comforte

COMFORTE SOLUTION BRIEF

# COMFORTE Connect

## PROTECT DATA OVER ITS ENTIRE LIFECYCLE IN ANY APPLICATION

### Fast deployment for quicker regulatory compliance

Diverse regulatory requirements make data protection an absolute necessity, but many applications offer minimal data security measures if any at all. Data-processing regulations specify minimum standards of information protection and require compliance from organizations operating within specific domains and jurisdictions. Companies must protect the sensitive, identifiable data of persons, patients, and customers under every condition. Keep in mind that it's the enterprise collecting, processing, and storing that data which owns the responsibility for data protection!

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. These highly convenient enterprise tools often have bare minimum data security capabilities, and because the data they generate is highly mobile, you need more robust protection.

Comforte's SecurDPS Connect accelerates data-centric protection of structured, semi-structured, and unstructured data in modern applications and hosted application workflows, rapidly reducing potential exposure and the risks associated with it. SecurDPS Connect facilitates deployment in hours rather than days or weeks, so you can quickly implement the right level of security for your enterprise applications.

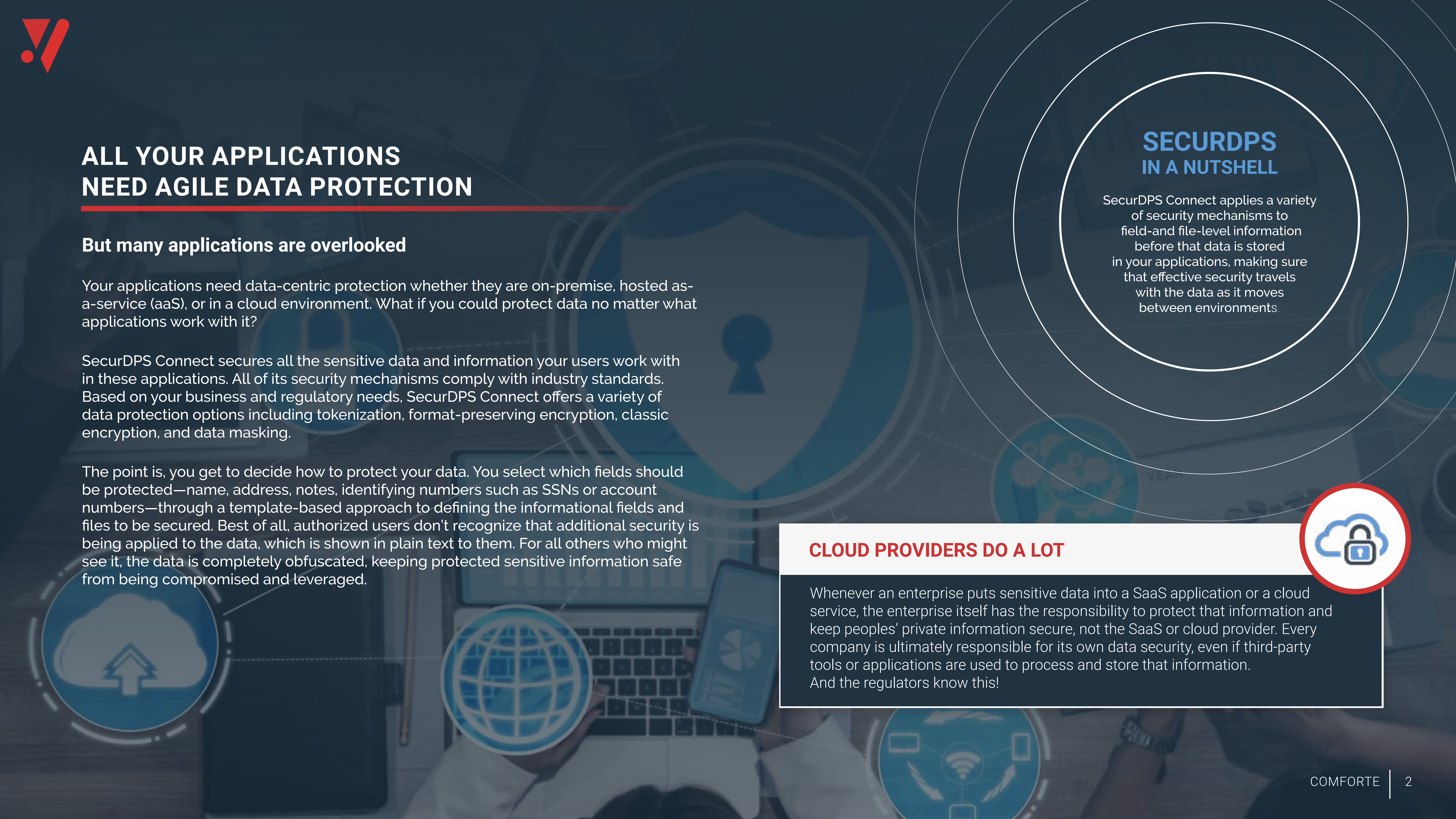
OVER **3/4** > of enterprises surveyed by McAfee indicated that they store sensitive data in public cloud environments.

