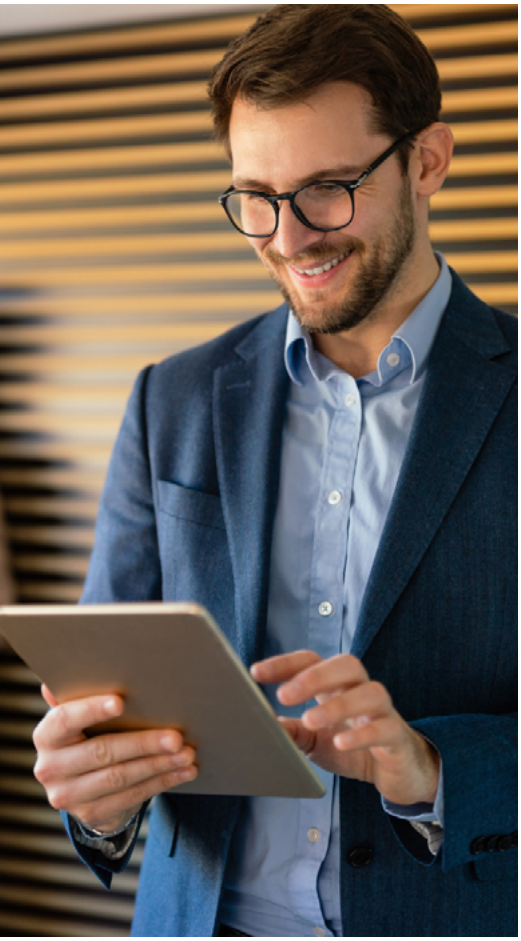
How to implement Zero Trust security for SAP data exports

‘Zero Trust’ is not new, but its importance is now undisputed.

Secude

www.secude.com

‘Zero Trust’ is not new, but its importance is now undisputed. With cloud migration and hybrid working moving businesses away from internal network security, Zero Trust has emerged as the only holistic cybersecurity framework fit for today’s reality. In particular, enterprises need Zero Trust to protect data in transit and when shared externally.



Although large organizations have embraced the idea of Zero Trust, successful Zero Trust implementation has lagged way behind. According to Cisco, over 86% of organizations have **started** adopting a Zero Trust security strategy, but only 2% have successfully put a mature Zero Trust framework in place.

2%

Of organizations have successfully put a mature Zero Trust framework in place.

Given the Zero Trust model covers a broad, interconnected range of security architecture - from identity and devices to applications and data - it’s no surprise that effective implementation is taking time.

But every extra week, every extra employee and every extra device increases the potential of a security breach.

Amidst rising cyber attacks and the increasing dominance of hybrid cloud environments, enterprise businesses need Zero Trust protection to close security gaps and protect their most sensitive data.

In this guide, we’re going to explain how you can implement an effective Zero Trust policy for SAP data exports without interrupting existing workflows.

Secude

Contents

What is Zero Trust for SAP data?

Why is Zero Trust increasingly relevant for SAP data?

What are the benefits of Zero Trust for SAP data?

5 signs that you need Zero Trust for SAP data

Use cases: how do companies secure their SAP data with Zero Trust?

How to launch Zero Trust for SAP data with Secude's HaloCORE

Secude

What is Zero Trust for SAP data?

Zero Trust doesn't trust you, your employees, your devices, your applications or your network. In fact, Zero Trust is hard-wired to treat every user as a bad actor and every access point as suspicious in order to minimize the potential for data breaches.

By incorporating multiple defensive layers and security technologies, Zero Trust aims to prevent unauthorized access to your data when shared within and outside your security system, such as downloading sensitive SAP data.

When it comes to protecting SAP data exports, the concept of Zero Trust is based on four key principles:

1. **Identity** - Zero Trust requires identity authentication for every access request. To prevent unauthorized users from both inside and outside your business from accessing sensitive information, Zero Trust encrypts data from inception with only verified users granted access. Identity control lasts for the lifetime of the data, so no matter whether someone is accessing the data for the 100th time or from a first-time location, they will need to prove their authorization.

