PROSTEP
integrate the future

WHITEPAPER

# DATA EXCHANGE MUST BE MADE MORE SECURE

Many companies pay too little attention to data security when exchanging data and compromise their intellectual property or - even worse - that of their customers. Thanks in part to the cloud, implementing a secure data exchange solution is no longer rocket science and is also not very expensive. But, as always, the devil is in the detail. The new PROSTEP white paper on data security in the context of data exchange reveals what you should look out for when selecting a provider and data exchange solution.

# Introduction

When collaborating in distributed development processes, it is necessary that the required data be made available to all the partners involved as quickly as possible. This means that data exchange requirements are becoming increasingly stringent. Security is one of these requirements and is not always met by every data exchange solution. PROSTEP's new white paper on data security in the context of data exchange takes a look at the requirements that companies should expect not only the software but also the vendor and its development processes to meet when selecting an appropriate solution.

# Data exchange as an open door for cyberattacks

Although most companies protect their data internally against cyberattacks by means of firewalls, restrictive access authorizations and backups, they neglect security during data transfer. Surveys indicate that only a small proportion of companies use a solution to ensure secure data exchange. In addition to a lack of human resources, high costs and the assumed complexity of such solutions, this is due to the fact that companies underestimate the risks of unencrypted data transmission.

Data transfer is increasingly becoming the Achilles' heel of cybersecurity and an open door for hackers. By sending their data unencrypted, companies risk losing their own, or even worse, their customers' data and run the risk of damaging their reputation and sacrificing the trust of their clients. According to Bitkom, Germany's digital association, the risk of cyberattacks attributed to organized crime has increased significantly. In 2023 alone, cyber-criminality cost the German economy 206 billion euros.

Companies must therefore seriously address the question of how they can protect their data on its journey through the global data networks. Simply installing a randomly chosen piece of data transmission software is not the answer. These solutions can also pose security risks that hackers can exploit in order to steal customer data.

When choosing an appropriate solution, it is therefore necessary to give due consideration to a whole set of criteria, starting with the question of how trustworthy the software vendor is and how it guarantees IT security in its own organization. Here, the compliance of the processes used in software development with applicable standards and approved practices is particularly important.

Thanks to the precautions taken, PROSTEP's OpenDXM and OpenDXM GlobalX data exchange solutions have not been the subject of a single security incident in 30 years, something that cannot be said about other vendors' products. This white paper explains why this is so.

# Ensuring the security of the organization and processes

Secure IT solutions can only be created in a secure environment. It is therefore absolutely essential that the issue of data security be firmly rooted in the organization and its IT processes. This can be done by implementing an effective security strategy that is underpinned by corresponding security standards. In addition, employees must receive regular training in the importance of data security and be made aware of the growing security risks as they are the first line of defense in the fight against potential cyberattacks.

At PROSTEP, data security is an integral part of our corporate DNA. We regularly analyze the potential risks and threats to which we are exposed and have implemented appropriate security measures. We have defined clear guidelines and procedures for handling sensitive data, including relevant password guidelines, access controls and communication paths. That is why we use our own secure data exchange platform, OpenDXM GlobalX, for transferring sensitive customer data. There is also a clearly defined process for reporting and processing security issues that ensures that we can respond quickly to situations that pose a risk.

To further strengthen our customers' and partners' confidence in our security management, we regularly undergo ISO 27001 certification. This certification attests to the fact that we meet the requirements of the most important international information security standard, not only in terms of the security of our IT systems but also at the level of our processes and the conduct of our employees. Another element in our security architecture is TISAX certification, which now forms the basis for the organization of the collaborative process for many carmakers and automotive industry suppliers. Taking ISO 27001 as its starting point, the standard defined by the VDA (German Automotive Association) establishes uniform requirements for handling confidential and personal data as well as for protecting the IT infrastructure.

What is more, our business processes meet the requirements of the ISO 9001 quality standard, which also covers aspects of data security and explicitly includes the development of our standard software products (OpenPDM, OpenCLM and OpenDXM GlobalX). We also fulfill the data protection provisions of the General Data Protection Regulation (GDPR). This set of security measures is neatly rounded off by a software development environment whose automated processes and mechanisms ensure an outstanding level of security.

