comforte

LET'S TALK ABOUT DATA SECURITY
FOR CLOUD & PII

IF YOU'RE BOTHERING TO READ THIS

Then you're all about protecting sensitive data in your cloud environment

The opportunities accompanying a cloud-based infrastructure and cloud-first enterprise offer huge technical and business benefits. Data security, though, is not necessarily a given.

> Security shouldn't be an afterthought. Unfortunately, many organizations don't think enough about a very relevant issue: data security.

You might think that your cloud provider has you covered from a data security perspective, right? Well, cloud providers do a lot for you, but you're still the responsible caretaker for data security. In addition, more sophisticated cloud deployments (hybrid cloud, multi-cloud) increase the complexity of your data workflows, making it harder to manage things like data security across them. Compliance with industry standards as well as a consistent, laser focus on security should be at the top of the list.

A WORD CLOUD ABOUT CLOUD RISKS

In a single glance, you can see the different aspects of cloud-based data security that prove problematic for IT organizations:

We know that you're trying to balance speed and agility for your organization with the need to protect your sensitive data from intentional and unintentional exposure. We also know that it's a juggling act, but these words shouldn't necessarily scare you. We have a solution.

WHAT IF YOU COULD?

Think about how your security posture (and your piece of mind) would be different if you could guarantee the following:

- **Protect sensitive personal identifiable information** even if it falls into the wrong hands? For most companies, it's only a matter of time before it happens. If it occurs to you, would it be different if you were confident that sensitive information would not be exposed?
- **Process and analyze sensitive, private data** without having to de-protect or compromise that information? Your business, like so many others, thrives on data analysis. However, that opens yourself up to risk. Why not have your cake and eat it too?
- **Avoid** over-provisioning, **eliminate** dependencies on traditional appliances, and **align** to agile IT/Ops processes. Data security in your cloud environment doesn't have to be complicated to manage or serve as an obstacle to productivity and agility. At least, not with comforte's data security platform.
- **Reduce** deployment complexity and avoid tight coupling that leads to vendor lock-in or lengthy coding integrations whenever possible. With snap-in deployment capabilities, our data security platform makes it easy to deploy into your infrastructure.

WHY YOU SHOULD CONSIDER DATA-CENTRIC SECURITY

Your cloud data is dynamic and mobile

Protect data before using it in your cloud applications. Data-centric security protects the data itself no matter where it goes, so it doesn't have to sit behind a protected perimeter to remain wholly secure. And, if you protect it as soon as you collect, process, and store it, then it's already secured when your users work with it in your cloud applications, or when it gets bundled into a container by your Dev-Ops team.

Enable your business to leverage cloud-native applications

Increased agility gives you a leg up. Dev-ops teams need to be as agile as possible to innovate with rapid iterative deliverables. Traditional security architectures are often incompatible with modern cloud-native operational requirements, automation, languages, and orchestration frameworks such as Kubernetes. In addition, infrastructure-centric security winds up being a piecemeal solution that's not consistent with cloud-first strategies and architectures.

Data security built into cloud and cloud-native platforms is very traditional

Security in cloud and cloud-native platforms is dependent on the underlying core infrastructure. Often, enterprises implement traditional security methods like container "isolation" to reduce the "blast zone," vulnerability scanning and behavior monitoring, access control lists (RBAC), and sometimes data-at-rest encryption. All of these approaches are outdated and have risks associated with them. On top of that, these counter-measures do not provide data security across the full lifecycle of your data, and they certainly don't help with data privacy compliance. Nor do they cover accidental data exposure from errors and vulnerability exploitation.

Most data security out there isn't designed for modern cloud architectures

PUSH THE ENVELOPE OF AGILITY WITHOUT SACRIFICING PROTECTION

Say 'yes' to cloud initiatives by securing your sensitive enterprise data first, allowing you to explore beyond the boundaries imposed by regulations and risk. Move faster toward a cloud native DevOps strategy.