2. **Devices** - Zero Trust requires encryption for all devices. While traditional network security trusts any device within the IT perimeter, the proliferation of IOT devices and hybrid working means authorized users are more likely to access sensitive data from 'unverified' devices. With the concept of device verification now outdated, Zero Trust requires encryption for all devices wherever they're located.

3. **Rights** - Zero Trust applies least-privilege user rights as standard. To ensure access exclusivity and minimize the risk of accidental leaks, Zero Trust provides data access on a classified 'need-to-know' basis so even internal employees can't stumble upon sensitive data by accident. As access rights at large organizations vary on a regular basis (i.e. an employee changing project or new team members onboarded), Zero Trust rights enforcement protects your data even as your internal teams change.

4. **Monitoring** - Zero Trust tracks data access beyond your IT perimeter. As security moves from location-centric (i.e. inside the network) to data-centric (i.e. individual files), Zero Trust provides in-depth monitoring of file access, usage and downloads beyond your IT perimeter, so you can see where your files are, who's attempting to view them and what users have done. The visibility analytics also simplify and speed-up compliance.

Why is Zero Trust increasingly relevant for SAP data?

Before the widespread proliferation of cloud computing around 2013-14, most enterprise companies relied on 'castle and moat' style security where the internal network was difficult to access from the outside, but everything inside was protected and trusted. But with large organizations now spreading data across the cloud, Zero Trust emerged as the default security framework by trusting no-one and demanding verification from all users.

In particular, three recent developments have made Zero Trust increasingly pressing for enterprise companies that use SAP.

Hybrid working = more vulnerability

The pandemic accelerated the cloud transition among large organizations, relegating office-based IT systems in favor of remote cloud-based applications. As corporate data footprints rapidly expanded beyond the safety of firewalls and VPNs, so did the fingerprints of enterprise organizations' workforce with an increasing number of employees working remotely at least some of the time. In 2023, for instance, 28% of full-time employees in the US **worked** in a hybrid model and only 20% of remote-capable employees **worked** fully on-site.

20%

Only a fifth of remote-capable employees work fully on-site.

Although some notable enterprise companies such as Boeing, JP Morgan Chase and UPS have made efforts to **return** to a full-time office environment, they remain the exception rather than the rule. What's more, with tech and cultural developments leading to more work outside of internal systems (no matter the location of employees), enterprises are now more vulnerable unless they have Zero Trust.

Increase in devices = more security gaps

With enterprise businesses, everything is bigger. On the one hand, enterprises can afford greater spend on cybersecurity resources and protection measures. But on the other hand, enterprises incur higher-than-average damage from data breaches (even a 1% hit could be hundreds of millions) and an elevated risk of data leaks (due to the size and spread of their workforces and their devices).

67

Unverified devices contain 67 installed applications on average.

Thanks to the shift to remote work, the enterprise workforce has become accustomed to using personal devices for work with the average employee **using** three internet-connected devices. Be it smartphones, tablets or laptops, these unsecured and unverified devices **contain** 67 installed applications on average - rising to over 100 applications in 10% of cases. Closing all these potential security gaps would be impossible for any security team let alone ones using a mix of different security tools and integrations, which further reduce threat visibility and prevention. It's far safer to assume no device is trustworthy with Zero Trust than to try and manage the increasing wave of new devices. (implementing Zero Trust would also reduce the amount of security tools needed).

Increase in cyber attacks = more pain

We live in an era of cyberwarfare. From phishing and malware to trojans and ransomware, there is a growing list of threats and a broadening range of methods used by malicious actors to attack, disrupt and ultimately hurt an organization. In particular, cyber attacks have **increased** 38% year-on-year with the average breach now **costing** $4.5 million - not to mention the wasted resources detecting and fixing the problem, and the reputational damage among customers, partners and regulators.

$4.5m

Average cost of a data breach.