## Continuous monitoring of security incidents

The security of the software products being used is currently probably one of the most important prerequisites for protecting a company's know-how. The software development environment and the organization of the development processes for the corresponding products have a significant impact on the inherent security of the applications. During the development of our software products, we apply certified processes in order to comply with the many different quality requirements.

Thanks to continuous tool integration and automated processes for building and testing our software products, we are able to identify and eliminate security vulnerabilities in the employed open-source components faster. Automated tests and checks against databases help identify the location of vulnerabilities as soon as their presence is reported.

We check OpenDXM GlobalX and the open-source components used in the software every night for security issues. If these tests reveal any such issues, our internal processes ensure the immediate analysis and evaluation of the corresponding security risks. In the case of critical shortcomings, such as the vulnerability in the Java library Log4j that was discovered at the end of 2021, we immediately inform our customers and provide them with a security patch as quickly as possible. When less critical security vulnerabilities are detected, the required measures are scheduled and incorporated into the release process.

Trust is good, checking is better. Based on this principle, we arrange for external penetration tests to be conducted to validate all major releases of our OpenDXM GlobalX data exchange platform. So far, no major security risk have been identified. We are also rated highly for data security by our major customers from the automotive industry, who also conduct penetration tests on the software solutions they use.

## Software with multilevel encryption

To a very large extent, the security of data transfer depends on how well the data is protected against misuse and unauthorized access on its journey through the global networks. This starts with comprehensive roles and rights management to ensure that only authorized users are able to send data and verify the identity of recipients before they access the data and extends through to secure encryption of the data for transfer and the data connections.

OpenDXM GlobalX provides high-performance roles and rights management including fully-integrated two-factor authentication (2FA). This means that when users log in to the data exchange portal, they not only have to enter their user ID and password but also a time-based token that can be generated on any end-user device. The 2FA procedure can be combined without difficulty with established LDAP/AD-based authentication procedures or an external IAM system (Identity Access Management) for single-sign-on (SSO).

OpenDXM GlobalX uses a multilevel encryption concept to provide the highest possible level of data security. Both internal data transfer and transfer via the Internet are always performed via an encrypted HTTPS connection. If, however, someone nevertheless tries to intercept the data, they cannot do anything with it because when it is uploaded to the platform, it is encrypted using public/private key cryptography methods with an encryption strength of up to 4096 bits. Moreover, data that requires particularly stringent protection measures is additionally safeguarded by a separate, individually generated key that is known only to the recipient. The keys can be managed separately from the encrypted data on a server in a country in which the intelligence services do not have the right to demand their disclosure.

A prerequisite for secure data exchange is controlled data management within the company itself, for example by means of a PDM/PLM solution Only in this way is it possible to ensure that no unauthorized data or incorrect versions leave the company. If data exchange is to be made even more secure, data exchange solutions need to be integrated in the existing system and IT infrastructure.

# Integration in the existing system landscape

Humans are often considered to be the weakest link in the security chain and, indeed, the risks to data security have grown as more and more people have started working from home. However, the insecure handling of data is also often due to the fact that the security measures are incompatible with the process requirements and working habits of employees. Anchoring the security measures in their working environments makes it easier for them to comply with security regulations.

What makes our OpenDXM GlobalX data exchange solution so secure is not just the encryption mechanisms, the high-performance roles and rights concept or the integration in identity access management (IAM) systems. These features can also be found in other products. What makes our solution so special is the fact that it can be seamlessly integrated in existing business processes and enterprise applications. This means that employees are never tempted to transfer their data via any channels other than the secure data exchange platform.

As part of PROSTEP's digital thread platform, OpenDXM GlobalX, together with the product families OpenPDM and OpenCLM, provides standardized, fully-maintained integration components for many PLM and ERP systems. Systems for which no integration components exist can be incorporated via the official programming interfaces. This makes it possible to implement secure, fully automated exchange of data from numerous backend systems. These integrations allow employees to send their data directly from their familiar working environment, while also restricting transmission to the data for which they possess authorization. In the automotive industry, the data exchange processes can often even be fully automated using OFTP/ENGDAT components.