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.**



# ALL YOUR APPLICATIONS NEED AGILE DATA PROTECTION

## But many applications are overlooked

Your applications need data-centric protection whether they are on-premise, hosted as-a-service (aaS), or in a cloud environment. What if you could protect data no matter what applications work with it?

SecurDPS Connect secures all the sensitive data and information your users work with in these applications. All of its security mechanisms comply with industry standards. Based on your business and regulatory needs, SecurDPS Connect offers a variety of data protection options including 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 data, which is shown in plain text to them. For all others who might see it, the data is completely obfuscated, keeping protected sensitive information safe from being compromised and leveraged.

## SECURDPS IN A NUTSHELL

SecurDPS Connect applies a variety of security mechanisms to field-and file-level information before that data is stored in your applications, making sure that effective security travels with the data as it moves between environments.

## CLOUD PROVIDERS DO A LOT

Whenever an enterprise puts sensitive data into a SaaS application or a cloud service, the enterprise itself has the responsibility to protect that information and keep peoples' private information secure, not the SaaS or cloud provider. Every company is ultimately responsible for its own data security, even if third-party tools or applications are used to process and store that information.
And the regulators know this!

## DATA-CENTRIC SECURITY IS THE ANSWER

Complacency in traditional data security methods or the basic security services offered by SaaS or cloud providers can actually bring about 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. This is the reason that more and more companies are turning to solutions that protect the actual data instead of the borders around that information. 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, or better yet not at all.

Data-centric security focuses on the data itself, not the virtual borders around that data. It also protects data even if that data moves outside a protected perimeter, so it protects data in motion and data at rest, no matter which application touches it.

# HOW SECURDPS CONNECT WORKS

SecurDPS Connect functions as a gateway technology. It resides between 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 no matter which application touches it.

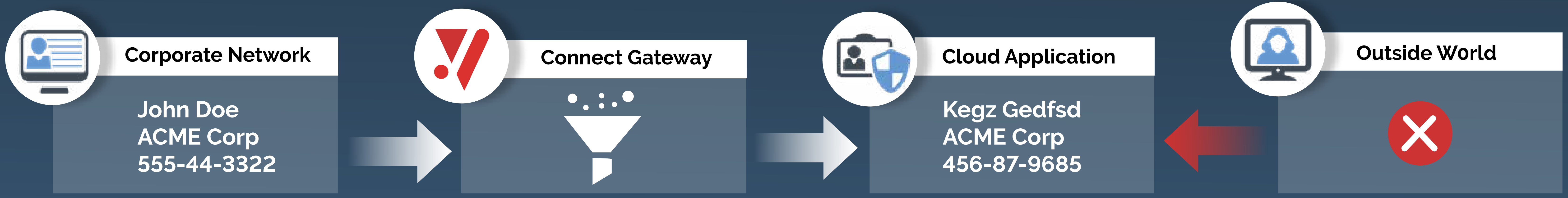
## Smart data security enables fast deployment

SecurDPS Connect allows 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 application or cloud 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.

## HOW ALL SECURDPS CONNECT IS DEPLOYED

SecurDPS Connect proxies reside between enterprise users and the 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 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.



