SecurDPS Connect

SecurDPS Connect is a security gateway that protects your data before it's stored in cloud applications. SecurDPS Connect analyses data streams based on customer - specified regulatory requirements.

What is it for?

Diverse regulatory requirements make data protection an absolute necessity. Patient health data processing regulations including HIPAA in the US, privacy regulations such as the EU's GDPR and Brazil's LGPD, and international transactional data regulations like PCI DSS all specify minimum standards of data protection and require compliance from organizations operating within specific domains. No matter what, the sensitive, identifiable data of persons, patients, and customers must be protected. SecurDPS Connect is a gateway-based security platform that implements strong measures to protect data before it is stored in the cloud.

Implementing data-centric security requires a platform that not only offers protection methods that fit your use cases, but that also integrates easily into your enterprise applications and existing cyber-security infrastructure. Ease of integration very often can be the deciding factor in determining the cost and risk associated with any data protection project.

Why should I care?

Every company is ultimately responsible for its own data security, even if that data is stored in a cloud service environment. Traditional security approaches depend on perimeter-based intrusion detection, password protection, and other access-based measures. However, the industry has seen time and again that nefarious actors always find a way to the data they seek. The answer is to focus on data-centric security, which travels with the data even if that data moves outside a protected perimeter.

Given the size of fines and the enormous reputational damage to corporate brands stemming from data breaches and unauthorized access of sensitive data, every business should follow two key measures: 1) protect sensitive data as soon as you touch it within your corporate workflows, and 2) only de-protect it when absolutely necessary within a controlled environment. SecurDPS Connect enables you to do just that by applying a variety of security mechanisms to field- and file-level information before it's stored in your cloud applications.

How does it work?

SecurDPS Connect secures all your sensitive data and information intended for cloud destinations. All of its security mechanisms comply with industry standards. Based on your business and regulatory needs, SecurDPS Connect offers various options for tokenization, format-preserving encryption, classic encryption, and data masking.

The point is, you get to decide how to protect your data. You select which fields should be protected—name, address, notes, identifying numbers such as SSNs or account numbers—through a template-based approach to defining the informational fields and files to be secured. Best of all, authorized users don't recognize that additional security is being applied to the cloud-based data, which is shown in plain text to them. For all others who might see the data, it is completely obfuscated.

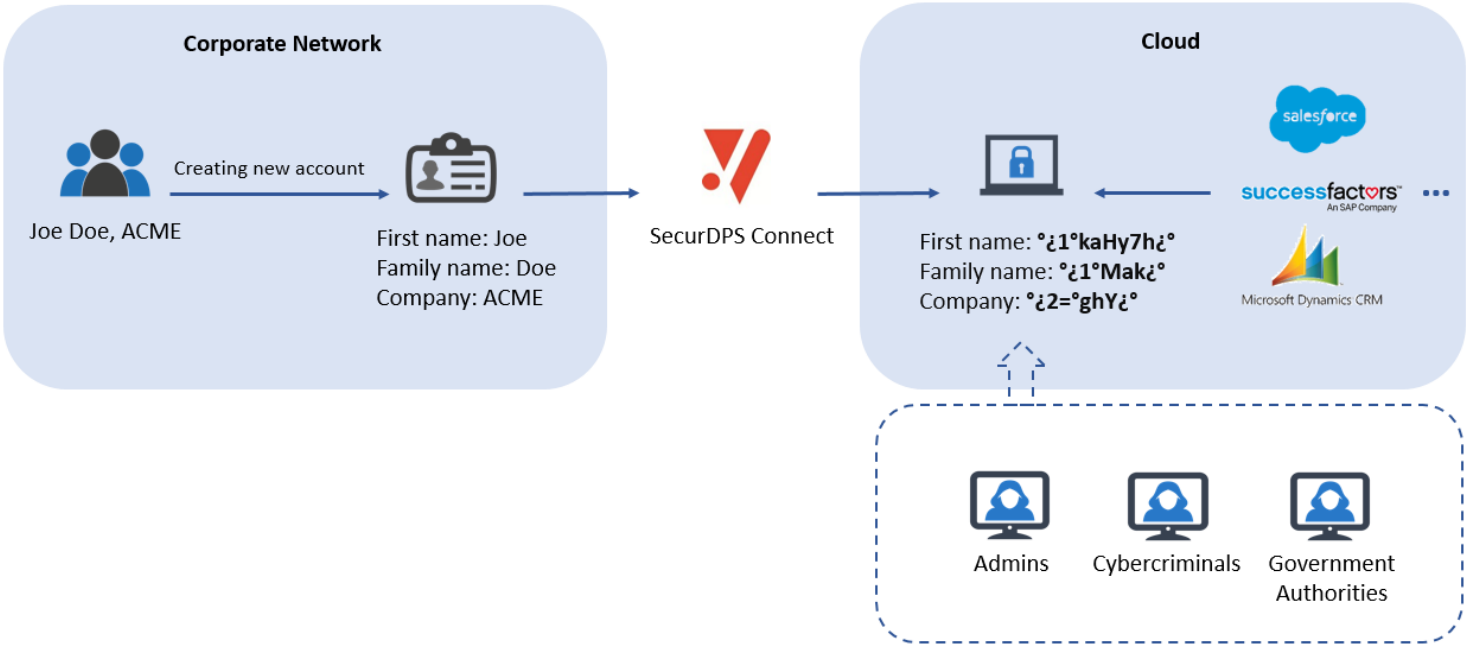
Gateway Security: SecurDPS Connect is a gateway technology that analyses data streams from an ICAP-enabled proxy and protects data based on customer-specified compliance rules. This approach provides strong protection against unauthorized access.

Multi-Cloud Protection: SecurDPS Connect offers highly secure protection across a large number of cloud services, including Salesforce, Microsoft Sharepoint and Dynamics 365, ServiceNow, Xing/LinkedIn, Oracle Sales Cloud, and many more.

Multi-Channel Protection: SecurDPS Connect supports multiple protocols (like HTTP, SMTP, OFTP, and ICAP), content types (such as JSON, PDF, DOCX, XLS, and CSV) and integration through multiple APIs (including REST, JDBC, ODBC, and binary). Flexibility is key!

Protection Mechanisms: SecurDPS Connect is not a one-trick pony. We support many data-centric protection mechanisms including strong encryption, format-preserving encryption, dynamic key generation, tokenization, and pseudonymization.

Template-Based Protection: SecurDPS Connect leverages templates to discover sensitive data within content and then protect that data through chosen protection mechanisms. Templates are created through our own Domain Specific Language (DSL).



Which benefits does it provide?

Reduce business liability and avoid accidental exposure by replacing in-the-clear sensitive data with obfuscating values that are meaningless if exposed.

Achieve regulatory compliance and reduce liability while also eliminating costly fines which can also have a negative effect on your brand reputation.

Reduce audit scope by implementing SecurDPS Connect, because a system that does not contain accessible sensitive information does not require the same level of audit as one which does. Reduced scope means a less costly audit.

Enable multi-cloud protection by having one consistent, interoperable approach to data security in cloud applications across different cloud service providers. Improve simplicity through a single, unified approach while still embracing all the value that cloud applications offer your business.

Enact IP protection that your business works hard to create and invests large amounts of money to develop and bring to market. SecurDPS works hard to keep your intellectual property safe. No reason to lose your IP and your shirt in the process!

Contact us

With more than 20 years of experience, in data protection, on truly mission-critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: their data.

We are here to enable your success by providing expertise, an innovative technology suite and local support.