With 60% of all corporate data **stored** in the cloud, attackers no longer need to infiltrate an organization's IT system to cause damage. Zero Trust security - that protects data within your systems, in cloud applications and even if it falls into attackers' hands - is the only way to prevent the pain of costly breaches.

What are the benefits of Zero Trust for SAP data?

By preventing unauthorized access to your SAP data exports, a Zero Trust approach helps to:

Safeguard business-critical information

As SAP files contain your most sensitive financial and non-public insider information, accidental data leaks or targeted attacks will cost you more than cash.

Zero Trust ensures your SAP data stays protected even if leaked or stolen, saving you money, time, stress and bad press. By reducing your attack surface, preventing data exfiltration and ensuring data privacy within a hybrid work ecosystem, Zero Trust protects your business-critical information and reputation.

Simplify regulatory compliance

Zero Trust does not simply protect your data, but gives full oversight of data access activities, such as who is attempting to gain access, at what time and from where. By storing this information in accessible logs, it's also easier for you to monitor data access and prove compliance.

Be it ensuring HR data held in SAP is compliant with General Data Protection Regulation (GDPR) or using automatic data-centric protection to demonstrate ISO27001 compliance, Zero Trust helps you fulfill your compliance mandates, prevent fines (i.e. GDPR violations can reach up to $20 million) and win contracts.

Secure collaboration

From collaborating cross-company to sharing sensitive information with external partners, workflows stretch across and beyond your company's borders. Every time you export financial data from SAP for external accountants or download SAP HR data for compliance purposes, there is potential for leaks or attacks.

But Zero Trust means you can export SAP data with peace of mind. As the authorization protections and access controls are established from the get-go, collaborators can access required data from anywhere with any device fully-secured. Zero Trust deployments prioritize user experience so you can collaborate productively and securely.

5 signs that you need Zero Trust for SAP data

Wondering if you need Zero Trust to protect your SAP data exports? Here are five signs that you could benefit from a Zero Trust approach.

1. **Unaware of the data you export from SAP?** Even if you know the number of specific SAP users at your organization, you may not know how often they export data from the SAP system or what data they are extracting. To minimize accidental or purposeful leaks, you need Zero Trust for all data leaving the system.

2. **Previously suffered a data breach?** If you've suffered a breach before, it's evident that your current protection is not fit for use. Whether it was an internal mix-up, a partner slip-up or outsider attack, you may also struggle to get cyber security insurance unless you implement Zero Trust.

3. **Share sensitive SAP data externally?** Whether it's year-end accounting or compiling information for a tender process, every time that SAP data leaves the system is a window of opportunity for leaks and attacks. Not only can Zero Trust better protect your sensitive information wherever it travels, but rights protection enables carefree collaboration with less security-focused partners.

4. **Have a high percentage of dispersed employees?** If a large proportion of your employees work remotely or you hire external contractors on a regular basis, Zero Trust helps prevent the slowdown of productivity that comes with traditional VPN style protection. Zero Trust also extends secure access control to cloud connections from anywhere and helps to rapidly onboard new internal users.

5. **Still rely on legacy systems?** Any company still relying on outdated 'castle and moat' defenses are most at risk. Exclusively using VPNs to protect your data in transit is like fighting modern weapons with medieval barriers. Only Zero Trust - applied at the file level - gives you the upper hand.

Use cases: how do companies secure their SAP data with Zero Trust?

Secude's HaloCORE is the only security solution that embeds Microsoft's Zero Trust protection and data governance into SAP data exports from creation. By extending Microsoft Purview Information Protection (MPIP) from the point of origin, SAP data is protected even if moved outside of your business, accidentally leaked or stolen.

Zero Trust for restricted periods

When preparing data during restricted or closed accounting periods (i.e. year-end accounts), SAP users regularly download confidential data to generate reports, spreadsheets and PDFs. But as soon as SAP data leaves the internal system, organizations lose control and sensitive information becomes vulnerable.

HaloCORE's MPIP extension embeds Zero Trust protection directly into your SAP data, so it's automatically protected when it leaves the SAP system. This not only prevents information leaks, but saves the time and cost of repairs (i.e. fixing servers), reputational damage and potential for lawsuits.