Corporate Network

John Doe
ACME Corp
555-44-3322

Connect Gateway

Cloud Application

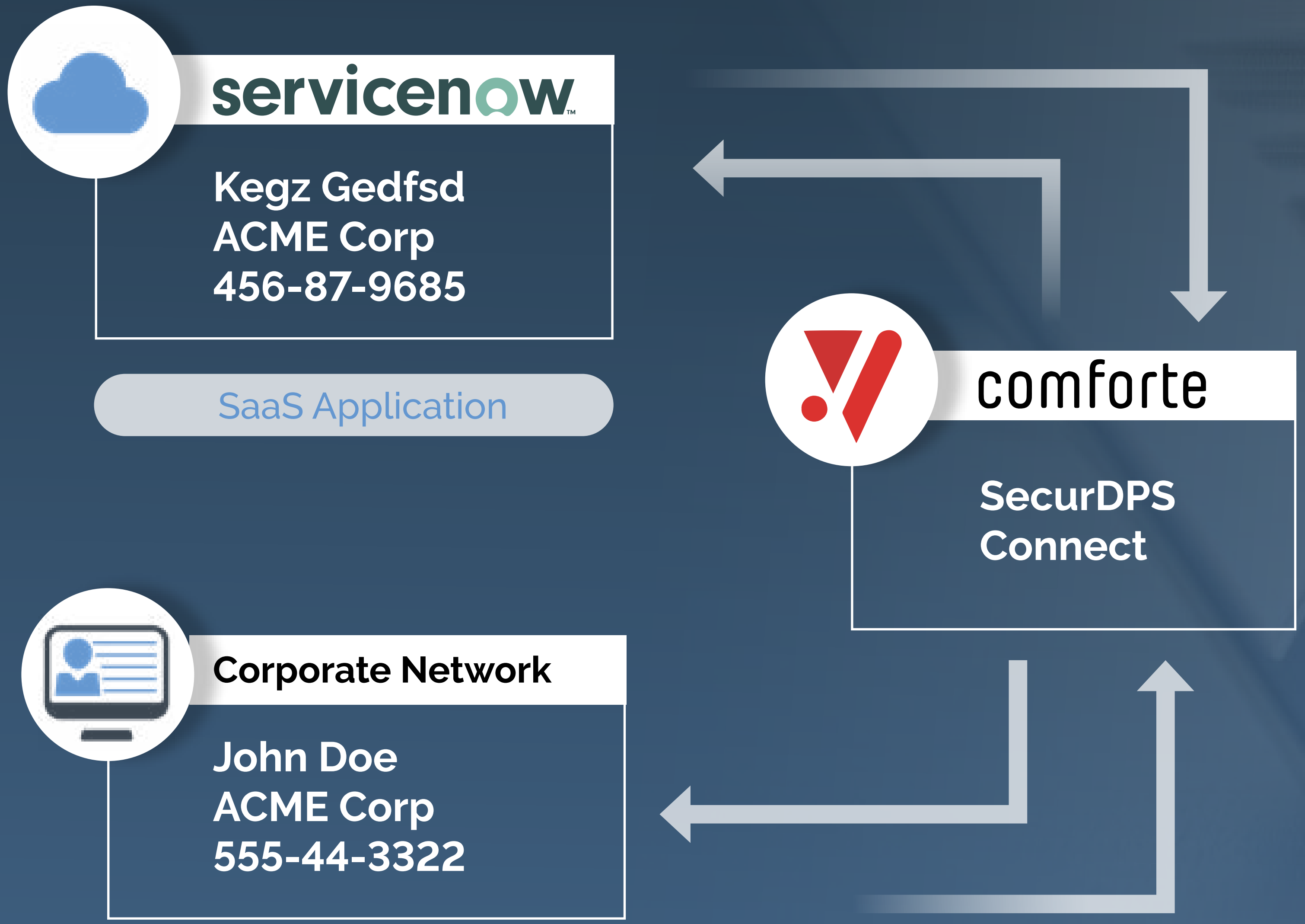
Kegz Gedfsd
ACME Corp
456-87-9685

Outside World

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

# EXAMPLE WORKFLOW USING SERVICENOW

An authorized user updating information in ServiceNOW (such as a support ticket) can see the contact's last name (in this case, Doe). However, SecurDPSConnect 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.



servicenow

Kegz Gedfsd
ACME Corp
456-87-9685

SaaS Application

comforte

SecurDPS
Connect

Corporate Network

John Doe
ACME Corp
555-44-3322

## ONE SOLUTION, MANY VALUABLE OUTCOMES

Especially with SaaS and cloud-based 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 applications on which they depend?

### 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.

### Gateway security:

SecurDPS Connect is a gateway tecnology that analyzed data streams from an ICAP-enabled proxy and protects data based on a customer-specifed compliance rules. This approach provides strong protection against unauthorized access.

### Protection Mechanism:

SecurDPS Conect is not a one-trick pony. We support many datacentric protection mechanisms including strong encryption, format-preserving encryption, dynamic key generation, tokenization, and pseudonymization.