DATA-CENTRIC SECURITY EXPLAINED

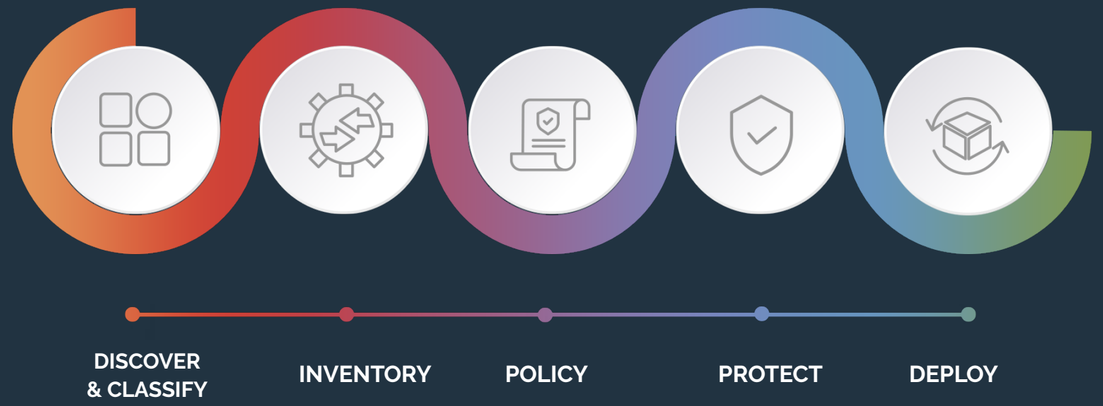
The best way to comply with data privacy regulations while still being able to use technologies like as-a-service (aaS) and cloud-native solutions is to implement data-centric protection for all sensitive information in your data ecosystem. This is what many enterprises already do today.

> Data-centric security protects the data itself no matter where it goes.

Data-centric security focuses on the protection of data itself rather than perimeters, boundaries, access control to data, or storage mechanisms around that data.

To ensure comprehensive data security, you need a specific set of technical capabilities going beyond just protection (such as encrypting the data). Organizations first need to be able to discover and classify sensitive data across various systems, repositories, and platforms. Gaining that knowledge allows organizations to get a clear picture of their data landscape and the associated levels of risk. With a focus on protecting all of their sensitive information, organizations can now create policies and deliver the right data protection methods that actually fit their business use cases and data types.

With appropriate protection mechanisms such as tokenization of structured data, the security mechanism travels with the data – independent of applications, databases, and containers – at rest, in motion, or in use. This allows organizations to take complete control of their sensitive data (control user access in real time and on granular levels leveraging behavior analytics, reports of data usage and security events), lowering compliance costs and significantly reducing the risk of data breaches.



OUR DATA SECURITY PLATFORM SHOWN ABOVE PROVIDES END-TO-END DATA DISCOVERY, CLASSIFICATION, AND PROTECTION, WITH EASE OF INTEGRATION AND CLOUD-NATIVE SUPPORT.

COMFORTE'S DATA SECURITY PLATFORM

We designed our platform from the ground up specifically for the modern, agile enterprise. This approach enables resilient data-intensive organizations to deliver privacy and security for their customers by design. We ensure that data protection can snap-in to applications, data processes, and workflows. Our platform also allows integration without changing the record format of the original data, which prevents costly development changes. Our data security platform is ideal for both hybrid IT and cloud-native infrastructures.

Architected for cloud-first enterprises

Adopt a modern DevSecOps strategy with the increased speed of development that DevOps brings to an organization comes the need for equally agile data security. This requires security processes and especially data security to be integrated with development and QA—doing so is not always a simple task.

Our API-first cloud-native platform architecture delivers to the modern Infrastructure as Code strategy, enabling a true 'data-security-as-code' delivery model for agile enterprises. Unlike solutions built pre-cloud and pre-privacy, comforte's platform is designed to be operated and used within modern operational DevOps processes, integrated into the CI/CD and robotic processes, and takes full advantage of modern application orchestration systems including Kubernetes for automated scale, operation, and management.

Protect data in applications everywhere

Comforte's data security platform secures all your sensitive data and information intended for applications using standard protocols – especially useful for aaS applications. All of its security mechanisms comply with industry standards.

Based on your business and regulatory needs, our platform offers various protection methods to secure data stored in applications. 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.

Architected for cloud-first enterprises. A platform for end-to-end data security. Automated operations with transparent integration.

What's not to like?

Won’t disrupt your business

Secure all your sensitive data and information intended for cloud destinations without disrupting your business processes and workflows.

Move rapidly to cloud agility

Ease of implementation ensures a quicker journey. Too many cloud projects stall at the outset due to complexity of deployment. And even if you get past the initial implementation, increasingly complex operations can cause heartburn and inefficiencies, too.

Make data privacy and security a natural fit with your cloud strategy

Privacy regulations make data protection an absolute necessity. Implement strong measures to protect cloud data before it travels to your cloud ecosystem while still enabling valuable analytics and data processing. Truly balance data use, privacy, customer data value, and security under a single integrated and intelligent platform.

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

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.

WHERE TO GO FROM HERE

Our data security platform has been helping organizations to discover where valuable and sensitive personal data is, to safely introduce new applications and data workflows into their operations, and to embrace the cloud and go cloud native, all while maintaining data security and compliance with governmental data privacy regulations for years now.

Check out our capabilities and some success stories by going to our website

www.comforte.com

or requesting a demo

www.comforte.com/contact