OpenDXM GlobalX can also be integrated in Microsoft Outlook so that employees outside of the engineering departments are able to send and receive confidential data via email. Attachments of a certain size or data type or for certain recipients are then automatically made available in encrypted form in the data exchange portal when they are sent or are displayed in Outlook for download (again in encrypted form) when they are received. Thanks to the integration with Windows Explorer, they can also be securely exchanged via drag-and-drop.

The use of OpenDXM GlobalX as an SaaS solution does not pose any problems with regard to integration in the existing IT infrastructure. The question is what impact cloud-based use has on data security.

# Security-related benefits of cloud-based use

Customers benefit in many ways from using OpenDXM GlobalX as a cloud-based SaaS solution (software as a service). They do not have to procure the hardware and software, the data exchange platform can be used practically as-is and it can be flexibly scaled if user numbers or data exchange volumes rise or fall. Most importantly, however, cloud-based use offers many companies greater security in terms of the IT infrastructure and available resources when compared to an on-premises installation.

The days when companies tended to be put off by the idea of cloud applications due to security concerns are over. Following the many, sometimes spectacular, cyberattacks that have been witnessed, companies are gradually realizing that their data is often safer in the IT infrastructure of a trusted cloud or SaaS provider than it is in their own data centers. There are many more members of staff on hand to ensure the secure, high-performance operation of the applications and accesses are continuously monitored so that potential security incidents can be identified and eliminated quickly.

OpenDXM GlobalX can run on the cloud stacks of any chosen provider and can also be used in hybrid on-premises/cloud scenarios. The architecture of an OpenDXM GlobalX environment and the interfaces that are made available offer precisely these capabilities. Operation in a cloud infrastructure also places particular demands on the browser-based user interface, which must be able to provide secure interaction via the Internet. Cross-network communication between the client and server components is performed via web service interfaces based on the HTTPS protocol.

Applications running in the cloud are usually installed automatically and continuously updated. This also means that patches and recommended security configurations can be imported more quickly than in an on-premises installation, where updates often demand months of preparation due to the many different adaptations that have to be made. The fact that administrators no longer need to intervene manually also helps provide a higher level of security.

# Secure in every way with OpenDXM GlobalX

In conclusion, we can say that many companies still do not pay enough attention to security when exchanging data and therefore run the risk of falling victim to cyberattacks. To protect their data effectively as it makes its way through the global data networks, they need a secure data exchange solution that dovetails seamlessly with their IT infrastructure and business processes. When choosing an appropriate solution, it is also necessary to consider how trustworthy the software vendor is and how it guarantees IT security in its own organization.

PROSTEP has therefore firmly anchored the issue of data security in the organization and its IT processes by implementing an effective security strategy which is underpinned by the corresponding security standards. We have set out clear guidelines for the way we handle sensitive data and introduced a clearly-defined process for dealing with security issues.

To further strengthen our customers' and partners' confidence in our security management, we regularly undergo certification in accordance with ISO 27001 and the TISAX standard builds on it. We also meet the requirements of the ISO 9001 quality standard and the General Data Protection Regulation (GDPR). Our software development is guided by these security standards. We scan OpenDXM GlobalX and the open-source components used in the software every night for security issues and perform regular penetration tests.

