SecurDPS Connect - Solution Brief

Protect Data Over Its Entire Lifecycle

Limiting data exposure to attack, accidents, or unauthorized access is more important than ever. To meet compliance objectives more quickly and lastingly, you need to protect data over its entire lifecycle. A critical step in the process is to address data generated, processed, and transmitted via web- and cloud-based applications, SaaS, COTS, and database applications.

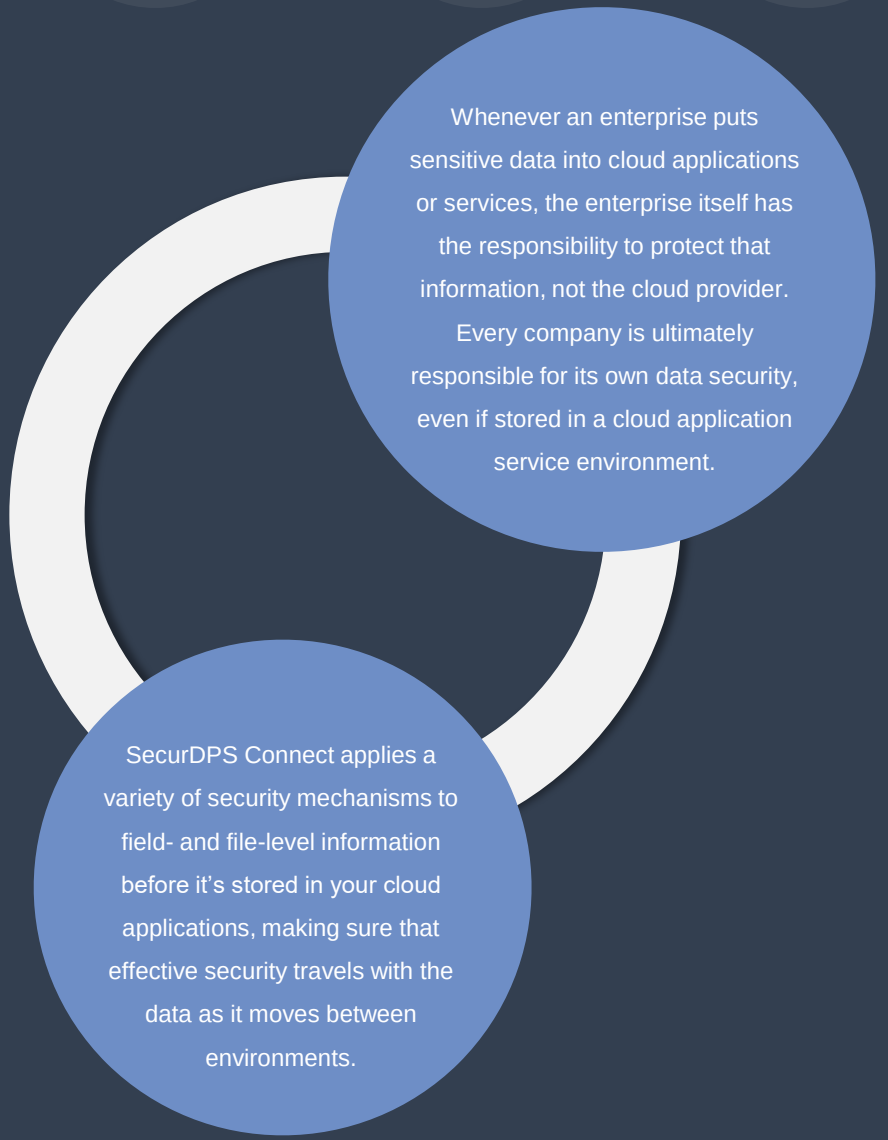
Comforte's SecurDPS Connect accelerates data-centric protection of structured, semi-structured, and unstructured data in modern application and cloud workflows, rapidly reducing potential exposure and the risks associated with it. SecurDPS Connect complements the built-in transparent integration in SecurDPS Enterprise for files and streaming processes, so no coding overhead is required.

What is SecurDPS Connect?

Cloud data is particularly vulnerable—and often overlooked

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 data protection 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, keeping protected sensitive information safe from being leveraged.



Data-centric Security is the Answer

Diverse regulatory requirements make data protection an absolute necessity, but many cloud applications offer minimal data security measures. Processing regulations for patient health data such as HIPAA in the US, 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. The sensitive, identifiable data of persons, patients, and customers must be protected under every condition. And it's the enterprise which collects, processes, and stores that data who bears the brunt of responsibility for data protection!

Complacency in traditional data security methods or the basic security services offered by cloud providers can actually create further risk and exposure. 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 threat actors always find a way to the data they seek. The answer is to focus on data-centric security with the following in mind:

1) Protect sensitive data as soon as you touch it within your corporate workflows

2) Only de-protect it when absolutely necessary within a very controlled environment.

Data-centric security protects the data itself, not the virtual borders around that data. It also protects data even if that data moves outside a protected perimeter.