For example, for global enterprises with brand values in excess of $10 billion, even a 1% hit from a leak would cost $100 million - but the damage would be even worse if information was exposed during restricted periods. With thousands of global employees exacerbating the risk of inadvertent data loss, enterprises rely on HaloCORE to ensure the risk is minimized during sensitive financial periods.

Zero Trust for regulatory compliance

The SAP system contains companies' most sensitive financial and management information, as well as private customer data and personal HR data on employees. Enterprises need to prove the security of this information for regulatory compliance with unauthorized access leading to heavy fines.

HaloCORE's automatic data security and in-depth tracking of internal and external SAP data helps enterprises demonstrate compliance to regulators (i.e. for ISO 27001) and avoid GDPR violations (with fines up to 4% of company revenue or €20 million) even if data is lost or an employee changes role with different access permissions.

For example, enterprises that suffer a data breach of customer records will incur regulatory fines, bad press and brand damage, as well as wasted time fixing the issue. To protect against breaches and ensure compliance with internal and external regulations, enterprises use HaloCORE to stop sensitive SAP data being leaked and damaging the company.

20 million

Avoid GDPR violations (with fines up to 4% of company revenue or €20 million in the EU) with HaloCORE.

How to launch Zero Trust for SAP data with Secude's HaloCORE

The chances are you're part of the 86% of organizations migrating to Zero Trust, but not part of the 2% who've successfully implemented a Zero Trust framework - yet.

To make Zero Trust work effectively, your security teams must align on a well-planned strategy and roadmap that covers various parts of your security architecture. To tick SAP security off that list, follow these three steps.

1. **Identify your critical data**
   First, identify which of your SAP data is the most critical and how often it's exported. Once you have discovered which data is sensitive, think about how the loss of this data's confidentiality, integrity or availability could impact your organization to determine your highest vulnerabilities.

2. **Consider your access needs**
   Determine which users need access to sensitive SAP data and the level of access they should have. This will enable you to set identity authentication, such as multi-factor authentication (MFA), biometrics or passwords. Many organizations grant excessive privileged access to a large number of their employees and internal staff, but remember that Zero Trust is most effective when least-privilege rights are enforced as standard.

3. **Implement HaloCORE**
   Up and running in just a few days, HaloCORE automatically applies MPIP authorization tags to SAP data exports at the point of origin, ensuring sensitive data is encrypted outside of your IT perimeter and only accessible by authorized users. Integrated at the application layer, HaloCORE goes beyond traditional threat detection by protecting sensitive data even if it falls into the wrong hands (i.e. accidental leaks or data breaches). Because HaloCORE encrypts all SAP data exports, sensitive files do not need to be actively managed and you can easily control access to documents according to the chosen MPIP sensitivity label. HaloCORE also monitors data access wherever it travels and stores the most relevant information for compliance purposes.

Why take the risk?

“Zero Trust = zero gaps. While SAP security protects sensitive data when it’s in the system, it becomes vulnerable as soon as it leaves the SAP perimeter. Every download or SAP data export therefore opens the door for a potential breach, but HaloCORE’s embedded MPIP Zero Trust protection closes the gaps.”

Mario Galatovic, CEO, Secude

Even tiny windows of opportunity expose companies to huge security risks, be it from accidental leaks or targeted attacks. Zero Trust takes away all the stress and gives companies peace of mind when downloading SAP data or sharing exported data with partners.

When looking to transition to Zero Trust, look for a solution that has no security gaps (i.e. integrated at the application layer) and provides an easy end-user workflow (i.e. the software doesn’t adversely impact the end-user experience). These concepts are at the heart of Secude’s Zero Trust offering for SAP data exports.

To learn more, watch our webinar: **Zero Trust Unveiled: Securing Critical Data in SAP, CAD, and PLM Systems**

Or secure a **demo**.

HaloCORE

Member of
Microsoft Intelligent
Security Association
Microsoft Security

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