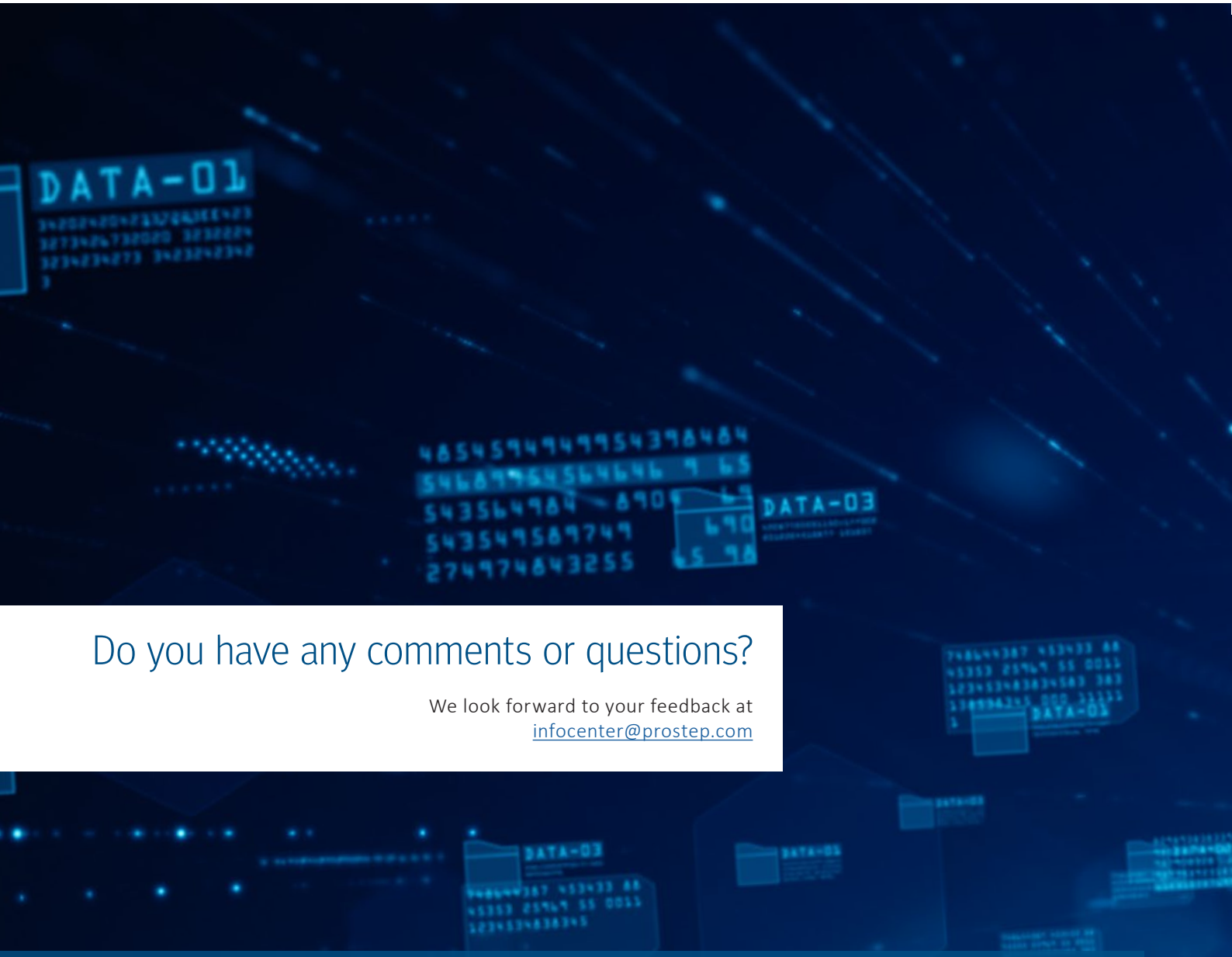
OpenDXM GlobalX provides the highest possible level of data security thanks to its high-performance roles and rights management with two-factor authentication, which can be combined with an external IAM process, as well as its multilevel encryption concept. Not only is the data for transfer encrypted when it is uploaded to the platform but the transfer itself is also performed using an encrypted connection.

One particular strength of the solution lies in the fact that it can be easily integrated in existing PLM/ERP landscapes as well as in Microsoft Outlook or Windows Explorer. This means that users can initiate data transfer directly from their familiar working environments and are never even tempted to use other data exchange channels.

OpenDXM GlobalX is used by customers in a variety of different industries that have very high data security requirements. The data exchange platform can be installed both on premises as well as in the form of an SaaS solution. Cloud-based use ensures additional security because the data is usually safer in the infrastructure of a trusted cloud or SaaS provider than it would be in the data centers of many companies.

PDF version of the white paper:
www.prostep.com/whitepapers
or scan the QR Code

PROSTEP
integrate the future




## Do you have any comments or questions?

We look forward to your feedback at
infocenter@prostep.com

PROSTEP AG
Heinrich-Hertz-Strasse 3-7 · 64295 Darmstadt · Germany
Telephone +49 6151 9287-0 · E-mail infocenter@prostep.com



**LEGAL NOTICE**

Published by
PROSTEP AG

Contact:
Daniel Wiegand
daniel.wiegand@prostep.com

Edition 1, 2024