### Multi-Channel protection:

SecureDPS Connect supports multiple protocolos (loke HTTP, SMTP, OFTP, and ICAP), content types (such as JSON, PDF, DOCX, XLS, and CVS) and integration trough multiple APIs (including REST, JDBC, and binary). Flexibility is key!

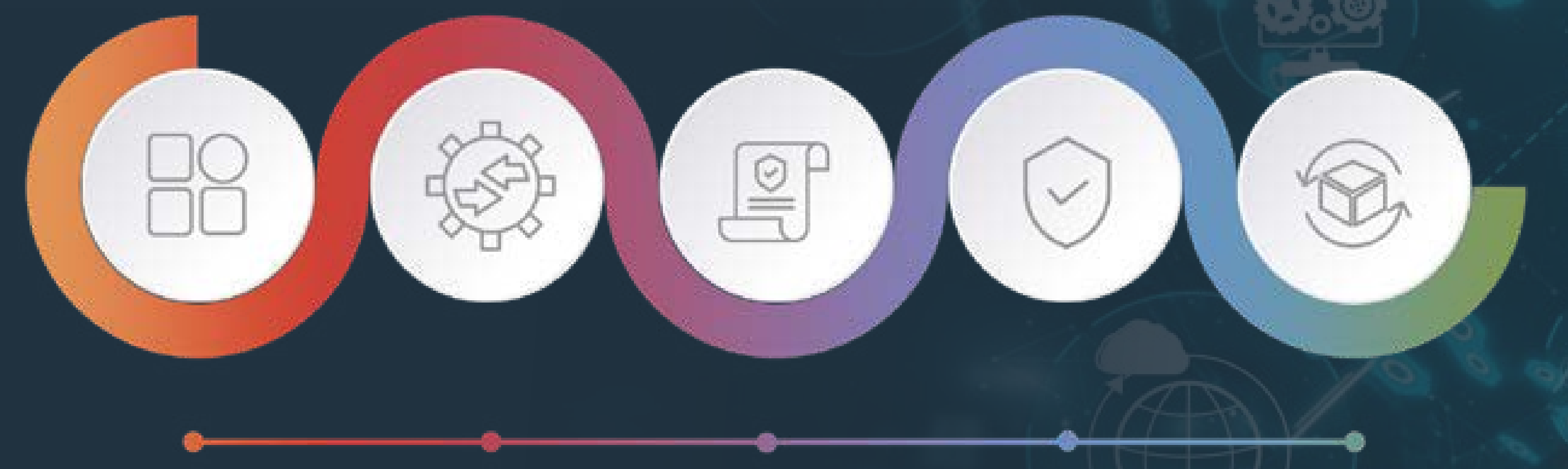
### Template-Bases Protection:

SecurDPS Connect leverages templates to discover sensitive data within content and then protect that data through chosen protection mechanism. Templates are created trough our own Domain Specific Language (DSL).

# SHOULDN'T YOU SOLVE THE WHOLE PROBLEM INSTEAD OF ONE PART OF IT?

Our customers are trying to solve the problem of data security not just with a single protection method but with an end-to-end solution that helps them know, understand, and then protect their data—wherever it is—in the most appropriate data-centric method possible. Shouldn't you too?

Our data security platform helps to streamline your data ecosystem so that you know where sensitive data really is. This eases audit and compliance activities. The platform comprise three integrated services to enable a comprehensive end-to-end data security strategy: SecurDPS Discovery & Classification, SecurDPS Enterprise for data protection, and SecurDPS Connect which is ideal for SaaS-based and on-premise applications.



**DISCOVER & CLASSIFY**
Instrument Sensitive Data Discovery as a Continuous Process

**INVENTORY**
Identify Data, Ownership, Lineage & Flows

**POLICY**
Enable Data Security as a Service from the CI/CD

**PROTECT**
Instrument Data Security in applications

**DEPLOY**
Reduce Implementation cost and effort. No code to low-code

**Comforte Data Security Platform**

## WHAT DO ANALYSTS SAY ABOUT US?

Analysts haves cited our SecurDPS Connect solution over a **dozen times** as an example of an ideal solution for data protection in cloud-based applications and services.

## SEE IT TO BELIEVE IT!

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
**comforte.com**
to schedule a demonstration today!

**Secure Your Growth**

comforte

**www.comforte.com**