Over 3/4 of enterprises surveyed by McAfee indicated that they store sensitive data in public cloud environments

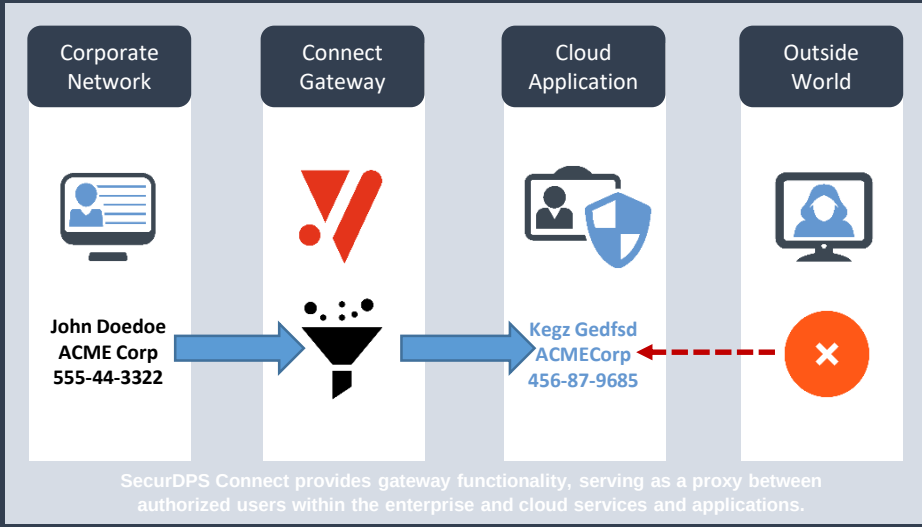
Over 50% of all enterprises rely on cloud services that have experienced stolen sensitive information

A report by IBM shows that the average cost of a data breach in 2020 is $3.86 million USD. Furthermore, enterprises can take upwards of 280 days to identify, contain, and mitigate a breach. SecurDPS Connect protects your organization against these repercussions.

How Does SecurDPS Connect Work?

SecurDPS Connect functions as a gateway technology. It resides between cloud applications and the users in your enterprise who collect, process, transmit, and store data using those applications. It intercepts data streams and protects that data based on the regulatory requirements of the customer as defined through flexible templates. In this way, SecurDPS Connect protects against unauthorized access.

SecurDPS Connect enables users to develop customized templates which train the solution to detect and replace sensitive data with encrypted or tokenized data before that information is stored in the cloud application or service. These templates provide the mechanism to define what types of information are sensitive and guide the type of protection for each data field. Only authorized users are able to view and work with unprotected data. To unauthorized users, sensitive information is completely incomprehensible, preserving information privacy and maintaining compliance with regulations and industry mandates.



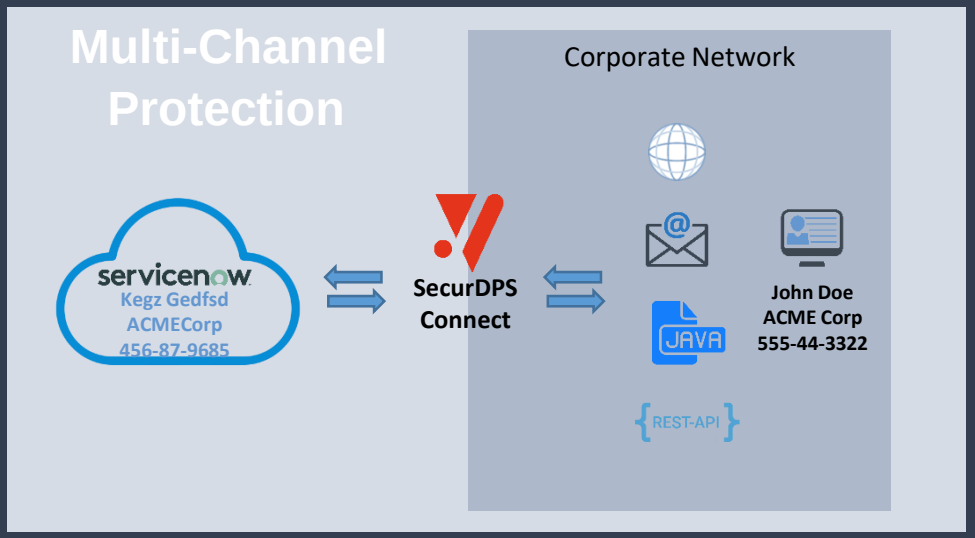
SecurDPS Connect provides gateway functionality, serving as a proxy between authorized users within the enterprise and cloud services and applications.

How Is SecurDPS Connect Deployed?

SecurDPS Connect proxies reside between enterprise users and the cloud applications and services they are accessing. These proxies are driven by an engine which determines, based on pre-defined templates, what fields of information need to be protected (and how to protect them) before forwarding that information on to the cloud application or service. Supported cloud applications include Salesforce, ServiceNOW, Microsoft Sharepoint, Microsoft Dynamics 365, Hubspot, Xing/LinkedIn, and Tableau. It also supports API-based integration via REST, JDBC, and ODBC connections.

Example Workflow: ServiceNOW

An authorized user updating information in ServiceNOW (such as a support ticket) can see the contact's last name (in this case, Smith). However, SecurDPS Connect intercepts that information, determines the sensitivity level of the field based on template definition, and protects the field accordingly before interacting with the cloud application. To any unauthorized users, the contact's last name is protected by the defined method (encryption, tokenization, or masking) and is incomprehensible to unauthorized users.



One Solution, Many Valuable Outcomes

With cloud-based services and applications, enterprises can get to market quickly and much more cost-effectively than with on-premise infrastructure services. The cost benefits of cloud are undeniable.

Problems arise, though, when enterprises depend on the minimal security provided by cloud vendors and aaS offers. Resulting data breaches can be catastrophic to the bottom line and to the brand. Why not ensure that you exceed regulatory requirements, thus reducing risk, by implementing SecurDPS Connect between your users and the cloud services on which they depend?

Gateway Security: SecurDPS Connect is a gateway technology that analyzes 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-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!

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.

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).

Secure Your Growth

Gartner has cited our solution over **a dozen times** as an example of an effective solution for data protection in cloud-based applications and services.

Watch SecurDPS Connect in action! Working with real applications and representative sensitive data, we can demonstrate how different users (both authorized and unauthorized) view the data fields and how the solution functions based on input from templates. Please contact us at www.comforte.com/contact to schedule a demonstration today!

comforte

www.comforte.com